2022-11

Development of a secure multi-factor authentication algorithm for mobile money applications

Guma, Ali

NM-AIST

https://doi.org/10.58694/1782

DEVELOPMENT OF A SECURE MULTI-FACTOR AUTHENTICATION ALGORITHM FOR MOBILE MONEY APPLICATIONS

Guma Ali

A Thesis Submitted in Fulfillment of the Requirements for the Degree of Doctor of Philosophy in Information and Communication Science and Engineering of the Nelson Mandela African Institution of Science and Technology

Arusha, Tanzania

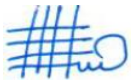
November, 2022

ABSTRACT

With the evolution of industry 4.0, financial technologies have become paramount and mobile money as one of the financial technologies has immensely contributed to improving financial inclusion among the unbanked population. Several mobile money schemes were developed but, they suffered severe authentication security challenges since they implemented two-factor authentication. This study focused on developing a secure multi-factor authentication (MFA) algorithm for mobile money applications. It uses personal identification numbers, one-time passwords, biometric fingerprints, and quick response codes to authenticate and authorize mobile money subscribers. Secure hash algorithm-256, Rivest-Shamir-Adleman encryption, and Fernet encryption were used to secure the authentication factors, confidential financial information and data before transmission to the remote databases. A literature review, survey, evolutionary prototyping model, and heuristic evaluation and usability testing methods were used to identify authentication issues, develop prototypes of native genuine mobile money (G-MoMo) applications, and identify usability issues with the interface designs and ascertain their usability, respectively. The results of the review grouped the threat models into attacks against privacy, authentication, confidentiality, integrity, and availability. The survey identified authentication attacks, identity theft, phishing attacks, and PIN sharing as the key mobile money systems' security issues. The researcher designed a secure MFA algorithm for mobile money applications and developed three native G-MoMo applications to implement the designed algorithm to prove the feasibility of the algorithm and that it provided robust security. The algorithm was resilient to non-repudiation, ensured strong authentication security, data confidentiality, integrity, privacy, and user anonymity, was highly effective against several attacks but had high communication overhead and computational costs. Nevertheless, the heuristic evaluation results showed that the G-MoMo applications' interface designs lacked forward navigation buttons, uniformity in the applications' menu titles, search fields, actions needed for recovery, and help and documentation. Similarly, the usability testing revealed that they were easy to learn, effective, efficient, memorable, with few errors, subscriber satisfaction, easy to use, aesthetic, easy to integrate, and understandable. Implementing a secure mobile money authentication and authorisation by combining multiple factors which are securely stored helps mobile money subscribers and other stakeholders to have trust in the developed native G-MoMo applications.

DECLARATION

I, Guma Ali, hereby declare to the Senate of the Nelson Mandela African Institution of Science and Technology that this thesis is my original work and has neither been submitted nor is concurrently submitted for a degree award in any other University.



30th November 2022

Guma Ali — Date

The above declaration is confirmed by:

30th November 2022

Prof. Anael Elikana Sam — Date

30th November 2022

Dr. Mussa Ally Dida — Date

COPYRIGHT

CERTIFICATION

The undersigned certify that they have read and hereby recommend for acceptance of the thesis titled "*Development of a Secure Multi-Factor Authentication Algorithm for Mobile Money Applications*" in fulfilment of the requirements for the degree of Doctor of Philosophy in Information and Communication Science and Engineering of the Nelson Mandela African Institution of Science and Technology.

30th November 2022

Prof. Anael Elikana Sam — Date

30th November 2022

Dr. Mussa Ally Dida — Date

ACKNOWLEDGMENTS

I thank the Almighty Allah for the gift of life, wisdom, strength, good health, protection, and love rendered to me to complete my PhD program successfully.

My heartfelt gratitude goes to my esteemed supervisors, Prof. Anael Elikana Sam and Dr. Mussa Ally Dida of Nelson Mandela African Institution of Science and Technology (NM-AIST), for their priceless guidance and support. Their deep knowledge of research motivated me to conduct this study. Their scholarly guidance, constant supervision, constructive criticism, and reading inferior drafts and correcting them under all conditions made the PhD research a tremendous learning experience.

I wish to thank the NM-AIST Community, School of Computational and Communication Sciences and Engineering (CoCSE), CoCSE academic staff like Prof. Dmitry Kuznetsov, Prof. Verdiana Masanja, Prof. Shubi Kaijage, Prof. Kisangiri F. Michael, Dr. Elizabeth Mkoba, Dr. Judith Leo, Dr. Devotha Nyambo, Dr. Neema Mduma, and Dr. Ramadhani Sinde, for their sincere cooperation and extensive recommendations regarding the study.

I owe appreciation to my extended network of friends, Dr. Taban Habibu, Dr. Kafula Chisanga, Dr. Elmugheira Mockarram Ibrahim Mohammed, Dr. Kivumbi Bernard, Mr. Cedric Maforimbo, Mr. Gustavio Okwir, Mr. Okello Tito Lutwa, Ms. Queen Lizbeth Simon, Mr. Frank Godlove Kilima, Ms. Calista Francis, Mr. Peter Kavishe, Mr. Mwita Machoke, Mr. Shadrack Madila, Mr. Raiton Ambele, and Mr. Cosmas Magashi, for the excellent time shared.

I want to express my special appreciation to my parents, brothers, sisters, relatives and friends for their love, encouragement, guidance, and support. I also want to express my gratitude and most profound appreciation to my beloved wife, Mrs. Hatima Kassim, and my children, Farhan AbdulAzeez Guma, Baheera Ayeesha Ali, and Erfan Qhassim Ali, for their endless love, patience, and support during my PhD studies. May Almighty Allah reward you abundantly.

Finally, I would like to acknowledge my employer Muni University for their support.

DEDICATION

To my parents, wife, children, relatives, friends, and colleagues

May the almighty Allah count the support they rendered upon their heavenly treasures

AMEEN!

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATIONS AND SYMBOLS

2FA	Two-Factor Authentication
3D	Three Dimensions
3DES	Triple Data Encryption Standards
ACSC	Australian Cyber Security Centre
AES	Advanced Encryption Standard
AFI	Alliance for Financial Inclusion
AP	Attack Point
API	Application Programming Interface
ATM	Automated Teller Machines
BDO	Banco de Oro
BoU	Bank of Uganda
CBC	Cipher Block Chaining
CoCSE	Computational and Computer Science and Engineering
DDoS	Distributed Denial-of-Service
DES	Data Encryption Standards
DoS	Denial-of-Service
DSR	Design Science Research
DStv	Digital Satellite Television
ECC	Elliptic Curve Cryptography
ERD	Entity Relationship Diagram
FIDO	Fast IDentity Online
FinTech	Financial Technologies
G-MoMo	Genuine Mobile Money
GPS	Global Positioning System
GSMA	Global System for Mobile Communications Association
H_0	Null Hypothesis
HCI	Human-Computer Interaction
HMAC	Hash-Based Message Authentication Code
ID	Identification
IMEI	International Mobile Equipment Identifier
iOS	iPhone Operating System
IoT	Internet of Things
IP	Internet Protocol

IR 4.0	Fourth Industrial Revolution
IS	Information System
IT	Information Technology
KYC	Know Your Customer
MD5	Message-Digest algorithm 5
MFA	Multi-Factor Authentication
MITM	Man-in-the-Middle
MMSP	Mobile Money Service Provider
MNO	Mobile Network Operator
MTN	Mobile Telephone Networks
MVVM	Model-View-View Model
MySQL	My Structured Query Language
NHS	National Health Service
NID	National Identity
NIN	National Identification Number
NIRA	National Identification and Registration Authority
NIST	National Institute of Standards and Technology
NM-AIST	Nelson Mandela African Institution of Science and Technology
NSA	National Security Agency
NWSC	National Water and Sewerage Corporation
OTP	One-Time Password
PIN	Personal Identification Number
PKCS7	Public-Key Cryptography Standards 7
QR	Quick Response
RFID	Radio Frequency Identification
RIB	Rwanda Investigation Bureau
RSA	Rivest-Shamir-Adleman
SFA	Single-Factor Authentication
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SMEs	Small and Medium Enterprises
SMS	Short Message Service
SQL	Structured Query Language
SSO	Single Sign-On

U2F	Universal Second Factor
UAF	Universal Authentication Framework
UBOS	Uganda Bureau of Statistics
UCC	Uganda Communications Commission
UML	Unified Modelling Language
USSD	Unstructured Supplementary Service Data
UTL	Uganda Telecom Limited
UUID	Universally Unique Identifier
Wi-Fi	Wireless Fidelity
XSS	Cross-Site Scripting

CHAPTER ONE

INTRODUCTION

1.1 Background of the problem

Financial technologies (FinTech) have revolutionised financial services in the fourth industrial revolution (4IR) in developed and developing countries through mobile money, which arose as the prospective mobile payment platform. Talom and Tengeh (2019) define mobile money as a service that requires mobile money subscribers to use their mobile phones to gain access to financial services by either dialling unstructured supplementary service data (USSD) codes or using mobile money applications. Today, mobile money subscribers perform mobile money services using a dedicated mobile money application installed on a smartphone or USSD, but the latter is frequently used (Ayeb *et al*., 2020).

In 2001, smart communications launched smart money, the world's first mobile money in the Philippines, collaborating with banco de Oro (BDO) to overcome the challenges of having inadequate banking infrastructure. Globe Telecom later launched the GCash in 2004 after the success story of smart money (Thenerve, 2019). The GSMA report of 2022 stated that, as of 2021, 316 mobile money were deployed in 98 countries, and there were 1.35 billion mobile money accounts registered in the world, where 518 million are active in 90 days. 5.6 million unique active mobile money agent outlets globally and 12.2 million registered mobile money agents. The global volume and value of total mobile money transactions are 54 billion and $1.0 trillion, with $16 billion in international remittances processed per year and $66 billion transacted by merchants (Awanis *et al*., 2022).

There are 173 live mobile money deployments in Africa and 621 million registered mobile money accounts, where 184 million are active. Africa's total mobile money transaction volume is 36.7 billion, while the mobile money transaction value stands at $701.4 billion (Awanis *et al*., 2022). In Eastern Africa, there are 59 mobile money deployments and 296 million registered mobile money accounts, and the volume and value of total mobile money transactions are 24 billion and $403.4 billion, respectively (Awanis *et al*., 2022).

The first mobile money deployment in the East African region took place in Kenya in March 2007 when Safaricom rolled out M-Pesa. In April 2008, Vodacom launched M-Pesa in Tanzania, followed by Zantel's Z-Pesa (Baganzi & Lau, 2017; Hove & Dubus, 2019). According to

Afolayan (2021), M-Pesa has become the most prominent mobile money platform globally, with 50 million active users and over $1.37 billion in revenue by March 2021.

In 2009, mobile telephone networks (MTN) launched the first mobile money service in Uganda after the successful deployment of M-Pesa in Kenya and Tanzania. The MTN Uganda, Airtel Uganda, Uganda Telecom Limited (UTL), M-Cash, Ezeey Money, and Micropay are Uganda's six mobile money service providers. They have a network of approximately 32.3 million registered mobile money accounts and 315 895 active mobile money agents at the end of September 2021, and the total mobile money transactions' volume and value were 3.89 billion and $31.9 billion (Uganda Communications Commission [UCC], 2021; Bank of Uganda [BoU], 2021). The UCC report of 2021 stated that 9.7 million smartphones and other gadgets were connected to the internet in Uganda. The number of smartphone users at the end of June 2021 surpasses the number of basic phones connected to the network because of social media and the internet. The total internet subscription was above 22 million (UCC, 2021).

In Uganda, mobile money provides services such as depositing and withdrawing money, sending and receiving money, paying for telecom network services, paying utility bills, saving money, and borrowing money. It is also used for goods and services payments, transfer of money to and from abroad, mobile banking, purchasing insurance, paying for school fees and taxes, and receiving a pension, salary, and state aid to urban, rural, and low-income people at affordable costs (BoU, 2018; Alliance for Financial Inclusion [AFI], 2019; Ali *et al*., 2020b).

The different mobile money service providers in Uganda have developed mobile money applications that run on smartphones and implement two-factor authentication (2FA) that uses a personal identification number (PIN) and one-time password (OTP) to verify mobile money subscribers to access mobile money services (Byun *et al*., 2020). These applications are downloaded from App Store and Google Play (Byun *et al*., 2020). Though promising, this current 2FA scheme is susceptible to severe security concerns that violate the security goals of confidentiality, integrity, authentication, availability, privacy, and non-repudiation (Kasat & Bhadade, 2018; Mbunge & Rugube, 2018; Phipps *et al*., 2018; Bultel *et al*., 2018; Lei *et al*., 2021).

According to the Rwanda Investigation Bureau (RIB), 80 cases of money stolen from people's mobile money accounts were reported. The fraudsters take advantage of the weak mobile money schemes and lack of protection of the weak PINs to steal about 12 million Rwandan Francs (Kanife, 2020). Adebowale (2020) also reported that MTN Zambia mobile money subscribers are

defrauded through smishing, where fraudsters send short message service (SMS) to their victims to gain access to their confidential mobile money PINs.

Similarly, Kafeero (2020) reported that on October 3rd, 2020, hackers breached the security of the payment system through Pegasus Technologies, a consumer finance aggregator, and stole over $3.2 million where the mobile money payment system was accessed using 2000 mobile subscriber identity module (SIM) cards. The money was then transferred from the banks to the telecommunication companies, i.e., bank-to-mobile wallet transfers, and paid to different SIM cards nationwide. Dornbierer (2020) reported that employees of MTN Uganda stole $2.4 billion over six months by taking advantage of the weaknesses in know-your-customer (KYC) processes and deficiencies in the information technology (IT) systems. In addition, the report in 2019 by Annual Crime and Road Safety stated that Ugandans lost over $11 million to fraudsters via SIM card swapping, pyramid schemes and other cybercrimes (Kasemiire & Bagala, 2020). These attacks and frauds negatively impact the mobile money industry, forcing many subscribers to leave the business because of security challenges. Therefore, there was a need to address these security issues and make the authentication service more secure without hindering usability.

The broad and rapid adoption and usage of smartphones with powerful inbuilt features such as full-display, fingerprint sensors, high-quality cameras, speedy graphics chips, fast processors, three dimensions (3D) depth-projection, and scanning systems can help provide extra security to the mobile money authentication scheme. Therefore, developing a secure MFA algorithm that uses a novel method combining multiple authentication factors and cryptographic techniques to secure the authentication factors and confidential financial information helped to address the authentication security challenges.

1.2 Statement of the problem

The continuous growth in the paradigm of mobile money requires the development and implementation of sound security systems. Researchers have developed many algorithms to improve mobile money authentication security. For example, Suwera (2021) suggested a 2FA algorithm that uses a PIN and unique code to end the mobile money fraud menace. Mega (2020) proposed a 2FA framework to improve mobile money authentication security in Tanzania. Osman and Nakanishi (2020) designed a high-correctness 2FA system that uses a unique identification number and iris biometric for mobile money. Islam *et al*. (2019) presented a secure 2FA algorithm that uses PIN and iris biometrics for mobile money transfer among Bangladesh's small and

medium enterprises (SMEs). Chetalam (2018) proposed a secure MFA system for M-PESA transactions. Mtaho (2015) proposed a 2FA model to boost mobile money security.

However, no strong security measures were proposed to mitigate the security challenges encountered by mobile money authentication systems. Much as the existing algorithms are promising, additional study is still needed to improve these algorithms because they are susceptible to USSD technology vulnerabilities, shoulder-surfing attacks, identity theft, replay attacks, insider attacks, brute-force attacks, and phishing attacks. They are also vulnerable to spoofing attacks, PIN leakage, eavesdropping, SIM-swapping attacks, salami attacks, man-in-the-middle (MITM) attacks, and malware attacks (Castle *et al*., 2016; Buku & Mazer, 2017; Alhassan *et al*., 2018; Kunda & Chishimba, 2018; Sharma & Mathuria, 2018; Phipps *et al*., 2018; Kasat & Bhadade, 2018; Bultel *et al*., 2018; Saxena *et al*., 2019; Altwairqi *et al*., 2019; Bosamia & Patel, 2019; Lei *et al*., 2021). The mobile money PINs used in the authentication have a short length of four or five digits; all mobile money services are authorised using the same PIN with no expiry date. The PINs do not follow effective password management policies and are entered when unmasked and in plaintext during transactions, and sharing the PINs by the subscribers poses more risks (Nyamtiga *et al*., 2013a; Nyamtiga *et al*., 2013b; Basigie & Mtaho, 2014; Mtaho, 2015). These attacks and frauds result in financial loss; damage to the reputation of the service providers; affect the transaction and customer growth; discourage mobile money agents from investing in float and cash because of fear of loss; and the service operations are threatened, which can bring an abrupt end to it (Gilman & Joyce, 2012; Mudiri, 2013; Akomea-Frimpong *et al*., 2019).

Considering the current mobile money authentication schemes' security challenges, it becomes essential to develop a secure MFA algorithm for mobile money applications to solve the problems of authentication attacks. The proposed algorithm authenticates mobile money subscribers with a novel method combining the PIN, OTP, and biometric fingerprint. It also uses the customers' biometric fingerprints and the agents' quick response (QR) codes to authorise money withdrawals. In addition, the authentication factors like PIN and OTP are secured by secure hash algorithm-256 (SHA-256), and the Fast IDentity Online (FIDO) protects the subscriber's biometric fingerprint, whereas the Rivest-Shamir-Adleman (RSA) encryption secures the public/private key pair and the fingerprint templates. The QR code, the confidential financial information in the databases, and all the data before transmission to the remote databases are secured using Fernet encryption. This algorithm provides secure and efficient authentication, data confidentiality, integrity, and privacy. It also guarantees non-repudiation, user anonymity, and effectiveness

against numerous security threats and attacks. In addition, it improves the overall performance of G-MoMo applications compared to the existing mobile money systems.

1.3 Rationale of the study

Secure mobile money authentication and confirmation is still a challenge in many developing countries because security issues encountered by many mobile money schemes have kept increasing since they implemented 2FA. Though various mobile money service providers and researchers have proposed and implemented different algorithms to enhance the mobile money schemes' security, they still encounter many security attacks. Many mobile money applications have been developed in Uganda that use different authentication factors like PIN and OTP. Most of the applications are weak and poorly designed, thus creating security loopholes that adversaries can comprise (Buku & Mazer, 2017; Lonie, 2017). Therefore, it was necessary to develop a robust and secure MFA algorithm to improve mobile money applications' authentication security by using multiple authentication factors to overcome these security attacks and improve the overall system performance. The algorithm helped improve the authentication scheme, preserve the identity of the subscribers and protect the authentication factors and confidential financial information in the database against unauthorised people. Additionally, deploying highly secure mobile money applications ensured secure authentication, data integrity, confidentiality, availability, non-repudiation, privacy, and subscriber anonymity.

1.4 Objectives of the study

1.4.1 General objective

The main objective of this study was to develop a secure MFA algorithm for mobile money applications to solve the problems of authentication attacks.

1.4.2 Specific objectives

The specific objectives of the research are:

(i) To review the existing literature on threat models in the current 2FA scheme for mobile money.

(ii) To identify and assess the key security issues associated with mobile money systems in Uganda.

(iii) To design a secure MFA algorithm for mobile money applications and develop prototypes of native mobile money applications to implement the designed algorithm.

(iv) To validate the developed algorithm and prototypes for native mobile money applications.

1.5 Research questions

The research questions that guided the study to achieve the research objectives are:

(i) What security attacks are encountered by the current 2FA schemes for mobile money and their countermeasures?

(ii) What are the key security issues experienced by mobile money systems in Uganda?

(iii) What are the security and performance analysis results for the proposed secure MFA algorithm for mobile money applications?

(iv) Is the designed algorithm secure enough for mobile money authentication?

1.6 Significance of the study

This research is significant in its theoretical and practical contribution to the existing research knowledge base. The contribution to the theory was through; firstly, it extended the theoretical knowledge of security challenges encountered by the current mobile money schemes that use 2FA. Secondly, it identified the critical security issues encountered by Uganda's mobile money systems. Thirdly, the study provided mobile money service providers, governments, and other mobile money decision-makers with practical information to ensure appropriate authentication approaches for mobile money security. Fourthly, it is helpful to the Bank of Uganda to ensure that Ugandans have access to secure banking and financial services, which is crucial in achieving a sustainable development goal. Fifthly, the study helps build a better policy for mobile money businesses. Lastly, it provides valuable insight and awareness to users about the safety of mobile money systems and builds trust among mobile money subscribers.

1.7 Delineation of the study

The current 2FA schemes for mobile money systems have suffered numerous attacks from insiders and adversaries in the past few years because of their weaknesses. Therefore, the principal focus of the research was to improve the current mobile money authentication process by developing a secure MFA algorithm for mobile money applications. Three prototypes of native

G-MoMo applications were developed to verify the algorithm's feasibility and provide high security against security threats and attacks encountered in the current 2FA schemes.

This research did not cover the entire mobile money because it only focuses on solving the authentication attacks by using multiple authentication factors such as the PIN, OTP, biometric fingerprint, and QR code, where SHA-256 protected the PIN and OTP, and FIDO secured the subscribers' biometric fingerprints, where the RSA encryption protects the public/private key pair and the fingerprint templates, and Fernet encryption secured the QR codes, the confidential financial information in the databases, and all the data before transmission to the remote databases. It should be noted that while implementing the proposed algorithm, no extra devices were required except smartphones connected to the internet. While collecting data about the security issues encountered by mobile money systems, only respondents ready to participate were selected to avoid biases toward the study. In addition, the mobile money service providers were not ready to give data about security challenges faced by the mobile money systems and subscribers since it is sensitive and classified information that could sabotage their business. The researchers only relied on quantitative data obtained from registered mobile money customers, agents, and mobile network operators' (MNO) IT officers. With the financial and time constraints, the algorithm and prototypes developed mainly focused on three phases, i.e., enrolment, authentication, and transaction, where security is highly required

Although the study helped to improve and provide robust mobile money authentication security by implementing a novel method combining multiple factors such as PIN, OTP, biometric fingerprint, and QR code, and securing the authentication factors by using multiple cryptographic techniques like SHA-256, FIDO with RSA encryption, and Fernet encryption, the three G-MoMo applications can only be used by people who have smartphones with fingerprint sensors and connected to mobile internet. The significant majority of mobile money subscribers without smartphones will never benefit from the innovation.

With the high computational cost coupled with the poor mobile internet network in Uganda, the few subscribers with smartphones will still face challenges while using the G-MoMo applications because it will take time to enrol, authenticate, perform transactions, and for the Twilio application programming interface (API) to send 5-digit OTPs to the subscribers' smartphones. This will affect the adoption and usage of the G-MoMo applications and revenue for the mobile money service providers and the industry.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter reviews the relevant literature on mobile money authentication algorithms and schemes, vulnerabilities and security attacks, and the mechanism for securing mobile money authentication schemes. The review is divided into the: (a) concept of authentication, (b) types of authentication mechanisms, (c) mobile money system architecture, (d) authentication factors used in mobile money, (e) threat model, (f) countermeasures for mobile money authentication attacks, (g) studies related to mobile money and mobile banking systems, (h) the security technologies, (i) the theoretical framework, and (j) conclusion.

2.2 Concept of authentication

User authentication has become paramount in financial technologies like mobile money because of the increasing security and privacy issues. Hammad *et al.* (2020) and Zaidi *et al.* (2021) define authentication as the process of confirming the identity of a user that requests access to a system resource, network, or device by matching the data received from the user with database data to prove their identity. User authentication can be executed from the device or a server (Baig & Eskeland, 2021). Authentication provides a security solution that requests users to have direct access to secure real-time information from the device, system resources, or network by availing either the knowledge factor, the possession factor, the biometric factor, or a combination of these factors (Vangala *et al.,* 2021; Thomas & Mathew, 2021).

The authentication factors must be convenient for users and secure to protect the stored information (Zaidi *et al*., 2021). The main aim of user authentication is to verify the legitimacy of the user trying to access the device, system resources, or network so that unauthorised users are prevented from accessing confidential information and services (Hayikader *et al*., 2016; Shi *et al*., 2021; Katsini *et al*., 2021; Wang *et al*., 2021). It also helps to ensure the security and privacy of legitimate users (Zhang *et al*., 2021). Authentication factors are categorised into knowledge, possession, inherence, location and behaviour.

(i) Knowledge factors (something you know)

These are the things that a user knows, like usernames & passwords, PINs, and answers to secret questions (Ali *et al*., 2020a; Vorakulpipat *et al.*, 2021). They are typically used for single-factor authentication and offer little security when implemented alone.

(ii) Possession factors (something you have)

These are the things that a user has, including a SIM card, mobile phone, Smart card, OTP token, or FIDO2 security key (Ali *et al*., 2020a; Vorakulpipat *et al*., 2021).

(iii) Inherence factors (something you are)

This is where users are identified using their unique biometrics features. They are unique physical and behavioural traits of the user. Examples of the inherence factor are biometric fingerprints, face, iris, retina, and voice (Ali *et al*., 2020a; Vorakulpipat *et al*., 2021).

(iv) Location factors (somewhere you are)

This is where a user's identity is recognised using a computing network or a global positioning system (GPS) signal by detecting their presence at a distinct location (Zin *et al*., 2019). Examples of the different methods for detecting the user's locations include GPS signal, wireless fidelity (Wi-Fi) locator, radio frequency identification (RFID) reader location, and internet protocol (IP) addresses (Baig & Eskeland, 2021; Boonkrong, 2021; Vorakulpipat *et al*., 2021).

(v) Behaviour factors (something you do)

This is where users are identified by observing the actions they perform. Examples of behaviour-based factors are keystroke dynamics, touch dynamics, and gestures (Baig & Eskeland, 2021). Table 1 summarized the authentification factors.

Table 1: Summary of the authentication factors and their examples

S/No	Authentication factors	Example
1.	Knowledge factors (Something you know)	Usernames & Passwords, PINs, answers to secret questions
2.	Possession factors (Something you have)	SIM card, mobile phone, Smart card, OTP token, FIDO2 security key.
3.	Inherence factors (Something you are)	Fingerprint, face, iris, retina, voice.
4.	Location factors (Somewhere you are)	GPS signal, Wi-Fi locator, RFID reader location, IP addresses.
5.	Behaviour factors (Something you do)	Gestures, keystroke dynamics, touch dynamics.

2.3 Types of authentications

Single sign-on (SSO), single-factor authentication (SFA), 2FA, and MFA are the four types of authentications used to verify users.

2.3.1 Single sign-on (SSO)

Single sign-on is where a user is authenticated with a single login credential to access multiple services or system resources without the system requesting a repeated login procedure (Ramamoorthi & Sarkar, 2020; Kebande *et al*., 2021). For example, with the same account and a single sign-on, Google, PayPal, Facebook, Microsoft, Alibaba, and Tencent allow users to access many network systems using the SSO protocols (Bao *et al*., 2019). A single sign-on aims to reduce the number of multiple authentications and credentials (e.g., passwords) remembrance by the user in a particular period (Lazarev *et al*., 2016). It provides improved security & compliance, monitors user accounts, and does not need users to remember multiple login credentials (Karunanithi & Kiruthika, 2011; Ramamoorthi & Sarkar, 2020). In addition, the process is convenient since it requires a single login credential (Kebande *et al*., 2021). Much as SSO provides numerous benefits, there is a high risk of the single password being compromised by attackers and is also vulnerable to identity theft and authentication issues (Lazarev *et al*., 2016; Kebande *et al*., 2021).

2.3.2 Single-factor authentication (SFA)

Rahav (2018) defines SFA as an identity verification process where the authenticating party requires users seeking access to the system to provide a single attribute linked to their identity. SFA is widely adopted because of its simplicity and user-friendliness and is a low-cost alternative

to authenticate users (Ometov & Bezzateev, 2017; Ometov *et al*., 2018; Ibrokhimov *et al*., 2019). Examples of SFA include using a PIN to unlock a smartphone or a username and password to log into an e-mail account. However, many organisations and companies opt for a more secure authentication method(s) for their systems and applications because SFA is the weakest authentication method for verifying users in online transactions (Ometov & Bezzateev, 2017). It is hard to remember the authentication factors like PINs and usernames & passwords. In addition, they are susceptible to shoulder-surfing attacks, guessing attacks, social engineering attacks, MITM attacks, replay attacks, and brute-force attacks (Rahav, 2018). Figure 1 shows an example of SFA.

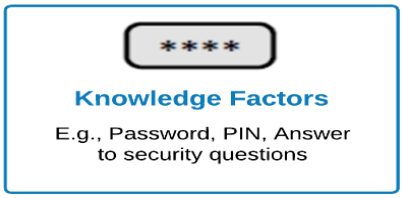


Figure 1: Single-factor authentication (Ometov *et al*., 2018)

2.3.3 Two-factor authentication (2FA)

Dutson *et al*. (2019) and Reynolds *et al*. (2020) define 2FA as an identity verification process where the authenticating party requires users seeking access to the system to provide two attributes linked to their identities, such as a knowledge factor and possession factor or inherence factor. For example, mobile money users must have mobile phones and PINs to perform transactions (Reynolds *et al*., 2020). The 2FA is widely implemented in Facebook, Twitter, Google, and banks because it helps strengthen the security against account compromise (Reese *et al*., 2019; Dutson *et al*., 2019; Reynolds *et al*., 2020). The primary purpose of 2FA is to boost the security of password-based authentication systems by making them useless in case it is compromised by an attacker who does not have the second factor (Reynolds *et al*., 2020). Nevertheless, the 2FA is perceived by users as difficult to adapt; it is susceptible to eavesdropping attacks, MITM attacks, Trojan attacks, and phishing attacks (Ometov *et al*., 2018; Dutson *et al*., 2019). Likewise, the attackers can compromise the second factor of authentication (Zhang *et al*., 2018). Figure 2 shows an example of 2FA.

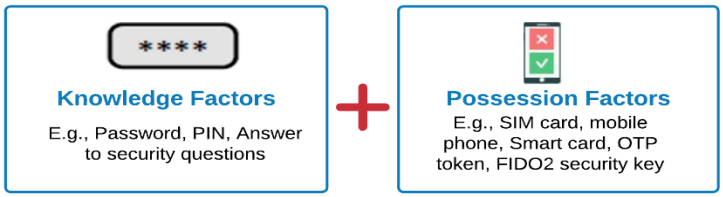


Figure 2: Two-factor authentication (Ometov *et al*., 2018)

2.3.4 Multi-factor authentication (MFA)

Ibrokhimov *et al*. (2019), Boonkrong (2021), and Kebande *et al*. (2021) define MFA as an identity verification process where the authenticating party requires users seeking access to the system to present multiple authentication credentials linked to their identity to ensure the security of the account. The primary purpose is to increase the safety of the authentication systems, services, information, and privacy so that it is challenging for attackers to compromise (Ometov *et al*., 2018; Devasena, 2018; Vorakulpipat *et al*., 2021). For MFA to be successfully implemented, one of the verification factors must be kept away from the device for accessing the system or resources (Australian Cyber Security Centre [ACSC], 2019). The MFA provides a higher security level through multiple user login credentials to protect the devices, systems, and resources from intruders (Taher *et al*., 2019; Ibrokhimov *et al*., 2019; Vorakulpipat *et al*., 2021; Chishti *et al*., 2021; Kebande *et al*., 2021). It also helps achieve consistency in organisations (Lone & Mir, 2021). Much as the MFA provides increased security, it does not prevent passwords or password-hash from being stolen (Obaidat *et al*., 2020). Figure 3 is a typical example of multi-factor authentication.

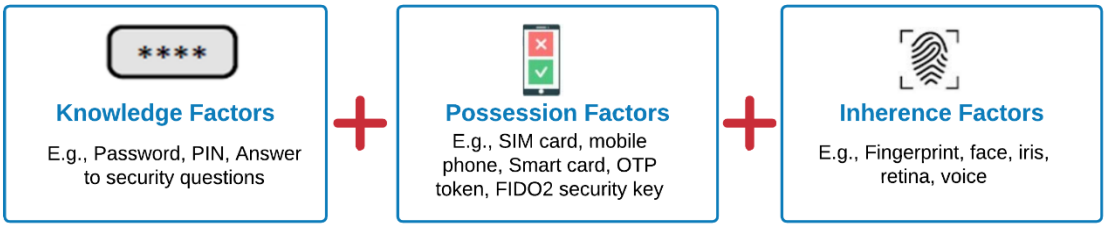


Figure 3: Multi-factor authentication (Ometov *et al*., 2018)

2.4 Mobile money system architecture

The mobile money system encompasses diverse components such as networks, mobile money subscribers, IT administrators and other administrators, financial institutions, base transceiver stations, databases, software, servers, and other core components of the MNO. It is also connected to internal and external interfaces and platforms to offer complete commercial functionality (Nyamtiga *et al*., 2013b; McGrath & Lonie, 2013; Pareek & Khandaker, 2018). All the components must work jointly to achieve the primary goal of the mobile money system (Ali *et al*., 2020a). Figure 4 illustrates the architecture of the mobile money system.

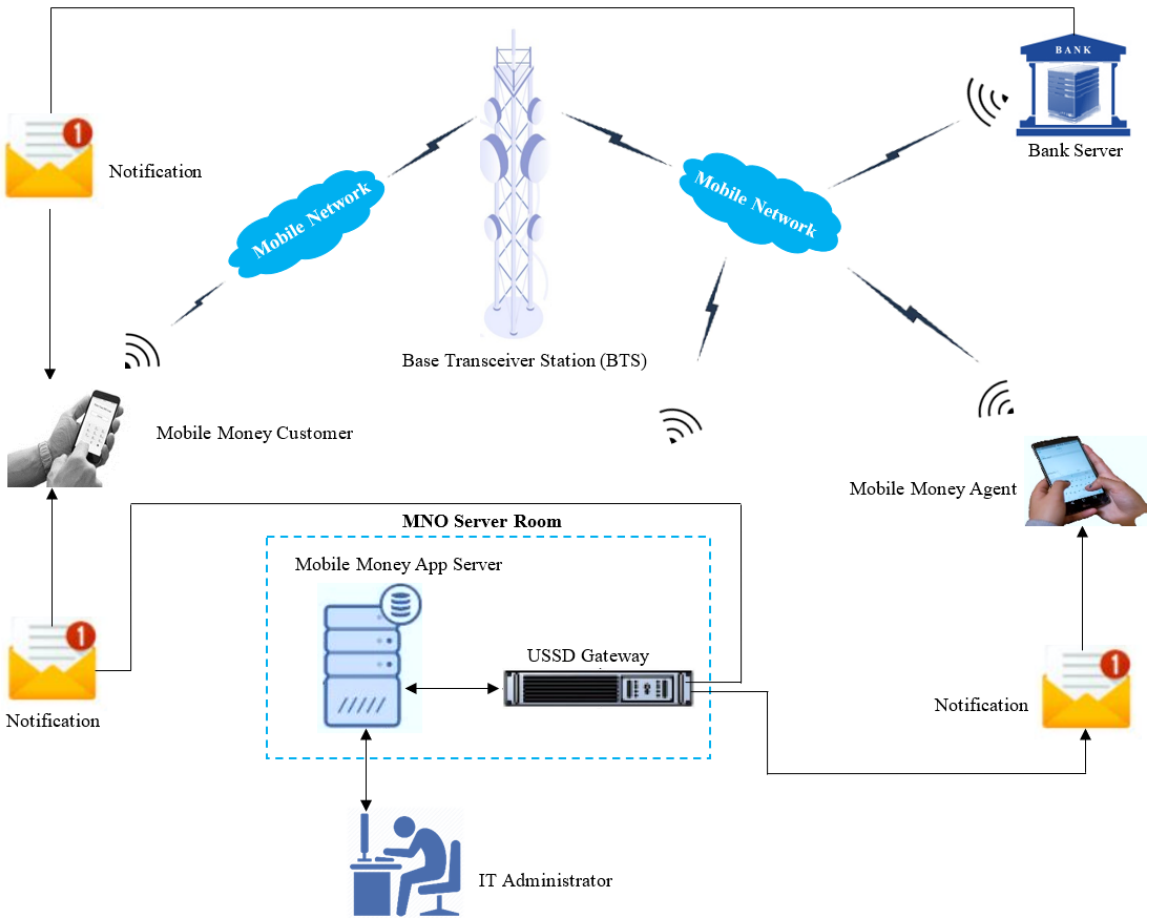


Figure 4: The architecture of the mobile money system (Ali *et al*., 2020a)

2.5 Authentication factors used in mobile money

The most common authentication factors used to verify mobile money subscribers are passwords, PINs, OTPs, QR codes, and biometrics (i.e., fingerprint, face, iris, retina, and voice).

2.5.1 Password

Passwords have been used for many decades and are the most widely used means of identifying and verifying users on the internet. Ali *et al*. (2020a) define a password as a series of characters to verify the user's identity and control access to a system, service, device, and resources. In most applications, passwords are used with usernames to authenticate users. Passwords have been implemented in many schemes, devices, and services, including mobile money systems (ArunPrakash & Gokul, 2011). The security of passwords depends on the selection and storage mechanism (Dubey & Martin, 2021). It is always suitable for organisations and companies to have a good password policy that helps to protect their resources. Strong passwords must comprise lowercase and uppercase letters, numbers, and special characters and should be at least eight characters long (Ali *et al*., 2020a). Using passwords helps to prevent attackers from accessing

systems, devices, services and resources. It is recommended that passwords be easy to remember and must be changed frequently (Ali *et al*., 2020a). It must be simple, user-friendly, robust, and effective in authenticating intended users (Rajamanickam *et al*., 2020; Shamshad *et al*., 2020; Szalachowski, 2021). Nevertheless, passwords are susceptible to brute-force attacks, dictionary attacks, phishing attacks, insider attacks, MITM attacks, and denial-of-service (DoS) attacks (Ahmadzadegan *et al*., 2015; Basharzad & Fazeli, 2017). They are also vulnerable to spoofing attacks, spyware attacks, eavesdropping attacks, and password-guessing attacks (Singh & Raj, 2019; Huang & Zhang, 2020; Shamshad *et al*., 2020). Likewise, passwords are easily cracked, stolen, forgotten, and weak (Basharzad & Fazeli, 2017). Therefore, passwords remain flawed in authenticating users (Wimberly & Liebrock, 2011).

2.5.2 Personal identification number (PIN)

Personal identification numbers (PINs) have been extensively implemented in mobile devices and financial applications to authenticate and verify users' identities. Shang and Wu (2020) and Ali *et al*. (2021) define a PIN as a numeric password to authenticate users in electronic transactions or access systems. The most common PINs used are four (4) or (5) digits (Ali *et al*., 2020a). The PINs have been widely implemented in automated teller machines (ATM), mobile money, smartphone & tablet, point-of-sale, digital door locks, smart locks, and mobile applications (Salman *et al*., 2019; Chakraborty *et al*., 2019; Shang & Wu, 2020; Hari *et al*., 2021; Caporusso, 2021). They must be kept secret when created until they are used. The PIN-entry method is widely adopted in systems and devices because of its simplicity, reliability, convenience, efficiency, and customer satisfaction. However, they are vulnerable to brute-force attacks, shoulder-surfing attacks, thermal tracking, PIN leakage, random guessing attacks, replay attacks, acoustics keyboard eavesdropping, social engineering attacks, spoofing attacks, smudge attacks, malware attacks, and are easily forged (Salman *et al*., 2019; Shang & Wu, 2020; He *et al*., 2020; Das *et al*., 2020; Ali *et al*., 2020a; Ali *et al*., 2020b; AbouSteit *et al*., 2020; Zhang *et al*., 2021; Hari *et al*., 2021; Jain *et al*., 2021; Caporusso, 2021; Binbeshr *et al*., 2021).

2.5.3 One-time password (OTP)

According to AbouSteit *et al*. (2020) and Wu *et al*. (2021), one-time password (OTP) is a dynamic password that provides the second layer of security during authentication and is only valid for one login session and a short time. A one-time password has been adopted as the second factor during user authentication because of password and PIN authentication vulnerabilities. It can be generated based on time, pattern, and random keys (AbouSteit *et al*., 2020; Wu *et al*., 2021). One-

time passwords are used to provide secure user authentication because they have a high level of randomness and are effective for a short time and one login session (Imamah, 2018; Janakiraman *et al*., 2018). It should be noted that OTPs are generated from the server side and sent to the user for authentication. Upon the user receiving the OTP message, they must enter the OTP into the system to verify their identity. The user is successfully authenticated if the entered OTP matches the copy stored on the server side (Srivastava & Sivasankar, 2016; Sharma & Nene, 2020; AbouSteit *et al*., 2020). After the user and the service provider mutually agree on how to deliver the OTP, it is encrypted and shared with the user in a secure network to complete their authentication process (Sharma & Nene, 2020; AbouSteit *et al*., 2020). Short message service, e-mail, and OTP applications are different means of delivering OTP to the user. However, SMS is the most common method for sending OTPs to users because it is easy and cheap (AbouSteit *et al*., 2020). With the use of OTP in 2FA, it helps prevent shoulder-surfing attacks, reverse engineering, MITM attacks, replay attacks, eavesdropping attacks, identity theft, spoofing attacks, brute-force attacks, and phishing attacks (Zadeh & Barati, 2019; Iftikhar *et al*., 2019; AbouSteit *et al*., 2020; Khalid *et al*., 2020). Furthermore, there is no need to remember OTP (Wu *et al*., 2021). Much as OTPs solve many problems passwords and PINs encounter, they are vulnerable to SIM-swapping, wireless SMS OTP interception, malware, and physical access to the mobile phone that receives the OTP (Reyes *et al*., 2018; Lei *et al*., 2021).

2.5.4 Quick response (QR) code

With the in-depth advancement of mobile technology and the internet of things (IoT), there is widespread adoption and usage of secure technology like quick response code (QR code) in all walks of life. Quick response code is a two-dimensional barcode of a black and white square-shaped module used to encode, store, process, and transmit information that can only be decoded with the help of a QR code scanner or QR code scanner App installed on the smartphone (Devendra, 2021; Shaik, 2021; Kurniawan *et al*., 2021). A bit of data is described in each module, and the black square stores a value of 1 while the white stores 0. The black and white squares allow encoding/decoding of information (Sabri *et al*., 2021; Cho *et al*., 2021). Quick response codes can encode 7089 numeric characters, 4296 alphanumeric characters, letters, symbols, 2953-byte characters, and 1817 Kanji/Kana (Chou & Wang, 2020; Sabri *et al*., 2021; Din *et al*., 2021; Shaik, 2021; Cho *et al*., 2021). Quick response Codes are being implemented in many fields, such as transactional payment, tourism, information security, manufacturing, e-commerce, health, marketing, transportation, warehouse, life sciences, inventory tracking, office automation, product tracking, education, gaming industry, mining because of its large storage capacity and fast

information decoding speed (Wahsheh & Luccio, 2020; Lv *et al*., 2020; Karrach *et al*., 2020; Huang *et al*., 2020; Li *et al*., 2020; Devendra, 2021; Shaik, 2021; Sabri *et al*., 2021; Din *et al*., 2021; Demuyakor & Demuyakor, 2021; Onyinyechi *et al*., 2021; Dey *et al*., 2021).

They are adopted in various fields because of their speed of encoding/decoding, flexibility, convenience, easy readability, ease of use, ample data storage, error correction capability, user-friendliness, versatility, cost-effectiveness, and accuracy (Ahmad *et al*., 2021; Din *et al*., 2021; Onyinyechi *et al*., 2021; Dey *et al*., 2021; Sun *et al*., 2021; Suebtimrat & Vonguai, 2021; Kosim & Legowo, 2021; Widaningsih & Suheri, 2021; Chaveesuk & Piyawat, 2021; Tao *et al*., 2021). They also ensure data confidentiality, integrity, and non-repudiation and prevents shoulder-surfing attacks. Besides, QR codes are resilient to identity theft and brute-force attacks (Ximenes *et al*., 2019). Nevertheless, QR codes are highly prone to phishing (QRishing) attacks, malware attacks, MITM attacks, structured query language (SQL) injection, bar-code-in-barcode attacks, pharming attacks, cross-site scripting (XSS), barcode tampering and counterfeiting, command injection, reader applications attacks (Focardi *et al*., 2019; Shruti *et al*., 2020; Huang *et al*., 2020; Onyinyechi *et al*., 2021).

2.5.5 Biometrics

Authenticating and identifying people using conventional methods such as passwords, PIN, and OTP has serious security challenges, thus forcing organisations and companies to embrace biometrics as an additional security factor. According to Alanezi *et al*. (2020), the word "biometrics" comes from the Greek words "*bio"* (life) and "*metrics"* (measure). Biometrics refers to a person's distinctive physical and behavioural traits for digital identification and verification to grant access to systems or services (Yang *et al*., 2021; Abdulrahman & Alhayani, 2021). Because of the advancements in sensing technologies, biometrics are becoming predominant, thus helping to solve the problem of password and PIN-based verification (Yang *et al*., 2021). Biometrics have been widely adopted in, but not limited to, law enforcement, border control, mobile authentication, military applications, access control, and financial services because of their universality, uniqueness, performance, permanence, acceptability, circumvention, and measurability (Yang *et al*., 2021; Tran *et al*., 2021). Additionally, biometric data are untransferable and are less vulnerable to fraud.

Enrolment and authentication are the two significant phases in biometric systems. Figure 5 shows the enrolment and authentication phases in biometric systems.

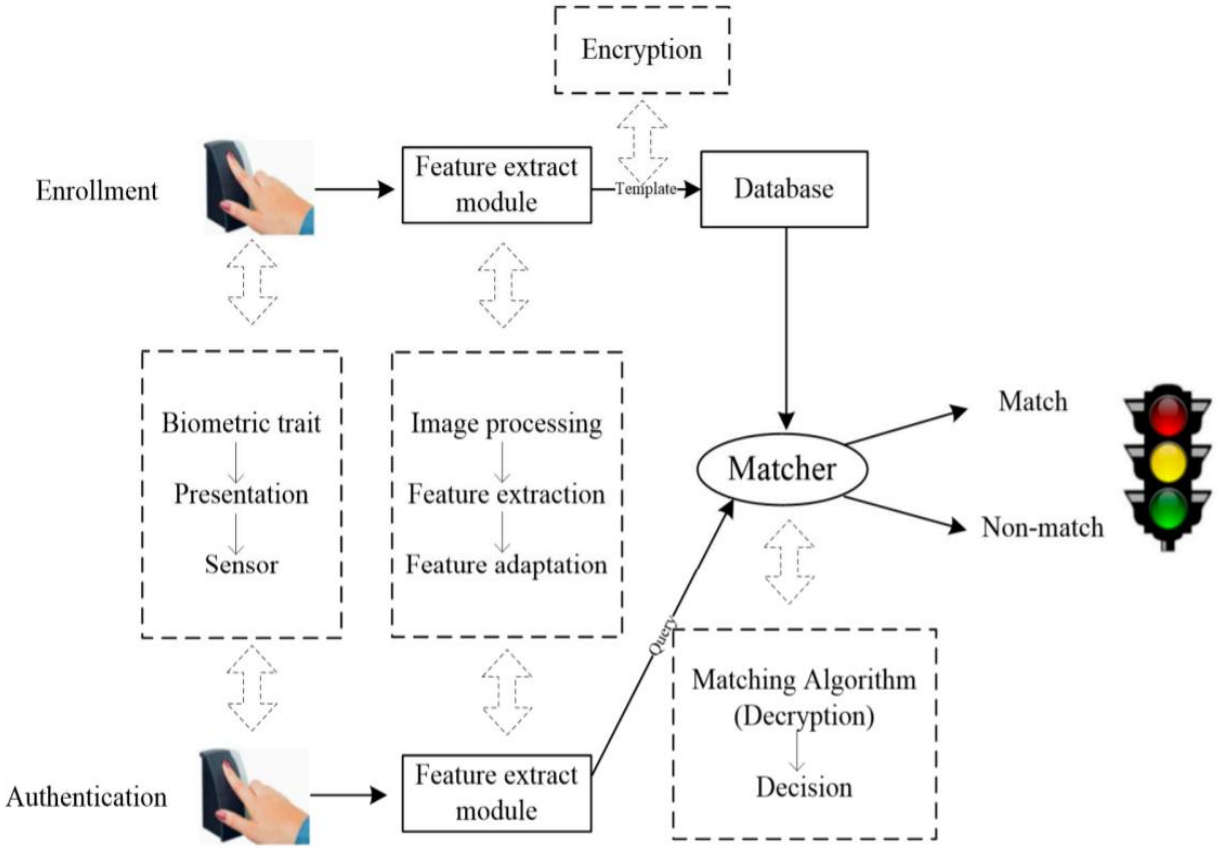


Figure 5: The enrolment and authentication phases in biometric systems (Yang *et al.*, 2019)

Physiological and behavioural biometrics are the two types of biometrics. Physiological biometrics uses a person's unique physical traits for digital identification and verification. Fingerprint, face, iris, and retina recognitions are physiological biometrics used in mobile money authentication (Ali *et al*., 2020a; Tran *et al*., 2021). Behavioural biometrics uses a person's unique behavioural traits for digital identification and verification, e.g., voice recognition in mobile money schemes (Ali *et al*., 2020a; Tran *et al*., 2021). Figure 6 illustrates the categorisation of physiological and behavioural biometrics.

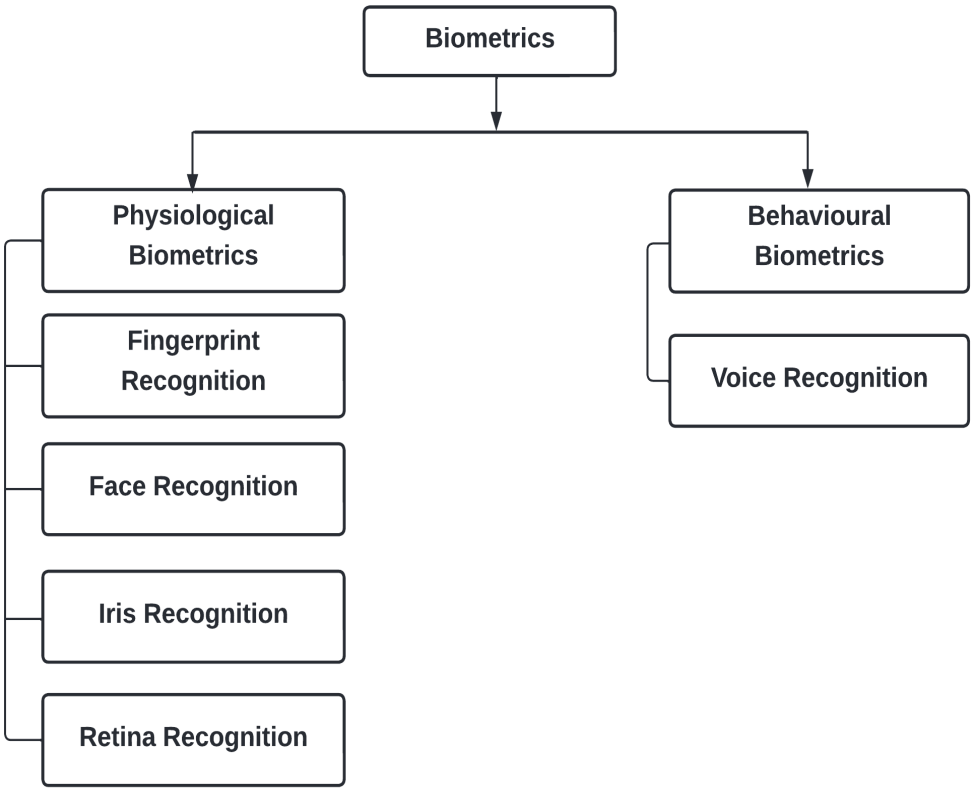


Figure 6: The categorisation of physiological and behavioural biometrics (Ali *et al.*, 2020a)

Some of the physiological and behavioural biometrics used in authenticating mobile money subscribers are:

(i) Fingerprint recognition

Fingerprint recognition is a broadly used biometric recognition system in computerised systems today because of the incorporation of the best biometrics features. Fingerprint recognition refers to the automated and visual verification where people are identified based on the patterns of ridges and valleys found on their fingertips (Dasgupta *et al*., 2017; Yang *et al*., 2021). The surface of the fingerprint contains raised folds of skin known as ridges which are separated by valleys. The numerous landmark points called minutiae describe the ridges, and examples of the minutiae are ridge endings, crossovers, cores, and bifurcations (Fingerprints, 2017). The ridges and valleys form a pattern on the fingertip shown in the fingerprint. Yang *et al*. (2021) stated that even identical twins do not have the same fingerprints.

Enrolment and authentication are the two main phases of fingerprint recognition (Priya, 2017). The enrolment phase involves the acquisition of a fingerprint, extraction of the feature, and storage of the template. The authentication phase involves the acquisition of a fingerprint, extraction of

the feature, and matching the extracted feature with the stored fingerprint templates (Priya, 2017; Yang *et al*., 2019; Alanezi *et al*., 2020; Abdulrahman & Alhayani, 2021).

Fingerprint recognition is mainly used in financial and commercial applications and the aviation industry because of its high matching accuracy and speed; ease to use; ease of acquisition; convenience; higher security and accountability; cannot be forgotten; and cost-effectiveness (Priya, 2017; Fingerprints, 2017; Yang *et al*., 2021). Fingerprint recognition has also been adopted in mobile money schemes. For instance, the systems proposed by Mtaho (2015), Okpara and Bekaroo (2017), Hassan and Shukur (2021a), and Hassan and Shukur (2021b) used fingerprint recognition to improve mobile money and payment security.

(ii) Face recognition

With the advancement in smart cameras and mobile device technologies coupled with the high demand for security and convenience, face recognition has gained acknowledgement in pattern recognition (Guha, 2021; Yang *et al*., 2021). Face recognition is defined as the process of using a person's facial features like eyes, eyebrows, nose, mouth, cheeks, skin colour, lips, chin, ears, face shape, beards, wrinkles, and the distance between them to identify users by comparing these features with the digital image or a video frame stored in the database (Alsrehin & Al-Taamneh, 2020; Lin & Xie, 2020; Shavetov & Sivtsov, 2020; Bai *et al*., 2020; Geetha *et al*., 2021; Badave & Kuber, 2021). During face recognition, a person's facial image is obtained using the cameras and videos from security and surveillance systems and applied to various pattern recognition algorithms to get unique features used for identification (Thomas, 2021; Yang *et al*., 2021; Preethi & Vodithala, 2021). The main aim of face recognition is to authenticate and authorise users to have secure access to a system or service (Mantoro *et al*., 2018; Ejaz *et al*., 2019; Geetha *et al*., 2021). Face recognition systems use artificial intelligence and other specialised technologies to identify and verify human faces (Yu *et al*., 2018).

Face detection, face alignment, face feature extraction, and feature matching with the stored template are the steps involved in face recognition (Sithara & Rajasree, 2019; Alsrehin & Al-Taamneh, 2020; Sahu & Dash, 2020; Malakar *et al*., 2021; Badave & Kuber, 2021; Preethi & Vodithala, 2021). Likewise, face recognition systems can be image-based, video sequence-based, and sensory data-based matching (Tran *et al*., 2021).

Face recognition is being implemented in many areas, such as surveillance and security applications, credit card, user identification in mobile devices, computer vision, communication,

and automatic control systems, industrial fields, government, military, banking, social welfare, e-commerce, passport checking, law enforcement, voter verification, healthcare, education (Sharmila *et al*., 2019; Geetha *et al*., 2021; Zhiqi, 2021; Paul *et al*., 2021; Badave & Kuber, 2021). For example, Zadeh and Barati (2019) implemented face recognition to improve mobile banking security.

Face recognition is mainly adopted in applications because of its uniqueness, security, and accuracy, and it requires a camera for verification that is easy to install and use (Abbas *et al*., 2017; Shavetov & Sivtsov, 2020; Thomas, 2021). Much as face recognition is implemented in many applications, they encounter many challenges such as similar faces, face deformation, age factor, illumination changes, direction, occlusion, pose and expression changes, shading, and dynamic background (Li, 2019; Sahu & Dash, 2020; Luo *et al*., 2021; Guha, 2021; Badave & Kuber, 2021).

(iii) Iris recognition

One of the reliable and acknowledged technologies in pattern recognition is iris recognition. Danlami *et al*. (2020) and Lee *et al*. (2021) define iris recognition as the process of identifying people using the unique patterns and features of the iris, compared with the iris template stored in the database. Iris is defined as the ring-shaped coloured area between the black pupil with a white sclera which has a unique structure and layer to manage the pupil to regulate the amount of light that enters the eye (Patil & Vasanth, 2019; Pattar, 2019; Gunasekaran & Muthuraman, 2020). The iris development in fetal life starts at 3 months, and the unique iris pattern begins to form one year after birth. This uniqueness of the iris is also between the identical twins, the left and right iris, thus, making it the best feature for biometric recognition (Vishwakarma & Patel, 2019; Danlami *et al*., 2020). Extracting information from either the left or right iris of a person can be used to develop a more accurate biometric system (Bharadi *et al*., 2018). Leonard Flom and Alan Safir recommended the iris for biometric identification in 1987, and John Daugman implemented the first iris recognition in 1994 (Ramli *et al*., 2017). Iris recognition uses high-resolution pupil images to perform pattern recognition. The image resolution helps to present all the information for recognition (Ribeiro *et al*., 2019; Radojicic *et al*., 2020).

Iris recognition consists of the enrolment and verification phases like fingerprint, face, iris, and voice recognition. Locating the iris position, iris image acquisition, iris localisation or segmentation, iris normalisation, feature extraction, and matching are the sub-processes during

enrolment and verification (Mohammed & Al-Gailani, 2019; Wang *et al*., 2020; Abdalla *et al*., 2020; Hsiao *et al*., 2021; Tran *et al*., 2021).

The primary purpose of iris recognition is to identify and authenticate people by examining their unique iris patterns (Zhuang *et al*., 2020). Iris recognition is extensively applied in biometric applications such as access control, passports, national ID program, internet security, border control, credit card authentication, defence security, airport, scientific laboratories, forensics, financial services, and school and hospital settings (Wang *et al*., 2020; Gunasekaran & Muthuraman, 2020; Wang & Kumar, 2020). Iris recognition is also applied in the mobile money sector. For example, Islam *et al*. (2019), Mega (2020), and Osman and Nakanishi (2020) proposed a 2FA using PIN and iris biometrics for mobile money.

Iris recognition is secure, stable, and accurate biometric system (Anand *et al*., 2020; Lee *et al*., 2021; Han, 2021; Hsiao & Fan, 2021). It has universality, uniqueness, permanence, collectability, and performance and is resilient to environmental perturbations, fraud, and immutability over time, ensuring non-repudiation (Chakraborty *et al*., 2020; Wang & Kumar, 2020; Abdalla *et al*., 2020; Moolla *et al*., 2021; Lee *et al*., 2021; Yang *et al*., 2021). However, iris recognition encounters many limitations, such as being prone to attacks, the iris patterns can be stolen, and abnormalities in the pattern of iris tissue (Pei *et al*., 2019; Azimi *et al*., 2019). It is challenging to acquire a good-quality iris image from a long distance (Patil & Vasanth, 2019; Pavaloi *et al*., 2019).

(iv) Retina recognition

Retina recognition identifies people by analysing the retina's unique patterns of blood vessels (Priya, 2017; Saha *et al*., 2019). The vascular images in the retina are obtained using the optical method, which is then used for identification (Borah *et al*., 2015; Feng, 2018). Saha *et al*. (2019) and Sultan and Ghanim (2020) define the retina as an ultra-thin layer of blood vessels positioned behind the human eyeball. These blood vessels are so unique that even identical twins do not have similar patterns (Waheed *et al*., 2016; Yuan *et al*., 2018). The distinctiveness of retinal vascular patterns in individuals was first identified by. Dr Carleton Simon and Dr. Isodore Goldstein in 1935, but Dr. Paul Tower found the uniqueness in identical twins (Waheed *et al*., 2016). Retina recognition provides a secure and accurate way of identifying and verifying people in systems and services (Yuan *et al*., 2018; Szymkowski *et al*., 2020).

Retina image acquisition, retinal vessel segmentation, unique feature extraction, and matching are the main steps in retina recognition (Waheed *et al*., 2016; Saha *et al*., 2019). Retina recognition is used for access control in government divisions, nuclear facilities, military, ATMs, research sites, managing an account, and high-security environments (Borah *et al*., 2015; Sadikoglu & Uzelaltinbulat, 2016; Haware & Barhatte, 2017). It also found its way into the mobile money industry. For example, Ray *et al*. (2016) developed a secure multi-purpose mobile-banking application that uses a retinal image.

Retina recognition is the most promising because it is perceived as the most secure, accurate, highly reliable, and robust method for identification (Priya, 2017; Haware & Barhatte, 2017). It has universality, time invariance, and uniqueness due to the distinct pattern of blood vessels; thus, it cannot be forged (Haware & Barhatte, 2017). Also, the retina remains stable over a person's lifespan; it is not exposed to external environmental threats, thus minimising its deformation (Waheed *et al*., 2016; Haware & Barhatte, 2017; Feng, 2018; Sultan & Ghanim, 2020). Retina recognition is not widely adopted despite having all these benefits because of the high cost, not convenient for people who wear glasses, and the long execution time affecting their performance (Priya, 2017; Feng, 2018; Yuan *et al*., 2018). The poor clarity of the vascular network of the retinal image affects the verification process, and the retina can be affected by diseases (Sadikoglu & Uzelaltinbulat, 2016; Haware & Barhatte, 2017). In addition, the internal location, the small size, and the difficulty in measuring the retina make it challenging to capture the image (Sadikoglu & Uzelaltinbulat, 2016).

(v) Voice recognition

Voice recognition identifies people using their unique voice acoustic features, matched with the copy of the digital template stored in the database (Thomas *et al*., 2020; Khotimah *et al*., 2020; Ye & Yang, 2021). Voice recognition determines the person's identity based on the voice, not the content of the speech (Kandhari *et al*., 2018; Al-Tekreeti & Ibrahim, 2020). In voice recognition, a person's voice is analysed to extract the intensity, duration, pitch information, and quality of a vocal sound used for identification (Yang *et al*., 2021). It also involves physiological and behavioural features where the physiological traits are based on the shape and size of vocal tracts, lips, nasal cavities, and mouth. In contrast, behavioural characteristics are based on the movement of lips, jaws, tongue, velum, and larynx.

Voice recognition has two phases, i.e., enrolment and verification. The phases involve speech signal/pre-processing, feature extraction, feature matching, and voice recognition (Tymchenko *et*

al., 2020; Krčadinac *et al*., 2021; Ye & Yang, 2021). The primary aim of voice recognition is to enhance security during identification and verification (Imario *et al*., 2017; Kiran *et al*., 2017).

Voice recognition is applied in various fields, including telebanking, video games, household appliances, surveillance and security systems, mobile application, voice dialling, online services, personal assistant services, and access control (Khotimah *et al*., 2020; Thomas *et al*., 2020; Krčadinac *et al*., 2021; Ye & Yang, 2021). Voice recognition is also applied in mobile money systems. For example, Chetalam (2018) developed a mobile money application to improve M-Pesa transactions' security using device-specific ID, PIN, and voice biometrics. Ombiro (2016) proposed a mobile-based MFA scheme for mobile banking where a PIN, OTP, or mobile flash call are used for authentication.

Voice recognition offers several benefits, such as the uniqueness of the human voice, security in access control, not requiring new hardware, and good compatibility (Thomas *et al*., 2020; Khotimah *et al*., 2020). Nevertheless, voice recognition is sensitive to background noise, harsh environments, playback spoofing, emotional states, voice changes over time, characteristics of the microphones used, accent differences, and quality of the communication channel during enrolment and authentication (Krčadinac *et al*., 2021; Cayir & Navruz, 2021).

2.6 Threat model

Adversaries, system administrators, and unscrupulous employees target mobile money systems to access mobile money subscribers' financial records since they know how they operate. These attacks can be passive or active or within the organisation (internal) or outside (external). Ali *et al*. (2020a) define the threat model as the various attacks, reasons for the attacks, the different locations within the system attackers can exploit to bypass the security, and the measures set up to control the attacks.

The attackers utilised the various points on mobile money systems to attack the mobile money subscribers and the system, as illustrated in Fig. 7.

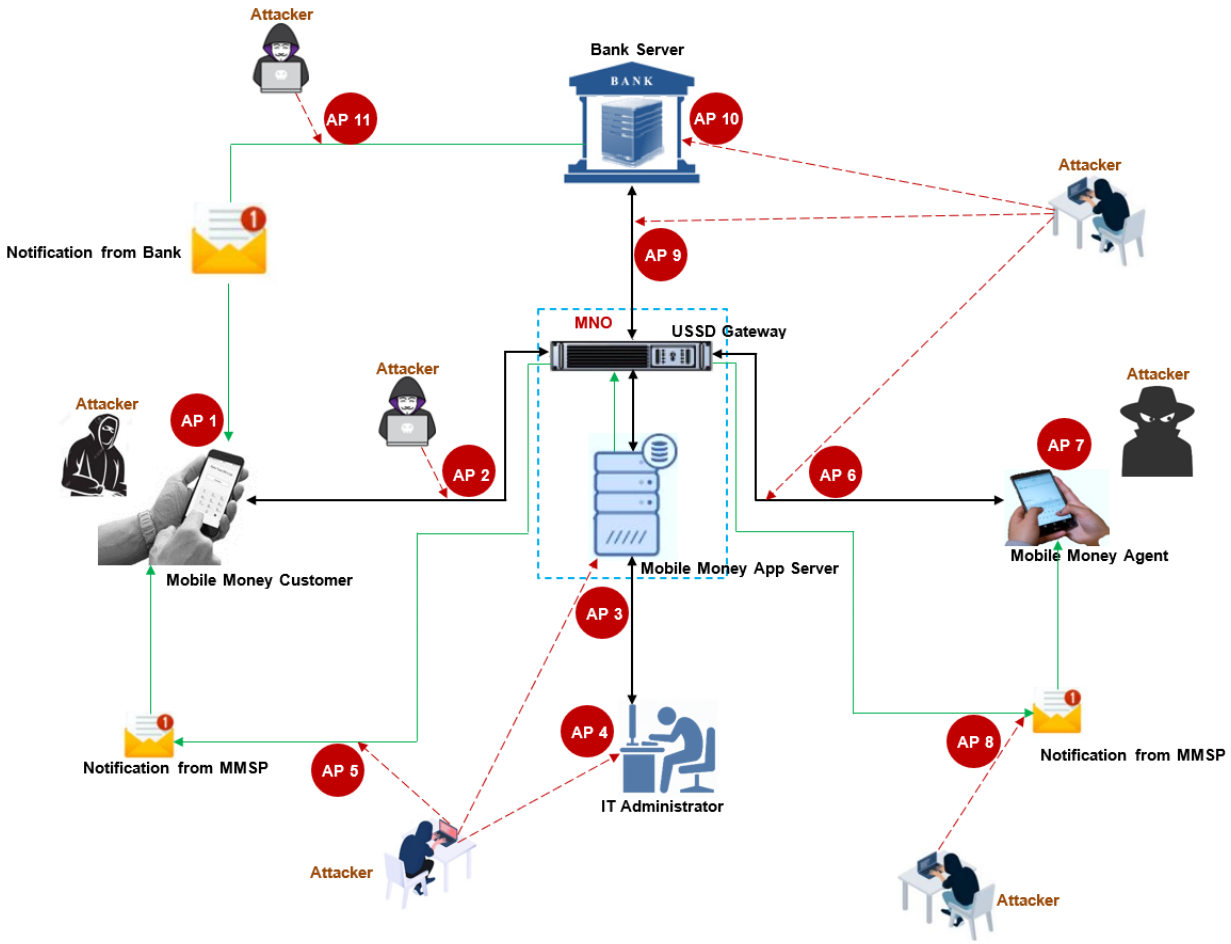


Figure 7: Illustrates the various attack points (AP) used by adversaries to attack mobile money systems (Ali *et al.*, 2020a)

The adversaries utilised AP 1 to attack mobile money customers; AP 2, AP 6, and AP 9 to attack the mobile money communication channels; and AP 3 to attack the mobile money application server. They also attack IT administrators from AP 4, mobile money agents from AP 7, bank servers from AP 10, and the communication channel for message notification from AP 5, AP 8, and AP 11 (Ali *et al.*, 2020a).

The various attacks against mobile money authentication schemes are grouped into five, i.e., attacks against privacy, authentication, confidentiality, integrity, and availability.

2.6.1 Attacks against privacy

Privacy is where an individual's right is not violated and interfered with by others (Makulilo, 2015). There are various forms of attacks against the privacy of mobile money subscribers and the system. Among these include: (a) illegally obtaining mobile money subscribers' PINs by attackers who use them to perform illegal transactions on behalf of the victims and access their financial records, which greatly invade the mobile money subscribers' privacy (Harris *et al.*, 2013; Kang, 2018; Ali *et al.*, 2020a), (b) disgruntled insiders illegally access and abuse mobile money

subscribers' sensitive financial data by generating a databank to gain access and control (Ali *et al*., 2020a; Ahmed *et al*., 2021), (c) during SIM card and mobile money registration, much information is collected about the mobile money subscribers, which MNOs use to generate a databank, thereby giving them free access and control without giving proper privacy protections, which can be abused by the corrupt insiders and government officials (Makulilo, 2015; Kang, 2018; Ahmed *et al*., 2021), (d) mobile money agents write the details of the mobile money customers in the transaction books issued by mobile money service providers during money withdrawal and deposit, which gives rise to worries about privacy (Makulilo, 2015; Ali *et al*., 2020a), (e) attackers use fake or genuine details of their victims, which they obtain through phishing, to swap the victim's SIM cards so that they have access to their mobile money accounts and can perform illegal transactions, which harms the privacy of the victims (Das *et al*., 2018; Mahlangu, 2018), (f) dishonest mobile money agents utilise the illiteracy of some mobile money customers by performing transactions on their behalf. They request the mobile money customers' PINs and later swap the victims' SIM cards, access their mobile money wallets, and perform unauthorised transactions, thus causing privacy issues (McKee *et al*., 2015; Martin, 2019; Ahmed *et al*., 2021).

2.6.2 Attacks against authentication

Adversaries apply authentication attacks to bypass the mobile money authentication process illegally. Ali *et al*. (2020b) define authentication attacks as crimes perpetrated by attackers by exploiting the weaknesses in mobile money authentication systems and the process of authenticating mobile money users to access the system illegally. Most of the mobile money authentication schemes in Uganda use either PIN and SIM cards or PIN and OTP, which are vulnerable to numerous attacks such as brute-force attacks, impersonation attacks, replay attacks, masquerade attacks, spoofing attacks, social engineering attacks, and Trojan horse attacks.

(i) Brute-force attacks

Ali *et al*. (2020a) define a brute-force attack as method adversaries, or cyber-criminals use to log into the victim's mobile money wallets by trying out or guessing several mobile money PINs until they are logged into the system. Most of the mobile money systems in East Africa use four to five-digit PINs to authenticate mobile money users, thus making them susceptible to a brute-force attack (Aloul *et al*., 2009; Rodrigues *et al*., 2016; Wang *et al*., 2021). Brute-force attacks on mobile money are simple and have a high success rate because of the simplicity of the PINs (Mtaho, 2015; Raphael, 2016; Castle *et al*., 2016; Reaves *et al*., 2017; Ali *et al*., 2020a). In

addition, mobile money agents and customers who use smartphones to carry out mobile money transactions have a high chance of their mobile money PINs being compromised because their hands leave a greasy residue and scratch on the smartphone's touchscreen that attackers can use to guess their mobile money PINs easily (Kunda & Chishimba, 2018).

(ii) Impersonation attacks

An impersonation attack is where attackers disguise themselves as employees of mobile money service providers and manipulate the mobile money agents and customers into transferring money into their accounts or sharing their mobile money PIN with the attackers. The adversaries can also disguise themselves as legitimate mobile money agents or customers to control and access mobile money systems and their services (Ali *et al*., 2020a). Mobile money subscribers have the habit of sharing their mobile money PINs among friends and family members, thus, making it easy for attackers to perform illegal transactions and even update the victims' PINs (Mtaho, 2015; Raphael, 2016; Buku & Mazer, 2017; Lonie, 2017; Das *et al*., 2018; Ali *et al*., 2020a; Ali *et al*., 2020b). Attackers use social engineering to lure mobile money agents and customers into revealing their confidential information. In addition, the attackers can also swap the SIM cards of their victims to control their mobile money wallets (Buku, 2017).

(iii) Replay attacks

A replay attack is where attackers sniff or eavesdrop on the mobile communication between the mobile money system and the mobile money subscriber or the bank and intercept the message, including the mobile money PIN and other financial records, deceitful delays, resends to the victim to misdirect them into doing what the attacker wants (Ali *et al*., 2020a). The attackers take advantage of the notification sent to the mobile money subscribers through SMS after performing transactions since it contains the subscriber's details. It should be noted that weak algorithms such as A5 are used to protect most of the SMS, and it becomes easy for adversaries with scanning software to capture, edit and resend them (Gilman & Joyce, 2012; Liu, 2013; Deshmukh & Naware, 2014). Likewise, adversaries can also use earlier stored and exchanged valid transaction packets and messages between mobile money subscribers and mobile money systems or the bank to perform replay attacks (Saxena & Payal, 2011; Deshmukh & Naware, 2014; Bojjagani & Sastry, 2017).

(iv) Masquerade attacks

A masquerade attack is where attackers use fake identities to swap the SIM card and obtain the PINs of their victims to gain unauthorised access to their mobile money wallets and perform illegal transactions or request money from the victims' relatives and friends (Ali *et al*., 2020a; Ali *et al*., 2020b). The attackers use social engineering techniques like phishing to obtain the credentials of the authorised mobile money subscribers to perform SIM swaps and PINs to access the mobile money wallets illegally. They take advantage of the laxity during SIM card and mobile money registration and weaknesses in the authentication system to gain unauthorised entry into the mobile money system, thus making them highly susceptible to masquerade attacks (Gilman & Joyce, 2012; Mudiri, 2012; Bosamia, 2017). Masquerade attacks result from identity theft and are inspired by data theft that people trigger within or outside the organisation.

(v) Spoofing attacks

A spoofing attack is where attackers pose as system administrators or authorised staff of a mobile money service provider to gain entrance to the system and send fraudulent messages to mobile money subscribers (Ali *et al*., 2020a; Ahmed *et al*., 2021). Adversaries use social engineering techniques to gather information about their victims. Furthermore, attackers utilise the weaknesses in mobile money systems to hack into systems (Reaves *et al*., 2017; Akomea-Frimpong *et al*., 2019). Building trust in mobile money systems is difficult for subscribers if the mobile money system and its services are not adequately secured (Sharma & Al-Muharrami, 2018).

(vi) Social engineering attacks

Kunda and Chishimba (2018) define social engineering attack as a form of attack where attackers manipulate mobile money subscribers to divulge sensitive personal information like mobile money PIN and other financial details through digital communication, which they use to control and fraudulently access the victims' mobile money wallets. Adversaries use different forms of social engineering like baiting, scareware, pretexting, phishing, and honey trap to trick their victims into revealing their mobile money PINs, bypass the mobile money authentication process, compromise victims' mobile money wallets, and circumvent fraud detection (Kunda & Chishimba, 2018). They take advantage of mobile money subscribers' trust and lack of awareness regarding online fraud (Buku, 2017; Salahdine & Kaabouch, 2019; Maina, 2019).

A phishing attack is the most common social engineering attack on mobile money. It is a type of social engineering attack where adversaries pose as staff of the mobile money service providers

by sending SMS to mobile money subscribers or calling them to obtain their PINs fraudulently or lure them into sending money to their accounts (Ali *et al*., 2020b; Alkhalil *et al*., 2021). While conducting the phishing attack, the adversaries follow steps like planning, phishing, infiltration, data collection & exploitation, and exfiltration to achieve their objective (Alabdan, 2020). The attackers create messages or voice calls as if they are coming from the mobile money service providers to persuade their victims into revealing their mobile money PINs (Buku, 2017; Castle *et al*., 2016; Bojjagani & Sastry, 2017; Wang *et al*., 2021). In mobile money, attackers use vishing, smishing, and malware-based phishing to launch the attacks (Deshmukh & Naware, 2014; Altwairqi *et al*., 2019; Jakhiya *et al*., 2020; Alkhalil *et al*., 2021). The impact of phishing attacks on mobile money systems, subscribers, banks, and the economy can lead to severe losses (Alkhalil *et al*., 2021).

(vii) Trojan horse attacks

A Trojan horse attack is where hackers or adversaries install malicious software into the victims' smartphones to monitor and steal their mobile money PINs or create back doors that attackers can use to bypass the authentication process (Ali *et al*., 2020a). Attackers utilise social engineering techniques to bait their victims into downloading and installing a trojan horse into their smartphones. When activated, they can monitor the victims' smartphones and mobile money accounts, steal victims' PINs, and create a backdoor for the attackers to infiltrate the mobile money system (Harris *et al*., 2013; Kunda & Chishimba, 2018; Nair *et al*., 2019; Wazid *et al*., 2019). The trojan horse also gives attackers the privilege to redirect mobile money subscribers to the attackers' network (Bosamia, 2017; Das *et al*., 2018).

2.6.3 Attacks against confidentiality

A confidentiality attack is where adversaries snoop on the communication between the mobile money systems and subscribers or banks to compromise confidential information like PINs and other transaction records (Ali *et al*., 2020a). Eavesdropping, guessing, and shoulder-surfing attacks are common attacks on mobile money confidentiality.

(i) Eavesdropping attacks

An eavesdropping attack is where adversaries secretly intercept the communication between mobile money subscribers and mobile money systems or banks without the knowledge of the trusted parties (Ali *et al*., 2020a). They use a network sniffer like Wireshark to seize all the vital data packets and network traffics in transit for later analysis (Mtaho, 2015). It is easy for attackers

to listen to communication channels that are not secured when data is transmitted in plaintext (Nyamtiga *et al*., 2013b; Talom & Tengeh, 2019). Attackers can capture mobile money subscribers' financial information during any stage of mobile money transactions. It can be carried out by insiders, external hackers, fake network base stations, and roaming technology (Baur-Yazbeck *et al*., 2019). They utilised the weaknesses in the encryption keys to snoop on the communication (Reaves *et al*., 2017).

(ii) Guessing attacks

A guessing attack is where attackers hunch the mobile money subscribers' PINs during the authentication (Ali *et al*., 2020a). Most mobile money schemes use PINs of four or five digits as one of the authentication factors, and these PINs are unmasked during their entry, thus making them guessable (Mtaho, 2015; Raphael, 2016; Reaves *et al*., 2017; Bani-Hani *et al*., 2019). Guessing attacks become easier and more successful only when the attacker has a clue about the victims' mobile money PIN, which helps minimise the PIN attempts (Wang *et al*., 2021).

(iii) Shoulder-surfing attacks

A shoulder-surfing attack is where the adversaries look over the shoulders of mobile money subscribers in crowded places when they are performing transactions to obtain their mobile money PINs (Ali *et al*., 2020a). The attackers can use hidden cameras to record the victims' process of entering their mobile money PINs (Salman *et al*., 2019; Wang *et al*., 2021). They find it easy to implement shoulder-surfing attacks since they cost almost nothing. The simplicity of mobile money PINs of four or five digits and entering them unmasked during mobile money authentication makes it easy for adversaries to see, record, and memorise. Once they get hold of the mobile money PINs, it becomes easy to perform fraudulent transactions (Lakshmi *et al*., 2017; Kunda & Chishimba, 2018; Jarecki *et al*., 2018; Ahmed *et al*., 2021).

2.6.4 Attacks against the integrity

An integrity attack is where adversaries use different methods to access and modify the subscribers' confidential and financial information stored in the mobile money systems (Ali *et al*., 2020a). Integrity attacks attempt to weaken subscribers' trust in the data or the system, and attackers illegally access mobile money systems to change the data stored in the system. The MITM attacks, salami attacks, and insider attacks are the different attacks that compromise data integrity in mobile money systems.

(i) Man-in-the-middle (MITM) attacks

A MITM attack is where attackers sit in the communication channels between the mobile money systems and subscribers or banks to intercept and manipulate their messages and send modified versions to the intended recipients (Sharma, 2019; Ali *et al*., 2020a). The adversaries control the conversation between the subscribers and the mobile money systems or banks without the victims' notice, thus, causing severe damage to the mobile money service providers, banks, and subscribers (Bojjagani & Sastry, 2017). After compromising the victims' credentials like mobile money PINs, the attackers can perform fraudulent transactions on their behalf (Liu, 2013; Mahajan *et al*., 2015; Castle *et al*., 2016; Reaves *et al*., 2017). Notification messages are usually sent to both the senders and recipients after mobile money transactions. Attackers can intercept such messages, edit their contents and forward them to the intended recipients since they are in plaintext (Mtaho, 2015; Phipps *et al*., 2018; Talom & Tengeh, 2019; Sharma, 2019). Similarly, attackers can utilise false base transceiver stations with the same mobile network codes as the mobile money service provider network to carry out MITM attacks (Deshmukh & Naware, 2014; Nair *et al*., 2019).

(ii) Salami attacks

A salami attack is where attackers or financial institution employees install a malicious program on the server hosting the applications to steal an unnoticeable sum of money from subscribers' wallet and transfer it into their accounts without the victims realising it (Ali *et al*., 2020a). The money is stolen in small increments by the malicious program that accrues a substantial amount over a long period without the victims detecting it, hence, incurring losses. Salami attacks can be internal or external. People who carry out internal attacks within the organisation know mobile money security systems and can easily install malware to steal little money from each subscriber (Altwairqi *et al*., 2019). At the same time, external attacks are carried out by attackers outside the organisation but steal money from the mobile money service providers. These attacks are conducted mainly by former employees and contractors who have inside knowledge about the organisation's security systems (Altwairqi *et al*., 2019). The installed malware changes the mobile money subscribers' financial records in systems by deducting the unnoticeable amount from their wallet, therefore, causing severe damage to the organisation and the subscribers (Kaur *et al*., 2015; Sadekin & Shaikh, 2016; Alhassan *et al*., 2018; Altwairqi *et al*., 2019; Ali *et al*., 2020a).

(iii) Insider attacks

An insider attack is where mobile money service providers' employees who know the mobile money security systems attack the system to steal subscribers' PINs or financial information for their gains (Ali *et al*., 2020a). They take advantage of being within the organisation to perform mobile money frauds, which has caused the service providers to lose a vast amount of money in billions of shillings (Trulioo, 2015; Musuva-Kigen *et al*., 2016). Disgruntled employees can access subscribers' records and steal money from their wallets (Gilman & Joyce, 2012; Trulioo, 2015). For example, Buku (2017) reported that in 2011, six employees of MTN Uganda stole $3.4 million from the company. Dornbierer (2020) stated that employees of MTN Uganda stole $2.4 billion over six months by taking advantage of the weaknesses in KYC processes and deficiencies in the IT systems. Furthermore, Morawczynski reported that the senior staff of MTN Uganda defrauded the company of $3.83 million and $900 000 (Morawczynski, 2015; Lonie, 2017). In Rwanda, the staff of Tigo manipulated the mobile money system and stole over $170 000 (Morawczynski, 2015).

2.6.5 Attacks against availability

Availability attack is where adversaries deny mobile money subscribers the opportunity to access mobile money services by making mobile money servers, bank servers, and mobile wallets unavailable (Ali *et al*., 2020a). The attackers use various attacks on mobile money systems that include:

(i) Denial-of-service (DoS) and distributed DoS (DDoS) attacks

A DoS is where adversaries overwhelm the servers hosting the mobile money systems and bank servers with fake traffic to deny legitimate mobile money subscribers from accessing mobile money services or networks (Ali *et al*., 2020a; Ahmed *et al*., 2021). At the same time, a distributed DoS attack is where the fake traffic that overwhelms the mobile money servers and bank servers come from various distributed sources, which is hard to stop (Ali *et al*., 2020a; Ahmed *et al*., 2021). The main aim of DoS and DDoS attacks is to cause the servers to crash and deny legitimate subscribers' real-time access to the mobile money systems, services, or networks, which causes the subscribers, mobile money service providers, and banks to lose money (Mutong'Wa & Khaemba, 2014; Raphael, 2016; Castle *et al*., 2016; Bosamia, 2017).

(ii) Mobile phone theft

When mobile money subscribers lose their mobile phones that have SIM cards with their mobile money wallets and in case, they find their way into the hands of adversaries who can switch them off (Castle *et al*., 2016; Reaves *et al*., 2017). The attackers who have access to such mobile phones can decide to change the mobile money PINs, making it difficult for legitimate subscribers to access their wallets (Trulioo, 2015; Bosamia, 2017; Jakhiya *et al*., 2020). Furthermore, stolen mobile phones may contain confidential information like mobile money PINs since many people prefer to store their PINs on their phones, and they may lose them (Tu *et al*., 2015). Figure 8 categorises the various threat models in the mobile money authentication schemes.

Figure 8: Categories of the numerous attacks in the mobile money authentication scheme (Ali *et al*., 2020a)

2.7 Countermeasures for mobile money authentication attacks

Mobile money service providers implement cryptographic and non-cryptographic techniques to prevent various attacks in mobile money authentication schemes (Ali *et al.,* 2020a). Figure 9 shows the cryptographic functions and personal identification to prevent mobile money authentication attacks.

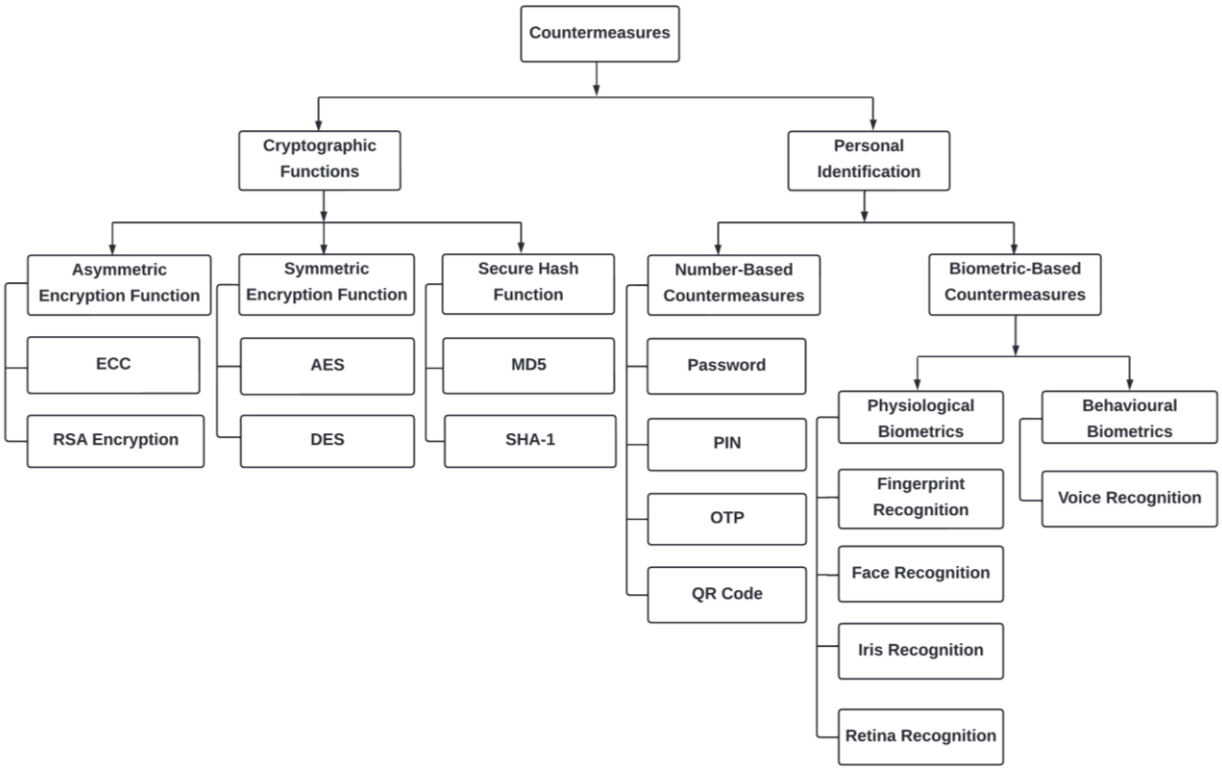


Figure 9: Shows the various cryptographic functions and personal identification used to prevent mobile money authentication attacks (Ali *et al*., 2020a)

2.7.1 Cryptographic functions

Cryptographic functions combine cryptographic algorithms and methods of operation (Barker & Barker, 2019). In mobile money schemes, asymmetric encryption, symmetric encryption, and secure hash functions are the most widely used cryptographic functions that help attain privacy, confidentiality, authenticity, integrity, non-repudiation, and availability as the security goals (Ali *et al*., 2020a).

(i) Asymmetric encryption function

Asymmetric encryption is public-key cryptography where two distinct keys (i.e., public and private) are used to encrypt and decrypt data (Hamza & Kumar, 2020). The public key encrypts data which can only be decrypted with the private key. The message recipient must keep the private key secret, while the sender can make the public key accessible to anyone (Hamza & Kumar, 2020). The most commonly used asymmetric encryption functions in mobile money schemes are elliptic curve cryptography (ECC) and RSA encryption (Ali *et al*., 2020a).

The ECC was proposed, designed, and developed by Neal Koblitz and Victor S. Miller in 1985 (Dua & Dutta, 2019). Keerthi and Surendiran (2017) define ECC as public-key cryptography that uses public and private keys to encrypt and decrypt messages based on an elliptic curve theory. It

is based on the algebraic structure of elliptic curves over finite fields (Fang *et al*., 2017; Dua & Dutta, 2019). The elliptic curve theory in ECC generates smaller and faster cryptographic keys, thus reducing the computational overhead, memory usage, and energy resource and providing higher security and efficiency (Fang *et al*., 2017; Shaikh *et al*., 2017; Dua & Dutta, 2019). According to Bojjagani and Sastry (2015), Ray *et al*. (2016), Shilpa and Panchami (2016), and Salim *et al*. (2020), ECC has been applied in mobile money, mobile banking, and mobile payments schemes to ensure data integrity, user authentication, and non-repudiation functions. It is also resilient to MITM attacks, DoS attacks, message modification, eavesdropping attacks, privacy attacks, masquerade attacks, Trojan horse attacks, guessing attacks, shoulder-surfing attacks, and insider attacks.

The RSA encryption is a public-key cryptographic algorithm proposed by Ron *et al.* (1977) in which data is encrypted using the public key but decrypted using the private keys (Wang *et al*., 2020; Ramtri & Patel, 2020; Pavani & Sriramya, 2021). It has the generation and distribution of keys, message encryption and decryption as the primary steps (Hassan *et al*., 2020; Al-Kadei *et al*., 2020). In RSA, the public key is created using two secret random prime numbers and an auxiliary value, making it difficult to crack because the key length varies (Alamsyah *et al*., 2020). Purnomo *et al*. (2016), Sharma and Bohra (2017), Hassan and Shukur (2021a), and Hassan and Shukur (2021b) used RSA in mobile banking and mobile payment schemes to provide information confidentiality, integrity, availability, and user anonymity, non-repudiation, and reliability. In addition, it is resistant to impersonation attacks and brute-force attacks. Much as the RSA algorithm offers some benefits, it is not widely used because it is slower in terms of encryption and decryption than ECC, and it requires more computational power, which reduces performance (Hamza & Kumar, 2020; Alamsyah *et al*., 2020).

(ii) Symmetric encryption function

Symmetric encryption is private key cryptography where a single secret shared key encrypts and decrypts information. The sender and recipient must use a secure channel to exchange the secret key. Data encryption standards (DES), triple-DES (3DES), and advanced encryption standards (AES) are the most widely used symmetric encryption in mobile money (Ali *et al*., 2020a).

According to Reyad *et al*. (2021), DES is a block cipher that encrypts 64-bit plaintext with a 56-bit key to generate the 64-bit ciphertext. It uses the same algorithm (Oukili & Bri, 2015; Reyad *et al*., 2021). Hu *et al*. (2012) and Mitra *et al*. (2017) used 3DES in mobile payment to provide

information confidentiality and prevent MITM attacks. They consume fewer resources and are less complicated to implement (Banani *et al*., 2021).

The United States National Institute of Standards and Technology (NIST) developed the AES in 2001 to overcome the problems encountered by the DES algorithm (Jindal *et al*., 2020; Khalifeh *et al*., 2020). The AES Algorithm is built on the network of substitution and permutation. It is a symmetric key block cipher that uses 128-bit, 192-bit, and 256-bit key lengths in AES-128, AES-192 & AES-256, respectively, to encrypt/decrypt a block of messages (Jindal *et al*., 2020; Khalifeh *et al*., 2020). The key size is highly dependent on the number of rounds, i.e., 10 rounds for 128-bit keys, 12 rounds for 192-bits keys, 14 rounds for 256-bit keys, and each of the rounds uses a different 128-bit round key (Kumar *et al*., 2020; Jindal *et al*., 2020). The substitution, transposition, and mixing of plaintext to ciphertext are the processing steps in a complete round (Jindal *et al*., 2020; Kumar *et al*., 2020). Rodrigues *et al*. (2016) and Zhang *et al*. (2017) implemented AES in mobile payment to thwart MITM attacks, replay attacks, and repudiation.

(iii) Secure hash function

According to Al-Odat *et al*. (2019), the United States NIST developed and standardised the secure hash function to ensure data integrity. A hash function is a mathematical and one-way function that takes a message of any size as input and compresses it to a fixed-size output known as a message digest or hash value (Al-Odat *et al*., 2019; Dubey *et al*., 2020). The main aim of the hash function is to compress big chunks of a message into smaller and fixed hash values (Dubey *et al*., 2020). Al-Odat *et al*. (2019) added that the hash function has properties such as: (a) fixed length message digest; (b) quick computation of the message digest; (c) impossible to generate a message with the same hash value; (d) infeasible for two messages to have the same message digest; and (e) any change to the message generates a new hash value different from the old message digest.

Merkle Damgård and Sponge structures are followed by hash algorithms where message-digest algorithm 5 (MD5), SHA-1, and SHA-2 are designed using the Merkle Damgård, and SHA-3 follow the Sponge structure. The 128-bit hash value is produced in MD5, while the 160-bit hash value is generated in SHA-1 (Al-Odat *et al*., 2019; Alawida *et al*., 2020). Companies like Google and Microsoft have stopped using the MD5 and SHA-1 because they are prone to collision attacks (Al-Odat *et al*., 2019; Maetouq & Daud, 2020; Alawida *et al*., 2020). The MD5 and SHA-1 are typical hash functions used in mobile money schemes.

Ron Rivest developed MD5 in 1994 as a more robust alternative to the MD4. The MD5 algorithm divides a message into a 512-bit input block where each block, when run through the mathematical function, produces a unique 128-bit fixed-length hash value (Wang & Li, 2015). It has been used widely in message authentication and checking message integrity (Wang & Li, 2015). Sharma and Bohra (2017) and Bosamia and Patel (2019) also used MD5 in mobile banking to improve information integrity and prevent privacy attacks.

The NIST published SHA-1 in 1995 as an alternative to SHA-0. SHA-1 takes a message of any length as input to produce a 160-bit fixed-length message digest which is a 40-digit hexadecimal number (Al-Odat *et al*., 2019). Coneland and Crespi (2013), Rodrigues *et al*. (2016), and Alhothaily *et al*. (2018) implemented SHA-1 in mobile money and mobile banking to provide security against privacy attacks, impersonation attacks, replay attacks, masquerade attacks, brute-force attacks, guessing attacks, insider attacks, and DoS attacks.

2.7.2 Personal identification

The personal identification countermeasures are further subdivided into number and biometric-based.

(i) Number-based countermeasures

The passwords, PINs, OTP, and QR codes offer number-based mobile money authentication solutions. For example, Mtaho (2015), Ugwu and Mesigo (2015), Singh and Jasmine (2015), Ombiro (2016), Rodrigues *et al*. (2016), Xu *et al*. (2016), Akoramurthy and Arthi (2017), Fan *et al*. (2017), Chetalam (2018), Sharma and Mathuria (2018), Bultel *et al*. (2018), Kasat and Bhadade (2018), Zadeh and Barati (2019), Ximenes *et al*. (2019), Islam *et al*. (2019), Iftikhar *et al*. (2019), Mega (2020), Osman and Nakanishi (2020), Hassan and Shukur (2021a), Hassan and Shukur (2021b), and Suwera (2021) used number-based counter steps such as passwords, PINs, OTP, and QR code in combination to ensure speed, convenience, accuracy, efficiency, non-repudiation, reliability, confidentiality, integrity, and security against authentication attacks.

(ii) Biometric-based countermeasures

The physiological and behavioural biometrics were used together with number-based countermeasures to improve the authentication security of mobile money systems. The fingerprint, face, iris, and retina recognitions are the common physiological biometrics used in mobile money authentication, while voice recognition is the only behavioural biometrics used.

Mtaho (2015), Islam (2015), Ray *et al*. (2016), Ahsan *et al*. (2016), Fan *et al*. (2017), Okpara and Bekaroo (2017), Sharma and Mathuria (2018), Salim *et al*. (2020), Hassan and Shukur (2021a), and Hassan and Shukur (2021b) used fingerprint recognition together with number-based. Zadeh and Barati (2019) and Ximenes *et al*. (2019) used face recognition and number-based. Islam *et al*. (2019), Mega (2020), and Osman and Nakanishi (2020) used iris recognition together with number-based. Ray *et al*. (2016) used retina recognition together with number-based. Ombiro (2016) and Chetalam (2018) used voice recognition alongside the number-based countermeasures to enhance efficiency, reliability, convenience, accuracy, dependability, and customer satisfaction. It also provides security against privacy attacks, identity theft, shoulder-surfing attacks, spoofing attacks, social engineering attacks, masquerade attacks, replay attacks, DoS attacks, phishing attacks, MITM attacks, impersonation attacks, and repudiation.

Other methods to prevent mobile money authentication attacks include: (a) enacting data privacy legislation and laws to avoid privacy attacks (Makulilo, 2015); (b) having policies, procedures and standards, using secure technologies, and training employees and customers about the dangers of social engineering attacks (Chinta *et al*., 2016; Conteh *et al*., 2016); (c) using anomaly-based intrusion detection systems to prevent adversaries from attacking the SMS (Hamandi *et al*., 2015); (d) using secure sockets layer (SSL), back-end analytics, filtering content, and mobile money subscriber training and sensitisation to thwart phishing attacks (Hamandi *et al*., 2015; Shahriar *et al*., 2015; Singh & Imphal, 2018); (e) using machine learning, profile matching, text mining, and honeypots to prevent phishing attacks (Aleroud & Zhou, 2017); (f) using malware detection and prevention techniques to address the issue of trojan horse attacks (Bosamia & Patel, 2019); (g) having well-defined user and security policies with apparent user privileges, constantly updating mobile money security schemes, alerting customers about transactions carried out through e-mail and SMS messages, and mobile money subscribers reporting unaware money deductions in their mobile wallets to prevent salami attacks (Alhassan *et al*., 2018); (h) using a hybrid intrusion detection system to avoid DDoS attacks (Cepheli *et al*., 2016); and (i) backing up data both online and offline, remotely wiping the phones or blocking them from being accessed by others to protect the data stored in them and enabling remote access to the GPS device tracking (Tu *et al*., 2015).

2.8 Studies related to mobile money and mobile banking systems

User authentication is paramount in mobile money schemes so that legitimate users can access the system and its services. Few studies focus on mobile money authentication algorithms, but there is a rich literature on mobile banking and mobile payments since they can be performed

using mobile money. Single-factor authentication, 2FA, and MFA are the authentication methods used to verify mobile money subscribers. This section mainly focuses on mobile money algorithms and schemes, mobile banking systems, and mobile payment systems.

2.8.1 Studies related to mobile money algorithms and schemes

Chetalam (2018) presented a secure MFA system for M-PESA transactions. During registration, the user's biodata, ID number, phone number, PIN, and voice biometrics are collected, checked, and saved in the system database. The user is authenticated using their device-specific ID, PIN, and voice biometrics. Once the credentials are matched with the stored copy, the user can perform transactions. The system is secure, accurate, convenient, efficient, and resilient against impersonation attacks. Nevertheless, it is prone to playback spoofing, MITM attacks, and voice biometrics vulnerabilities because the data are not encrypted while in transit and the voice biometrics are saved directly in the database without encryption.

In 2021, Suwera (2021) proposed a 2FA algorithm that uses PINs and unique codes to end the mobile money fraud menace. The user's biodata, valid ID number, phone number, and PIN are collected, verified, and saved in the system database during the enrolment phase. During the transaction phase, if the mobile money user wants to send money, they dial a USSD code, e.g., *180#, where a menu is displayed requesting them to enter the amount and the recipient's phone number. The system then generates a unique code using the sender's and recipient's phone numbers and the amount and then sends it to the money sender. The sender then dials *180# and enters the unique code to initiate the transfer. The unique code is compared with the stored copy, and if it is correct, the transaction is completed, and SMS messages are sent to both the sender and recipient confirming the transaction. Else, the transaction is cancelled. Note that the unique code is valid for only 5 minutes. The algorithm is simple and convenient but vulnerable to USSD technology vulnerabilities, shoulder-surfing attacks, SIM-swapping attacks, replay attacks, social engineering attacks, malware attacks, spoofing attacks, and interception of unique code messages.

Mega (2020) proposed a 2FA framework to improve mobile money authentication security in Tanzania. Enrolment, verification, and transaction are the three phases in the framework. The mobile money agent and customer's name, citizenship ID number, PIN, and iris biometrics are collected, confirmed, and stored in the system's database during the enrolment phase. The mobile money agent and customer begin the transaction by entering their PINs. Once the PIN is confirmed, the system requests the agent or customer to select the mobile money service they want to perform and enter their ID number. The ID number is matched with the copy in the

database. If it is correct, the system requests them to enter the amount. After the amount is entered, the system will request them to scan their iris for final verification. The captured iris image is matched with the stored template, and if it is verified, the transaction is accepted successfully. The proposed scheme is secure and convenient, thus preventing illegal access. Despite the benefits offered by the framework, it is vulnerable to PIN challenges, and iris recognition is affected by abnormalities in the iris patterns due to diseases. It may also be challenging to acquire a high-quality iris image from a distance due to the poor quality of the camera used, which affects the recognition.

Osman and Nakanishi (2020) designed a high-correctness 2FA system that uses a unique identification number and iris biometrics for mobile money. The user biodata, unique identification number, and iris biometrics are captured and saved in the database for authentication during enrolment. The user logs into the system using the unique identification number and iris biometric during the verification process. When the system verifies the unique identification number and iris biometrics, the user is provided with a menu to perform a transaction(s). The designed system has high security, robustness, reliability, and accuracy, are immutable over time, and ensures non-repudiation. Nevertheless, the developed system encounters many limitations, like a high non-match error rate because of age and the difficulty of acquiring a good quality iris image from a long distance.

Islam *et al*. (2019) presented a secure 2FA algorithm that uses PIN and iris biometrics for mobile money transfer among SMEs in Bangladesh. Two algorithms were designed for user registration and transaction (i.e., sending money). The user registration involves capturing the biodata, phone number, national identity (NID) number, and iris biometrics which are then sent to the national identification database. When the data is verified, the user is requested to set their PIN for the account. During a transaction, i.e., sending money, the user first logs in to the system using their PIN. After successful login, the system requests the user to enter the recipient's name and account number. The account number is sent to the national identification database for verification. Once the account number is verified, the system requests the user to enter the amount of money to be sent and then scan their iris for verification. The system then sends the user's NID number and the iris photo to the national database for confirmation. After successful verification, the money is sent to the recipient, and an acknowledgement message is sent to the user. The transaction details (i.e., sender's and recipient's account number, transaction time, and amount) will be stored in the system. The proposed algorithm is secure, reliable, accurate, and convenient. It also ensures

non-repudiation of money transactions and is resilient to impersonation attacks. However, the algorithm faces PIN and iris biometric challenges, thus hindering its performance.

Mtaho (2015) proposed a 2FA model to boost mobile money security. The user's biodata, phone number, PIN, and biometric fingerprint are captured and saved in the MNO server during the enrolment phase. The user dials a USSD code like *150*00# during the authentication phase, where a login interface is displayed. The user is requested to enter their PIN for matching, and if it is correct, the user is requested to scan their fingerprint using the fingerprint recognition software on the smartphone. If the fingerprint is verified, the system then displays a menu containing the mobile money services; else, the user is denied access. The model is convenient, prevents unauthorised entrance into mobile money systems, and improves security. Still, it is vulnerable to spoofing attacks, replay attacks, trojan horse attacks, and intrusion attacks.

Mtaho (2015) discussed the popular USSD-based scheme for authenticating mobile money users. The system involves registration and transaction phases. The user's biodata, phone number, ID number, and PIN are captured, checked, and saved in the MNO's database. The transaction phase involves the user dialling a USSD code and selecting the service they want to perform from the menu. The system requests the user to enter their four or five-digit PIN. The system then verifies the PIN, and if it matches, the user is granted the service; else, required to try again. The system is simple, convenient, and user-friendly. However, it is prone to USSD technology vulnerabilities, malware attacks, insider attacks, and masquerade attacks. Also, it is vulnerable to shoulder-surfing attacks, guessing attacks, identity theft, snooping attacks, replay attacks, MITM attacks, social engineering attacks, brute-force attacks, and PIN challenges.

2.8.2 Studies related to mobile banking systems

In 2019, Zadeh and Barati (2019) suggested a hybrid authentication scheme that uses a PIN, OTP, and face recognition to improve mobile banking security. The bank captures the user's personal information during the registration phase, including the phone number, face photo, and PIN. The user must log in using their six-digit PIN and face image to perform a transaction. Once the PIN and face photo is verified, the system displays a menu where the user is requested to choose a service to perform. After selecting the service (e.g., deposit money, pay bills or check balance) and entering the required information, the system will generate OTP and send it to the user for verification. When the user enters the OTP and is verified, the service is performed successfully. The proposed scheme is fast, convenient, secure, and reliable. However, it is vulnerable to

malware attacks, insider attacks, masquerade attacks, identity theft, snooping attacks, replay attacks, MITM attacks, and brute-force attacks.

Sharma and Mathuria (2018) proposed a mobile banking transaction using a username & password, and fingerprint. During authentication, the user login using the username and password and then scans the fingerprint for verification. After successful authentication, a menu screen appears that allows the user to perform the transaction. When they select a service like paying a bill, the user is again requested to authenticate themself by using a fingerprint. The fingerprint is matched with the stored template, and if it is verified, the transaction is completed successfully. The system is reliable because it prevents impersonation and shoulder-surfing attacks. Nevertheless, it is vulnerable to spoofing attacks, spyware attacks, eavesdropping attacks, password-guessing attacks, trojan horse attacks, and fingerprint template reconstruction & modification. Also, passwords are easily cracked, stolen, forgotten, and weak.

Ombiro (2016) designed a mobile-based authentication scheme that uses a PIN, OTP, or mobile flash call for mobile banking. The user's phone number and four-digit PIN are sent to the server during the registration phase. The system then requests the user to choose PIN and OTP or PIN and a phone call or OTP and phone call as the default authentication type. Then a user account is created after verifying the phone number, PIN, and device ID. If the user chooses PIN and OTP as the default authentication type, during the authentication phase, the system will request them to enter their PIN and the OTP, which is then verified. When the PIN and OTP match, the user is authenticated, and a transaction menu is displayed; else, advised to try again. The scheme is efficient, convenient, and resilient to identity theft and dictionary attacks. Nevertheless, it is liable to MITM attacks and sniffing attacks.

2.8.3 Studies related to mobile payment systems

Hassan and Shukur (2021a) suggested a framework for improving the security of electronic payment systems that use passwords, biometric fingerprints, and OTP. During registration, the user's biodata, password, and biometric fingerprint are collected, confirmed, and saved in the system's database. During the authentication phase, the user enters their password and scans the biometric fingerprint. The password and fingerprint are matched, and if they are correct, the user is authenticated and allowed to perform transactions; else, denied access. If the user wants to send money in the transaction phase, they must enter the amount and scan their biometric fingerprint for verification. The fingerprint is matched with the stored template, and if it is proven, OTP is created and forwarded to the user's phone number for a second verification. The user enters the

OTP, which is then compared with the stored copy, and if it matches, the money is sent to the recipient, and the successful transaction message is displayed; otherwise, the transaction is terminated. The framework is reliable and easy to use. It is also resilient to attacks like shoulder-surfing, password guessing, phishing, brute-force, dictionary, and password-based attacks. However, they are prone to MITM attacks, spoofing attacks, insider attacks, identity theft, and malware attacks.

Hassan and Shukur (2021b) proposed a secure user authentication scheme using passwords, biometric fingerprints, international mobile equipment identifier (IMEI), and OTP for e-wallet (Zamwallet). The user's phone number, password, IMEI, and fingerprint are captured, checked, and saved in the real-time databases of the Firebase server during the registration phase. The system then generates OTP and forwards it to the user for the registration completion process by entering it. The OTP is then matched with the copy stored, and if verified, the user is registered successfully, and the user information is saved in the database. The user logs in using a password and biometric fingerprint during the authentication phase. If they match, OTP is generated and forwarded to the user for final verification. The user must key in the received OTP, and if it is verified, they are successfully authenticated and can perform transactions such as top-up money. If the user wants to top-up money, they must enter the amount and the bank account. The system will check whether the bank account has enough money and is valid. If correct, the system will request the user to confirm the transaction by entering their password and biometric fingerprint. If they match, OTP is generated and forwarded to the user to complete the confirmation process by entering it. Once the OTP is verified, a successful top-up message is displayed. The proposed Zamwallet is secure against various attacks, stable, consistent, user-friendly, and cost-effective since no extra device is required to authenticate the user's fingerprint. But, are susceptible to MITM attacks, spoofing attacks, insider attacks, identity theft, and malware attacks.

Ximenes *et al*. (2019) suggested a secure authentication scheme using a face biometric and QR code for online payment. During the registration, the user's biodata and photos are captured. The images are sent to the Azure face API to identify the face's data on the picture. A user ID is generated for the user based on the face data. The face data and user ID are encrypted using AES-256 and sent to the bio database in the cloud server. The system then generates a QR code based on face data and user ID. During the transaction phase, the user scans the user QR code, which is then decrypted to generate the user ID and take a face photo to get the face data. The user then uploads the face image for verification. If the face image matches the face template stored in the bio database, the transaction is verified; else rejected. All registration and transaction data are

communicated securely using the SSL. The proposed system is fast and has a high accuracy rate. However, it slows performance, has weak cipher, and it takes a long time to encrypt and decrypt data which hinders efficient communication.

Rodrigues *et al*. (2016) presented a unique 2FA system using a QR code for Android smartphone users. The user's biodata, e-mail address, username & password, and IMEI number are collected, checked, and stored in the system's database during the enrolment phase. Then, for verification, the user login using their username and password. When the username and password are verified, the system requests the user to scan the QR code. After scanning the QR code, a 4-digit code (OTP) is generated and forwarded to the user to finish the authentication process. The user then enters the OTP, which is verified by the system. If it is correct, the user is authenticated; else rejected. It should be noted that the authentication factors are secured using AES and SHA-1, thus making them secure against attacks. Nevertheless, it is prone to collision attacks, has slow performance, weak cipher, and it takes a long to encrypt and decrypt data which affects efficient communication. Table 2 summarizes the strengths and weaknesses of each of the studies related to mobile money, mobile banking, and mobile payment systems.

Table 2: Summary of the strengths and weaknesses of each of the studies related to mobile money, mobile banking, and mobile payment systems

S/No	Reference	Technique	Strengths	Weaknesses
1.	Chetalam (2018)	A secure MFA system that uses device-specific ID, PIN, and voice biometrics	Secure, accurate, convenient, efficient, and resilient against impersonation attacks	Vulnerable to playback spoofing, MITM attacks, voice biometrics vulnerabilities
2.	Suwera (2021)	2FA algorithm that uses PINs & unique codes	Simple, convenient	Prone to replay attacks, USSD technology vulnerabilities, shoulder-surfing attacks, SIM-swapping attacks, replay attacks, malware attacks, spoofing attacks, social engineering attacks, interception of unique code messages
3.	Mega (2020)	2FA that uses citizenship ID	Secure, convenient	Vulnerable to PIN challenges, difficult to

S/No	Reference	Technique	Strengths	Weaknesses
		number, PIN, & iris biometrics		acquire a high-quality iris image from a distance due to the poor-quality camera
4.	Osman and Nakanishi (2020)	High-correctness 2FA system that uses a unique identification number and iris biometrics	High security, robustness, reliability, accuracy, immutable over time, and ensures non-repudiation	High non-match error rate, the difficulty of acquiring a good quality iris image from a long distance
5.	Islam *et al*. (2019)	A secure 2FA algorithm that uses PIN and iris biometrics	Secure, reliable, accurate, convenient, non-repudiation, resilient to impersonation attacks	Faces PIN and iris biometric challenges
6.	Mtaho (2015)	2FA model that uses PIN and biometric fingerprint	Convenient, secure, prevent unauthorised entrance into mobile money systems	Vulnerable to spoofing attacks, replay attacks, trojan horse attacks, and intrusion attacks
7.	Mtaho (2015)	USSD-based scheme	Simple, convenient, user-friendly	Malware attacks, insider attacks, USSD technology vulnerabilities, masquerade attacks, shoulder-surfing attacks, identity theft, snooping attacks, replay attacks, MITM attacks, social engineering attacks, brute-force attacks
8.	Zadeh and Barati (2019)	Uses a PIN, OTP, and face recognition	Fast, convenient, secure, reliable	Susceptible to malware attacks, insider attacks, masquerade attacks, identity theft, snooping attacks, replay attacks, MITM attacks, brute-force attacks

S/No	Reference	Technique	Strengths	Weaknesses
9.	Sharma and Mathuria (2018)	Uses username password, and fingerprint	Prevents impersonation, shoulder-surfing attacks	Vulnerable to spoofing attacks, spyware attacks, eavesdropping attacks, password-guessing attacks, trojan horse attacks, template reconstruction and modification, passwords are easily cracked, stolen, forgotten, and weak
10.	Ombiro (2016)	Uses a PIN, OTP, or mobile flash call	Efficient, convenient, and resilient to identity theft and dictionary attacks	Liable to MITM attacks and sniffing attacks
11.	Hassan and Shukur (2021a)	Uses passwords, biometric fingerprints, and OTP	Resilient to shoulder-surfing attacks, password-guessing attacks, phishing attacks, brute-force attacks, dictionary attacks, and password-based attacks	Prone to MITM attacks, spoofing attacks, insider attacks, identity theft, and malware attacks
12.	Hassan and Shukur (2021b)	Uses passwords, biometric fingerprints, IMEI, and OTP	Stable, consistent, user-friendly, and cost-effective	Susceptible to MITM attacks, spoofing attacks, insider attacks, identity theft, and malware attacks
13.	Ximenes *et al*. (2019)	Uses face biometric and QR code	Fast and accuracy rate	Slow performance, weak cipher, takes a long time to encrypt and decrypt data which hinders efficient communication

To address the above-mentioned challenges/weaknesses, a secure MFA algorithm for mobile money applications was proposed where the mobile money subscribers are authenticated and authorized by multiple factors such as PIN, OTP, biometric fingerprint, and QR code. The security of the PINs and OTPs is ensured by SHA-256, subscribers' biometric fingerprint by FIDO, where

RSA encryption protects public/private key pair and fingerprint template, and Fernet encryption secures the QR codes, the confidential financial information in the database, and all the data before transmission to the remote databases, which guaranteed data confidentiality. In addition, the QR code contains the encrypted universally unique identifier (UUID) of the mobile money agent which is encoded to ensure the agent's privacy. The proposed secure MFA algorithm addressed all the challenges encountered by other algorithms that implemented 2FA schemes and also the scheme proposed by Chetalam (2018) that implemented a secure MFA system that uses device-specific ID, PIN, and voice biometrics.

2.9 The security technologies

2.9.1 Secure hash algorithm-256 (SHA-256)

Secure hash algorithm-256 (SHA-256) is the most widely used and deployed cryptographic hash function under the SHA-2 banner because of its safety. Bouam *et al*. (2021), Wang *et al*. (2021), Ali *et al*. (2021), and Zhang *et al*. (2021) define SHA-256 as a one-way and collision-resistant cryptographic hash function designed by the National Security Agency (NSA) in 2001 and standardised by the NIST to overcome the weaknesses created by SHA-1. The SHA-256 is one of the six hash functions that belong to the family of SHA-2. It takes messages with arbitrary lengths and compresses them to produce a 256-bit fixed-length hash value which is in a 64-digit hexadecimal number (Tran *et al*., 2021; Bensalem *et al*., 2021; Bouam *et al*., 2021; Nakamura *et al*., 2021; Phan *et al*., 2021; Patra & Patra, 2021).

Preprocessing and hash computation are the two stages in the SHA-256 algorithm. During preprocessing, the original messages are padded and expanded for round computation. Here, the 256-bit hash value is calculated from the 512 bits input message by dividing it into several 512-bit data blocks and processing using the compression function one at a time. When the last block is less than 512 bits, padding is added by appending bits until it is 512-bit (Wu *et al*., 2020; Bouam *et al*., 2021). In hash computation, a hash value is obtained by repetitive generation of the message schedule, functions, constants, and word operations. A message schedule is created from the padded message by the hash computation, and the hash computation generates a hash value used to establish the message digest (Suhaili & Watanabe, 2017; Wu *et al*., 2020; Phan *et al*., 2021; Tran *et al*., 2021).

Because of the increased security, the SHA-256 algorithm is being widely implemented because of its reliability. The SHA-256 is broadly used in various applications like blockchain, information

encryption, transport layer security, cryptocurrencies, digital signatures, IoT micro-devices, wireless local area networks, message authentication codes, secure electronic transactions, IP security, and high-performance systems because of its easy implementation, speed, and good portability (Qiuyun *et al*., 2017; Chen & Li, 2020; Wu *et al*., 2020; Wang *et al*., 2021; Phan *et al*., 2021; Tran *et al*., 2021; Bensalem *et al*., 2021). It is collision-resistant and impossible to construct the input message from the hash value (Wu *et al*., 2020; Phan *et al*., 2021; Patra & Patra, 2021). In addition, it guarantees data integrity, confidentiality, and authenticity and is more resilient to attacks (Qiuyun *et al*., 2017; Sghaier *et al*., 2017; Al-Odat *et al*., 2019; Martino & Cilardo, 2019; Kammoun *et al*., 2020; Zhang *et al*., 2021).

2.9.2 Fast Identity Online (FIDO)

According to Ali *et al.* (2021), Fast Identity Online (FIDO) is a platform-independent technology that enhances authentication security by applying public-key cryptography. The FIDO has been applied in many modern solutions due to the increasing demand for security and usability. A non-profit organisation known as FIDO Alliance developed FIDO to provide strong authentication in web and native applications by storing biometrics data and other personal identification locally on the user's smartphones for security purposes. In December 2014, the Alliance proposed FIDO specifications to permit strong authentication through MFA and public-key cryptography (Hu & Zhang, 2016; Panos *et al*., 2017; Chadwick *et al*., 2019; Klieme *et al*., 2020; Feng *et al*., 2021). The FIDO protocols are implemented in many applications, including T-Mobile, Facebook, Revolut, Google, Twitter, NokNok, Bank of China, Dropbox, Apple, Cloudflare, Bank of America, Github, Paypal, Yahoo Japan, National Health Service (NHS) (Klieme *et al*., 2020). The FIDO architecture is also implemented in ATM withdrawals, single sign-on, and money transfers (Ali *et al*., 2021). In addition, it is also supported by Android and Windows operating systems, Google Chrome, Microsoft Edge, Mozilla Firefox, Samsung, and Huawei (Guo *et al*., 2020). Universal authentication framework (UAF), universal second factor (U2F), and FIDO2 are the three sets of FIDO specifications published by the FIDO Alliance.

The three main actors participating in FIDO registration and authentication are the FIDO relying party (i.e., FIDO server, front-end application), authenticator, and client. The FIDO-relying party is accountable for storing the user's credentials and public data. The FIDO authenticator is accountable for generating the public/private key pair, holding the private key securely, confirming the user's presence, and verifying the user's identity using biometric features. The

FIDO client acts as a medium between the relying party and the authenticator and provides an interface for user configuration (Klieme *et al*., 2020; Kim *et al*., 2020).

Registration and authentication are the two phases in the operation of FIDO. The FIDO registration phase begins when the user is required to choose a FIDO authenticator (e.g., smartphone) that is used to sign on, and it should match the online service acceptance policy. The user then unlocks the FIDO authenticator by scanning their fingerprint using the smartphone scanner. The user's smartphone will create a new public/private key pair unique for the online service, user account, and smartphone for authentication. The public key is sent to the online service linked with the user's account. The private key and biometric templates safely remain on the smartphone. During the authentication phase, the FIDO server challenges the user to log in using their previously registered smartphone that matches the online service acceptance policy by scanning their biometric fingerprint to verify their identity. The smartphone then uses the user's account identifier provided by the service to choose the correct private key and sign the online service challenge to confirm that the smartphone has the private key. The smartphone sends the signed challenge to the online service for verification using the stored public key, and the user is successfully authenticated (Kim *et al*., 2018; Ali *et al*., 2021; Guo *et al*., 2020; Klieme *et al*., 2020). It should be noted that the public/private key pair, fingerprint template, and communications are encrypted throughout the registration and authentication phases using public-key cryptography (RSA). The FIDO protocol uses asymmetric cryptography to create a secure communication channel for the server and the client (Klieme *et al*., 2020).

Implementing FIDO in applications helps to ensure secure authentication and protection of users' privacy and access credentials (Kim *et al*., 2020). The FIDO Authentication is unique, convenient, and scalable, and improves user experience and performance (Han *et al*., 2018; Shin, 2018; Canales, 2020). They are also resilient to phishing attacks, sniffing attacks, identity theft, replay attacks, and MITM attacks (Kim *et al*., 2017; Klieme *et al*., 2020; Feng *et al*., 2021).

2.9.3 Fernet encryption

Fernet encryption is private-key cryptography that uses a single secret shared key to encrypt and decrypt messages, and without the key, the message cannot be read or manipulated (Tanseer *et al*., 2020; Dijesh *et al*., 2020; Chaithra & Ajay, 2020; Ali *et al*., 2021). It uses multiple cryptographic primitives, i.e., AES-128-bit symmetric encryption in cipher block chaining (CBC) mode with public-key cryptography standards 7 (PKCS7) padding and a hash-based message authentication code (HMAC) using SHA-256 for authentication (Dijesh *et al*., 2020; Ayala, 2021;

Nawal *et al*., 2021). Python was used to implement Fernet because it has libraries like *cryptography.fernet*, and *cryptography.hazmat*, which facilitates the generation of keys, encryption & decryption using the encrypt and decrypt methods and HMAC to protect data integrity.

Fernet ensures the secure generation of the key, key rotation through MultiFernet, random allocation of the safe "salt" value for encryption, timestamping the ciphertext, and signing the message to ascertain any endeavours to modify it (Agarwal *et al*., 2019; Bornare *et al*., 2020; Nawal *et al*., 2021). The Fernet algorithm has encryption and decryption facilities (Dijesh *et al*., 2020). During encryption, a message in plaintext is encrypted by passing it through the Fernet algorithm that rotates the keys generated through MultiFernet. The encryption process involves generating the key, assigning the key value to the selected variable, and converting the plaintext to ciphertext. Decrypting the ciphertext consists of an inverse function to produce a plaintext displayed as a string value (Pronika & Tyagi, 2021). The Fernet was used to provide improved security and privacy. It also ensured user authenticity, data confidentiality, integrity, and non-repudiation (Chang *et al*., 2015; Dijesh *et al*., 2020; Ali *et al*., 2021).

2.10 Theoretical framework

Organisations and researchers use innovative approaches, like theories, to support information systems (IS)/IT studies. According to Ngulube *et al*. (2015) and Ravitch and Riggan (2016), a theoretical framework helps to evaluate the research problem and research question and provides a background to support the study. It guides a research study since it comprises concepts, definitions, assumptions and references to a pertinent topic or existing theory, and its selection depends on their appropriateness and ease of implementation (Walliman, 2015; Ravitch & Riggan, 2016). Two theories were reviewed for this study, and they include; IS design theory (Walls *et al*., 1992) and the soft systems theory (Checkland, 1994). The theories were used to design the algorithm and develop the prototypes of native G-MoMo applications. The theories were considered vital since they support the generation of knowledge in societies.

2.10.1 Information systems design theory

The IS design theory was developed to solve the problems encountered by the specialised classes of IS designs by practically implementing guidelines and principles to develop an artefact that follows (Walls *et al*., 1992; Gregor, 2002). Walls *et al*. (1992) define IS design theory as the theory that combines multiple theories into a system design to produce an artefact. The main aim

of the IS design theory is to enable software developers to define and understand the research problem, provide guidelines and principles, explain relationships between components and integrate them to formulate systems, design an artefact, and test the artefact (Walls *et al*., 1992; Gregor, 2002; Venable, 2006; Gregor & Jones, 2007; Kuechler & Vaishnavi, 2012; Gregor & Hevner, 2013). It has a product and development process as its main components and is divided into design and product (Walls *et al*., 1992; Janiesch *et al*., 2020). The IS design theory provides knowledge to solve the problem by designing an artefact, provides development reliability and credibility, and provides principles that guide the artefact's design and empirical testing (Markus *et al*., 2002; Gregor, 2006; Haj-Bolouri *et al*., 2016).

2.10.2 Soft systems theory

Peter Checkland formulated the soft systems theory in 1969 to solve consensual structure problems using many participation strategies and make decisions about the vaguely complicated human activity systems (Checkland & Scholes, 1999; Balram & Dragicevic, 2006). Its main aim is to provide a framework for solving poor and ill-structured problems (Checkland, 2000). Soft systems theory presents the problem state using multiple views, expresses them using rich presentations, compares the conceptual models to real-world circumstances, and provides suggestions for improving the studied problem (Checkland, 1994; Checkland, 2000). The problems are grouped into 'hard' or 'soft' based on the distinctive characteristics that will require different methods to solve them. Seven iterative stages are used to carry out the soft system's design, i.e., (a) investigating the difficulty of the problem situation and decomposing them into manageable abstractions; (b) collecting the relevant data about the problem to accumulate the rich baseline knowledge on which judgments and decisions will depend; (c) encouraging participants to explore the problem situation using new methods to generate relevant systems or scenarios; (d) creating a logical model of what needs to be done to satisfy the pertinent system; (e) using structured debates to differentiate between the conceptual model and the rich baseline knowledge to determine and resolve differences; (f) elaborating and agreeing on the changes; and (g) implementing them (Balram & Dragicevic, 2006).

2.11 Conclusion

In summary, the research introduced the concept of authentication, the types of authentication mechanisms, mobile money system architecture, authentication factors used in mobile money authentication, various points of attacks on mobile money systems, identified the attacks on mobile money authentication, countermeasures to the various mobile money authentication

attacks, the security technologies, and theoretical framework for the study. Most mobile money authentication schemes use PINs and SIM or PIN and OTP to authenticate mobile money subscribers. The PINs and OTP are entered when unmasked and in plaintext, making it easy for adversaries to intercept them. Once they have access to the authentication factors, it becomes easy to access the victim's mobile wallets and perform fraudulent transactions.

Nevertheless, numerous methods were deliberated, such as the use of cryptographic functions like asymmetric encryption (ECC and RSA), symmetric encryption (DES, 3DES, and AES), and hash functions (MD5 and SHA-1) to protect the authentication factors and the records in the database. The use of personal identification like number-based (password, PIN, OTP, QR code) and biometric-based (fingerprint, face, iris, retina, and voice recognition) enhances mobile money authentication and prevents attacks. It was found that the database records and authentication factors were not securely protected, hence giving rise to authentication attacks. The establishment of which authentication factors to be used depends on their operation and how to protect them. This study, therefore, addressed the weaknesses related to privacy, authentication, confidentiality, integrity, non-repudiation, and user anonymity.

With the identified numerous threat models, the research, therefore, proposed the development of a secure MFA algorithm for mobile money applications to solve authentication attacks. The proposed algorithm authenticates mobile money subscribers by combining PIN, OTP, and biometric fingerprints. The customers' biometric fingerprints and the agents' QR codes also authorise money withdrawal. The authentication factors, i.e., PIN and OTP, are protected by SHA-256, the subscribers' biometric fingerprints by FIDO, where the RSA encryption secures the public/private key pair and the fingerprint templates. The QR codes, confidential financial information in the databases, and all the data before transmission to the remote databases are secured using Fernet encryption. Three prototypes of the native G-MoMo applications were developed to justify that the algorithm is feasible and offers outstanding security. Once subscribers are registered with the application, their phone numbers are sent to the Twilio API to deliver the 5-digit OTP required during authentication. The OTP is valid for only 60 seconds and can be tracked by Twilio API. With this novel approach, mobile money applications are secure from various authentication attacks.

CHAPTER THREE

MATERIALS AND METHODS

3.1 Introduction

The essential components of the study, such as the research philosophies, research design, population, sample size, sampling technique, data collection instruments, data analysis, validity and reliability, development approach, materials and tools, the methods used to evaluate the algorithm and the prototypes of the native G-MoMo applications, and ethical considerations, are presented in this chapter.

3.2 Research philosophies

Saunders *et al*. (2007) define research philosophy as developing research assumptions, knowledge, and nature. However, Žukauskas *et al*. (2018) define scientific research philosophy as the method that allows scientists to create ideas into knowledge in the research context. It is a philosophy that offers the process of conducting and implementing research in a specific direction and defines the scientific research philosophy (Gliner & Morgan, 2000; Žukauskas *et al*., 2018). The scientific research paradigm has a broad structure, including perception, beliefs, and awareness of various theories and practices that can be used to conduct scientific research (Cohen *et al*., 2007; Žukauskas *et al*., 2018). It comprises ontology, epistemology, methodology, and methods (Žukauskas *et al*., 2018).

This study adopts a realist ontology within the positivist and pragmatic research paradigm that tries to find verifiable artefacts, i.e., mobile money schemes, that are definable, assessable and can be developed. Ontology is the philosophical study that deals with existence, the nature of reality, and truth (Žukauskas *et al*., 2018; Kaushik & Walsh, 2019). The research focused on mobile money algorithms and schemes that exist in reality. The main research philosophies in this study are positivist and pragmatic research philosophies.

3.2.1 Positivist research philosophy

Positivist research philosophy relies on scientific evidence from experiments, and statistical, and mathematical computations that exhibit the true nature of the phenomenon being studied by utilising the quantitative data that results in statistical analyses (Morgan, 2014; Ryan, 2018). They are typically carried out on large data sets to objectively understand the phenomenon and verify a

hypothesis stated quantitatively, where functional relationships are drawn from independent and dependent variables that predict and control the phenomenon (Ryan, 2018; Žukauskas *et al*., 2018). The positivist paradigm assumes a single tangible existence of a reality that does not depend on the researcher's interest. Positivist research includes realist ontology and objective epistemology and follows the empirical experimentation method. The Positivist ontology paradigm was used to analyse the different mobile money algorithms and schemes independently to ascertain the reality of the mobile money authentication security attacks, which remained constant over time. The identified attacks helped researchers propose a novel secure MFA algorithm to solve the various authentication attacks.

3.2.2 Pragmatic research philosophy

Pragmatic research philosophy is where research practices, methods and strategies are used to investigate the research problem, and the practical results are significantly taken into consideration (Tashakkori & Teddlie, 1998; Goldkuhl, 2012; Morgan, 2014; Sefotho, 2015; Žukauskas *et al*., 2018; Kaushik & Walsh, 2019). It states that multiple methods can be used to investigate reality to provide a more comprehensive understanding of the research problem under investigation using innovative and dynamic approaches to find solutions to research problems, i.e., solving practical problems in the real world (Maxcy, 2003; Teddlie & Tashakkori, 2009; Creswell & Clark, 2010). Positivist and interpretivism positions are combined within the scope of the research based on the research questions used to determine the research philosophy. It is argued that in pragmatic research philosophy, knowledge and reality are based on experience, thoughts, and habits that are constructed socially (Kaushik & Walsh, 2019).

3.3 Research design

Design science research (DSR) was employed in this study. Peffers *et al*. (2007) and Venable *et al*. (2017) define DSR as the ultimate problem-solving research that aspires to create artefacts to solve identified organisational problems, evaluate the artefact, and communicate the results to suitable people to improve human knowledge. The primary aim is to address organisations' unresolved issues by creating innovative artefacts such as algorithms, constructs, computer interfaces, models, system design methodologies, and social innovations (Peffers *et al*., 2007; Baskerville *et al*., 2018; Costa *et al*., 2020). The artefacts created must be relevant and address the identified problem. Its usefulness and quality must be rigorously assessed to show its verifiable contributions and effectively communicate to the intended people (Peffers *et al*., 2007). The researcher used the DSR methodology process, which consists of six sequential activities to design

the secure MFA algorithm and develop the prototypes of the native G-MoMo applications. The activities included: (a) identifying the problem, (b) defining the objectives for the artefact, (c) designing and developing the artefact, (d) demonstrating and using the artefact, (e) evaluating the solution, and (f) communicating the problems, the artefact and its utility and effectiveness through publications (Peffers *et al*., 2007; Schorr & Hvam, 2018). This process of the DSR methodology ensured consistency with previous DSR theories and practices; it provided a nominal process for carrying out DSR in IS, and it guaranteed that the evidence obtained enabled the researchers to answer the initial research question (Peffers *et al*., 2007). Figure 10 shows the DSR process model by Peffers *et al*. (2006).

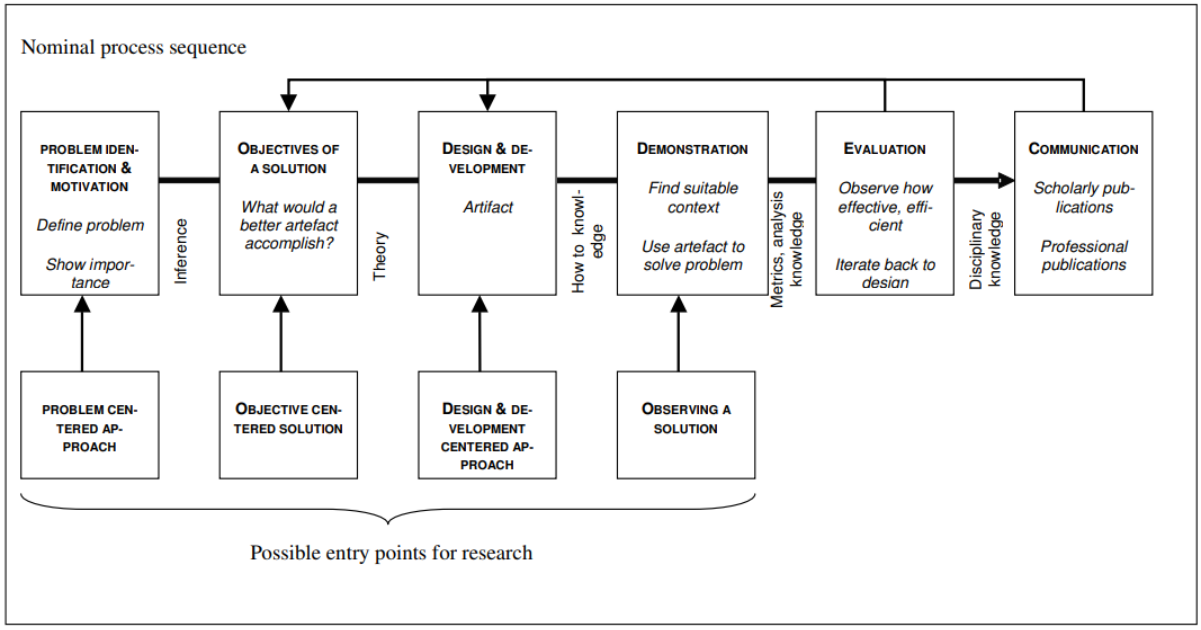


Figure 10: Design science research process model (Peffers *et al*., 2006)

3.4 Population, sample size, and sampling technique

3.4.1 Population

Best and Kahn (2006) and Creswell (2011) define a population as the group of people or objects the researcher wishes to generalise the study findings. This study was carried out in Uganda's central, western, eastern, and northern regions. It was selected as a study area because it had a population of 25.8 million registered mobile money customers and 200 857 registered mobile money agents at the end of 2019 (Uganda Bureau of Statistics [UBOS], 2019; UCC, 2019). The study targeted a population of 25.8 million registered mobile money customers, 200 857 mobile money agents, and 100 MNO IT officers.

3.4.2 Sample size

Haq and Shabbir (2014) define a sample as a set of people selected by the researcher from the larger population using a predefined selection technique for study purposes. On the other hand, sampling is choosing a suitable representative from the people to evaluate the attributes of the entire population (Singh & Masuku, 2014). The people selected to participate in the research are sample size. The researchers used the Yamane (1973) formula to establish the sample size for the study with a 95% confidence level:

$$n = \frac{N}{1 + Ne^2}$$

Where *n* is the sample size, *N* is the population under study, and *e* is the margin error (0.05). The sample size collected from the registered mobile money customers, agents, and MNO IT officers is summarised in Table 3.

Table 3: Summary of the sample size for registered mobile money customers, agents, and MNO IT officers

S/No	Category	Population (N)	Sample size (n)
1.	Mobile money customers	25 800 000	400
2.	Mobile money agents	200 857	399
3.	MNO IT officers	100	80
	Total	**26 000 957**	**879**

3.4.3 Sampling technique

The research used a stratified random sampling technique where the population was split into the strata of registered mobile money customers, agents, and MNO IT officers, which was independently more homogeneous. The researcher confidently chose samples from each stratum to make up the sample for the study (Kothari, 2004; Bryman, 2012).

3.5 Data collection instruments

Data for the research were collected using structured questionnaires, documentary reviews, and direct observation to find the security attacks on the mobile money's 2FA systems, security challenges encountered by Uganda's mobile money schemes, and ascertain the essential requirements for the proposed secure MFA algorithm for mobile money applications.

3.5.1 Structured questionnaires

The study employed structured questionnaires to collect quantitative data from the registered mobile money customers, agents, and MNO IT officers in the four regions of Uganda. The structured questionnaires comprised simple and short closed-ended questions to ensure a higher response rate. The questionnaires were designed using Google Forms and administered online to the selected participants. The researcher also self-administered the printed questionnaires to participants who did not have access to the internet. The questionnaires were divided into: (a) the respondents' social-demographic characteristics; (b) the mobile money services; (c) the benefits of using mobile money services; (d) the security challenges encountered by Uganda's mobile money schemes; (e) the correlation between demographic variables and the security challenges; and (f) the different ways to alleviate the security challenges (Appendix 2, 3 & 4).

The G-MoMo applications were assessed using heuristic evaluation and usability testing. Post-test questionnaires were designed and administered to evaluation experts and selected participants to evaluate the G-MoMo applications after performing some tasks. Questionnaires were chosen because they help explain the phenomena' variability, give the experts and participants time to respond accurately to questions conveniently, and collect data from many participants at a minimum cost and time (Saunders *et al*., 2015).

3.5.2 Documentary review

This study employed the document review method to collect background information to understand the operation of the existing systems and develop data collection tools for evaluation. The researchers reviewed documents like reports, journal articles, conference papers, books and e-books, magazines, newspapers, brochures, reference works, standards, training materials, government statistical publications, and other internet sources. Data were collected about mobile money schemes and algorithms, authentication attacks, and different approaches to mitigate the attacks from the reviewed documents. The researcher opted for this data collection approach because it is easy to access, contains rich background information, is an effective means of collecting data, and is more reliable and cost-effective than other data collection methods (O'Leary, 2004; Bowen, 2009).

3.5.3 Direct observation

The researcher, who is also a mobile money customer, participated in evaluating the functionalities of the mobile money systems by performing mobile money transactions using both

the USSD code and Airtel and MTN mobile money applications to collect data through direct observation. The direct observation method was adopted because it enables the researcher to observe what is happening directly (Rahman, 2016). The researcher also used the mobile money agent application to conduct and confirm mobile money services. The aim was to ascertain an apparent response to mobile money customers' challenges and the procedure to handle the issues.

3.6 Data analysis

The data collected using Google Forms were automatically stored in a predefined format for analysis, and those collected using printed questionnaires were given meaningful descriptions and entered into Google Forms using the preview option to ensure that the datasets contained all the participants' opinions (Saunders *et al*., 2015; Mihas, 2019). After coding, the data was cleaned to remove incomplete responses and meet the analysis requirements. Later, the Microsoft Excel (.xlsx) dataset files were downloaded from Google Forms and analysed. The RStudio software was used to analyse the statistical data collected because it allows researchers to clean data and interact with other databases (Silverman, 2017). The downloaded Microsoft Excel (.xlsx) dataset files were uploaded into the RStudio and SPSS version 27 software to perform the descriptive analysis, Pearson chi-square tests, and generate graphs presenting the participants' opinions.

The descriptive analysis was used to analyse the participants' opinions regarding mobile money service characteristics, the security challenges associated with the mobile money systems, and the various controls to alleviate the security challenges. The graphs presented the respondents' social demography characteristics and the services offered by mobile money. However, the correlation between demographic variables and the security challenges was determined using the Pearson chi-square test. The results for the *mean (M)* ≥ 3.41 and the *p-value* < 0.05 were considered statistically significant (Pimentel, 2010; Morgan *et al*., 2012).

In addition, data collected from evaluation experts and participants using post-test questionnaires in the heuristic evaluation and usability testing were analysed in RStudio software. The researchers performed descriptive analysis and generated graphs to present the results for heuristic evaluation and usability testing of the native G-MoMo applications.

3.7 Validity and reliability

3.7.1 Validity

Validity is the degree to which a data collection instrument precisely measures what it is supposed to measure (Sürücü & Maslakçı, 2020). The validity of the research instrument is important because it establishes which questions to use, and the questions used by the research measure the critical issues (Sürücü & Maslakçı, 2020). A reliable research design must make the best use of validity to provide a clear description of the study's phenomenon and regulate the apparent biases that could alter the research results (Sürücü & Maslakçı, 2020). The content validity index was used to ascertain the validity of the structured questionnaires used in the research. Sürücü and Maslakçı (2020) define content validity as the degree to which questions used in the questionnaires and their scores represent likely questions that can be put forward to tap the concept. Higher content validity is only achieved when the scale items representing the concept's area being measured are more. According to Zamanzadeh *et al*. (2015), the content validity index ensures content validity when developing questionnaires. It was calculated using the item-content validity index (I-CVI) by dividing the number of experts rating for each item (very relevant) by the total number of experts, as shown in the formula. 0 to 1 is the range of values used to measure the I-CVI. If the I-CVI is above 0.79, the item in the questionnaire is *'relevant'.* If it is between 0.70 and 0.79, it *'needs revision.'* Otherwise, it *'should be removed'* (Zamanzadeh *et al*., 2015):

$$\mathrm{I-CVI} = \frac{\text{The number of experts rating "very relevant" for each item}}{\text{The total number of experts}}$$

3.7.2 Reliability

To produce accurate results for making a correct decision, the reliability of the research items should be consistent and dependable. Reliability is the level of agreement that the items in the research instrument generate similar results when carried out on the same individuals in similar situations over time (Sürücü & Maslakçı, 2020). In this research, the questions in the questionnaires were pre-tested for consistency and accuracy checking, hence, ensuring their reliability. A Cronbach alpha test was used to determine the reliability of the items in the questionnaire, and SPSS version 27 software was used to determine the Cronbach alpha test. The four (4) variables, along with their respective Cronbach alpha scores are summarized in Table 4. The items with Cronbach's alpha value ≥ 0.70 were considered high and satisfactory (Cronbach, 1951; Downing, 2004).

Table 4: Reliability scores for each variable used in the structured questionnaire

S/No	Variables	Cronbach's Alpha score	Number of items
1.	Services performed using mobile money	0.719	10
2.	Benefits of using mobile money services	0.796	11
3.	Security issues associated with mobile money systems	0.754	7
4.	The different measures to mitigate the mobile money systems security challenges	0.729	10

3.8 Development approach

The evolutionary prototyping model was used to develop the prototypes of the native G-MoMo applications. Before the actual development of the native G-MoMo applications, functional and non-functional requirements were identified and unified modelling language (UML) was used to visualise the designs of the native G-MoMo applications by designing use case diagrams, sequence diagrams, and flowchart diagrams. The prototypes were developed using Vue JS Framework for the front end, Python for the back end, MySQL for back-end databases, and Twilio programmable SMS to send 5-digit OTP to the mobile money subscribers' smartphones. Heuristic evaluation and usability testing were conducted to analyse the usability issues with the interface designs of the three G-MoMo applications and their usability by installing them on experts' and participants' smartphones. They performed different tasks using the three applications and provided recommendations that were later incorporated into the latest versions of the applications.

3.9 Materials and tools

The Vue JS Framework, Python, and MySQL were used to develop the native G-MoMo applications' front-end, back-end, and back-end databases, respectively. Twilio Programmable SMS was used to generate and send 5-digit OTP to the mobile money subscribers' smartphones to complete enrolment and authentication.

3.9.1 Vue JS framework

The Vue JS framework was used to develop the native G-MoMo applications' front end. Vue.js is a progressive and open-source JavaScript framework for developing simple front-end user interfaces. It is based on the model-view-view model (MVVM) (Baida *et al*., 2020; Pšenák & Tibenský, 2020; Arévalo *et al*., 2020; Li & Zhang, 2021). In February 2014, Evan You developed Vue.js for building small projects and single-page applications with minimum effort to achieve responsive data binding and user interface components (Putra *et al*., 2019; Xing *et al*., 2019;

Pšenák & Tibenský, 2020). The Vue.js framework has several core features like declarative rendering, directives, and system reactive data binding (Putra *et al*., 2019; Baida *et al*., 2020). It has core libraries that focus on the view layer and easily integrate with other libraries (Xing *et al*., 2019; Pšenák & Tibenský, 2020). In addition, it works on component-based architecture where the components interact with each other, and it adopts the bottom-up incremental development design (Li & Zhang, 2021). It is widely used in developing native applications because they are user-friendly, scalable, fast, and reliable, and its library is easy to use. They enhance development efficiency and performance, easily integrate with other libraries, and consume less memory (Kostelidis & Maniatis, 2017; Macrae, 2018; Nelson, 2018; Song *et al*., 2019; Quan, 2019; Li & Zhang, 2021). It is open-source, thus making the codes modifiable, readable, and fast code execution. They are designed to be adopted progressively (Baida *et al*., 2020; Pšenák & Tibenský, 2020; Arévalo *et al*., 2020).

3.9.2 Python

The native G-MoMo applications' back-end was implemented using Python. Python is an open-source, object-oriented, interpreted, general-purpose, and high-level programming language with easy syntax for developing rapid prototypes of applications (Li & Wang, 2019; Vyas & Virparia, 2020; Arévalo *et al*., 2020; Bati, 2021). Guido Van Rossum developed Python in 1989 as a free, open-source, simple, easily interoperate with other languages, and portable to support object-oriented, procedural, and functional programming (Mészárosová, 2015; Shi & Chen, 2020; Huggi & Jamuna, 2020). It is a cross-platform language that runs on different operating systems and supports third-party libraries (Mészárosová, 2015; Bati, 2021). Python has comprehensive features such as platform independence, data structures, an extensive standard library, automatic memory management, open-source, clean syntax, and easily readable codes (Kumar & Panda, 2019; Vyas & Virparia, 2020; Huggi & Jamuna, 2020; Wang, 2020; Bati, 2021). It can be used to create applications that can quickly communicate with database systems, handle big data, and develop fast prototypes (Huggi & Jamuna, 2020). Python language is widely adopted in various fields because it can quickly generate program prototypes, efficiently help developers to complete tasks, is easy to learn because of the simplicity of the syntax, and has high performance in parallel programming (Li & Wang, 2019; Shi & Chen, 2020; Xinyuan *et al*., 2020; Wang, 2020; Bati, 2021).

3.9.3 My structured query language (MySQL)

My structured query language (MySQL) was used to design the back-end databases for the native G-MoMo applications. It is an open-source database rolled out in 1995. My structured query language was developed, distributed, and supported by Oracle Corporation and runs as a server that uses SQL as a query language to provide multi-user access to several databases (Dawodi *et al*., 2019; Eyada *et al*., 2020; Raj & D'Souza, 2020; Sholichah *et al*., 2020). It was used as a back-end database because of its encryption and decryption functions, speed, scalability, high performance, accessibility, platform independence, reliability, robustness, easy configuration, and backup and recovery utilities (Dawodi *et al*., 2019; Raj & D'Souza, 2020; Sadeq *et al*., 2020; Eyada *et al*., 2020; Vyas & Virparia, 2021). It also provides large-scale data sharing, has low implementation costs, and maintains data consistency (Zhang *et al*., 2016; Ongo & Kusuma, 2018).

3.9.4 Twilio programmable SMS

The OTP used to authenticate the mobile money subscribers in the native G-MoMo applications is delivered using Twilio. Premkumar *et al*. (2018), Pendurthi *et al*. (2021), and Geetha *et al*. (2021) define Twilio as a cloud communication platform with a web service API to send and receive SMS text messages. The mobile money subscribers' phone numbers are sent and registered with the Twilio API to send 5-digit OTP via SMS, which is only valid for 60 seconds. After receiving the OTPs, the subscriber is requested to enter them where they are verified with the stored copy. The Twilio API also tracks the sent SMS OTP in case of repudiation.

3.10 Evaluation of the algorithm and the prototypes of the native G-MoMo applications

The proposed MFA algorithm was evaluated by analysing the communication overhead and computational cost and comparing it with other algorithms to determine their performance. It also involved comparing the proposed algorithm's security features with existing algorithms, which helped understand their efficiency.

The developed prototypes of the native G-MoMo applications were analysed using heuristic evaluation and usability testing. Heuristic evaluation was carried out by five evaluation experts that used the 10 principles proposed by Jakob Nielsen to inspect the usability issues with the interface designs of the three native G-MoMo applications for improvement (Nielsen, 1994; Quiñones *et al*., 2020; Poltronieri *et al*., 2021; Tremoulet *et al*., 2021). In usability testing, researchers selected forty (40) participants to use the native G-MoMo applications and verify their

usability based on some attributes to determine whether they are convenient, efficient, and satisfactory. The researchers used the heuristic evaluation post-test questionnaire to collect qualitative data from evaluation experts about the usability issues with the interface designs of the native G-MoMo applications after performing tasks. Quantitative data were collected from the selected participants about the usability of the native G-MoMo applications using a post-test questionnaire after performing tasks.

3.11 Ethical considerations

Research ethics is an essential component that explains how the codes of practice and standards guide the research process. The aim is to ensure the voluntary engagement of the participants in the study, their informed consent of involvement in the research, and that the participant's privacy and confidentiality are not violated. The School of CoCSE of the NM-AIST issued the researcher a letter that helped him request the mobile money service providers in Uganda to permit him to carry out the research (Appendix 1). The letter detailed the purpose of the study and guaranteed the confidentiality of information provided in the survey. The respondents' privacy and confidentiality were guaranteed by designing structured questionnaires that did not require them to reveal their identities, thus, eliminating biases. In addition, the registered mobile money customers, agents, and MNO IT officers in the four regions of Uganda were requested to partake in the study voluntarily by filling out the structured questionnaires.

CHAPTER FOUR

RESULTS AND DISCUSSION

4.1 Results

The survey, algorithm, prototypes of native G-MoMo applications, performance and security analysis, heuristic evaluation and usability testing results are presented in this chapter. The secure MFA algorithms for mobile money applications and the developed native G-MoMo applications are explained. It also covered the discussions of the survey results, algorithm, heuristic evaluation and usability testing results. Tables and graphs were used to present the results that helped the researcher to make decisions.

4.1.1 The security challenges with mobile money systems in Uganda

A survey was conducted to assess the main security challenges encountered by the mobile money systems in Uganda. The social demography characteristics, mobile money service characteristics, services carried out using mobile money systems, and benefits of using mobile money services are presented. It also explains the security challenges, the correlation between demographic variables and the security challenges, and the different measures to mitigate them.

(i) Social demography characteristics

One thousand six hundred fourteen structured questionnaires were administered online and offline to registered mobile money customers, agents, and MNO IT officers in the four regions of Uganda. One thousand two hundred forty filled questionnaires were returned, with a 76.8% response rate. Out of 1240 returned questionnaires, 741 (59.8%) were filled by mobile money customers, 447 (36.0%) by mobile money agents, and 52 (4.2%) by MNO IT officers. The RStudio and SPSS version 27 software were used to analyse the data collected. Descriptive analysis, Pearson's chi-square tests, and graphs were used to analyse the data to help researchers make decisions.

The participants' social demography characteristics are gender, age, marital status, and education level. From Fig. 11, the findings from the analysis indicated that 55.8% of the MNO IT officers were male and 44.2% were female; 54.6% and 45.4% of mobile money agents were male and female, while 57.0% and 43.0% of mobile money customers were male and female.

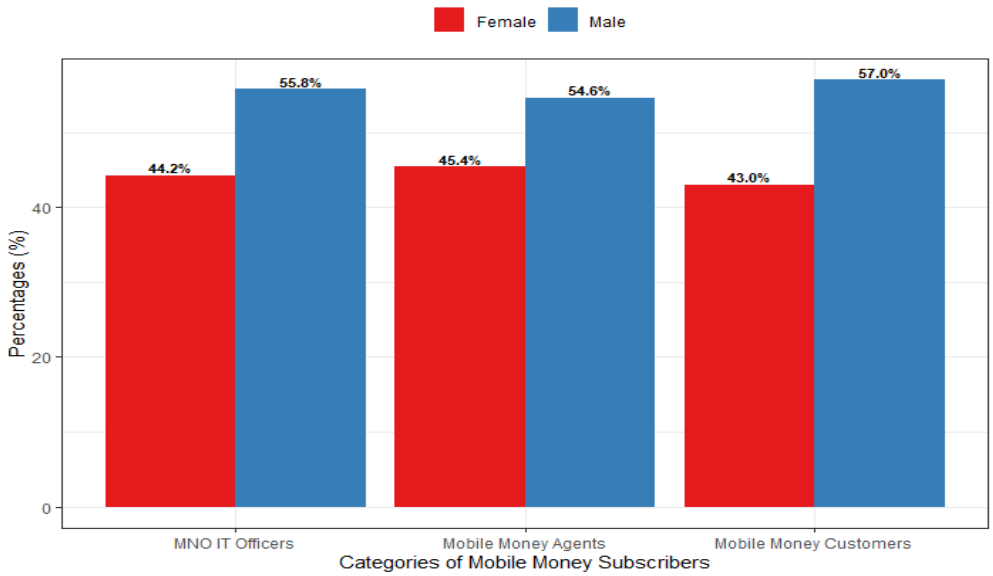


Figure 11: Respondents' gender

Regarding the mobile money agents' age, 4.9% were less than 18 years, 73.8% were between 18–30 years, 20.1% were between 31–50 years, and 1.1% were more than 50 years. In the case of MNO IT officers, none was less than 18 years, 88.5% were between 18–30 years, 9.6% were between 31–50 years, and 1.9% were more than 50 years; while for mobile money customers, 5.9% were less than 18 years, 67.1% were between 18–30 years, 23.6% were between 31–50 years, and 3.4% were more than 50 years as shown Fig. 12.

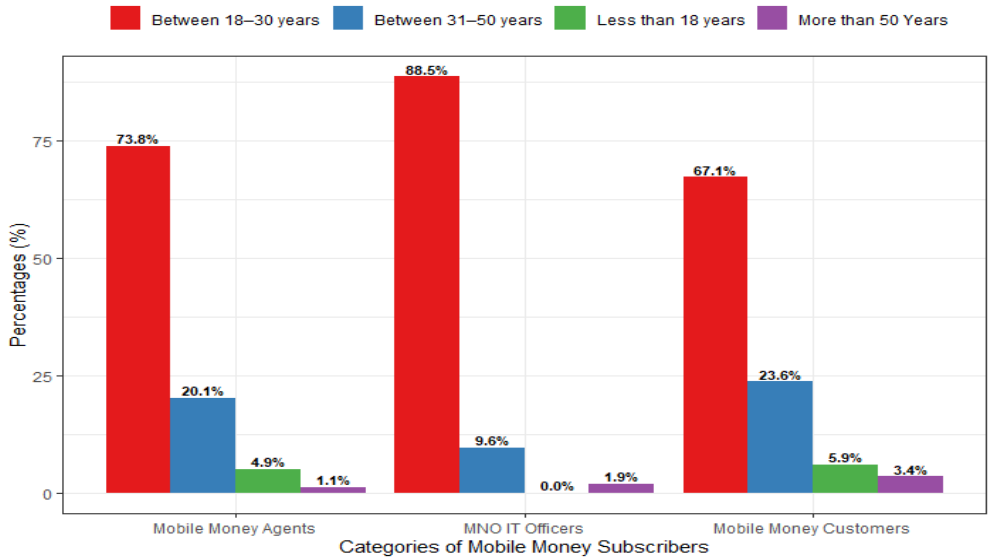


Figure 12: Respondents' age category

Sixty-four point nine percent of mobile money agents were single, 30.6% were married, 3.1% were divorced, and 1.3% were widowed. In the case of MNO IT officers, 67.3% were single, 30.8% were married, 1.9% were divorced, and none were widowed. While 72.1%, 24.8%, 2.2%, and 0.9% of the mobile money customers were single, married, divorced, and widowed, respectively, as presented in Fig. 13.

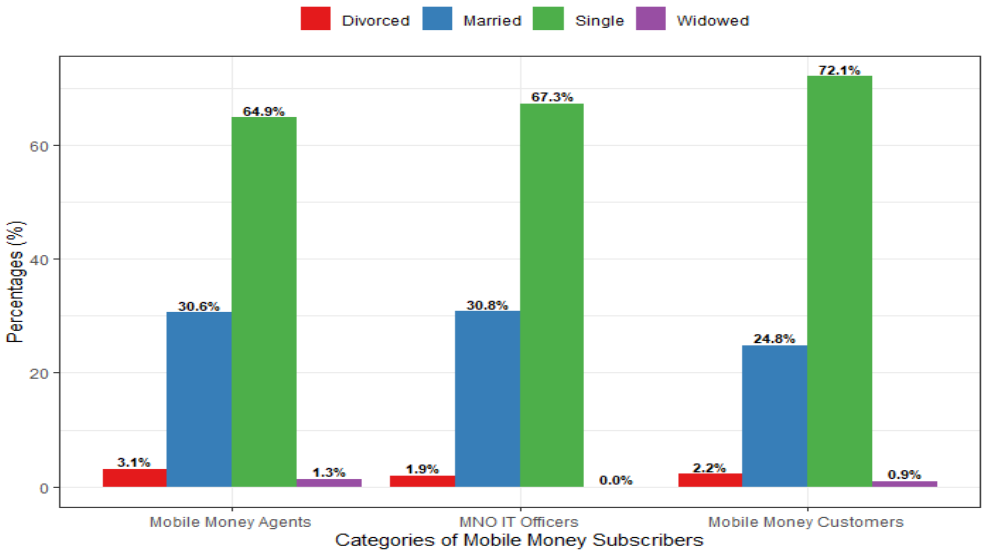


Figure 13: Respondents' marital status

The respondents' education levels were analysed to ascertain their contribution to the mobile money security challenges. Three-point one percent of the mobile money agents had a primary school certificate, 13.2% owned an ordinary level certificate, 25.3% held an advanced level certificate, 13.4% had a tertiary certificate, 9.6% had a diploma, 33.8% had a bachelor's degree, 1.6% had a master's degree, and none had a PhD. In the case of mobile money customers, 3.6% had a primary school certificate, 10.4% owned an ordinary level certificate, 24.2% held an advanced level certificate, 5.0% had a tertiary certificate, 10.1% had a diploma, 35.1% had a bachelor's degree, 9.4% had a master's degree, and 2.2% held a PhD. Regarding MNO IT officers, 5.8% held an advanced level certificate, 7.7% had a tertiary certificate, 7.7% owned a diploma, 71.2% had a bachelor's degree, 7.7% had a master's degree, but none had a primary school certificate, ordinary level certificate, and PhD, as shown in Fig. 14.

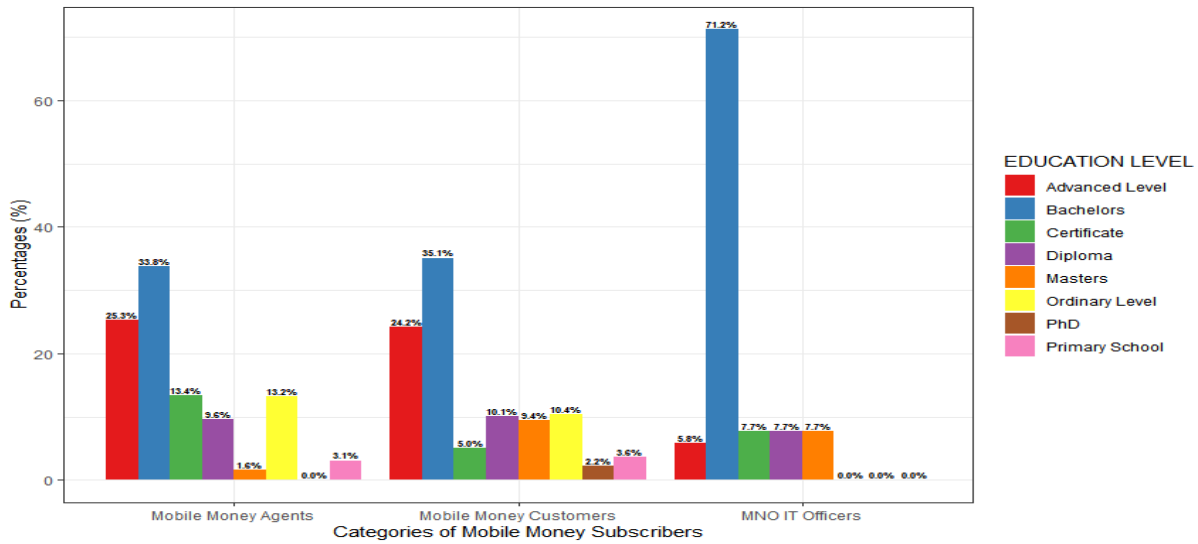


Figure 14: Respondents' education levels

(ii) Mobile money service characteristics

From Table 5, the findings from the analysis showed that 45.1% of the mobile money customers used MTN mobile money, 50.7% Airtel money, 2.2% Africell money, 0.8% M-Sente, 0.4% Ezeey money, 0.4% M-Cash, and 0.5% Others (African pay, ChapChap, Micropay, Payway, Remit money service). Forty-five-point three percent, 41.9%, 7.2%, 0.8%, 3.3%, 0.9%, and 0.6% of mobile money agents use MTN mobile money, Airtel money, Africell money, M-Sente, Ezeey money, M-Cash, and Others, respectively. At the same time, 46.8% of MNO IT officers worked for MTN mobile money, 43.5% for Airtel money, 4.8% for Africell money, 3.2% M-Sente, and 1.6% for Ezeey.

The respondents' experience in mobile money services usage, ways of accessing mobile money services, and the number of mobile money transactions they perform in a month were analysed to establish their relationship with the security challenges associated with the mobile money systems. Eight-point nine percent of mobile money customers reported using mobile money for less than 1 year, 47.1% between 1-5 years, 32.0% between 6-10 years, and 12.0% for more than 10 years. In the case of mobile money agents, 14.8% used mobile money for less than 1 year, 51.0% between 1-5 years, 29.8% between 6-10 years, and 4.5% for more than 10 years, while 9.6%, 71.2%, 15.4%, and 3.8% of MNO IT officers used mobile money for less than 1 year, between 1-5 years, between 6-10 years, and more than 10 years, respectively.

Eighty-nine-point eight percent of the mobile money customers accessed mobile money by dialling the USSD code, 9.5% through mobile Apps, and 0.8% through a mobile phone web browser. Eighty-seven-point six percent of mobile money agents accessed mobile money by dialling USSD code, 10.2% through mobile Apps, and 2.2% through a mobile phone web browser. While 72.9% of the MNO IT officers accessed mobile money by dialling the USSD code, 27.1% through mobile Apps, and no MNO IT officer used a mobile phone web browser to access mobile money services.

One-point eight percent of mobile money customers did not perform a transaction at all in a month, 28.2% perform 1 – 5 times, 21.5% 6 – 10 times, 10.0% 11 – 15 times, 15.5% 16 – 20 times, 23.1% 21 and above transactions in a month. Zero-point four percent of mobile money agents reported that they did not perform mobile money transactions in a month, 6.9% 1 – 5 times, 9.2% 6 – 10 times, 6.0% 11 – 15 times, 9.6% 16 – 20 times, 67.8% 21 and above, while 7.7%, 9.6%, 3.8%, 1.9%, 76.9% of the MNO IT officers performed 1 – 5 times, 6 – 10 times, 11 – 15 times, 16 – 20 times, 21 and above in a month, respectively.

Table 5: Summary of the participants' mobile money service characteristics

S/No	Variable	Mobile money customers (%)	Mobile money agents (%)	MNO IT officers (%)
1.	**Mobile money service providers**			
	MTN mobile money	45.1	45.3	46.8
	Airtel money	50.7	41.9	43.5
	Africell money	2.2	7.2	4.8
	M-Sente	0.8	0.8	3.2
	Ezeey money	0.4	3.3	1.6
	M-Cash	0.4	0.9	0.0
	Others	0.5	0.6	0.0
2.	**Period of using mobile money service**			
	Less than 1 year	8.9	14.8	9.6
	Between 1–5 years	47.1	51.0	71.2
	Between 6–10 years	32.0	29.8	15.4
	More than 10 years	12.0	4.5	3.8
3.	**Ways of accessing mobile money services**			
	USSD code	89.8	87.6	72.9
	Mobile Apps	9.5	10.2	27.1
	Mobile phone web browser	0.8	2.2	0.0
4.	**The number of mobile money transactions performed in a month**			
	Not at all	1.8	0.4	0.0
	1–5	28.2	6.9	7.7
	6–10	21.5	9.2	9.6
	11–15	10.0	6.0	3.8
	16–20	15.5	9.6	1.9
	21 and above	23.1	67.8	76.9

(iii) Mobile money services

The participants were asked what services they performed with mobile money, and they responded that they used it for sending and receiving money within Uganda (24.6%), withdrawing money (21.0%), paying for telecom network services (16.5%), paying for utilities (15.8%), saving and borrow money (8.1%). They also used it for buying goods and services (5.6%), mobile banking

(4.8%), transferring money internationally (2.7%), buying insurance (0.6%), and receiving state pensions (0.3%), as presented in Fig. 15.

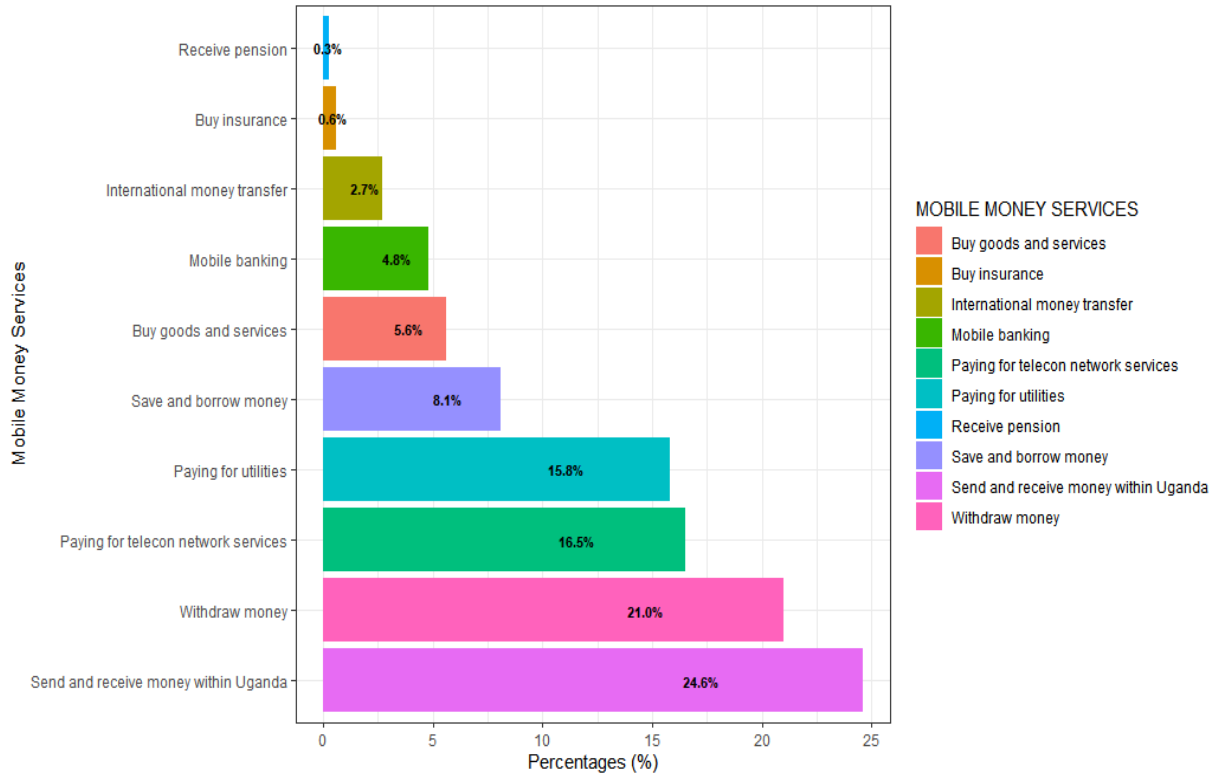


Figure 15: Mobile money services

(iv) Benefits of using mobile money services

The majority of respondents agreed that the benefits of using mobile money services are presented in Table 6. They included offering convenience in terms of sending and receiving money (*M*=4.64, *Std Dev*=0.643), more reliable than physically sending money (*M*=4.45, *Std Dev*=0.756), it saves time (*M*=4.33, *Std Dev*=0.850), it is trustworthy (*M*=4.09, *Std Dev*=0.949). It is quicker and easier to do transactions (*M*=4.27, *Std Dev*=0.841), increases access to financial services (*M*=4.30, *Std Dev*=0.804), and reduces the time and costs spent on maintaining bank accounts (*M*=4.13, *Std Dev*=0.964). Mobile money results in economic growth (*M*=3.90, *Std Dev*=1.059); it provides mobile financial services (*M*=4.53, *Std Dev*=0.688); it improves the standard of living of the subscribers (*M*=3.96, *Std Dev*=1.028); and boosts the diffusion of banking services (*M*=4.06, *Std Dev*=0.941). Therefore, it was statistically significant to say that the benefits of using mobile money services are presented in Table 6 because their mean is greater than 3.41.

Table 6: Opinion of participants concerning the benefits of using mobile money services

No	Benefits of using mobile money	SD	D	N	A	SA	M	Std Dev
1.	It offers convenience in terms of sending and receiving money.	0.4	1.3	2.8	25.1	70.4	4.64	0.643
2.	It is more reliable than physically sending money.	0.3	1.0	6.4	30.4	61.9	4.45	0.756
3.	It saves time.	1.0	1.0	6.8	34.3	56.9	4.33	0.850
4.	It is trustworthy.	0.8	3.4	10.1	33.6	52.1	4.09	0.949
5.	Quicker and easier to do transactions.	0.6	2.2	11.4	38.1	47.7	4.27	0.841
6.	Increases access to financial services.	0.7	1.8	15.9	33.5	48.1	4.30	0.804
7.	Reduces the time and costs spent on maintaining bank accounts.	0.8	6.6	16.2	31.9	44.4	4.13	0.964
8.	Mobile money results in economic growth.	1.0	5.3	18.5	33.5	41.7	3.90	1.059
9.	It provides mobile financial services.	1.5	4.8	18.3	37.1	38.4	4.53	0.688
10.	Improves the standard of living of the subscribers.	2.4	6.9	19.8	34.3	36.5	3.96	1.028
11.	Boosts the diffusion of banking services.	2.5	8.9	20.2	33.4	35.1	4.06	0.941

SD = Strongly Disagree, D = Disagree, N = Neutral, A = Agree, and SA = Strongly Agree, M = Means, and Std Dev = Standard Deviation

(v) Security challenges with mobile money systems

The significant majority of the participants acknowledged that the security challenges in Table 7 affected the operation of mobile money schemes in Uganda. These security issues were identity theft (*M*=3.63, *Std Dev*=1.347), authentication attacks (*M*=3.69, *Std Dev*=1.290), phishing attacks (*M*=3.51, *Std Dev*=1.449), and PIN sharing (*M*=3.68, *Std Dev*=1.291). Therefore, it was statistically significant to say that they are the key security issues encountered by the mobile money schemes in Uganda because their mean is greater than 3.41.

Table 7: Participants' opinions regarding security challenges with the mobile money systems

S/No	Security challenges	SD	D	N	A	SA	M	Std Dev
1.	Identity theft	8.7	18.1	9.4	29.0	34.7	3.63	1.347
2.	Authentication attacks	6.5	18.3	9.6	31.0	34.5	3.69	1.290
3.	Phishing attacks	11.7	19.8	11.6	19.4	37.5	3.51	1.449
4.	PIN sharing	7.6	16.2	10.4	32.4	33.4	3.68	1.291

(vi) The correlation between demographic variables and the security challenges

The researcher also analysed the correlation between demographic variables and security challenges. The aim was to determine whether these demographic variables influenced the security challenges. Null hypotheses (H_0) were formulated and independent and dependent variables were identified for the study. The Pearson chi-square test was computed to determine whether there is a statistically significant relationship between demographic variables and security challenges. The level of statistical significance was expressed as a *p-value* which is between 0 and 1. The result of the security challenges with a *p-value > 0.05* was not statistically significant, therefore, the null hypothesis was accepted. However, the results with a *p-value < 0.05* were statistically significant, therefore, the null hypothesis was rejected in favour of the alternative hypothesis. The correlation between demographic variables and security challenges are presented in Tables.

Correlation between gender and security challenges

The results in Table 8 showed that the Pearson chi-square test recommended that there is no statistically significant correlation between gender and identity theft (χ^2 (4) = 1.625, p = 0.804), authentication attacks (χ^2 (4) = 6.312, p = 0.177), and PIN sharing (χ^2 (4) = 1.214, p = 0.876) because the *p*-values are greater than 0.05, then the null hypothesis was accepted. However, there was a statistically significant correlation between gender and phishing attacks (χ^2 (4) = 9.679, p < 0.046); because the *p*-value is less than 0.05, then the null hypothesis was rejected.

Table 8: Correlation between gender and security challenges

S/No	Security challenges	M	Std Dev	df	χ^2	*p*-value
1.	Identity theft	3.63	1.347	4	1.625	0.804
2.	Authentication attacks	3.69	1.290	4	6.312	0.177
3.	Phishing attacks	3.51	1.449	4	9.679	0.046*
4.	PIN sharing	3.68	1.291	4	1.214	0.876

df = degrees of freedom, χ^2 = Chi-Square, and p-value = probability value

Correlation between age and security challenges

As presented in Table 9, the Pearson chi-square test recommended that there is no statistically significant correlation between age and identity theft (χ^2 (12) = 8.956, p = 0.707), authentication attacks (χ^2 (12) = 20.086, p = 0.065), and PIN sharing (χ^2 (12) = 17.476, p = 0.133) because the *p*-values are greater than 0.05, then the null hypothesis was accepted. Nevertheless, there was a statistically significant correlation between age and phishing attacks (χ^2 (12) = 45.549, p < 0.000); because the *p*-value is less than 0.05, then the null hypothesis was rejected.

Table 9: Correlation between age and security challenges

S/No	Security challenges	M	Std Dev	df	χ^2	*p*-value
1.	Identity theft	3.63	1.347	12	8.956	0.707
2.	Authentication attacks	3.69	1.290	12	20.086	0.065
3.	Phishing attacks	3.51	1.449	12	45.549	0.000*
4.	PIN sharing	3.68	1.291	12	17.475	0.133

Correlation between education level and security challenges

In Table 10, a Pearson chi-square test results showed that there was statistically significant correlation between education level and identity theft (χ^2 (28) = 62.972, $p < 0.000$), phishing attacks (χ^2 (28) = 103.450, $p < 0.000$), and PIN sharing (χ^2 (28) = 49.025, $p < 0.008$) because the *p*-values are less than 0.05, then the null hypothesis was rejected. However, the authentication attacks (χ^2 (28) = 40.446, $p = 0.060$) had no statistically significant correlation with education level. Therefore, the null hypothesis was accepted because the *p*-value is greater than 0.05.

Table 10: Correlation between education level and security challenges

S/No	Security challenges	M	Std Dev	df	χ^2	*p*-value
1.	Identity theft	3.63	1.347	28	62.972	0.000*
2.	Authentication attacks	3.69	1.290	28	40.446	0.060
3.	Phishing attacks	3.51	1.449	28	103.450	0.000*
4.	PIN sharing	3.68	1.291	28	49.025	0.008*

Correlation between the experience with mobile money usage and security challenges

The results in Table 11 showed that identity theft (χ^2 (12) = 26.785, $p < 0.008$), phishing attacks (χ^2 (12) = 46.647, $p < 0.000$), and PIN sharing (χ^2 (12) = 21.734, $p < 0.041$) had statistically significant correlation with the experience with mobile money usage, therefore, the null hypothesis was rejected because the *p*-values were less than 0.05. Nonetheless, authentication attacks (χ^2 (12) = 12.757, $p = 0.387$) had no statistically significant correlation with the experience with mobile money usage; therefore, the null hypothesis was accepted since the *p*-values were greater than 0.05.

Table 11: Correlation between experience with mobile money usage and security challenges

S/No	Security challenges	M	Std Dev	df	χ^2	*p*-value
1.	Identity theft	3.63	1.347	12	26.785	0.008*
2.	Authentication attacks	3.69	1.290	12	12.757	0.387
3.	Phishing attacks	3.51	1.449	12	46.647	0.000*
4.	PIN sharing	3.68	1.291	12	21.734	0.041*

Correlation between the number of mobile money transactions in a month and security challenges

In Table 12, Pearson chi-square test results showed that there was a statistically significant correlation between identity theft (χ^2 (20) = 42.570, $p < 0.02$), phishing attacks (χ^2 (20) = 158.042, $p < 0.000$) and the number of mobile money transactions in a month because the *p*-values were less than 0.05; therefore, the null hypothesis was rejected. However, authentication attacks (χ^2 (20) = 21.641, $p = 0.360$) and PIN sharing (χ^2 (20) = 29.827, $p = 0.073$) had no statistically significant correlation with the number of mobile money transactions in a month because the *p*-value was greater than 0.05, therefore, the null hypothesis was accepted.

Table 12: Correlation between the number of mobile money transactions in a month and security challenges

S/No	Security challenges	M	Std Dev	df	χ^2	*p*-value
1.	Identity theft	3.63	1.347	20	42.570	0.002*
2.	Authentication attacks	3.69	1.290	20	21.641	0.360
3.	Phishing attacks	3.51	1.449	20	158.042	0.000*
4.	PIN sharing	3.68	1.291	20	29.827	0.073

(vii) The different controls to alleviate the security challenges with mobile money systems

From Table 13, the significant majority of the participants agreed that all the controls/ measures mentioned are high priorities in mitigating the different mobile money security challenges because their means (M) are above 3.41. Therefore, it was statistically significant to say that they were the best measures to mitigate the different security challenges.

Table 13: Participants' opinions about the different controls to alleviate the security challenges

S/No	Controls to alleviate the security challenges	NP	LP	N	MP	HP	M	Std Dev
1.	Use of MFA for better access controls.	2.7	5.2	5.1	22.3	64.7	4.41	0.994
2.	The victims of mobile money fraud should report the cases to regulators and security agencies.	0.8	2.9	8.2	23.6	64.4	4.48	0.828
3.	Training mobile money agents on standard practice.	1	3	10.5	25.1	60.4	4.41	0.870
4.	Know your customer Controls.	1.9	4.7	14.9	29	49.4	4.19	0.984
5.	Severe punishment of the offenders.	1.2	3.7	9.5	17	68.5	4.48	0.899
6.	Mobile money service providers must have a comprehensive legal document to guide mobile money service.	1.5	5.3	13.6	28.5	51	4.22	0.970
7.	There should be an increase in customer awareness campaigns.	0.8	1.8	8.1	28.5	60.9	4.47	0.784
8.	Mobile money service providers must monitor high-value transactions.	2.3	2.9	11.3	26.9	56.5	4.32	0.949
9.	There is a need for mobile money service providers and the government to publish all the reported incidents.	2.1	5	10.2	27.7	54.9	4.28	0.980
10.	There is a need for mobile money service providers and the government to develop a portal where mobile money subscribers can anonymously share their incidents.	3.8	5.7	11.7	28.3	50.5	4.16	1.080

4.1.2 The existing mobile money authentication scheme

The most common method of accessing mobile money services in Uganda is by using USSD codes and mobile money applications. The mobile applications authenticate the mobile money

subscribers by using PIN and OTP. The three essential phases in the existing mobile money schemes are registration, authentication, and transaction.

(i) Registration phase

In the case of MTN mobile money, the registration of a new mobile money customer begins with the customer visiting the nearest authorised mobile money agent and swapping their SIM to upgrade to a mobile money-enabled card. The mobile money agent then captures their biodata, face photo, fingerprint, national identification number (NIN), valid national ID or valid passport or driver's license or voter's card photo, which are confirmed, and stored in the database of the MNO. The NIN is matched with the copy stored in the national identification and registration authority (NIRA) database. If verified, the customer must set their five-digit mobile money PIN. The information provided by the mobile money customer is then saved in the database. A mobile money account is created with a balance of UGX 0, and a confirmation message for successful mobile money account registration is sent to the subscriber's mobile phone. If it fails, the customer is sent a confirmation message requesting to attempt three times. The registered mobile money customer can then download and install the MTN MoMo App and use it to perform mobile money services. Figure 16 illustrates the flowchart for the registration phase.

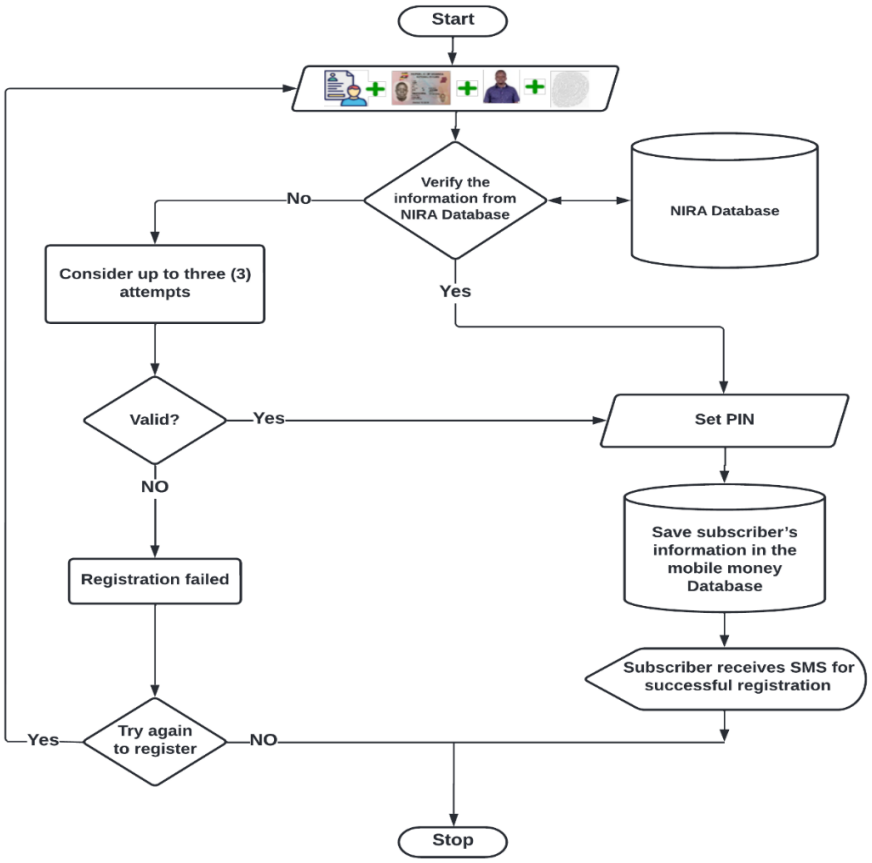


Figure 16: Flowchart for mobile money registration phase

(ii) Authentication phase

The mobile money customer begins the authentication process by running the installed MTN MoMo App on their smartphone connected to the internet. Once they launch the MTN MoMo App for the first time, they must select their country from the available list of countries and enter their phone number. The entered phone number is compared with the copy stored in the mobile money database. If the phone number matches, a 4-digit OTP will be generated and sent to the customer's phone number via SMS and the MTN MoMo App will automatically detect the OTP and will be compared. If it matches, the customer must enter their 5-digit mobile money PIN, which will be verified, and if it is correct, again, a 4-digit OTP will be generated and sent to the customer's phone number. The MTN MoMo App will automatically detect the OTP and match it. If it matches, the customer is displayed with a menu containing the services offered by MTN that they wish to perform. However, if the phone number, OTPs, and PIN are wrong, the authentication process will be terminated, and the customer can try again. Figure 17 illustrates the flowchart for the authentication phase.

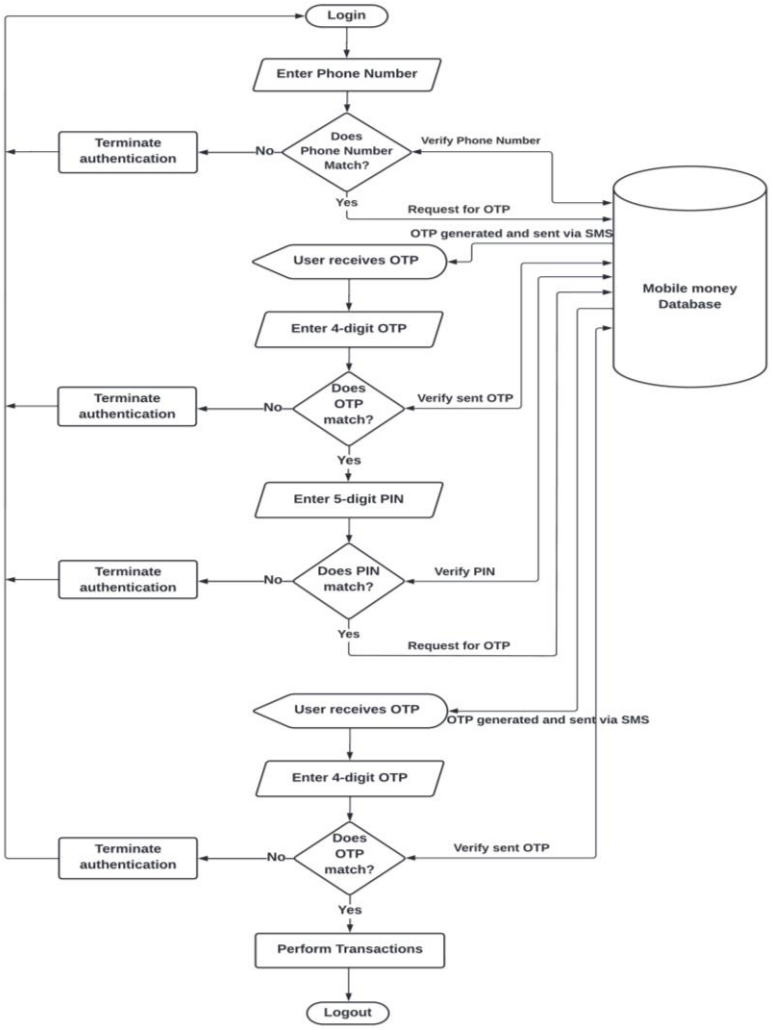


Figure 17: Flowchart for mobile money transaction phase (e.g., buying Airtime)

Several challenges related to mobile money authentication security were identified through the survey, which are explained in the following subsections:

Authentication attacks

Were identified as a security challenge to mobile money systems where adversaries used brute-force attacks, social engineering attacks, and shoulder-surfing attacks to compromise the victims' weak 4 or 5-digit PINs to have access to their mobile money accounts. The attackers also took advantage of the weaknesses in the mobile money systems, such as poor system security, to compromise the victims' mobile money PINs and encryption keys and perform fraudulent transactions on behalf of the victims.

Identity theft

Mobile money subscribers acknowledged identity theft as one of the security challenges. Many mobile money customers prefer to store their mobile money PINs on their phones, and if such phones are stolen, the attackers can get access to the PINs and defraud the subscribers. It was reported that mobile money subscribers usually share their PINs among friends and relatives, thus, making it easy for them to perform illegal mobile money transactions. Fraudsters also compromised the mobile money subscribers' PINs through SIM swaps, where they easily control the victims' mobile money accounts and carry out fraudulent transactions without their knowledge. It was also reported that unscrupulous mobile money service providers' employees performed identity theft since they had access to the mobile money systems, their victims' mobile money PINs and financial records.

Phishing attacks

Were reported as common attacks in the mobile money industry. Here, attackers used different methods such as voice calls (vishing), SMS (smishing), and malware-based phishing to lure their victims into revealing their mobile money PINs. The adversaries also requested their victims to transfer money directly to their mobile wallets.

Exposing PINs to Close Relative

Mobile money subscribers share their mobile money PINs with the people close to them. The subscribers' friends and relatives can reveal such PINs to unknown people, resulting in identity theft and authentication attacks.

4.1.3 System analysis

(i) System requirement analysis

System requirements describe the mobile application's functionalities, services, and constraints. Requirement analysis explains the customer's expectations about the system to be developed by determining the new system's requirements to meet the expectations. The user requirements for the new system were collected, analysed, and categorised into functional and non-functional requirements.

Functional requirements

Functional requirements are collected from the end-users for the system development. Gabriela (2017) defines functional requirements as the system's expected behaviour, responses to the specific inputs, and the functions, services, and tasks they perform. It also explains what the system can accept as inputs, what it can produce as output, what it can store, and the computations performed by the system. Table 14 summarises the functional requirements of the proposed native G-MoMo applications.

Table 14: Functional requirements of the proposed native G-MoMo applications

S/No	Function	Description
1.	User enrolment	The mobile money IT support staff and agents must register other IT support staff, agents, and customers, by capturing their first name, last name, phone number, PIN, and biometric fingerprints.
2.	User authentication	The G-MoMo applications allow registered mobile money subscribers to log in to the G-MoMo applications using their PIN, OTP, and biometric fingerprints.
3.	Deposit money	The G-MoMo Agent application allows mobile money agents to deposit money into mobile money customers' mobile wallets.
4.	Withdraw money	The G-MoMo Customer application allows mobile money customers to withdraw money from their mobile wallets by scanning their biometric fingerprints and the agent's QR code.
5.	Send money	The G-MoMo applications allow mobile money customers to send money to other customers.
6.	Check balance	It allows mobile money agents and customers to check their electronic balances from their mobile wallets using the G-MoMo agent and customer applications.
7.	Bill payments	The G-MoMo Customer application can allow customers to make payments for digital satellite television (DStv), GOtv, and national water and sewerage corporation (NWSC), once integrated with external interfaces of DStv, GOtv, & NWSC applications.
8.	Mini statement	The G-MoMo Customer application displays the mini statement for the transactions performed by mobile money customers.
9.	Statistics	The G-MoMo IT Support application displays statistics about the total number of registered mobile money subscribers.
10.	Account management	The G-MoMo applications allow IT support staff, agents, and customers to change their mobile money PINs and biometric fingerprints.
11.	Logout	It allows mobile money subscribers to log out of the system after performing transactions.

Non-functional requirements

Shahid and Tasneem (2017) define non-functional requirements as constraints that apply to the entire system during development. It describes the performance of the native G-MoMo applications. Table 15 summarises the non-functional requirements of the proposed system.

Table 15: Non-functional requirements of the proposed system

S/No	Function	Description
1.	Security	The MFA was implemented in the native G-MoMo applications where mobile money subscribers must enter their PINs, OTPs, and biometric fingerprints during authentication. Mobile money customers' biometric fingerprints and mobile money agents' QR codes authorise money withdrawal.
2.	Privacy	The G-MoMo application ensures the privacy of user information by using SHA-256 to secure the PINs and OTP, and FIDO to secure the biometric fingerprints, where the RSA encryption protects the public/private key pair and the fingerprint templates. The QR code, the confidential financial information in the databases, and all the data before transmission to the remote databases are secured using Fernet encryption.
3.	Usability	The G-MoMo applications provide systematic, simple, and user-friendly interfaces which do not require specialised training.
4.	Maintainability	The G-MoMo applications shall be easily maintained if there are changes to functionalities. The maintenance of the system will not cause the applications to shut down for long hours.
5.	Platform constraint	The G-MoMo applications are supported by the Android operating system version 7.0 and above.
6.	Performance	The G-MoMo applications can process user requests in the shortest time possible. It provides enough time for mobile money subscribers to access and interact with the databases.
7.	Reliability	The G-MoMo applications maintain their performance.
8.	Flexibility	It is easy to add new modules to the G-MoMo applications.
9.	Robustness	The G-MoMo applications shall continue to function accurately if multiple requests are received.
10.	Availability	The G-MoMo applications shall be available in the mobile application stores such as the Google play store when needed.
11.	Responsiveness	The G-MoMo applications require a short response time.
12.	Scalability	The G-MoMo applications provide services to many customers concurrently without crushing.
13.	Portability	The G-MoMo applications run successfully on many Android smartphones, e.g., Tecno Camon 18 Premier, Tecno Camon 16 Pro, and Samsung Galaxy S7 Edge running on Android 11, 10, and 7 with different pixels resolution.
14.	Look and feel	The user interfaces of the G-MoMo applications are aesthetic and interactive.

(iii) System modelling

Ali *et al*. (2021) define system modelling as the process of creating abstract system replicas where each model presents a distinct perspective. It represents a system using the graphical notation in UML. The UML was used to visualise the designs of the native G-MoMo applications. It explained the overview of the system, the relationship between the several components of the applications, and the existing system's functionalities to the analyst, supported the development of the applications and communicated the proposed requirements to the stakeholders (Petre, 2013). The existing and new systems models were used during requirements engineering. The models helped analyse the system from external, interaction, structural, and behavioural perspectives. The Lucidchart's web-based platform was used to design use case diagrams, sequence diagrams, and flowchart diagrams, and each was designed for a particular modelling motive.

Use case diagrams

The use case diagrams depict the system functionalities and the interactions between external actors and the system. The full functionality of the native G-MoMo applications was captured in the conceptual use case diagrams. While designing the use cases, the actors for the G-MoMo applications were identified. The actors included the mobile money IT support staff, agents, customers, and mobile money. They were categorised based on the functions they performed.

- **The use case diagram for mobile money IT support staff**

The mobile money IT support staff uses the G-MoMo IT Support Applications to log in, register new IT support staff and mobile money agents, authorise new smartphones, generate statistics about the registered subscribers, manage their accounts, and log out shown in Fig. 18.

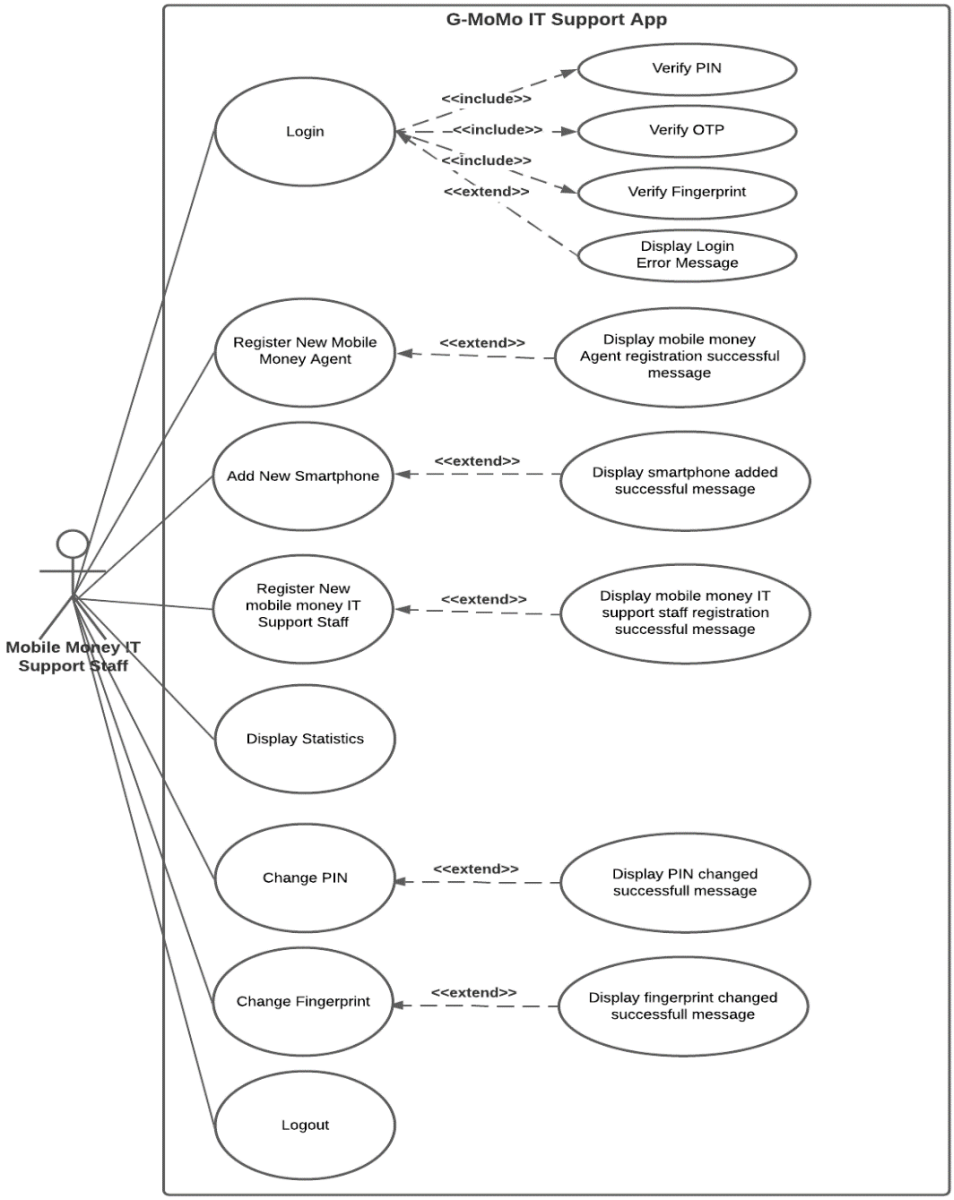


Figure 18: Use case diagram for the mobile money IT support staff

- **The use case diagram for mobile money agents**

The mobile money agents use the G-MoMo Agent Application to log in, enrol new customers, deposit money, authorise money withdrawal by scanning the agent's QR code, check electronic balance, manage accounts, and log out of the system, as shown in Fig. 19.

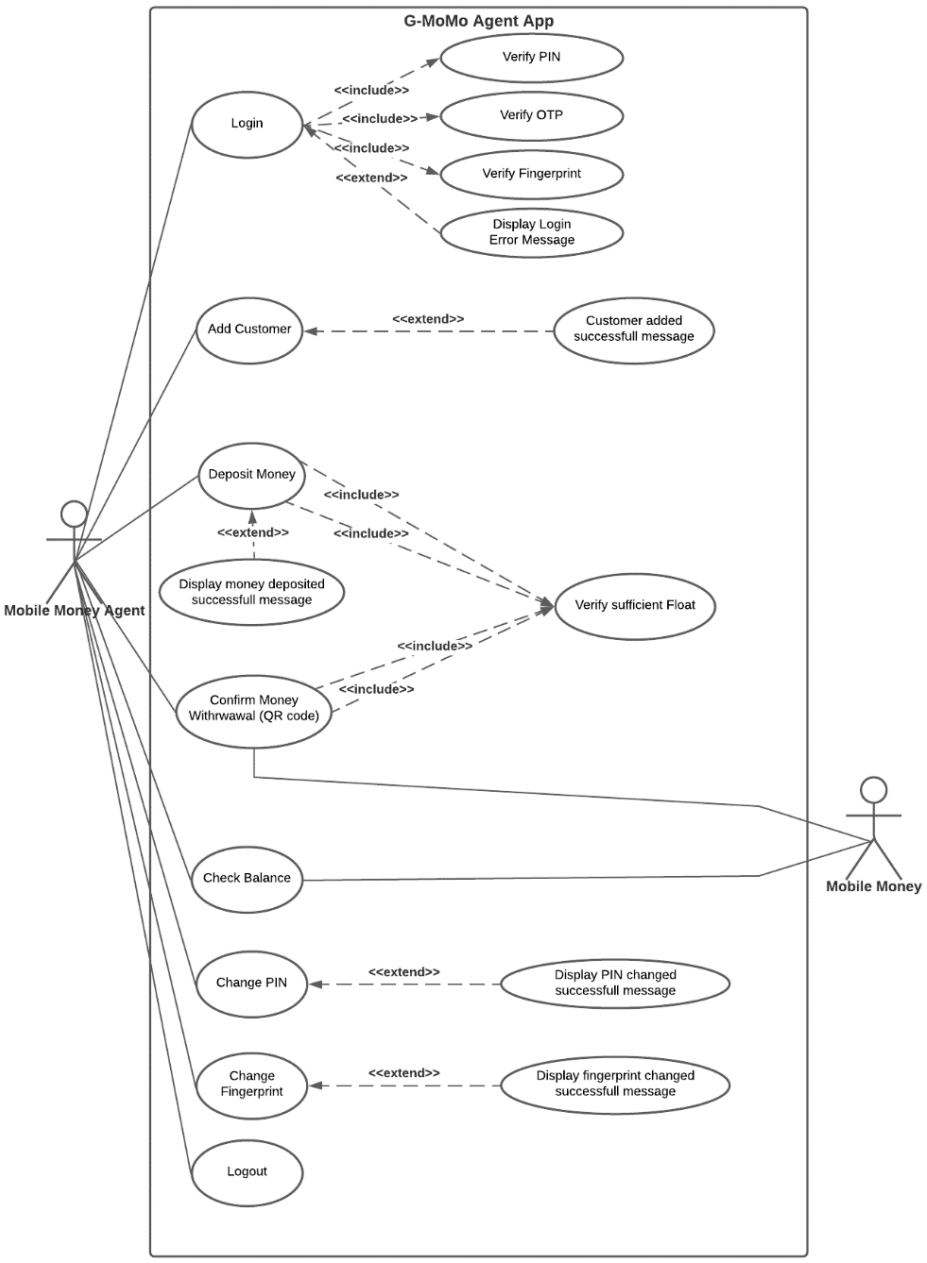


Figure 19: Use case diagram for the mobile money agent

- **The use case diagram for mobile money customer**

The G-MoMo Customer Application allows mobile money customers to perform services such as logging in, checking their available balance and mini statements, withdrawing money, sending money, paying bills, managing their accounts, and logging out, as presented in Fig. 20.

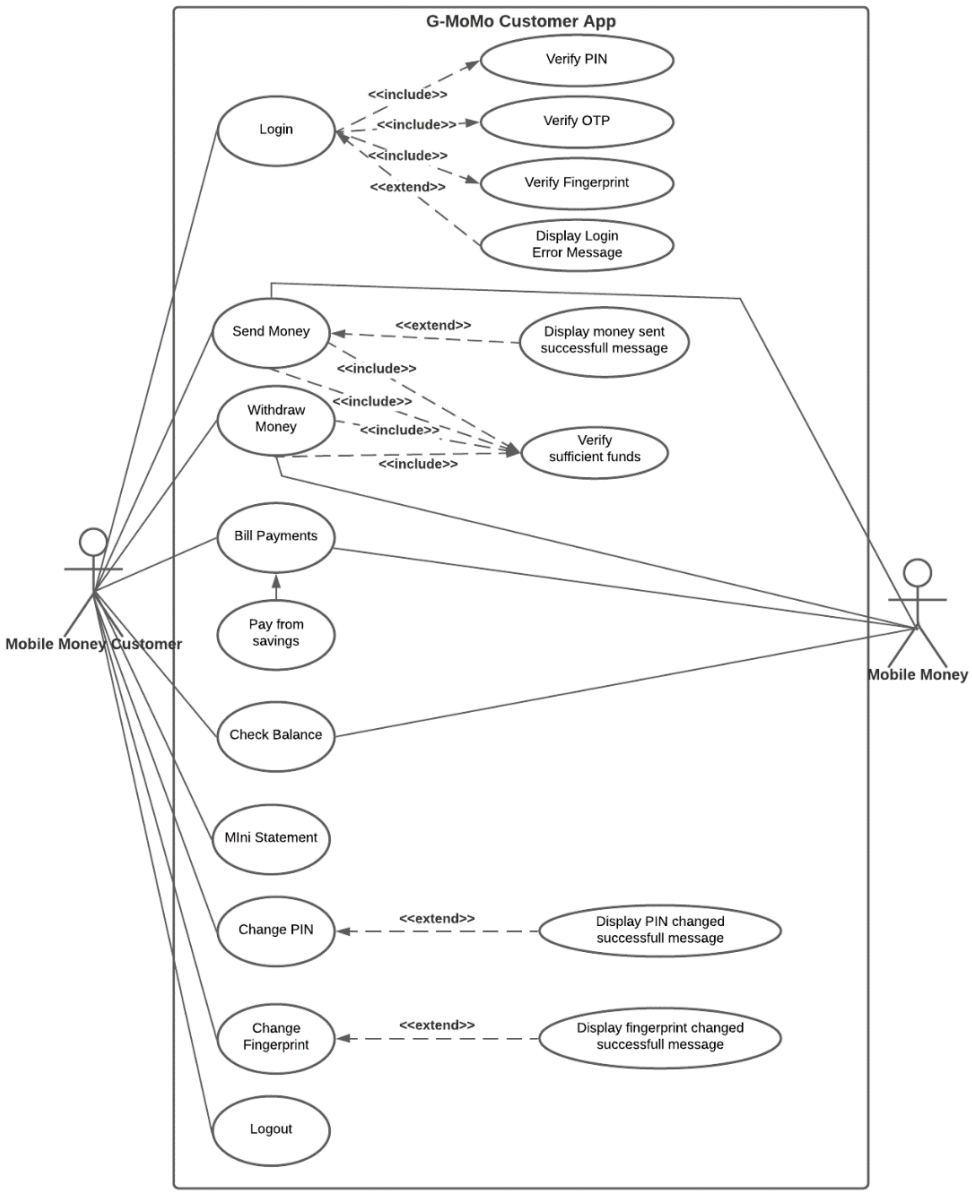


Figure 20: Use case diagram for the mobile money customer

- **Entity relationship diagram (ERD)**

The ERD is the essential tool widely utilised in the structured analysis and conceptual modelling of database design in information systems. Peter Chen of the Massachusetts Institute of Technology developed the entity-relationship model for database design in 1976 (Sinha *et al*., 2013). Saad and Muniandi (2020), Rashkovits and Lavy (2021), and Al-Sulaiti *et al*. (2021) define ERD as a conceptual data model that describes and represents entities, attributes, and the relationships between the entities in database design. The ERD's primary purpose is to visually represent data objects (Saad & Muniandi, 2020). From the designed ERD, the entity-relationship schema presents the entities, their attributes, primary keys, and relationships (Sinha *et al*., 2013). The ERD is used to design database structures effectively, minimises and saves time in coding

and documentation processes, models real-world problems into a database schema, facilitates communications, helps to describe the components using entity-relationship models, allows database designers and users to preview the logical structures of the database, and provides reverse engineering (Wong *et al*., 2012; Cagiltay *et al*., 2013; Javed & Lin, 2018; Yuen *et al*., 2019; Al-Sulaiti *et al*., 2021). Figure 21 shows the entity-relationship schematic for the G-MoMo main database.

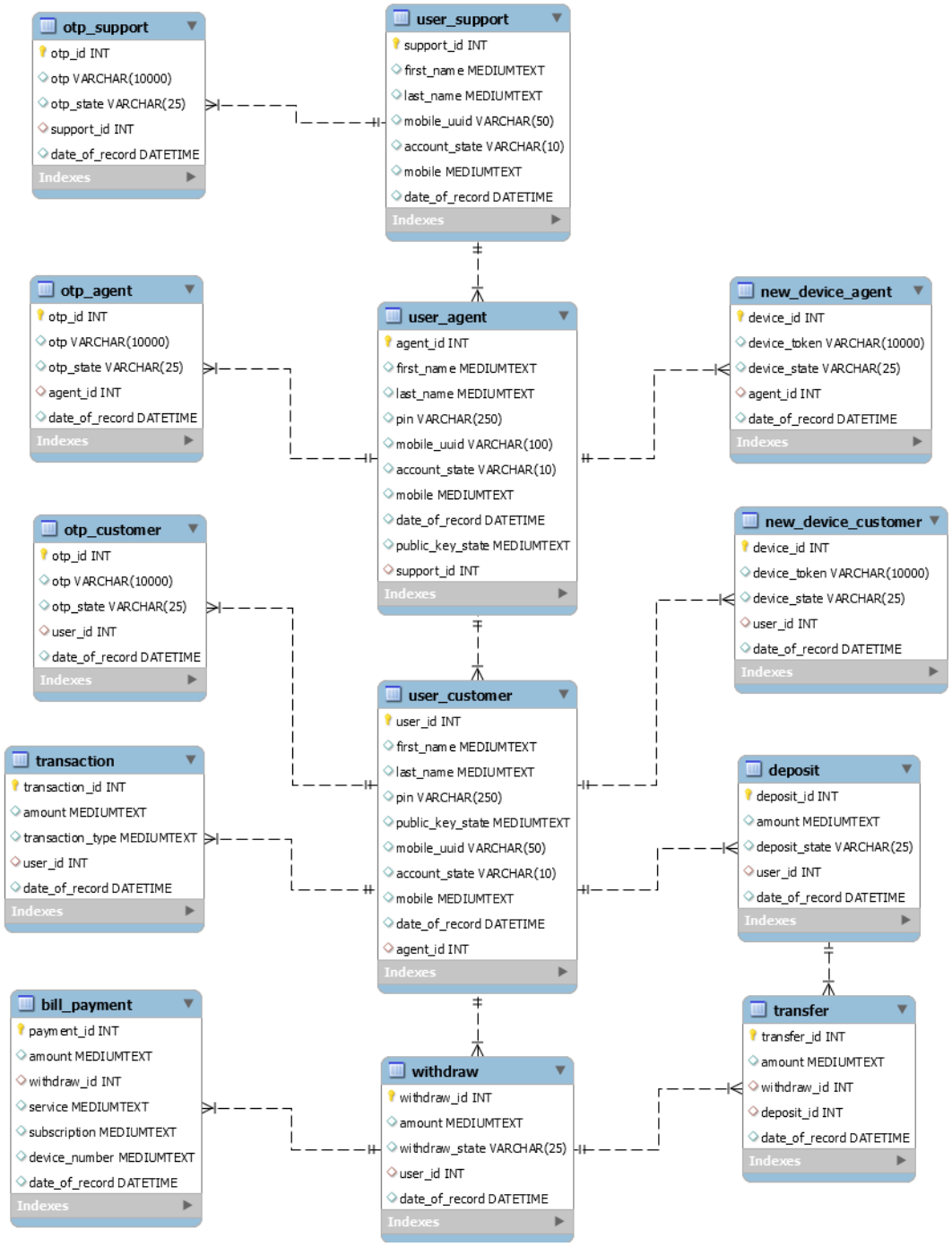


Figure 21: The entity-relationship schematic for the main database

Figure 22 shows the entity-relationship schematic for the FIDO database.

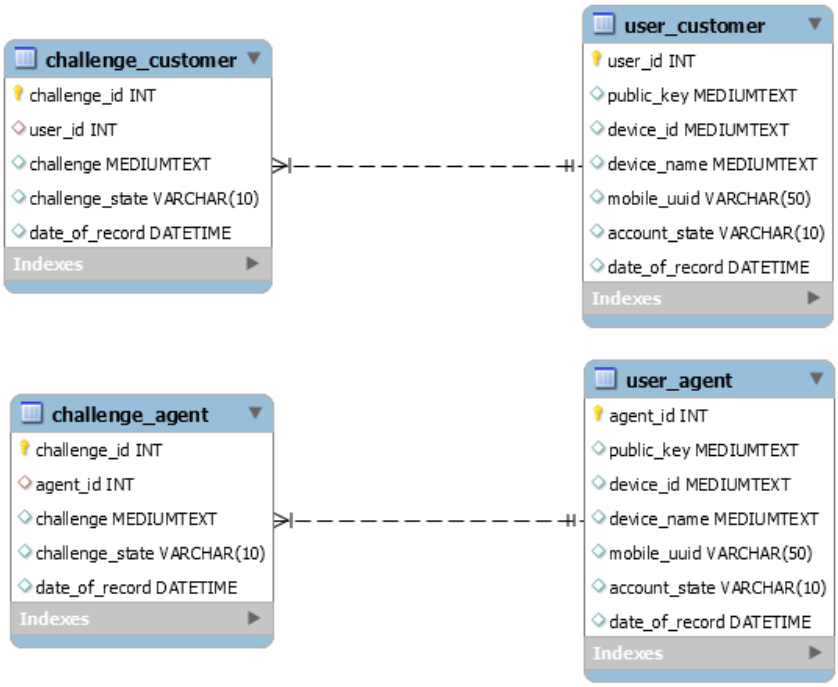


Figure 22: The entity-relationship schematic for the FIDO database

4.1.4 System design

(i) The security technologies used in the proposed algorithm

In the proposed secure MFA algorithm for mobile money applications, mobile money subscribers are authenticated by a novel method that combines PIN, OTP, and biometric fingerprint. The mobile money customer's fingerprint and the agent's QR code are used to authorising money withdrawal. The security of the PINs and OTPs is ensured by SHA-256, subscribers' biometric fingerprint by FIDO, where RSA encryption protects public/private key pair and fingerprint template, and Fernet encryption secures the QR codes, the confidential financial information in the database, and all the data before transmission to the remote databases.

(ii) System architecture

The system architecture illustrates the interaction among the various parts of the proposed system, i.e., mobile money applications, databases, servers, services, users, networks, access devices, and other external systems. The mobile money subscribers (i.e., IT support staff, agents, and customers) have confidential information and public keys stored in the databases (main and FIDO). The private keys and fingerprint templates are stored in the subscriber's smartphone. The main and FIDO databases for the native G-MoMo applications are running on the server so that

different subscribers can request mobile money services efficiently and securely. The mobile money subscribers use the native G-MoMo applications to enrol other subscribers, register new smartphones for the subscribers, deposit money into customers' accounts, withdraw money, and check electronic balances. They are also used to send money, pay bills, confirm money withdrawals, check mini statements, generate statistics about subscribers, and manage accounts. These components work in a coordinated manner to achieve the system's primary goal. Figure 23 illustrates the system architecture for the proposed native G-MoMo applications.

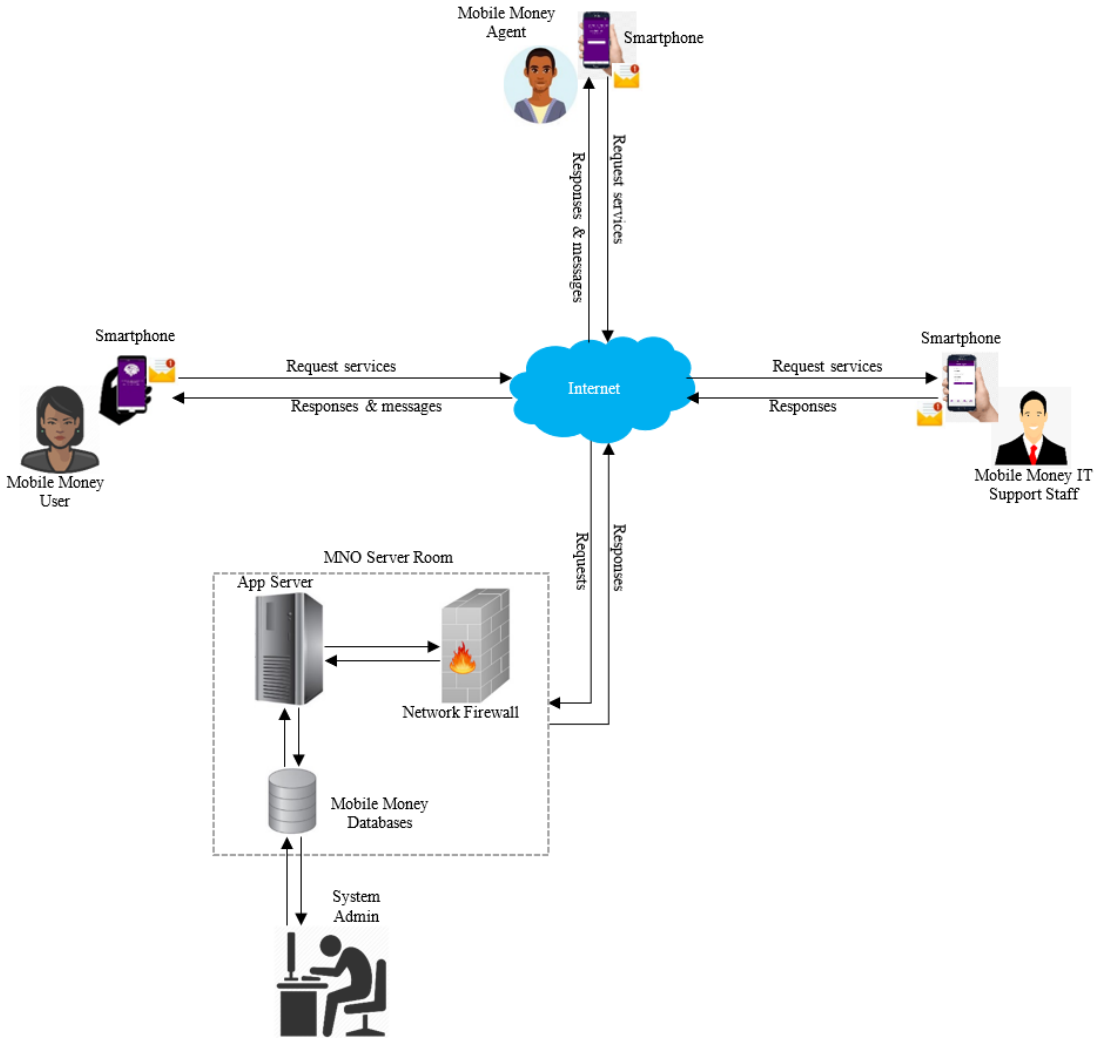


Figure 23: System architecture for the proposed native G-MoMo applications

(iii) The proposed secure MFA algorithm for mobile money applications

The proposed secure MFA algorithm authenticates subscribers using a novel method combining PIN, OTP, and biometric fingerprints. It also authorises money withdrawal using the mobile money customer's biometric fingerprint and the agent's QR code. In the developed algorithm, cryptographic techniques such as SHA-256, RSA in FIDO, and Fernet encryptions protect the

authentication factors (e.g., PINs, OTP, biometric fingerprints - public/private key pair and the fingerprint templates, QR codes), the confidential financial information in the databases, and all the data before transmission to the remote databases.

Mobile money subscriber enrolment, authentication, and transaction are the three main phases of the proposed algorithm. Table 16 summarises the symbols and the bytes sizes used to explain the algorithm.

Table 16: Summary of the symbols and the bytes sizes used to explain the proposed algorithm

Symbols	Meaning	Length (bytes)
U_i	Customer	8
FN_i	Customer's first name	16
LN_i	Customer's last name	16
$UUID_{pn}$	Universally unique identifier	16
PN_i	Customer's phone number	16
PIN_i	Customer's PIN	8
PIN_j	Re-entered PIN	8
OTP_i	Customer's OTP	8
BF_i	Customer's biometric fingerprint	16
B_t	Fingerprints template	16
P_i	Customer's public key	32
F_i	Customer's private key	32
SP_i	Customer's smartphone	8
ID_i	Customer's ID	8
ID_{sp}	Smartphone ID	8
$h(.)$	One-way hash function – SHA-256	32
$E_u(.)/D_u(.)$	Fernet encryption/decryption with key u	16
$E(.)$/D(.)	Public key encryption/decryption - RSA	256
DB_m	Main database	256
DB_{fd}	FIDO database	256
Bal_i	Customer's electronic balance	16
A_a	Mobile money agent	8
$QRcode_a$	Agent QR code	16
Amt_i	Amount	16

The enrolment phase

Before beginning the enrolment process, the A_a and U_i must have smartphones with fingerprint sensors and are connected to the internet, then adhere to the following steps:

Step 1. The A_a after successful login can enrol new U_i by capturing their FN_i, LN_i, PN_i, i.e., $k_i = (FN_i, LN_i, PN_i)$.

Step 2. The A_a then validates the k_i values availed by the U_i. If k_i does not match, the A_a can attempt up to three times; else, the k_i values are encrypted using Fernet $\{E_u(k_i)\}$ and stored in the DB_m.

Step 3. The newly registered U_i is requested to register their SP_i and PN_i by entering their 12-digit PN_i, which will be used to send OTP_i and must make sure that the PN_i is active in the SP_i. OTP_i is generated and sent to the PN_i, and the copy of the sent OTP_i is hashed using the SHA-256, $v_i = h(OTP_i)$, encrypted using Fernet, $E_u(v_i)$, and saved in the DB_m. Once the U_i receives the OTP_i , they must enter it to verify their PN_i. If the OTP_i is verified, the SP_i and PN_i is registered, and $UUID_{pn}$ is created for the PN_i and SP_i and encrypted using the Fernet, $E_u(UUID_{pn})$, and saved in the DB_m. Else, SP_i and PN_i not registered, and $UUID_{pn}$ not created.

Step 4. The A_a then requests the U_i to complete the enrolment process by inputting a five-digit PIN_i and re-entering the five-digit PIN_j.

Step 5. If the PIN_i and the re-entered PIN_j are not similar; the U_i is requested to enter the correct PIN; else, PIN_i and PIN_j is hashed using the SHA-256, $l_i = h(PIN_i, PIN_j)$, encrypted using Fernet, $E_u(l_i)$ and stored in the DB_m.

Step 6. The system will request the U_i to register their BF_i and the U_i's BF_i is captured using their SP_i fingerprint sensor. If the BF_i is scanned successfully, the SP_i creates new public and private key (P_i, F_i) pair unique for the mobile money, SP_i and U_i's account. The P_i is encrypted using RSA, $m_i = E(P_i)$ and Fernet, $E_u(m_i)$ and sent to the DB_{fd}. The F_i and the B_t are also encrypted using RSA, $n_i = E(F_i)$, $o_i = E(B_t)$ but stored in the U_i's SP_i under cryptographic Keystore and SP_i.

Step 7. The DB_m verifies whether the ID_i and ID_{sp} exists. If ID_i and ID_{sp} exist, the U_i is requested to register with a new PN_i and $UUID_{pn}$; else, a successful enrolment and a mobile money account is created with a balance of UGX 0 and a notification message is displayed to the U_i.

Algorithm 1(Fig. 24) is for the mobile money customer enrolment phase (Fig. 25).

Algorithm 1: Enrolment Phase

Input : $FN_i, LN_i, PN_i, OTP_i, PIN_i, PIN_j, BF_i$
Output: j
Function `CustomerEnrollment`$(FN_i, LN_i, PN_i, OTP_i, PIN_i, PIN_j, BF_i)$:
  $k_i \leftarrow FN_i, LN_i, PN_i$
  $i \leftarrow 0$;
  while $i \leq 3$ **do**
    if k_i $isTrue$ **then**
      $E_u(k_i)$ and save it in the DB_m.
      $UUID_k \leftarrow PIN_i, OTP_i$
      if $(PN_i.length = 12)$ *AND* $(OTP_i\ isTrue)$ **then**
        The PN_i and SP_i is registered, $UUID_{pn}$ is created for the PN_i and SP_i and encrypted using Fernet, $E_u(UUID_{pn})$, saved in the DB_m.
      else
        Invalid PN_i and OTP_i, and $UUID_{pn}$ not created.
      end
      $PIN_k \leftarrow PIN_i, PIN_j$
      if $((PIN_i.length = 5)$ *AND* $(PIN_j.length = 5)$ *AND* $(PIN_i = PIN_j))$ **then**
        Hash the PIN_k using SHA-256, l_i=$h(PIN_k)$, encrypt the hashed l_i=$h(PIN_k)$ using Fernet, i.e., $E_u(l_i)$, and save it in the DB_m.
      else
        Enter a Valid PIN_i and PIN_j.
      end
      $BF \leftarrow BF_i$
      Scan the BF_i using the SP_i's Fingerprint Sensor.
      if BF $isTrue$ **then**
        P_i/F_i pairs are generated. P_i is encrypted using RSA, m_i=$E(P_i)$, and again encrypted using Fernet, $E_u(m_i)$. F_i and B_t are encrypted using RSA, i.e., n_i=$E(F_i)$, and o_i=$E(B_t)$.
        The SP_i stores $\langle ID_i, ID_{sp}, n_i, o_i \rangle$, and $\langle ID_i, ID_{sp}, l_i \rangle$ is sent to the DB_m, and $\langle m_i, ID_i, ID_{sp} \rangle$ to the DB_{fd}.
        if *Is*ID_i *Exists AND Is*ID_{sp} *Exists* **then**
          The U_i is requested to enrol with a new PN_i and $UUID_{pn}$.
        else
          The records are encrypted using the Fernet, i.e., e_i=$E_u(k_i, l_i, ID_i, ID_{sp})$ and saved in the DB_m. While ID_i and m_i are encrypted using the Fernet, i.e., v_i=$E_u(ID_i, m_i)$ and saved in the DB_{fd}.
          A mobile money account is created with a balance of UGX 0 and a successful registration message is displayed for the U_i.
        end
      else
        Invalid BF data. Try to Scan Your Fingerprint Again.
      end
      $j \leftarrow e_i, v_i$
    else
      Try Again.
    end
    return j;
  end
End Function

Figure 24: Illustrates the algorithm for the enrolment phase

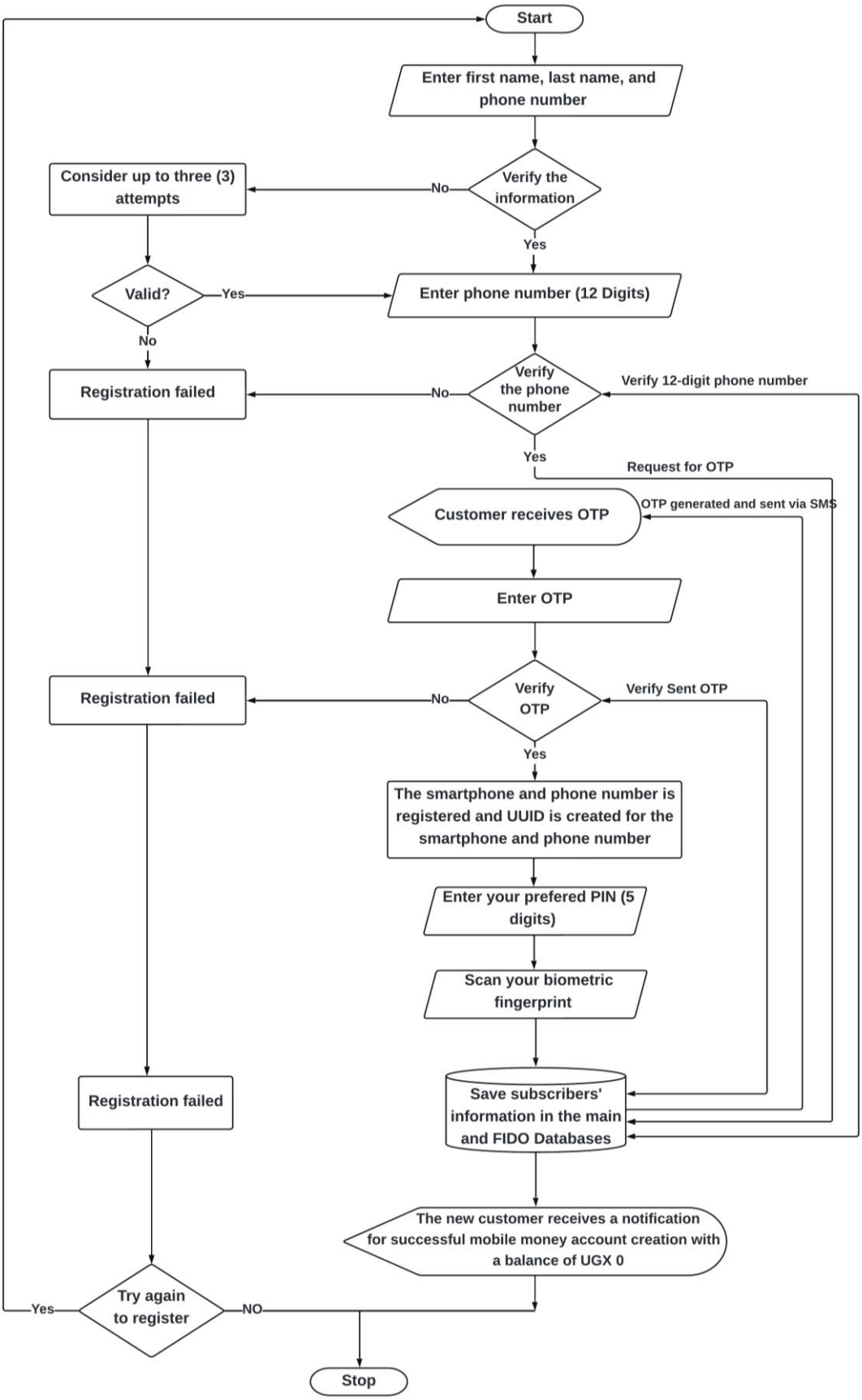


Figure 25: Flowchart for mobile money enrolment phase in the proposed algorithm

The authentication phase

The U_i follows the steps below during the authentication phase:

Step 1. The U_i must use their previously registered SP_i that matches the mobile money service acceptancy policy to run the G-MoMo Customer application and enter their five-digit PIN_i. It should be noted that the U_i can only attempt to login into the system three (3) times.

Step 2. The SP_i sends $w_i = \langle ID_i, ID_{sp}, PIN_i, Request \rangle$ to the DB_m for verification.

Step 3. The DB_m verifies whether the $ID_i, ID_{sp}, and\ PIN_i$ match. If not, the authentication is ended; else, OTP_i is generated and forwarded to the U_i through SMS, and a copy of the sent OTP_i is hashed using the SHA-256, $b_i = h(OTP_i)$, encrypted using Fernet, $E_u(b_i)$, and saved in the DB_m.

Step 4. The U_i is required to key in the received OTP_i. It should be noted that the OTP_i is only valid for 60 seconds.

Step 5. When the entered OTP_i does not match the stored copy in the DB_m, i.e., $E_u(b_i)$, the authentication is terminated; else, the mobile money service will challenge the U_i to log in by using their previously registered SP_i that matches the mobile money service acceptance policy by scanning their BF_i to verify their identity.

Step 6. If the BF_i is scanned successfully, the SP_i uses the U_i's account identifier (e.g., ID_i, $ID_{sp}, UUID_{pn}$) to choose the correct F_i and sign the challenge to confirm that the SP_i has the F_i. The SP_i sends the signed and encrypted challenge to the DB_{fd} for verification using the stored P_i.

Step 7. If the challenge is verified by the P_i, the U_i is successfully authenticated and signed in.

Algorithm 2 (Fig. 26) is for the mobile money customer authentication phase (27).

Algorithm 2: Authentication Phase

Input : PIN_i, OTP_i, BF_i
Output: w

Function `CustomerAuthentication`(PIN_i, OTP_i, BF_i)**:**
  $PIN \leftarrow PIN_i$
  $i \leftarrow 0$;
  while $i \leq 3$ **do**
    if $(PIN_i.length = 5)$ *AND* $(PIN = PIN_k)$ **then**
      Request for the generation of OTP_i,
      Send OTP_i to the U_i's SP_i,
      Hash the sent OTP_i using the SHA-256, y_i=$h(OTP_i)$, and encrypt it using Fernet, $E_u(b_i)$, and store $E_u(b_i)$, in the DB_m,
      Display the OTP_i for the U_i to read.
    else
      Invalid PIN, authentication terminated, and Try again.
    end if
    $OTP \leftarrow OTP_i$
    if $(OTP_i.length = 5)$ *AND* $(OTP\ isValid)$ **then**
      Scan the U_i's BF_i for recognition using the SP_i's Fingerprint Sensor.
    else
      Invalid OTP and authentication terminated.
    end if
    $BF \leftarrow BF_i$
    Scan the U_i's BF_i using the SP_i's Fingerprint Sensor.
    if $BF\ isValid$ **then**
      The SP_i uses the U_i's account identifier (e.g., ID_i, ID_{sp}, $UUID_{pn}$) to choose the correct F_i and sign the challenge to confirm that the SP_i has the F_i.
      The SP_i sends the signed and encrypted challenge to the DB_{fd} for verification using the stored P_i.
      If the challenge is verified, the U_i is successfully authenticated and signed in.
    else
      Invalid BF_i and authentication terminated. The U_i Must Scan their BF_i Again.
    end if
    return w;
  end while
End Function

Figure 26: Illustrates the algorithm for the authentication phase

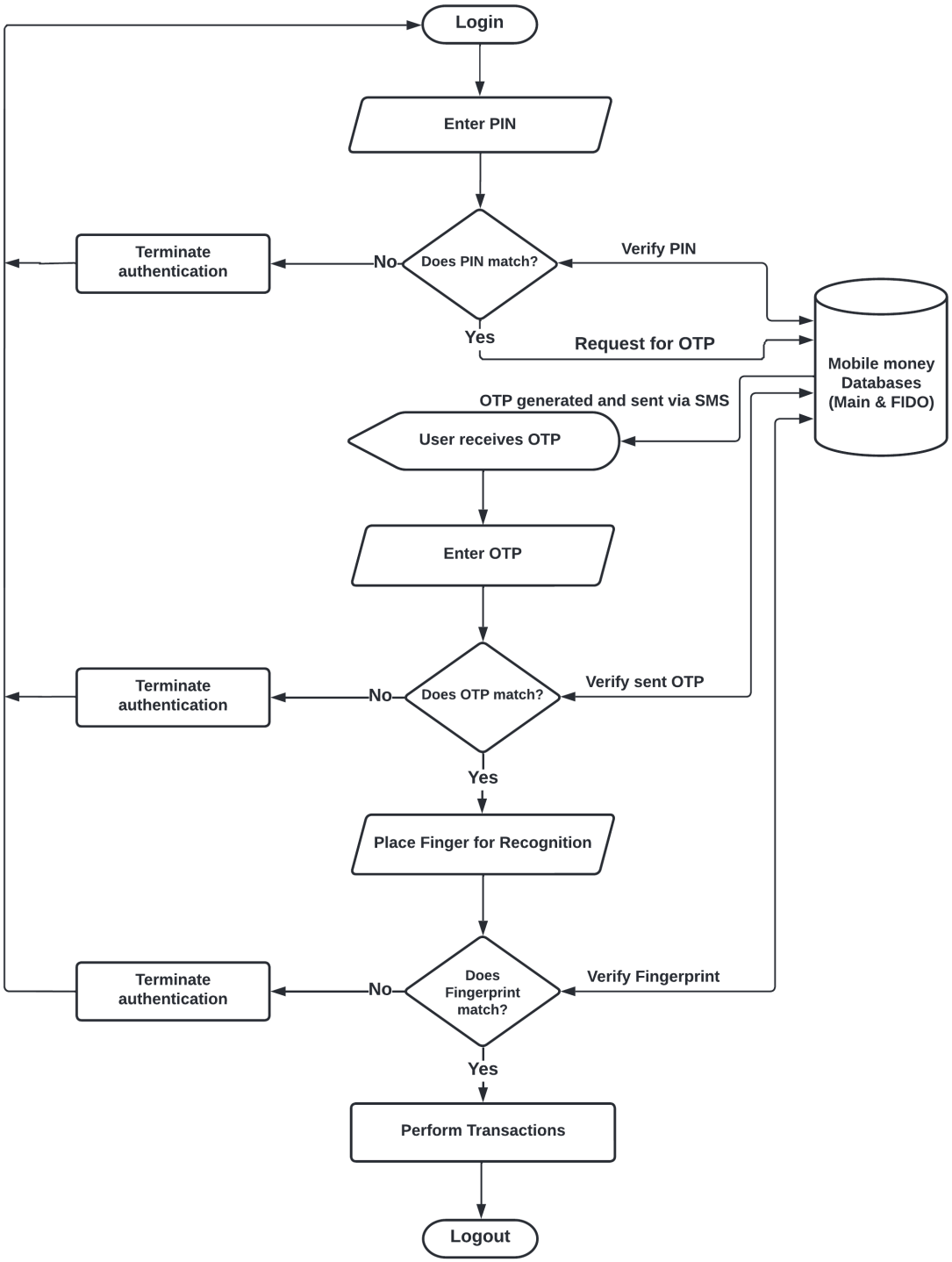


Figure 27: Flowchart for mobile money authentication phase in the proposed algorithm

The transaction phase

For U_i to withdraw money from their mobile wallet, they must adhere to the following steps:

Step 1. The U_i begins the money withdrawal transaction by signing in to the G-MoMo Customer Application by entering their PIN_i, OTP_i, and BF_i.

Step 2. If the PIN_i, OTP_i, and BF_i are verified, the U_i is successfully logged in; Otherwise, the authentication is terminated.

Step 3. If the U_i wants to perform a transaction, e.g., withdraw money, they must make sure that their available $Bal_i \geq 5000$, and must enter an $Amt_i \leq Bal_i$.

Step 4. The system will then challenge the U_i to confirm the transaction by scanning their BF_i using their previously registered SP_i that matches the mobile money service acceptance policy.

Step 5. If the BF_i is scanned successfully, the SP_i uses the U_i's account identifier (e.g., ID_i, $ID_{sp}, UUID_{pn}$) to choose the correct F_i and sign the challenge to prove that the SP_i has the F_i. The SP_i sends the signed and encrypted challenge to the DB_{fd} for verification using the stored P_i. If the challenge is verified by the P_i, the transaction is confirmed.

Step 6. Then the U_i is again requested to scan the A_a's secure $QRcode_i$ for authorisation purposes by using the smart scanner. Note that, $QRcode_i$ contains the A_a's encrypted UUID.

Step 7. If the A_a's UUID encoded in $QRcode_i$ matches with the copy stored in the database, the money is withdrawn, and the U_i's Bal_i is updated in the database. The system will then display a message showing money withdrawn successfully and request the U_i to collect the cash from the A_a.

Algorithm 3 (Fig. 28) is for the transaction phase (money withdrawal [Fig. 29]).

Algorithm 3: Transaction Phase (Withdraw Money)

Input : $PIN_i, OTP_i, BF_i, Bal_i, Amt_i, QRcode_a$
Output: z

Function `Transaction`$(PIN_i, OTP_i, BF_i, Bal_i, Amt_i, QRcode_a)$**:**
  $identifier \leftarrow PIN_i, OTP_i, BF_i$
  $i \leftarrow 0$;
  while $i \leq 3$ **do**
    if $IsIdentifierValid$ **then**
      The U_i successfully signs in and the system checks for the U_i's available Bal_i.
    else
      Invalid PIN_i, OTP_i, and BF_i.
    end if
    if $(Bal_i \geq 5000)$ **then**
      Enter the Amt_i to withdraw.
    else
      Insufficient Bal_i.
    end if
    $Amt \leftarrow Amt_i$
    if $(Amt \leq Bal_i)$ **then**
      Scan U_i's BF_i for authorisation.
      $BF \leftarrow BF_i$
      if $BF\ isValid$ **then**
        The SP_i uses the U_i's account identifier (e.g., ID_i, ID_{sp}, $UUID_{pn}$) to choose the correct F_i and sign the challenge to confirm that the SP_i has the F_i.
        The SP_i sends the signed and encrypted challenge to the DB_{fd} for verification using the stored P_i.
        If the challenge is verified, the transaction is confirmed.
        Scan the A_a's secure $QRcode_a$ for confirmation.
      else
        Invalid BF_t and transaction terminated.
      end if
      $QR \leftarrow QRcode_a$
      if $QR\ isValid$ **then**
        Withdraw money from U_i's account, Update the remaining U_i's Bal_i, and the Successful money withdrawn message is displayed for the U_i.
        $z \leftarrow Bal_i$
      else
        Invalid $QRcode_a$.
      end if
    else
      Insufficient Bal_i and transaction terminated.
    end if
    return z;
  end while
End Function

Figure 28: Illustrates the algorithm for the transaction phase (i.e., money withdrawal)

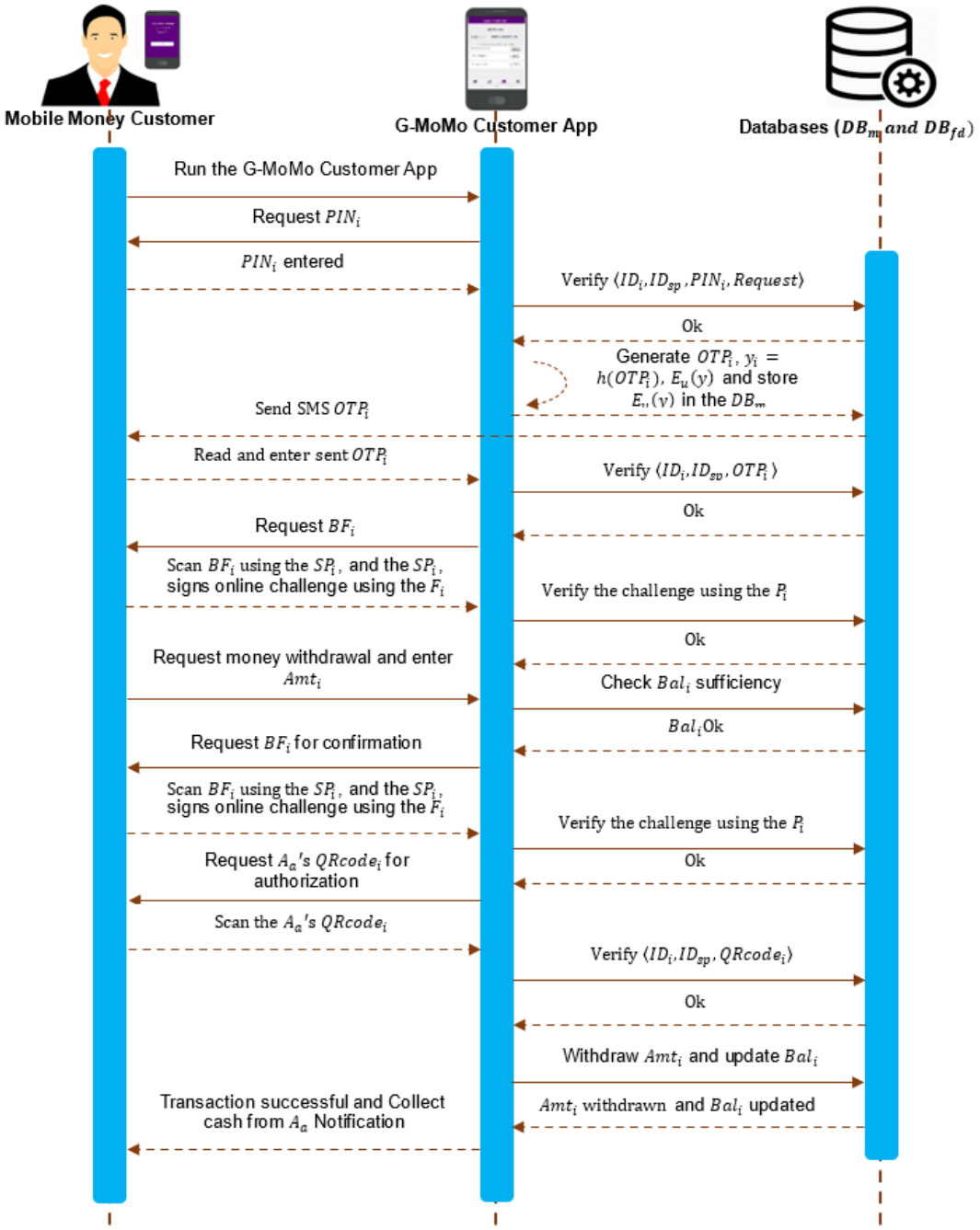


Figure 29: Sequence diagram for the transaction phase (money withdrawal) in the proposed algorithm

4.1.5 System overview

(i) System development approach

The evolutionary prototyping model was adopted in this research to develop the prototypes of the native G-MoMo applications. Sherrell (2013) and Guerrero-García (2014) define evolutionary prototyping as a software development approach where the developers create a prototype for customers to get feedback which is then used to develop subsequent prototypes with added functionality until a final product is built and accepted by the customers. The prototypes were

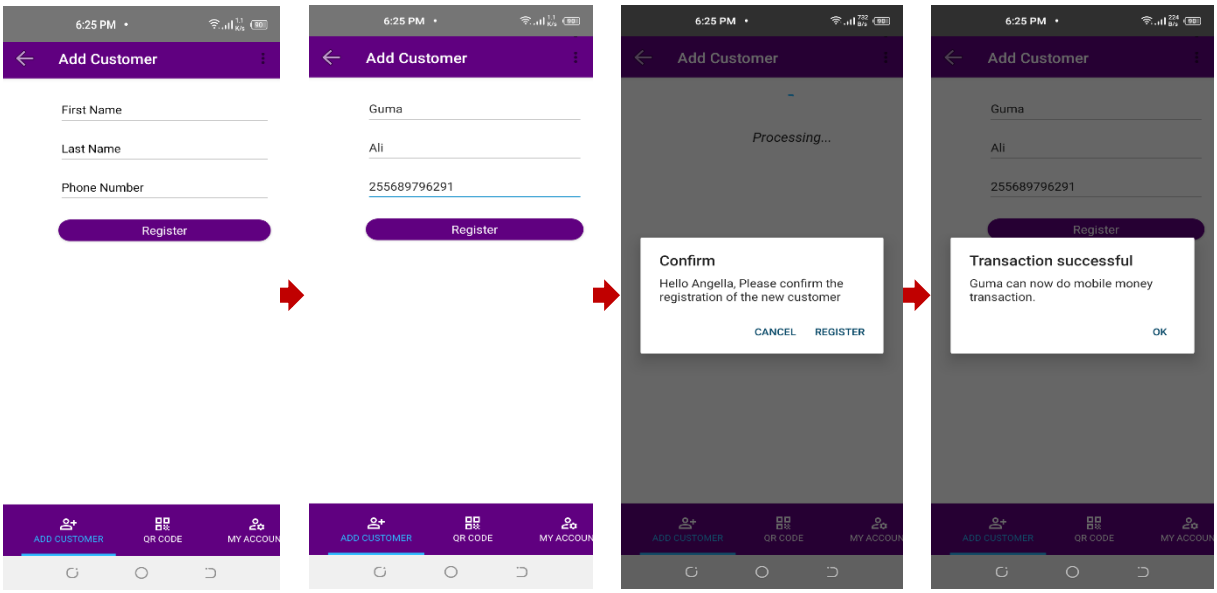
incrementally and iteratively developed, and the final product was engineered (Carter *et al*., 2001; Pretschner *et al*., 2001; Adarsh *et al*., 2017). The primary purpose of using the evolutionary prototyping model in this study was to develop robust prototypes in a structured manner that are constantly updated. The evolutionary prototyping model involves: (a) the system requirement collection and analysis, (b) rapid designing, (c) developing the working prototypes, (d) initial customer evaluation, (e) improving the prototypes, (f) implementing the final products, and (g) maintaining the products (Carter *et al*., 2001; Guerrero-García, 2014; Bai, 2014). The evolutionary prototyping approach improves the flexibility of the system prototypes, helps to save time and effort during software development, allows developers to concentrate on the main functionalities of the system that they understand, and increase user requirement satisfaction since customers are involved throughout the development process (Chen & Huang, 2002; Xiaoshuan *et al*., 2009; Guerrero-García, 2014; Adarsh *et al*., 2017). The researchers adopted it because some of the system requirements were unclear and required customer feedback, and it reduces severe and critical flaws during the system testing (Carter *et al*., 2001). Additionally, the evolutionary prototyping model helps reduce software errors, and new requirements can easily be added. It is also used in complex projects where the functionalities must be checked and in projects that use new technology the developers do not understand sufficiently.

4.1.6 The implementation of the native G-MoMo applications

The three (3) native G-MoMo applications (i.e., G-MoMo IT Support Application, G-MoMo Agent Application, and G-MoMo Customer Application) were developed for mobile money IT support staff, agents, and customers, respectively. The prototypes are organised into five (5) sections, namely, the enrolment phase, authentication phase, transaction (e.g., deposit money, withdraw money, and send money) phase, account management (i.e., changing the PIN and biometric fingerprint), and logout.

(i) Customer enrolment phase

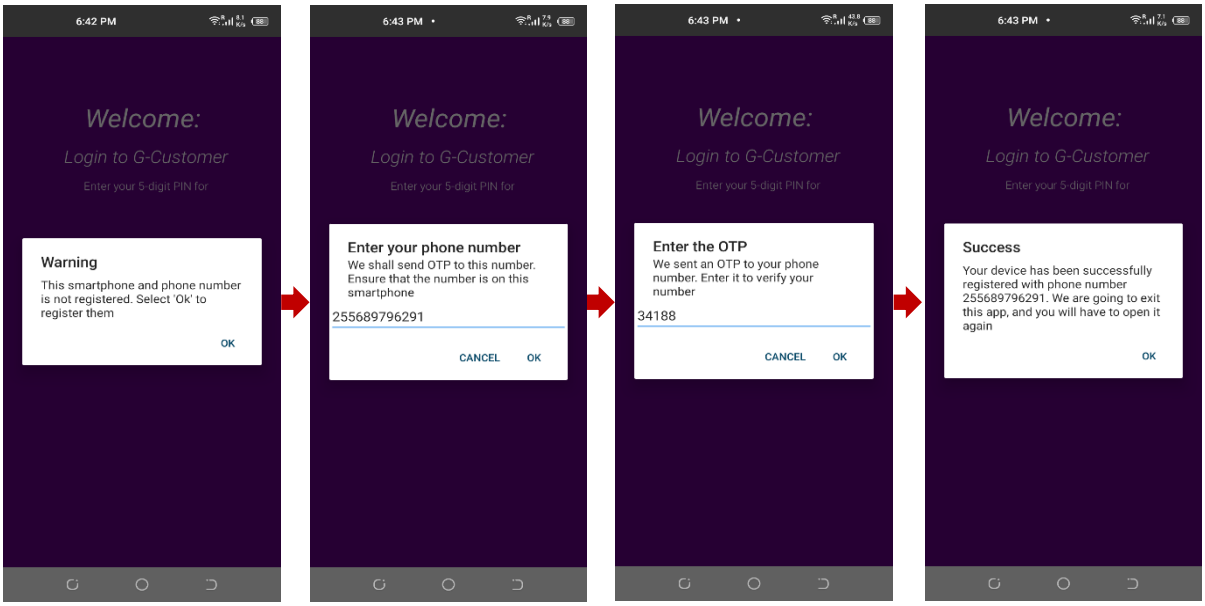
For a registered mobile money agent to enrol a new mobile money customer, they must run the G-MoMo Agent Application and successfully log into the G-MoMo Agent Application and click add customer tab, where they are required to enter the new customer's first name, last name, and phone number and verify the details. Once the details are verified, they are encrypted with Fernet and saved in the main database. Figure 30(a)–(d) illustrates the steps the mobile money agent follows to enrol a new mobile money customer using the G-MoMo Agent Application.



(a) (b) (c) (d)

Figure 30(a)–(d): Illustrates the steps the mobile money agent follows to enrol a new mobile money customer using the G-MoMo Agent Application

When the newly registered customer runs the G-MoMo Customer Application for the first time, they are requested to register their smartphone and phone number. The mobile money customer must enter their phone number, which will be used to receive the sent OTP and make sure that the phone number is active in the smartphone. The OTP is generated and sent to the phone number and a copy of the sent OTP is hashed using SHA-256, encrypted with Fernet, and saved in the database. Once the mobile money customer receives the OTP, they must enter it to verify their phone number. If the OTP is verified, the smartphone and phone number are registered, and a UUID is created for the phone number and smartphone, encrypted with Fernet and saved in the main database. Otherwise, the smartphone and phone number are not registered, and a UUID is not created. Figure 31(a)–(d) illustrates the steps the mobile money customer must follow to register the smartphone and phone number using the G-MoMo Customer Application.



(a) (b) (c) (d)

Figure 31(a)–(d): Illustrates the steps the mobile money customer must follow to register the smartphone and phone number using the G-MoMo Customer Application

Once the new mobile money customer's smartphone and phone number are registered, the customer is requested to complete the registration process by re-running the G-MoMo Customer Application using their smartphone connected to the internet. When the G-MoMo Customer Application runs successfully, the system will request them to enter a five (5)-digit PIN and confirm the 5-digit PIN. If the entered 5-digit PIN and re-entered 5-digit PIN do not match, the PIN is rejected; otherwise, the 5-digit PIN is hashed using SHA-256 and encrypted with Fernet and saved in the main database. The mobile money customer is requested to scan their biometric fingerprint using the smartphone fingerprint scanner that matches the mobile money service acceptance policy. A new public-private key pair unique for the smartphone, mobile money, and customer's account is created when the customer scans their fingerprint successfully. The public key is encrypted with the RSA and again encrypted with Fernet and stored in the FIDO database. While the private key and fingerprint template are encrypted with RSA and stored in the customer's smartphone. After successful enrolment, a mobile money account is created with a balance of UGX 0 and a notification message is displayed to the new mobile money customer. Figure 32(a)–(g) illustrates the steps the mobile money customer must follow to complete the enrolment process using the G-MoMo Customer Application.

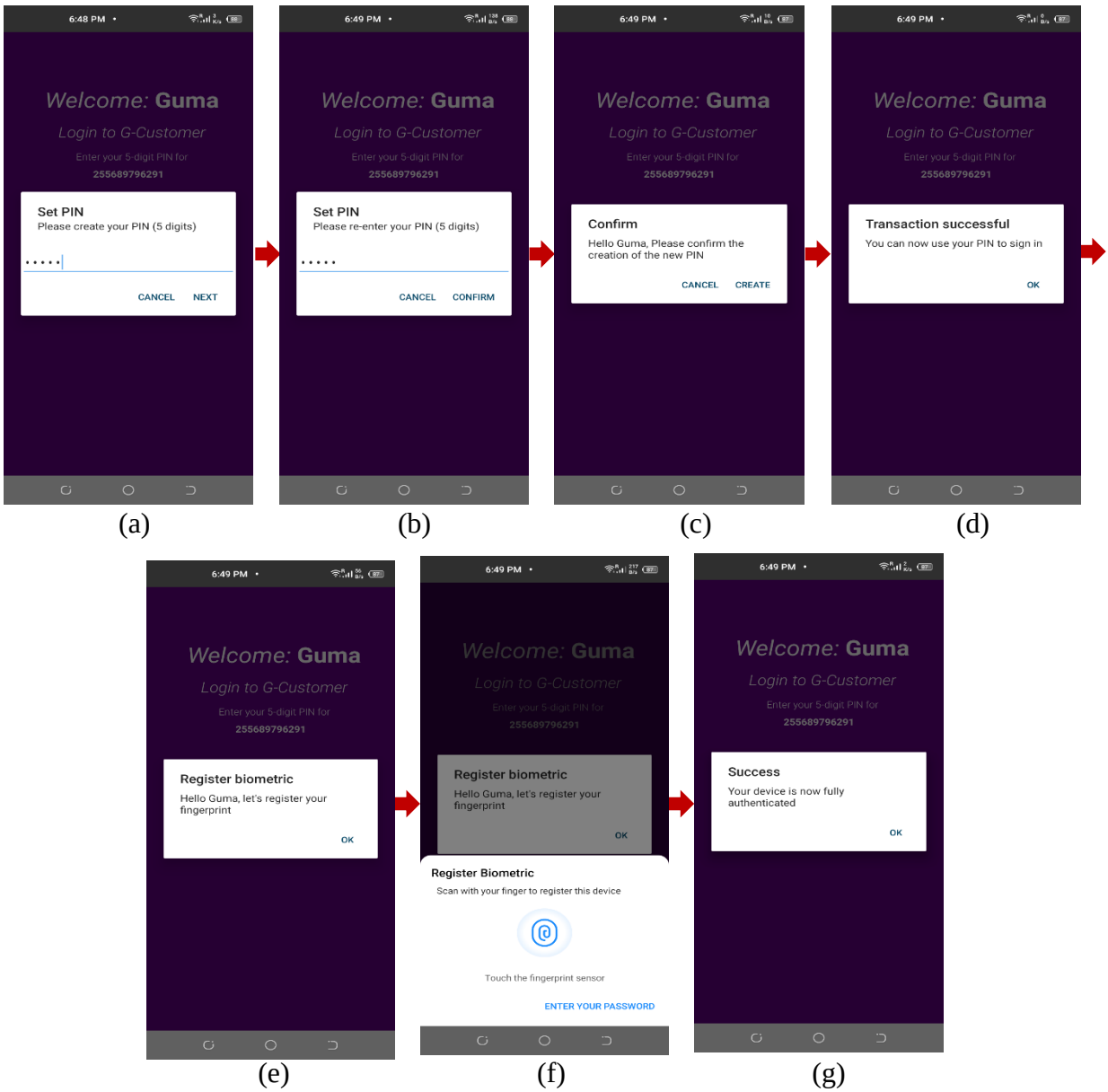
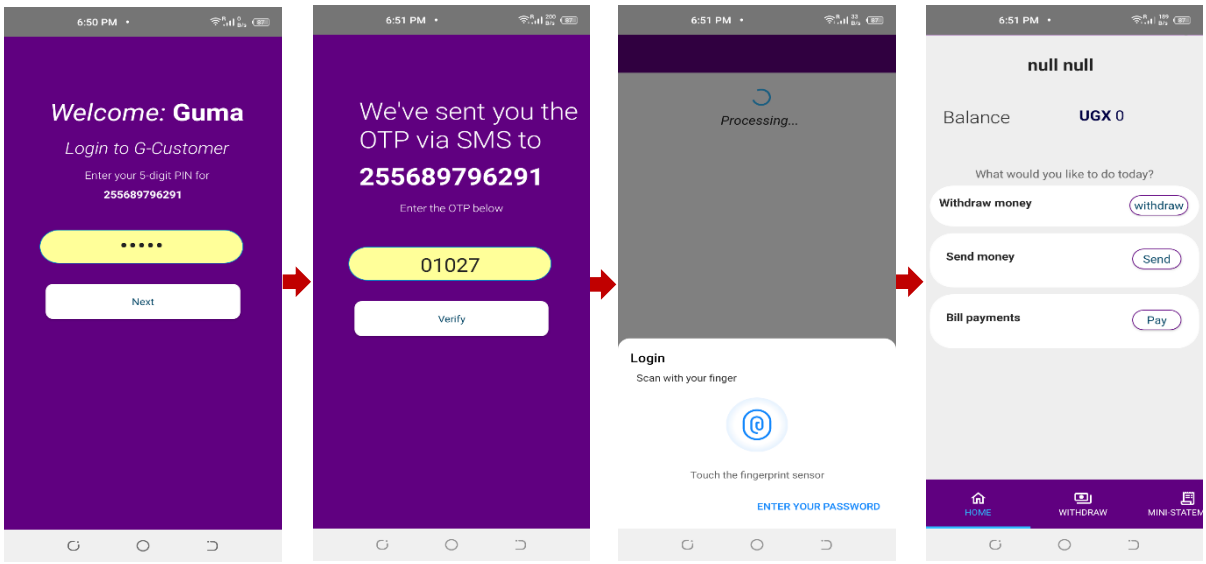


Figure 32(a)–(g): Illustrates the steps the mobile money customer must follow to complete the enrolment process using the G-MoMo Customer Application

(ii) Customer authentication phase

For the registered mobile money customer to perform a transaction, they must log in to the G-MoMo application by entering their 5-digit PIN. If the entered PIN is verified, OTP will be generated and forwarded to the customer's smartphone. A copy of the sent OTP is hashed using SHA-256, encrypted with Fernet, and saved in the main database. The customer must enter the received OTP, which will be verified, and if it is correct, the customer will be requested to scan their biometric fingerprint for verification using the previously registered smartphone that matches the mobile money service acceptancy policy. The scanned biometric fingerprint will be verified, and if it matches, the customer will be authenticated and can now perform a transaction;

else authentication process will be terminated. Figure 33(a)–(d) illustrates the steps the mobile money customer follows to log into the G-MoMo Customer Application.



(a) (b) (c) (d)

Figure 33(a)–(d): Illustrates the steps the mobile money customer follows to log into the G-MoMo Customer Application

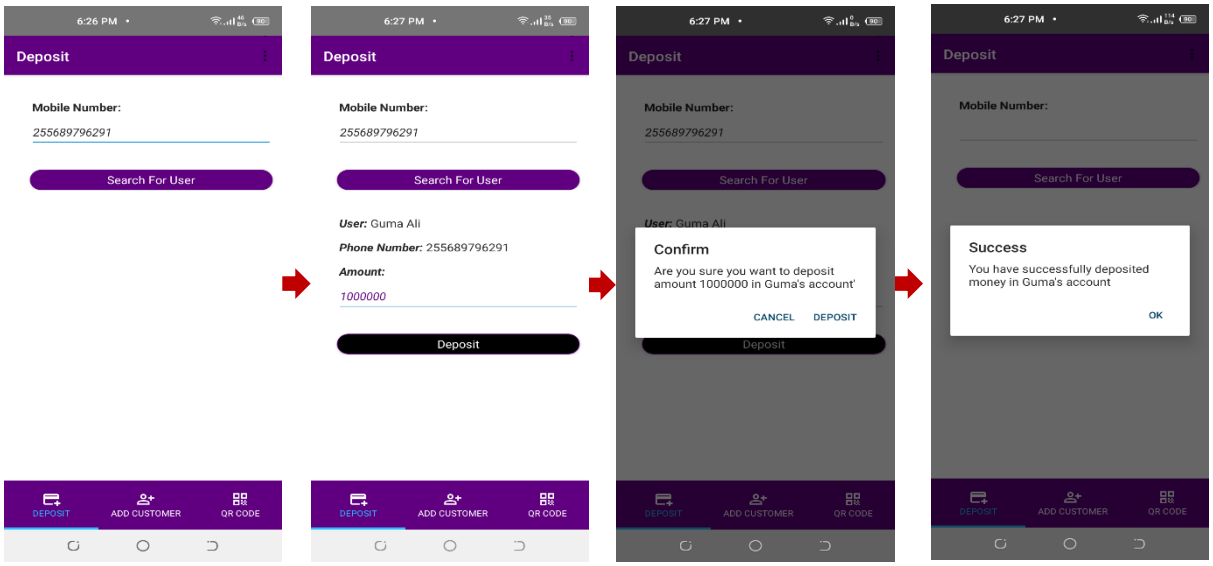
(iii) Transaction phase

The transaction phase is explained using the money deposit, withdrawal, and send money functionalities. For the G-MoMo Agent Application, the deposit money functionality allows mobile money agents to deposit money into mobile money customers' accounts, and mobile money customers can withdraw and send money using the G-MoMo Customer Application.

Money deposit

For the mobile money agent to deposit money into a mobile money customer's account, they must run the G-MoMo Agent Application and log into the system by key-in their PIN, OTP, and biometric fingerprint. The system will then verify the authentication factors, and if they match, the mobile money agent is successfully logged in. Before performing the deposit transactions, the mobile money agent must check their available electronic balance and ensure that it is more than the amount to be deposited into the customer's account. The mobile money agent will enter the recipient's phone number and search to verify whether the recipient is registered with the G-MoMo Customer Application. If the recipient's phone number is registered, the system will display the recipient's name and phone number. It will then request the mobile money agent to enter the amount they wish to deposit into the mobile money customer's account and click the deposit button. The system will verify whether the entered amount is less than the available

electronic balance and if it is yes, the money will be transferred from the mobile money agent's account to the mobile money customer's account. The accounts will be updated, and the message for successful money deposited will be displayed. Figure 34(a)–(d) illustrates the steps the mobile money agent follows to deposit money into a customer's account using the G-MoMo Agent Application.



(a) (b) (c) (d)

Figure 34(a)–(d): Illustrates the steps the mobile money agent follows to deposit money into the mobile money customer's account using the G-MoMo Agent Application

Money withdrawal

If the mobile money customer requests to withdraw money from their electronic wallet, they must first log in and check their available electronic balance. If they have money, they can enter any amount less than the available balance and click withdraw button. The system will request them to scan their fingerprint for authorisation. The scanned fingerprint will be matched, and if it is correct, the mobile money customer is required to scan the agent's QR code to confirm the money withdrawal. When the QR code is confirmed, the money is withdrawn from the account, the electronic balance is updated, and a successful money withdrawal notification authorising the customer to collect money from the agent is presented. Figure 35(a)–(g) illustrates the steps followed by the mobile money customer to withdraw cash from their e-wallet using the G-MoMo Customer Application.

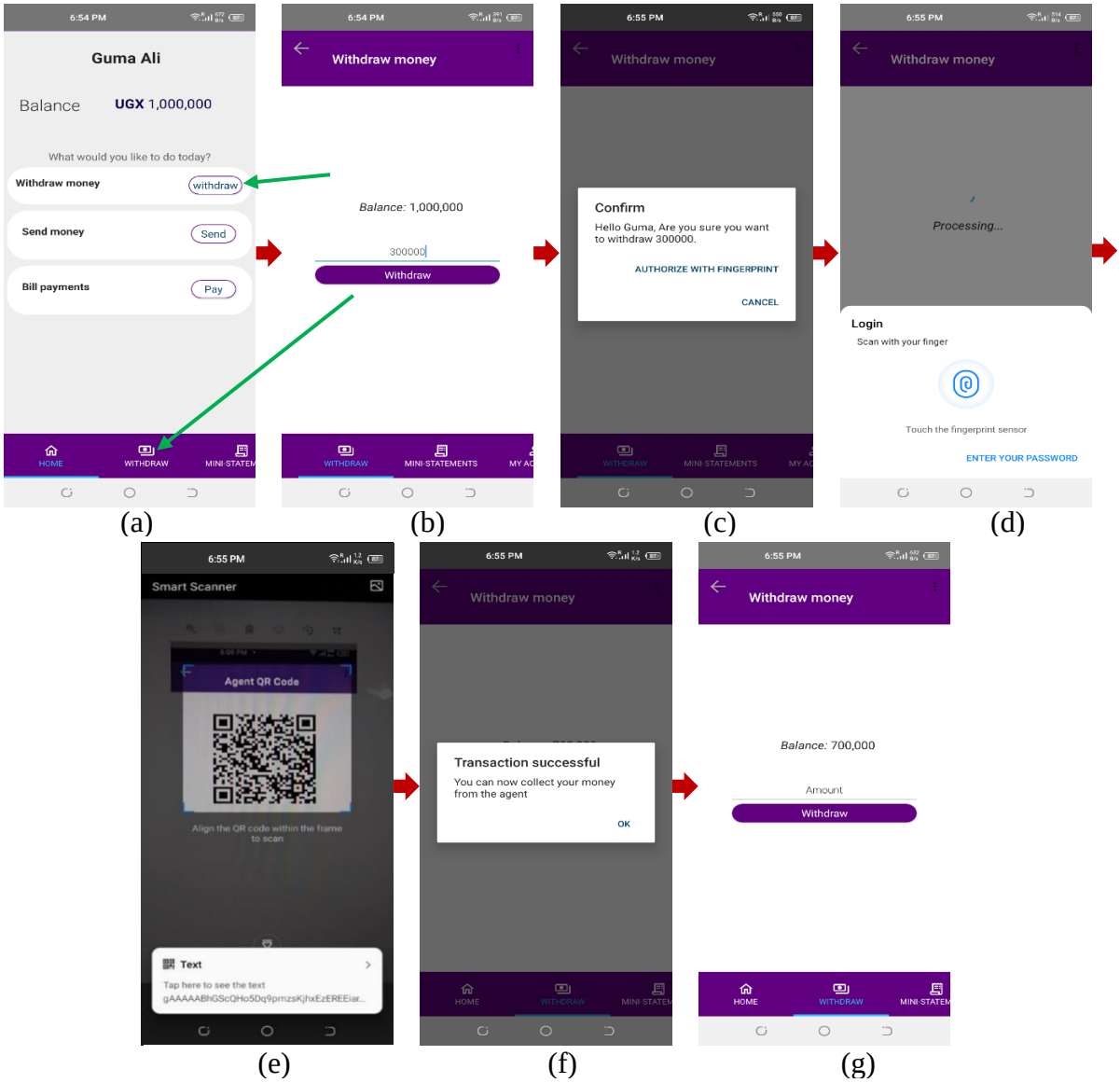


Figure 35(a)–(g): Illustrates the steps followed by the mobile money customer to withdraw money from their e-wallet using the G-MoMo Customer Application

Send money

For the mobile money customer to send money to a registered customer, they must first log in and check their available electronic balance. If they have money, they can enter the recipient's phone number and amount. Note that the amount entered must be less than or equal to the available balance, and click send button. The system will request them to scan their biometric fingerprint for confirmation. If the fingerprint is verified, the money is sent, and the sender's and recipient's electronic balances are updated. A successful transaction message is displayed to the sender. Figure 36(a)–(g) illustrates the steps followed by the mobile money customer to send money to a fellow customer using the G-MoMo Customer Application.

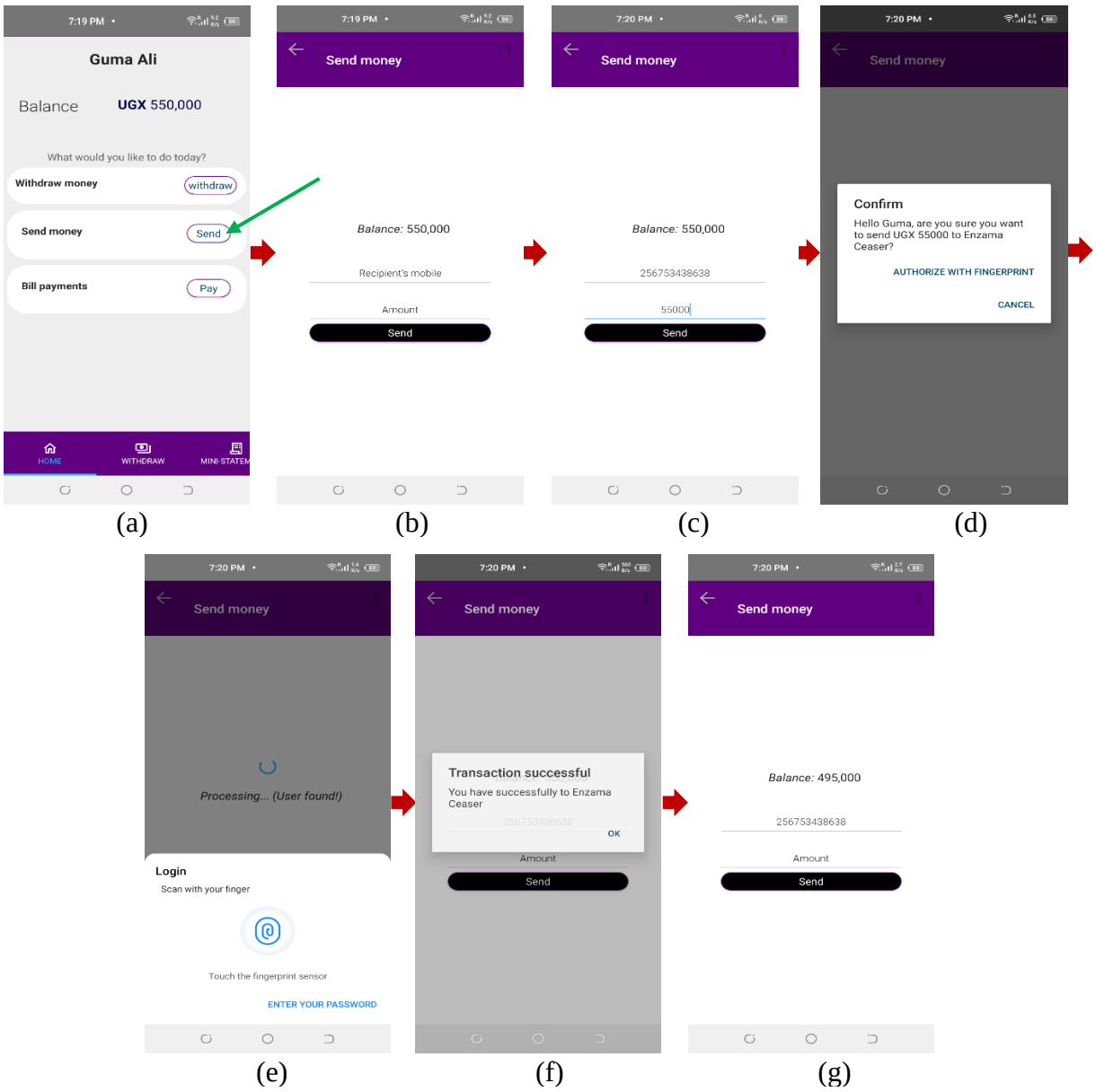


Figure 36(a)–(g): Illustrates the steps followed by the mobile money customer to send money to a fellow customer using the G-MoMo Customer Application

(iv) Account management

It is a requirement that mobile money subscribers must regularly change their mobile money PINs and biometric fingerprints for security reasons.

Changing the PIN

When mobile money customers want to change their mobile money PIN, they must log in, select the account management page, where they are required to enter their current 5-digit PIN and new 5-digit PIN and click the change PIN button. The system will request them to scan their fingerprint for authorisation. A successful PIN change message is displayed if the scanned fingerprint

matches the one used for authentication. Figure 37(a)–(e) shows the steps followed by the mobile money customer to change their PIN.

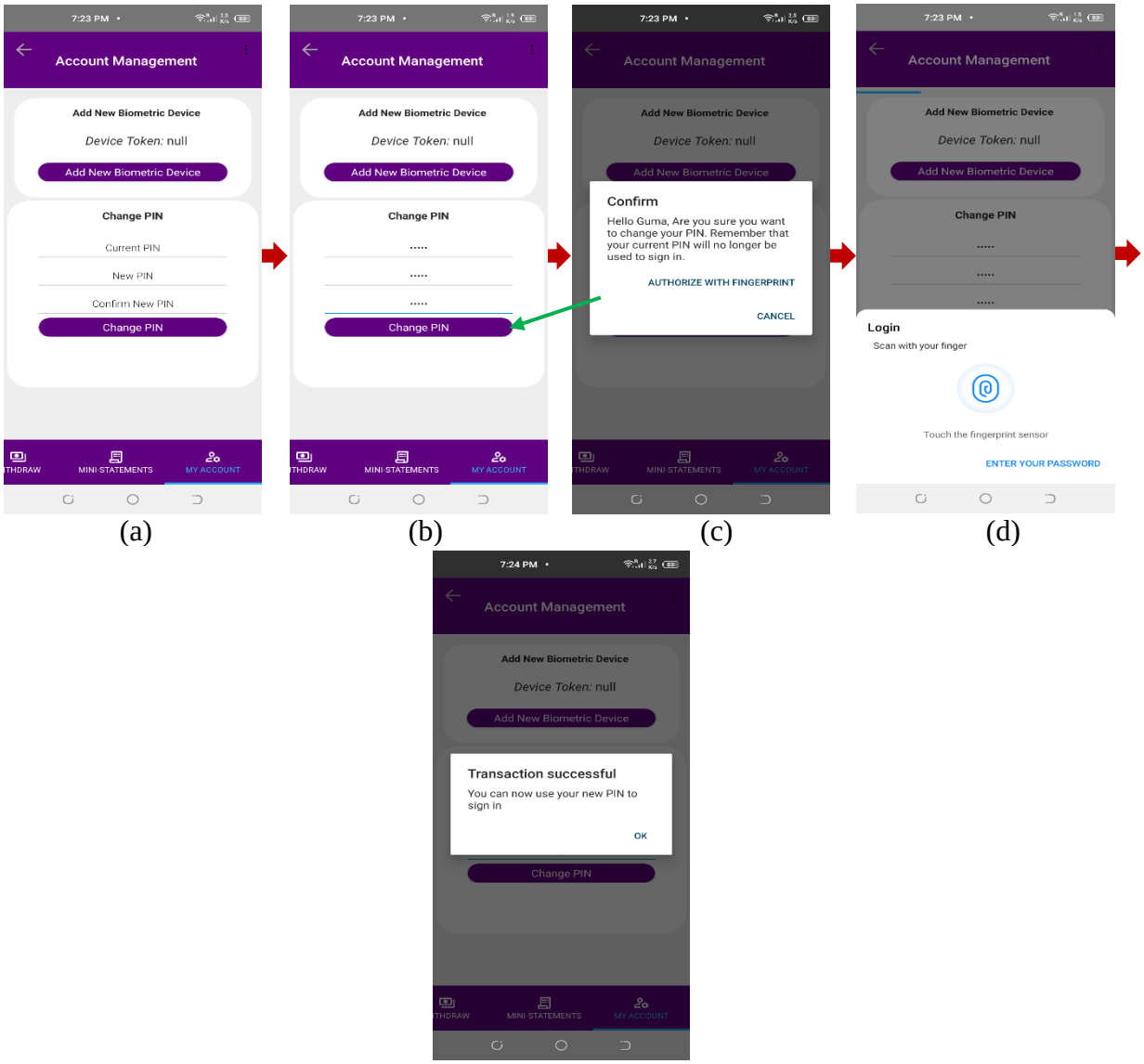


Figure 37(a)–(e): Illustrates the steps followed by mobile money customers to change their

Changing the biometric fingerprint

Suppose mobile money customers want to change their biometric fingerprints. They must log in, select the account management page, and click the change fingerprint button where they are requested to scan their fingerprint, and a device token is generated, which is required when changing the biometric fingerprint. The G-MoMo Customer Application will authorise a new device, and then it requests the mobile money customer to verify the new device by entering the device token generated. If the device token is verified, the system will ask the customer to scan their new biometric fingerprint to register the device. If the biometric fingerprint is captured, a

message showing that their biometric details have been successfully registered is displayed. The customer must log in using the new biometric fingerprint. Figure 38(a)–(h) shows the steps followed by the mobile money customer to change their biometric fingerprint using the G-MoMo Customer Application.

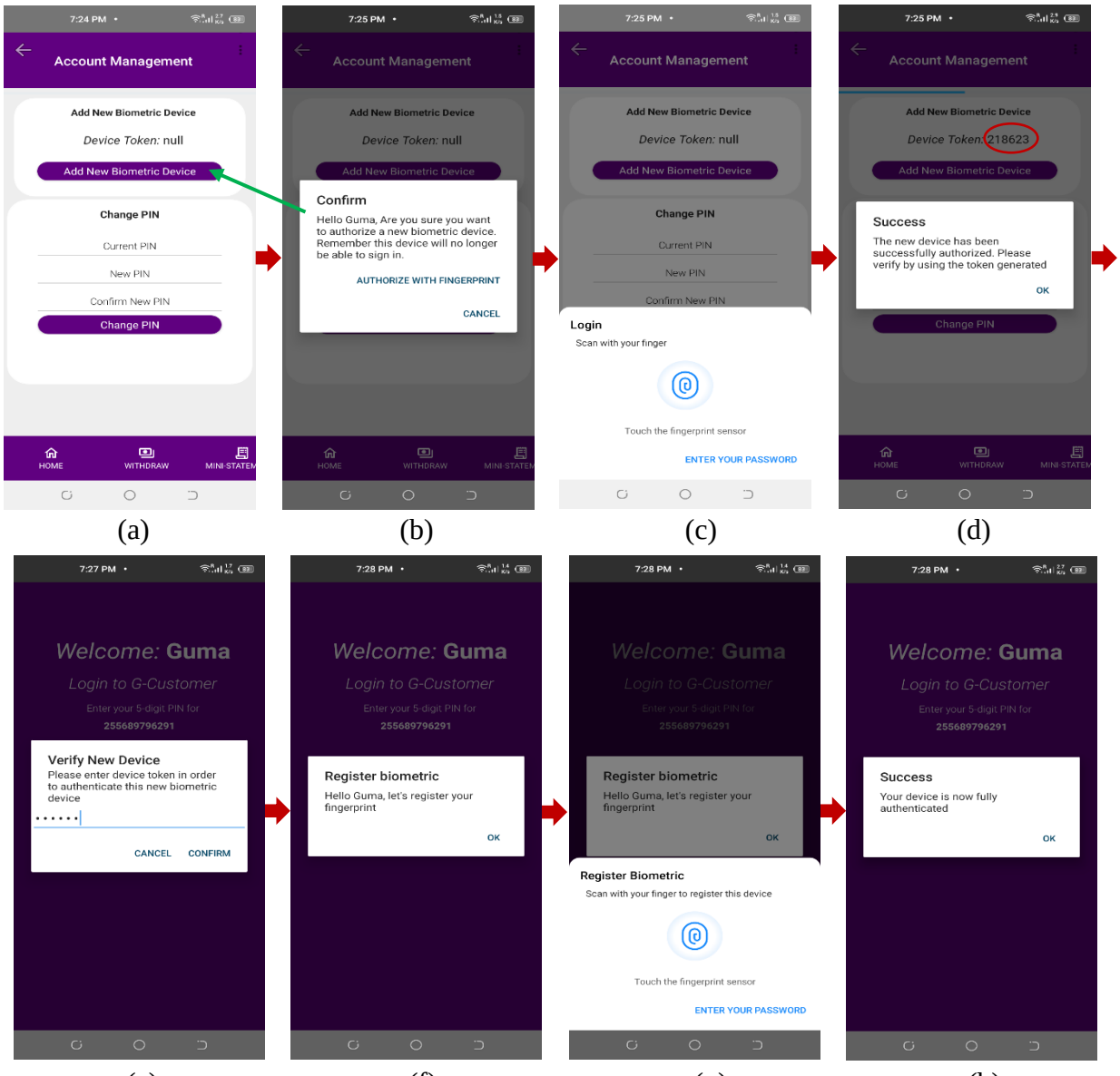


Figure 38(a)–(h): Illustrates the steps followed by the mobile money customer to change their biometric fingerprint change using the G-MoMo Customer Application

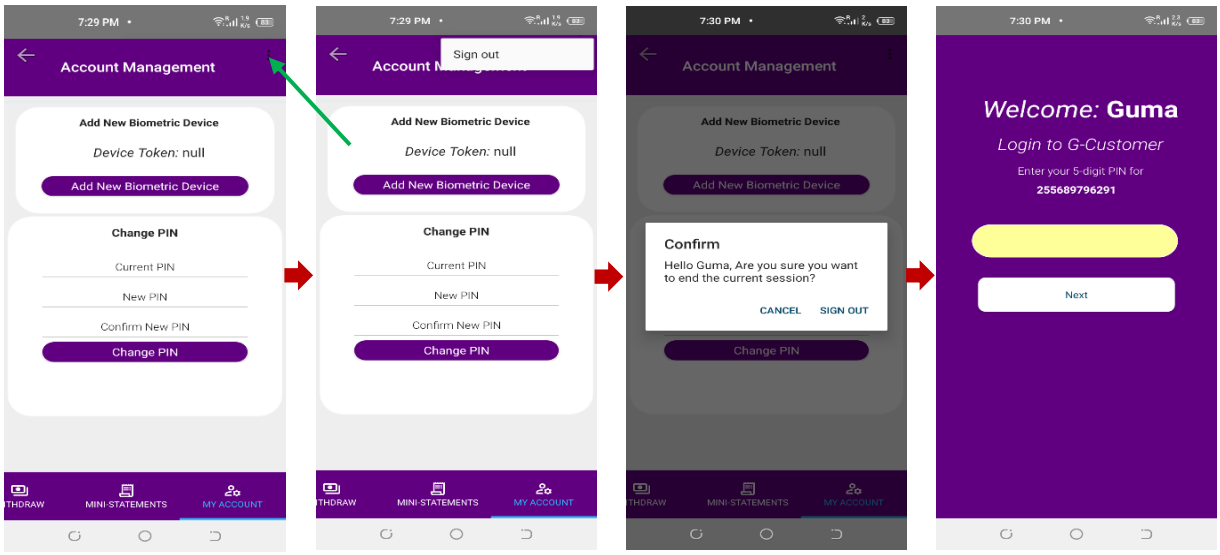
Secured customer detail storage

Figure 39 shows the details of mobile money customers in the customer table encrypted with Fernet.

Figure 39: Displays the details of customer in the customer table encrypted with

(v) System logout

After performing transactions, if the mobile money customer wants to log out, they can click the sign-out, and the system will request them to confirm by clicking the Sign-out. If they confirm signing out, the system will log them out. Figure 40(a)-(d) illustrates the steps the mobile money customers must follow to sign out of the G-MoMo Customer Application.



(a) (b) (c) (d)

Figure 40(a)–(d): Illustrates the steps the mobile money customers must follow to sign out of the G-MoMo Customer Application

4.1.7 System validation results

(i) Performance analysis of the proposed secure MFA algorithm using the communication overhead and computational cost

There was a need to evaluate the proposed secure MFA algorithm's performance by analysing the communication overhead and computational cost, which helped to understand the algorithm's

efficiency. The performance comparison was based on the proposed algorithm's enrolment, authentication, and transaction phases and compared it with other existing related algorithms.

Communication overhead

Communication overhead in the proposed algorithm is related to calculating the number of bytes in each message exchanged during communications in the three phases, i.e., enrolment, authentication, and transaction (Ali *et al*., 2021). Every message packet size is computed by adding the bytes for each message transmitted using the information in Table 16.

Table 17: The sum of the byte sizes for messages interchanged during mobile money subscriber enrolment, authentication, and transaction phases

Phase	Message Content	Message Size (bytes)
Enrolment	$\{FN_i, LN_i, PN_i\}$	16 + 16 + 16 = 48 bytes
	$\{PN_i, OTP_i\}$	16 + 8 = 24 bytes
	$\{PIN_i, PIN_j\}$	8 + 8 = 16 bytes
	$\{PIN_k, P_i, ID_i, ID_{sp}\}$	16 + 32 + 8 + 8 = 64 bytes
	$\{FN_i, LN_i, PN_i, PN_i, OTP_i$ $PIN_k, P_i, ID_i, ID_{sp}\}$	16 + 16 + 16 + 16 + 8 + 16 + 32 + 8 + 8 = 136 bytes
Authentication	$\{ID_i, ID_{sp}, PIN_i\}$	8 + 8 + 8 = 24 bytes
	$\{ID_i, OTP_i\}$	8 + 8 = 16 bytes
	$\{ID_i, ID_{sp}, OTP_i\}$	8 + 8 + 8 = 24 bytes
	$\{BF_i(F_i, B_t)\}$	16 + 32 + 16 = 64 bytes
	$\{ID_i, ID_{sp}, P_i\}$	8 + 8 + 32 = 48 bytes
Transaction	$\{ID_i, Bal_i\}$	8 + 16 = 24 bytes
	$\{ID_i, Amt_i\}$	8 + 16 = 24 bytes
	$\{BF_i(F_i, B_t)\}$	16 + 32 + 16 = 64 bytes
	$\{ID_i, ID_{sp}, P_i\}$	8 + 8 + 32 = 48 bytes
	$\{ID_i, QRcode_i\}$	8 + 16 = 24 bytes
	$\{ID_i, ID_{sp}, QRcode_i\}$	8 + 8 + 16 = 48 bytes

The results in Table 17 show that seventeen (17) messages were exchanged during mobile money subscriber enrolment, authentication, and transaction phases. Therefore, communication overhead is computed by adding the bytes of the messages exchanged, excluding the byte sizes of cryptographic techniques. The proposed algorithm had a total of 696 bytes of messages exchanged. Therefore, it was concluded that the proposed algorithm had high communication

overhead when compared with other related algorithms proposed (Islam *et al*., 2019; Vincent *et al*., 2020; Mega, 2020; Suwera, 2021). This slightly reduced the algorithm's performance but provided strong security against various security attacks (Zhao *et al*., 2016).

Computational cost

Computational cost is the time taken by network devices to execute asymmetric encryption, symmetric encryption, and secure hashing (ElGhanam *et al*., 2021). It is also known as computation time. In the proposed algorithm, the total computational cost was calculated for each phase (i.e., authentication and transaction) by analysing the sequence of messages exchanged and compared with the total computation time for each step in the algorithm (Ray *et al*., 2016), as shown in Fig. 29 and Table 18. While comparing the computational cost of the proposed algorithm, the symbol T_h represented the time required for secure hashing using SHA-256, T_{Re} *and* T_{Rde} denoted the time required by RSA to encrypt & decrypt public/private key pair and fingerprint template, and $T_{F\varepsilon}$ and $T_{Fd\varepsilon}$ represented the time required for encrypting and decrypting messages using Fernet. For the algorithm proposed by Ray *et al*. (2016), the symbols T_h denoted the time required for a hashing operation with SHA-1 and T_{ECC} represented the time required to perform encryption & decryption operations using the ECC-160.

The researchers considered the algorithms proposed by Ray *et al*. (2016) for a computational cost comparison because they implemented a one-way hash function to ensure information security using SHA-1 and ECC-160 for encryption and decryption. However, the algorithms of Islam *et al*. (2019) and Suwera (2021) were never considered for comparison purposes because they did not implement cryptographic techniques. Nevertheless, there was a difference between the proposed algorithm and the algorithm by Ray *et al*. (2016) regarding the enrolment, authentication, and transaction phases, thus prompting computational cost comparison.

Table 18: Calculation of the computational cost for the authentication and transaction phases

Algorithm	Authentication Phase	Transaction Phase
Proposed Algorithm	$3T_h + 1T_{Fd\varepsilon} + 3T_{Rde} + 1T_{F\varepsilon}$	$2T_{Fd\varepsilon} + 1T_{Rde} + 1T_{Fd\varepsilon} + 1T_{F\varepsilon}$
Ray *et al*. (2016)	$2T_h + 1T_{ECC}$	$2T_h + 3T_{ECC}$

The computational cost for the proposed algorithm was higher than the algorithm by Ray *et al*. (2016) because our algorithm implemented asymmetric encryption (RSA), symmetric encryption (Fernet), and secure hashing (SHA-256) to protect the authentication factors and confidential financial information. However, the algorithm by Ray *et al*. (2016) only used asymmetric

encryption (ECC) and secure hashing (SHA-1) to secure the information. Table 19 compares the computational cost of the proposed algorithm with the existing algorithm (Ray *et al*., 2016).

Table 19: Comparison of the computational cost for the proposed Secure MFA algorithm for mobile money application with the existing algorithm by Ray *et al*. (2016)

Proposed Algorithm	Authentication Phase	Transaction Phase	Total
Our Algorithm	$3T_h + 1T_{Fd\varepsilon} + 3T_{Rde} + 1T_{F\varepsilon}$	$2T_{Fd\varepsilon} + 1T_{Rde} + 1T_{Fd\varepsilon} + 1T_{F\varepsilon}$	$3T_h + 2T_{Fd\varepsilon} + 4T_{Rde} + 2T_{F\varepsilon}$
Ray *et al*. (2016)	$2T_h + 1T_{ECC}$	$2T_h + 3T_{ECC}$	$4T_h + 4T_{ECC}$

Enrolling and authenticating new mobile money subscribers and performing transactions using the native G-MoMo applications were simple than the existing schemes. Our proposed algorithm offered better protection for the authentication factors and confidential financial information than the algorithm proposed by Chetalam (2018), Ray *et al*. (2016), Islam *et al*. (2019), Hassan *et al*. (2020), Vincent *et al*. (2020), Suwera (2021), and Hassan and Shukur (2021b). However, the biometric fingerprint used to authenticate users in the algorithm by Ray *et al*. (2016) were stored directly in the database, thus making them easy to be compromised. It was concluded that the proposed algorithm was more reliable because of its efficiency.

(ii) Comparing the security features of the secure MFA algorithm for mobile money applications with existing algorithms

The few existing algorithms were chosen for the comparison because they offered some security benefits which can be compared with the proposed algorithm. Therefore, the security analysis proved that the proposed secure MFA algorithm is safe and secure against well-known security attacks, as discussed in the following subsections.

Secure authentication, data confidentiality, integrity and privacy

The proposed secure MFA algorithm uses a PIN, OTP, and biometric fingerprint to authenticate mobile money subscribers. It also uses the mobile money agent's QR code in authorizing money withdrawal which guaranteed authenticity. The security of the authentication factors such as the PIN and OTP are ensured by SHA-256, subscribers' biometric fingerprint by FIDO, where RSA encryption protects public/private key pair and fingerprint template, and Fernet encryption secures the QR codes, the confidential financial information in the database, and all the data before transmission to the remote databases, which guaranteed data confidentiality.

Ensures non-repudiation

During the enrolment phase, the mobile money subscriber's biodata, phone number, UUID, PIN, and biometric fingerprint are captured, verified, and stored in the main and FIDO databases. The UUID and phone number uniquely identified the mobile money subscribers. During authentication, OTP is created and sent to the mobile money subscriber's phone number and a copy is hashed using SHA-256, the hash value is encrypted with Fernet and saved in the subscriber's table, linked to the phone number. It is difficult for the mobile money subscriber to deny having received the sent OTP because it can be tracked by Twilio API since their phone numbers are sent to the Twilio API to deliver the 5-digit OTP required during enrolment and authentication. The QR code contains the encrypted and encoded unique UUID of the mobile money agent that the mobile money customer scans during mobile money withdrawal which helped to ensure non-repudiation by the mobile money agent. In addition, in FIDO registration, the mobile money subscriber's smartphone is registered and it creates a new public/private key pair unique for the mobile money service, subscriber's account, and smartphone for authentication. The public key is encrypted with RSA and the ciphertext is again encrypted with Fernet and then sent to the FIDO database linked with the subscriber's account. While the private key and biometric templates are only encrypted with RSA and stored on the subscriber's smartphone. The registered smartphone then uses the subscriber's account identifier to choose the correct private key to sign the challenge sent by the FIDO to confirm that the smartphone has the private key during the authentication. Then, the smartphone sends the signed challenge to the FIDO database for verification using the public key.

Ensures subscriber anonymity

In the proposed secure MFA algorithm, mobile money subscribers' anonymity is ensured by entering a unique PIN and biometric fingerprints that uniquely identifies them. There is no physical contact between mobile money agents and users and the mobile money service provider in mobile payments. Therefore, only the mobile money payment gateway has records that can trace and identify them.

Resilient to shoulder-surfing attacks, PIN-guessing attacks, brute-force attacks, replay attacks, insider & identity fraud, MITM attacks, impersonation attacks, and social engineering attacks

The proposed secure MFA algorithm for mobile money applications use multiple factors, such as PIN, OTP, biometric fingerprint, and a QR code to prevent the various attacks. The mobile money

subscribers' PINs are masked when entered during authentication. The OTP sent to mobile money subscribers is 5-digits, randomly generated and valid for only 60 seconds, making it difficult for the attacker to guess. It is hashed using SHA-256 and encrypted using Fernet before saving it in the main database. The subscribers' biometric fingerprint is also secured by FIDO, where RSA and Fernet encryptions protect public/private key pair and fingerprint template, and Fernet encryption secures the QR codes, the confidential financial information in the database, and all the data before transmission to the remote databases.

The proposed MFA algorithm's security features were compared with a few related algorithms, as summarised in Table 20. The tick [✓] indicated the strengths of the algorithms, while the [×] showed the weaknesses of the algorithms.

Table 20: Comparison of the proposed secure MFA algorithm's security features with a few related algorithms

S/No	Security feature	Ray *et al.* (2016)	Vincent *et al.* (2020)	Hassan & Shukur (2021a)	Our Algorithm
1.	Ensures efficient authentication	×	×	×	✓
2.	Ensures data confidentiality	✓	✓	×	✓
3.	Ensures data integrity	✓	✓	×	✓
4.	Ensures non-repudiation	✓	✓	×	✓
5.	Ensures anonymity	×	×	×	✓
6.	Ensures privacy	×	✓	×	✓
7.	Prevents shoulder-surfing attacks	×	×	✓	✓
8.	Thwarts social engineering attacks	×	×	×	✓
9.	Prevents phishing attacks	×	×	✓	✓
10.	Prevents PIN-guessing attacks	×	×	✓	✓
11.	Prevents brute-force attacks	×	×	✓	✓
12.	Resilient to replay attacks	✓	×	×	✓
13.	Resilient to insider attacks	×	×	×	✓
14.	Resilient to impersonation attacks	×	×	×	✓
15.	Resilient to identity fraud	×	✓	×	✓
16.	Resilient to MITM attacks	✓	×	✓	✓

(iii) Results of heuristic evaluation and usability testing of the native G-MoMo applications

Heuristic evaluation and usability testing methods were used to verify the three native G-MoMo applications by identifying usability issues with their interface designs, suggesting recommendations for improvement, and analysing their usability.

Heuristic evaluation

This study adopted and chose the ten (10) heuristic guidelines established by Jakob Nielsen to serve as a framework for evaluating the user interface design of the three G-MoMo applications. Heuristic evaluation was used to obtain qualitative data from evaluation experts about the interface designs of the three G-MoMo applications and assess their user interfaces to identify usability problems. The heuristic guideline checklist and a list of tasks to be performed by the evaluation experts were used in the heuristic evaluation.

Five evaluation experts were selected to analyse the usability problems with the user interfaces of the three native G-MoMo applications because, according to Nielsen and Mack, conducting heuristic evaluation requires 3-5 evaluators (Nielsen & Mack, 1994). Among the five evaluation experts chosen to conduct the heuristic evaluation, two have expertise in usability evaluation and knowledge base and three experts have expertise in the knowledge base. They are comprised of four males and one female who are between 28 to 40 years old. Three experts are web and mobile application developers who have used the three G-MoMo applications for some days. The evaluation experts were chosen based on their profiles. The two experts are teaching staff who have experience in human-computer interaction (HCI) and have conducted research in the heuristic evaluation, and mobile applications, and had used the three G-MoMo applications for three weeks before analyzing them. The three experts in the second group included web and mobile application developers focusing on developing mobile-friendly web and mobile applications to enhance user experience and application security. They have experience in designing and developing special-purpose smartphone applications with enhanced security. The participants acquired two hours of training on using Nielsen's heuristics to evaluate the three G-MoMo applications before conducting the evaluation. The profiles of the experts are summarized in Table 21.

Table 21: The profile of the usability evaluation experts

S/No	Participant	Gender	Age	Profession	Years of experience
1.	Expert 1	Female	37	PhD in Information Technology	8
2.	Expert 2	Male	39	PhD in Computer Science	10
3.	Expert 3	Male	30	Web and Mobile Application Developer	6
4.	Expert 4	Male	31	Web and Mobile Application Developer	6
5.	Expert 5	Male	29	Mobile Application Developer	5

The heuristic evaluation process involves: (a) identifying the number of appropriate evaluation experts, (b) arranging an appointment with the experts, (c) briefing each evaluation expert about the background, objectives of the study, heuristics applied, the apparatus, target users, features and functionalities of the three G-MoMo applications, and list of tasks to be performed, (d) distributing the questionnaire to evaluation experts to review the questions for better understanding, (e) testing the three G-MoMo applications by evaluation experts using a smartphone, (f) recording successful task completion rate by experts filling up the questionnaire, (g) identifying severe defects from the three G-MoMo applications by mentioning in the comments for improving the application design, and (h) redesigning the three G-MoMo applications based on evaluation expert's feedback for better interactive application interface.

The three G-MoMo applications were installed and tested on several Android-based smartphones with fingerprint sensors such as Tecno Camon 18 Premier, Tecno Camon 16 Pro, and Samsung Galaxy S7 Edge running on Android 11, 10, and 7 with different pixels resolution without distorting their interfaces, and functionalities, and keeping them up and running.

The experts used the heuristic evaluation post-test questionnaire to assess the three G-MoMo applications interfaces by giving their opinion about the usability issues with the interfaces after performing tasks such as enrolment, authentication, transaction, and account management. The heuristic evaluation post-test questionnaire contained five-point Likert scale statements developed based on the 10 heuristic guidelines proposed by Jakob Nielsen to inspect the three G-MoMo applications (Nielsen, 1994a). Table 22 shows Jakob Nielsen's 10 heuristics for user interface design.

Table 22: Jakob Nielsen's ten (10) heuristics for user interface design (Nielsen, 1994a)

ID	Heuristic name
H1	Visibility of system status
H2	Match between the system and the real world
H3	User control and freedom
H4	Consistency and standards
H5	Error prevention
H6	Recognition rather than recall
H7	Flexibility and efficiency of use
H8	Aesthetic and minimalist design
H9	Help users recognize, diagnose, and recover from errors
H10	Help and documentation

Each heuristic item in the post-test questionnaire was thoroughly explained with examples to help the experts accurately identify usability problems. The usability issues' severity was rated based on applying the Jakob Nielsen rating scale of 0 - 4 which provided the evaluation experts with a better insight into the usability issues with their degrees of severity which the application developers can consider a priority and make the essential corrections (Nielsen, 1994c; Nabovati *et al*., 2014). Table 23 summarizes the Jakob Nielsen rating scale used to rank the severity of usability issues.

Table 23: Jakob Nielsen rating scale for ranking the severity of usability issues (Nielsen, 1994c)

Rating	Severity	Description of the severity
0	No problem	I do not agree that this is a usability problem at all.
1	Cosmetic problem only	Need not be fixed unless extra time is available on the project.
2	Minor usability problem	Fixing this should be given low priority.
3	Major usability problem	Important to fix, so it should be given high priority.
4	Usability Catastrophe	Imperative to fix this before the product can be released.

After the evaluation, the results obtained using the post-test questionnaires were compiled and a consensus was generated for the ratings, and recommendations were provided. The collected data was analysed using RStudio software and descriptive statistics were computed about the usability issues with the user interfaces of the three native G-MoMo applications.

- **Results of heuristic evaluation**

The five selected evaluation experts separately evaluated the user interfaces of the three native G-MoMo applications, and 63 usability issues were identified and used to perform the analysis. Out of the 63 identified usability issues, 33 (52.4%) were minor, and 30 (47.6%) were major (Ali *et al*.,

2022). Table 24 summarises the frequency of severity of usability issues with the user interfaces of the native G-MoMo applications using the 10 principles of heuristics evaluation.

Table 24: The severity frequency of usability issues with the interface designs of the three native G-MoMo applications

Heuristic principles	Severity				Total		Average severity
	Cosmetic	Minor	Major	Catastrophe	Frequency	%	
H1: Visibility of system status	0	1	0	0	1	**1.6**	**2**
H2: Match between the system and the real world	0	4	0	0	4	**6.3**	**2**
H3: User control and freedom	0	8	3	0	11	**17.5**	**2.2**
H4: Consistency and standards	0	5	0	0	5	**7.9**	**2**
H5: Error prevention	0	3	0	0	3	**4.8**	**2**
H6: Recognition rather than recall	0	4	0	0	4	**6.3**	**2**
H7: Flexibility and efficiency of use	0	3	3	0	6	**9.5**	**2.5**
H8: Aesthetic and minimalist design	0	1	0	0	1	**1.6**	**2**
H9: Help users recognize, diagnose, and recover from errors	0	3	0	0	3	**4.8**	**2**
H10: Help and documentation	0	1	24	0	25	**39.7**	**3**
TOTAL	**0**	**33**	**30**	**0**	**63**	**100.0**	**2.2**
	0.00%	52.4	47.6	0.00%		100%	

The distribution of the usability issues among the three G-MoMo applications showed that the G-MoMo Customer Application had the highest number of minor (13) and major (12) usability issues, followed by the G-MoMo Agent Application with 10 minor and 10 major usability issues. At the same time, the G-MoMo IT Support Application had the least usability issues with 10 minor and 8 major (Ali *et al*., 2022). Figure 41 shows the number of usability issues among the three G-MoMo applications.

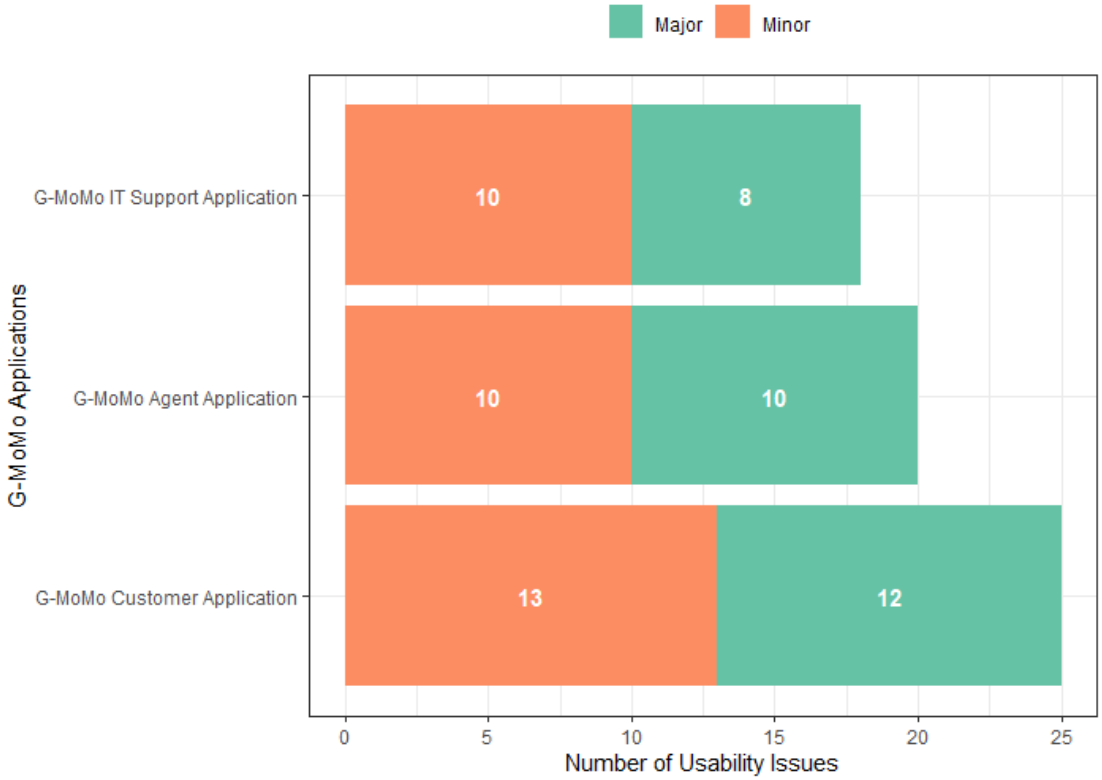


Figure 41: The number of usability issues among the three native G-MoMo applications

From the analysis of the results, the severity rating results showed that the "help and documentation (H10)" principle was mentioned 25 times (39.7%) with a mean severity score of 3.0 and had the most frequency and was regarded as a major problem. The "visibility of system status (H1)" and "aesthetic and minimalist design (H8)" principles had the lowest frequency of 1.6% and mean severity scores of 2.0; thus, they were regarded as minor problems. The "user control and freedom (H3)" and "help and documentation (H10)" account for 57.1% of the usability problems and were considered minor and major issues. The "match between system and the real world (H2)," "consistency and standards (H4)," "error prevention (H5)," "recognition rather than recall (H6)," "flexibility and efficiency of use (H7)," and "help users recognize, diagnose, and recover from errors (H9)" principles were categorised as a minor problem with a mean severity score of 2.0 (6.3%), 2.0 (7.9%), 2.0 (4.8%), 2.0 (6.3%), 2.5 (9.5%), and 2.0 (4.8%), respectively (Ali *et al*., 2022). Figure 42 shows the frequency of severity of usability issues among the 10 heuristic guidelines used to evaluate the user interfaces of the three G-MoMo applications.

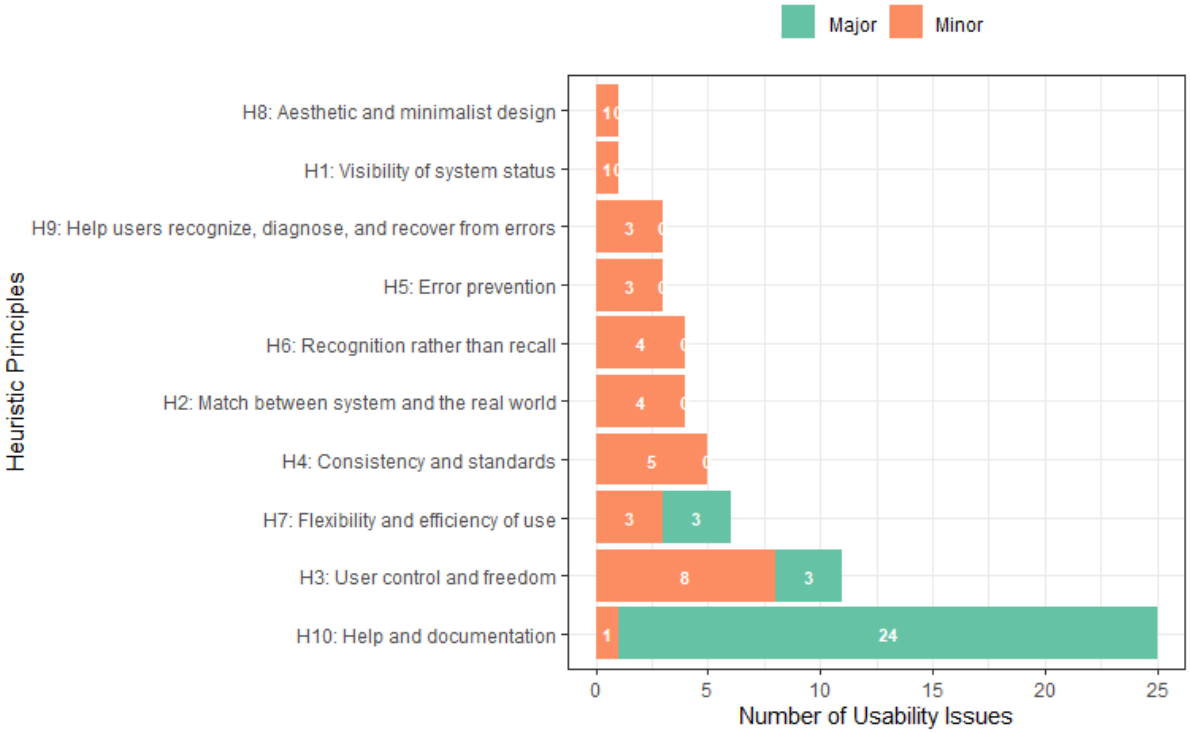


Figure 42: The frequency of severity of usability issues among the 10 heuristic guidelines used to evaluate the user interfaces of the three native G-MoMo applications

The three G-MoMo applications had more usability issues related to "help and documentation (H10)". The G-MoMo IT Support Application had a few usability issues related to the "match between system and the real world (H2)", "flexibility and efficiency of use (H7)", "aesthetic and minimalist design (H8)", "help users recognize, diagnose, and recover from errors (H9)", but more usability issues with "user control and freedom (H3)", "error prevention (H5)", "recognition rather than recall (H6)", "and help and documentation (H10)". The G-MoMo Agent Application, on the other hand, had few usability issues related to "recognition rather than recall (H6)", "flexibility and efficiency of use (H7)", "help users recognize, diagnose, and recover from errors (H9)", but more usability issues with the "match between system and the real world (H2)", "consistency and standards (H4)", "user control and freedom (H3)", and "help and documentation (H10)". In addition, G-MoMo Customer Application had a few usability issues related to the "visibility of system status (H1)", "error prevention (H5)", "recognition rather than recall (H6)", "help users recognize, diagnose, and recover from errors (H9)", but more usability issues with "flexibility and efficiency of use (H7)", "user control and freedom (H3)", and "help and documentation (H10)" (Ali *et al.*, 2022). Figure 43 shows the distribution of the usability issues among the user interfaces of the three G-MoMo applications.

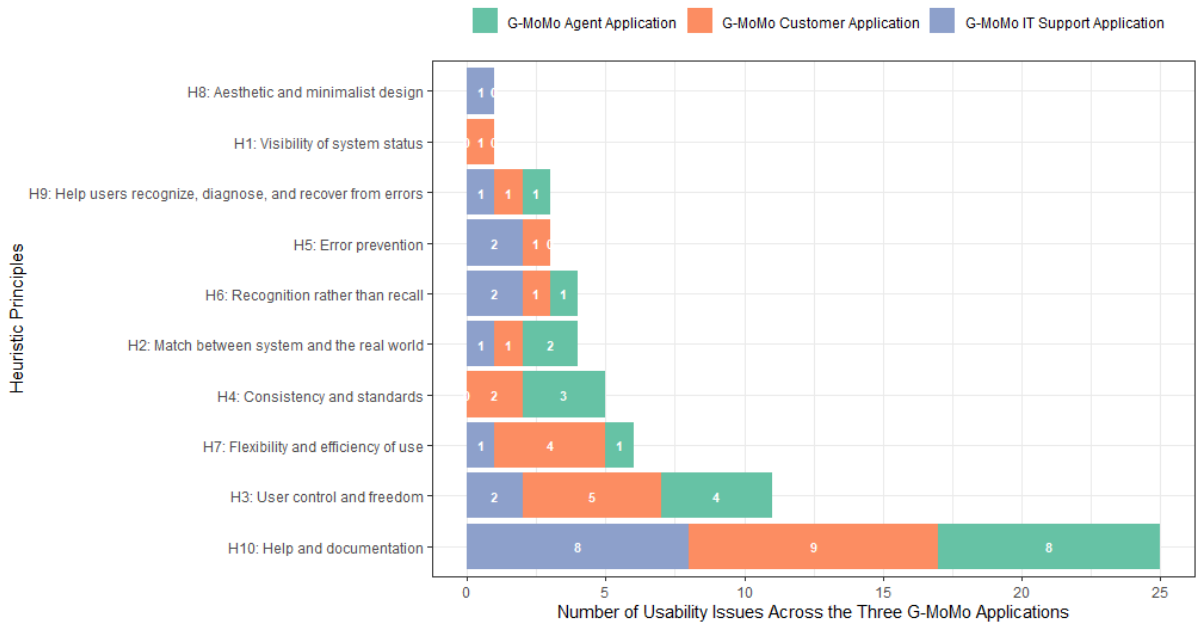


Figure 43: The distribution of the usability issues among the user interfaces of the three native G-MoMo applications

In summary, several usability issues were identified from the user interfaces of the three G-MoMo applications and among them include:

(i) Lack of forward navigation buttons: The interfaces of the three native G-MoMo applications have backward navigation buttons but lack forward navigation buttons, making it difficult for mobile money subscribers to move forward. Instead, they had to go to the home page and select the pages they wanted to access, thus, affecting user control and freedom (Ali *et al*., 2022).

(ii) Lack of uniformity in the applications menu titles: The menu titles or headings of the user interfaces were not uniformly aligned. Some headings are aligned to the left and others centre, affecting consistency and standards in the G-MoMo applications (Ali *et al*., 2022).

(iii) Lack of search field options: The G-MoMo applications do not have search field options, making it difficult for mobile money subscribers to search for required services and help. This has affected the applications' flexibility & efficiency, user control & freedom (Ali *et al*., 2022).

(iv) Lack of actions needed for recovery: The G-MoMo applications lack detailed steps required for recovery in case the G-MoMo applications crash, thus affecting the applications' error diagnosis and recovery (Ali *et al*., 2022).

(v) Lack of help and documentation: The G-MoMo applications lacked help and documentation features and a panel of tips and tricks, making it difficult for new mobile money subscribers to use the applications and recall the steps followed. This has resulted in errors during the usage of the G-MoMo applications and made it difficult for mobile money subscribers to recall the steps involved in the applications' usage (Ali *et al*., 2022).

Usability testing

This study also employed a usability testing method with the end-users of the system to ascertain whether they had fulfilled the agreed requirements and the usability of the three G-MoMo applications. Usability testing was used to obtain quantitative data from the selected participants about the G-MoMo applications.

Forty participants were chosen using a stratified random sampling method to verify the usability of the three G-MoMo applications. The selected sample size was enough to carry out usability testing because, according to Nielsen (2012) the number of respondents to participate in usability testing is at least 20 people. Of the 40 participants, 25 were male (62.5%), and 15 (37.5%) were female. The participants were between the ages of 20 to 40. However, 19 (47.5%) of the participants were between 20-29 years, 16 (40.0%) between 30-39 years, and the remaining 5 (12.5%) were above 39 years. Among the participants, 32 (80%) had bachelor's degrees, 6 (15%) had master's degrees, and 2 (5%) had PhD. The selected participants were computer literate. Nevertheless, not all participants were familiar with the functioning of the three G-MoMo applications. The participants were divided into mobile money IT support staff, agents, and customers. Four (10%) of the participants were grouped as mobile money IT support staff, 10 (25%) as mobile money agents, and 26 (65%) as mobile money customers. Table 25. Summarizes the social demography characteristics of the participants.

The researchers began the usability testing process by briefing and checking the participants' smartphones to ensure that the smartphones' fingerprint sensors functioned well and connected to the internet. Based on the participants' category, a functioning version of G-MoMo applications was downloaded and installed on their smartphones. The participants were introduced to G-MoMo applications, their features, functionalities, and workflow. The three G-MoMo applications were demonstrated to each category of the participants and were allowed to carry out tasks using the G-MoMo applications so that the researchers could learn what they were doing. Three moderators supervised the process to ensure smooth running. After completing tasks, the participants were required to validate the three G-MoMo applications by filling out the post-test questionnaire.

Table 25: Participants' social demography characteristics

S/No	Variable	Frequency	Percentage (%)
1.	**Gender**		
	Male	25	62.5
	Female	15	37.5
2.	**Age**		
	Less than 20 years	0	0.0
	Between 20–29 years	19	47.5
	Between 30–39 years	16	40.0
	More than 39 Years	5	12.5
3.	**Level of education**		
	Bachelors	32	80.0
	Masters	6	15.0
	PhD	2	5.0
4.	**Category of evaluation**		
	Mobile money IT support staff	4	10.0
	Mobile money agent	10	25.0
	Mobile money user	26	65.0

The post-test questionnaire contained five-point Likert scale statements developed based on the usability testing attributes of learnability, effectiveness, efficiency, memorability, errors, user satisfaction, ease of use, aesthetic, usefulness, integration, and understandability. They were used to verify the usability of the three G-MoMo applications. The agreement scale used in the post-test questionnaire was: (a) strongly disagree, (b) disagree, (c) undecided, (d) agree, and (e) strongly agree.

After completing the tasks, the selected participants appraised their satisfaction with the three G-MoMo applications and shared their experiences and recommendations with the moderators. Data collected using post-test questionnaires in the usability testing was analyzed in RStudio software. Percentages, means, and standard deviations were computed and analyzed to understand the general usability of the three G-MoMo applications. The results for the mean (M) $\geq$ 3.41 were considered statistically significant (Pimentel, 2010).

- **Results of usability testing**

Descriptive statistics were performed to help analyse and interpret the results. The results in Table 26 summarise the participants' opinions about the usability of the native G-MoMo applications. The significant majority of the participants agreed that the usability testing attributes summarised in Table 26 were achieved while using the native G-MoMo applications. These usability testing attributes included the learnability (*M* = 4.13, *Std Dev* = 0.853), effectiveness (*M* = 3.73, *Std Dev* = 0.554), efficiency (*M* = 4.43, *Std Dev* = 0.636), memorability (*M* = 3.95, *Std Dev* = 0.552), errors (*M* = 4.28, *Std Dev* = 0.599), user satisfaction (*M* = 4.00, *Std Dev* = 0.599), ease of use (*M* = 4.03, *Std Dev* = 0.577), aesthetic (*M* = 4.03, *Std Dev* = 0.620), usefulness (M = 3.95, *Std Dev* = 0.639), integration (M = 4.23, *Std Dev* = 0.620), and understandability (*M* = 4.10, *Std Dev* = 0.496). Therefore, it was statistically significant to say that the mobile money subscribers were satisfied with the usage of the native G-MoMo applications because their mean is greater than 3.41.

Table 26: Opinion of participants about the usability of native G-MoMo applications

S/No	Usability testing attributes	SD	D	N	A	SA	M	Std Dev
1.	Learnability	0.0	5.0	15.0	42.5	37.5	4.13	.853
2.	Effectiveness	0.0	0.0	32.5	62.5	5.0	3.73	.554
3.	Efficiency	0.0	0.0	7.5	42.5	50.0	4.43	.636
4.	Memorability	0.0	0.0	17.5	70.0	12.5	3.95	.552
5.	Errors	0.0	0.0	7.5	57.5	35.0	4.28	.599
6.	User satisfaction	0.0	0.0	17.5	65.0	17.5	4.00	.599
7.	Ease of use	0.0	0.0	15.0	67.5	17.5	4.03	.577
8.	Aesthetic	0.0	0.0	17.5	62.5	20.0	4.03	.620
9.	Usefulness	0.0	0.0	22.5	60.0	17.5	3.95	.639
10.	Integration	0.0	0.0	10.0	57.5	32.5	4.23	.620
11.	Understandability	0.0	0.0	7.5	75.0	17.5	4.10	.496

4.2 Discussion of the results

4.2.1 Different controls to mitigate the security challenges

Several mitigation measures were proposed to prevent the security challenges, and they included:

Mobile money subscribers must use secure MFA to control mobile money systems' access and safeguard confidential information (Bosamia, 2017; Lonie, 2017). There is also a need to implement cryptographic techniques to protect authentication factors and confidential financial information (Lonie, 2017).

Customer sensitisation about security, risk, and fraud awareness campaigns must be encouraged to ensure the safety of mobile money wallets and build mobile money subscribers' trust in the mobile money business (Gwahula, 2016; Bosamia, 2017; Akomea-Frimpong *et al*., 2018).

Mobile money service providers must develop legal documents, fraud policies, and subscriber and security policies to protect the mobile money industry. These documents will help combat mobile money security challenges (Lonie, 2017; Akomea-Frimpong *et al*., 2018; Alhassan *et al*., 2018).

There is a need for the government and mobile money service providers to monitor high-value transactions to control the risk of fraud and money laundering. The mobile money service providers must monitor and supervise the mobile money agents and train mobile money agents on terms, conditions, and practices accepted by the mobile money service providers (Gilman & Joyce, 2012; Mudiri, 2013).

Some of the measures suggested included: (a) severe punishment of the fraudsters when caught; (b) communicating the security challenges, incidences and frauds to the mobile money service providers and regulators; (c) the mobile money service providers and government must publish the security challenges, frauds, and incidences to keep the subscribers aware; and (d) the mobile money service providers must develop a portal for the victims to share the security challenges, scams, and incidences anonymously.

4.2.2 Security analysis of the proposed secure MFA algorithm for mobile money applications

The security analysis results proved that the proposed algorithm was secure against various security attacks.

It ensured strong security and efficiency in authentication by implementing MFA where PINs, OTP, biometric fingerprints, and QR codes authenticate, authorise, and confirm mobile money subscribers. The authentication factors like PINs and OTP were secured using SHA-256, the subscribers' biometric fingerprints by FIDO, where the RSA encryption protects the public/private key pair and the fingerprint templates. The QR codes, confidential financial information in the databases, and all the data before transmission to the remote database are secured by Fernet encryption (Ximenes *et al*., 2019; Arief *et al*., 2019; Hassan *et al*., 2020; Mega, 2020; Osman & Nakanishi, 2020; Canales, 2020; Pramusinto *et al*., 2020; Feng *et al*., 2021).

It ensured data confidentiality, integrity, privacy, and subscribers' anonymity by implementing PINs, OTP, biometric fingerprints, and QR codes to authenticate them. It also used SHA-256 to protect PINs and OTP, FIDO to protect the subscribers' biometric fingerprints, where the RSA encryption secures the public/private key pair and the fingerprint templates, and Fernet encryption to protect the QR codes, confidential financial information in the databases, and all the data before transmission to the remote database (Chang *et al*., 2015; Purnomo *et al*., 2016; Ray *et al*., 2016; Mohit *et al*., 2017; Husny *et al*., 2017; Ximenes *et al*., 2019; Vincent *et al*., 2020; Hassan *et al*., 2020; Dijesh *et al*., 2020).

It ensured non-repudiation by only allowing mobile money subscribers with PINs, OTP, and biometric fingerprints to access the mobile money systems. The subscribers' smartphones with encrypted private keys and biometric templates were only used when authenticating the subscribers. The mobile money subscribers cannot deny receiving OTP because their phone numbers can be traced to the Twilio API. Furthermore, it is difficult for mobile money agents to deny having authorised mobile money transaction(s) because the QR codes contain the mobile money agents' encrypted UUID (Ray *et al*., 2016; Mohit *et al*., 2017; Ximenes *et al*., 2019; Vincent *et al*., 2020; Hassan *et al*., 2020).

It is resilient to shoulder-surfing attacks, impersonation attacks, social engineering attacks, identity fraud, and phishing attacks because the mobile money subscribers only enter the PINs when masked, making it hard for the attackers to access them. Implementing multiple factors like PINs, OTP, biometric fingerprints, and QR codes makes it difficult for adversaries to crack all the factors. Even if they succeed in accessing the PINs and OTP, getting the encrypted public/private key pairs and fingerprint templates needed for authenticating the biometric fingerprint will not be easy, and the OTP used is only valid for 60 seconds. The use of SHA-256 to secure PINs and OTP, FIDO to protect the subscribers' biometric fingerprints, where the RSA encryption secures the public/private key pair and the fingerprint templates, and Fernet encryption to secure the QR codes, confidential financial information in the databases, and all the data before transmission to the remote database, makes it difficult for the attackers to see the authentication factors (Mtaho, 2015; Goel *et al*., 2017; Kim *et al*., 2017; Han *et al*., 2018; Shin, 2018; Sharma & Mathuria, 2018; Ximenes *et al*., 2019; Canales, 2020; Feng *et al*., 2021; Hassan & Shukur, 2021a).

It is resilient to brute-force attacks, PIN-guessing attacks, replay attacks, insider attacks, and MITM attacks. These attacks are prevented by implementing MFA using PINs, OTP, biometric fingerprints, and QR codes. The SHA-256 guarantees the security of the PINs and OTP;

subscribers' biometric fingerprints are protected by FIDO, where the RSA encryption secures the public/private key pair and the fingerprint templates; and the QR codes, confidential financial information in the databases, and all the data before transmission to the remote database are secured using Fernet encryption. The encrypted private keys and fingerprint templates remain in the subscribers' smartphones, but the encrypted public keys are saved in the FIDO database (Ray *et al*., 2016; Mohit *et al*., 2017; Kim *et al*., 2017; Han *et al*., 2018; Shin, 2018; Ximenes *et al*., 2019; Dijesh *et al*., 2020; Canales, 2020; Feng *et al*., 2021; Hassan & Shukur, 2021a).

4.2.3 Heuristic evaluation and usability testing

(i) Several usability issues that were identified during the heuristic evaluation of the native G-MoMo applications

The native G-MoMo applications lack forward navigation buttons. This makes mobile money subscribers go backwards or to the home page when they want to access other services, thus, affecting user control and freedom. This is similar to the studies conducted by Yusoh and Matayong (2017) and Jeddi *et al*. (2020), who reported a lack of navigation links with the applications.

The menu titles of the user interfaces of the native G-MoMo applications lacked uniformity because some menu titles were aligned to the centre and others left, which caused inconsistency in the design. This has negatively impacted the consistency and standards of the user interfaces. Othman *et al*. (2018) and Vingen *et al*. (2020) described menu heading title inconsistency as lacking adherence to conventions, design principles, and application patterns.

It was also reported that the user interfaces lacked search field options, thus making it difficult for the subscribers to search for services, which affected the applications' user control and freedom, flexibility and efficiency (Paramitha *et al*., 2018). Eliseo *et al*. (2017) suggested that search features should be strategically placed on the applications.

The native G-MoMo applications interfaces lacked actions required for recovery, which greatly affected error diagnosis and recovery. The applications did not display errors and explained errors to the mobile money subscribers in simple language plus the actions required for recovery, making it difficult to recover if it occurs (Eliseo *et al*., 2017; Caro-Alvaro *et al*., 2018; Höhn & Bongard-Blanchy, 2020).

The native G-MoMo applications also lacked help and documentation features and a panel of tips and tricks, making it difficult for new mobile money subscribers to use the applications and recall the steps followed (Salman *et al*., 2018; Paramitha *et al*., 2018; Kekkonen & Oinas-Kukkonen, 2019; Jeddi *et al*., 2020). Abidin *et al*. (2019) recommended that applications must have help and documentation features explained in simple language and easily accessible.

(ii) The usability testing results obtained from verifying the three native G-MoMo applications

It was reported that the native G-MoMo applications were learnable, i.e., easy to learn the features and functionalities and the usage hence, improving the mobile money subscribers' performance level. This is similar to the studies conducted by Byun *et al*. (2020), Zakaria *et al*. (2020), Sukmasetya *et al*. (2020), Al-Kinani *et al*. (2020), Alturki *et al*. (2020), Al-Gayar *et al*. (2021), and A'bas *et al*. (2021) where they found that applications were easy to learn.

The native G-MoMo applications were effective for mobile money subscribers because they could complete their tasks accurately. This is in line with the works of Byun *et al*. (2020), Hussain *et al*. (2020), Alturki *et al*. (2020), Tyas and Khairunisa (2020), Emanuela *et al*. (2020), Mubeen *et al*. (2020), Lowe *et al*. (2021), and A'bas *et al*. (2021), who reported that there was effectiveness with the applications.

It was reported that the usability testing result showed that the native G-MoMo applications were highly efficient because mobile money subscribers could take less time to complete the given tasks accurately (Lynn *et al*., 2020; Byun *et al*., 2020; Hussain *et al*., 2020; Zakaria *et al*., 2020; Sukmasetya *et al*., 2020; Tyas & Khairunisa, 2020; Emanuela *et al*., 2020; Mubeen *et al*., 2020; A'bas *et al*., 2021; Putri *et al*., 2021).

It was found that the steps followed while performing tasks using the native G-MoMo applications were easily remembered by mobile money subscribers. This finding is similar to earlier studies conducted by Zakaria *et al*. (2020), Sukmasetya *et al*. (2020), Alturki *et al*. (2020), and Putri *et al*. (2021).

Fewer errors were encountered by the mobile money subscribers while using the native G-MoMo applications. This result is logical to the studies conducted by Zakaria *et al*. (2020), Alturki *et al*. (2020), and Putri *et al*. (2021), where it was noted that there were few errors encountered while using the applications.

The mobile money subscribers were satisfied with the features and functionalities of the G-MoMo applications, the information, and the display quality. This attribute was reported in other studies conducted by Byun *et al*. (2020), Zakaria *et al*. (2020), Alturki *et al*. (2020), Tyas and Khairunisa (2020), Emanuela *et al*. (2020), Mubeen *et al*. (2020), Ahmad *et al*. (2021), Al-Gayar *et al*. (2021), Putri *et al*. (2021), Lowe *et al*. (2021), and A'bas *et al*. (2021), where it was found that the users were satisfied with the applications.

The new mobile money subscribers found it easy to use the native G-MoMo applications because of the simplicity of the interfaces, features, and functionalities, which helped achieve total satisfaction (Byun *et al*., 2020; Merks *et al*., 2020; Lersilp *et al*., 2020; Sukmasetya *et al*., 2020; Al-Gayar *et al*., 2021; Kairy *et al*., 2021).

The G-MoMo applications were highly aesthetic because of the designs used. This finding is similar to the studies of Gilmore *et al*. (2019) and Santesteban-Echarri *et al*. (2020), where it was found that applications' interfaces were beautifully designed.

The usability testing results showed that the native G-MoMo applications were helpful because their features allowed mobile money subscribers to register, deposit money, withdraw money, send money, update their mobile money PINs and biometric fingerprints, and so on. This is consistent with the studies conducted by Kumar *et al*. (2019) and Al-Gayar *et al*. (2021), where they found the applications helpful in achieving their goals.

Other usability testing results reported about the native G-MoMo applications included easy integration and understandability.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

The main aim of this research was to develop a secure MFA algorithm for mobile money applications. The primary objective of the research was achieved by formulating four specific objectives and their related research questions. The specific objectives included: (a) a review of the existing literature on threat models in the current 2FA scheme for mobile money; (b) identification and assessment of the key security issues associated with mobile money systems in Uganda; (c) design a secure MFA algorithm for mobile money applications and develop prototypes of native mobile money applications to implement the designed algorithm; and (d) validation of the designed algorithm and developed prototypes of native G-MoMo applications.

The literature review on the threat models in the mobile money's 2FA scheme identified several attacks, which were grouped into attacks against privacy, authentication, confidentiality, integrity, and availability. Moreover, cryptographic functions and personal identification were identified as countermeasures to the security attacks. This prompted the researchers to carry out a survey in Uganda to identify and assess the key security challenges with mobile money systems. The survey analysis found identity theft, authentication attacks, phishing attacks, and PIN sharing as the key security issues encountered by mobile money schemes.

The results obtained from the review and survey motivated the researchers to design a secure MFA algorithm for mobile money applications. Three native G-MoMo applications were developed to prove the algorithm's feasibility and provide robust security. The Vue JS framework was used to develop the G-MoMo applications' front-end, Python for the back-end, MySQL for the back-end databases, and Twilio for sending 5-digit SMS OTP to the registered mobile money subscribers. The security analysis proved that the proposed algorithm provided secure authentication, data confidentiality, integrity, subscribers' privacy, and anonymity. It ensured non-repudiation and offered higher security against numerous attacks. The performance analysis revealed that the algorithm had high communication overhead and computational cost but with more robust security.

The heuristic evaluation results showed that the user interfaces of G-MoMo applications lacked forward navigation buttons, uniformity in the applications' menu titles, search field options, actions needed for recovery, and help and documentation. Similarly, the usability testing revealed

that the native G-MoMo applications were easy to learn, effective and efficient, memorable, and had few errors. The subscribers were satisfied with the features and functionalities of the application; they are easy to use, aesthetic, easy to integrate, and understandable.

The contribution of this research included: (a) creating awareness about the security issues encountered by the current mobile money authentication schemes; (b) designing a secure MFA algorithm for mobile money applications and developing secure native G-MoMo applications that implemented MFA and cryptographic techniques like SHA-256, FIDO, RSA, and Fernet encryptions to protect the authentication factors and the information in storage and transit; (c) it helps mobile money service providers and governments to implement a secure and efficient mobile money authentication scheme, and (d) the scientific publications extended the theoretical knowledge in information security and the prototypes of native G-MoMo applications enabled mobile money subscribers to perform mobile money services.

In conclusion, implementing a secure mobile money authentication, authorisation, and confirmation using the secure novel approach combining multiple authentication factors such as PINs, OTP, biometric fingerprints, and QR codes helps mobile money subscribers and other stakeholders to have trust in the mobile money industry since the security goals are highly maintained.

5.2 Recommendations

Based on the research findings reported in this study, it is highly recommended that:

(i) There is a need for the developers to audit the mobile money authentication and confirmation at the database level to ascertain successful and failed login attempts for analysis and detecting flaws, and identifying threats to the native G-MoMo applications.

(ii) There is a need to develop G-MoMo applications that can run on the iPhone operating system (iOS) so that mobile money subscribers with iPhones can use them to perform mobile money services.

(iii) There is a need to improve the security of the authentication and authorisation using other technologies such as blockchain.

(iv) The government and mobile money service providers must monitor high-value transactions to control the risk of fraud and money laundering.

(v) There is a need for mobile money service providers and the government to publish the different security challenges, frauds, and incidences to keep the subscribers aware.

(vi) The mobile money service providers must develop a portal that the victims of mobile money fraud can use to share their experiences anonymously.

(vii) Mobile money service providers and governments must sensitize customers about the security challenges encountered by mobile money subscribers.

(viii) The victims of mobile money fraud must communicate the incidents to the mobile money service providers and regulators.

(ix) The mobile money service providers and governments must develop legal documents, fraud policies, and subscriber and security policies to protect the mobile money industry.

(x) The government must lower internet costs so that everyone can afford it and use it to access and perform mobile money services using the G-MoMo applications.

REFERENCES

A'bas, N. N., Rahim, S. S., Dolhalit, M. L., Saifudin, W. S. N., Abdullasim, N., Parumo, S., Omar, R. N. R., Khair, S. Z. M., Kalaichelvam, K., & Izhar, S. I. N. (2021). Development and Usability Testing of a Consultation System for Diabetic Retinopathy Screening. *International Journal of Advanced Computer Science and Applications*, *12*(5), 178–188. https://doi.org/10.14569/ijacsa.2021.0120522

Abbas, E. I., Safi, M. E., & Rijab, K. S. (2017, April). *Face Recognition Rate using Different Classifier Methods based on PCA. In 2017 International Conference on Current Research in Computer Science and Information Technology (pp. 37-40).* https://scholar.google.com

Abdalla, M. A., Abdo, A. A., & Lawgali, A. O. (2020, December). *Utilizing Discrete Wavelet Transform and Discrete Cosine Transform for Iris Recognition. In 2020 20th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA) (Pp. 283-286)*. https://scholar.google.com

Abdulrahman, S. A., & Alhayani, B. (2021). *A Comprehensive Survey on the Biometric Systems based on Physiological and Behavioural Characteristics. Materials Today: Proceedings*. https://scholar.google.com

Abidin, S. R. Z., Fadzilah, S., & Sahari, N. (2019). Heuristic Evaluation of Serious Game Application for Slow-reading Students. *International Journal of Advanced Computer Science and Applications*, *10*(7), 466–474.

AbouSteit, M. H., Tammam, A. F., & Wahdan, A. (2020, July). *A Novel Approach for Generating One-Time Password with Secure Distribution. 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability.* https://scholar.google.com

Adarsh, S., Harish, D., Balaganapathy, K., Venkatachalapaty, R., Abishiek, E., & Nagarajan, M. (2017). Improved Software Quality and Design Standards-Based on Customer Preferences by Applying Evolutionary Prototyping Software Development Model. *International Journal of New Technology and Research*, *3*(5), 7–11.

Adebowale, A. (2020, August 19). *MTN Mobile Money Fraud on the Rise in Ghana as Usage Increases Following BoG's Transaction Fee Waiver*. https://www.google.com

Afolayan, D. (2021, September 9). *M-Pesa Hits 50m Users, Cements Position as Largest Mobile Money Platform in Africa*. https://www.google.com

Agarwal, S., Bharti, P. K., & Pathak, R. K. (2019). Implementation of Des Algorithm in Python. *International Journal of the Computer, the Internet and Management*, *27*(2), 1–6. http://www.ijcim.th.org/past_editions/2019V27N2/27n2Page1.pdf

Ahmad, L., Al-Sabha, R., & Al-Haj, A. (2021, March). *Design and Implementation of a Secure QR Payment System based on Visual Cryptography. In 2021 7th International Conference on Information Management (ICIM) (Pp. 40-44).* https://www.google.com

Ahmad, N. A. N., Hamid, N. I. M., & Lokman, A. M. (2021). Performing Usability Evaluation on Multi-Platform Based Application for Efficiency, Effectiveness and Satisfaction Enhancement. *International Journal of Interactive Mobile Technologies*, 15(10), 103–117. https://doi.org/10.3991/ijim.v15i10.20429

Ahmadzadegan, M. H., Khorshidvand, A. A., & Pezeshki, M. (2015, November). *A Method for Securing Username and Password against the Keylogger Software Using the Logistic Map Chaos Function. In 2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI) (Pp. 1071-1073)*. https://www.google.com

Ahmed, W., Rasool, A., Javed, A. R., Kumar, N., Gadekallu, T. R., Jalil, Z., & Kryvinska, N. (2021). Security in Next Generation Mobile Payment Systems: A Comprehensive Survey. *Access*, 9, 115932–115950. doi:10.1109/access.2021.3105450

Ahsan, K., Iqbal, S., Hussain, M. A., & Nadeem, A. (2016). A Mobile Payment Model Using Biometric Technology. *International Journal of Advances in Science Engineering and Technology*, 4(4), 17–20. http://www.iraj.in/journal/journal_file/journal_pdf/6-305-147944672517-20.pdf

Akomea-Frimpong, I., Andoh, C., Akomea-Frimpong, A. & Dwomoh-Okudzeto, Y. (2019). Control of fraud on mobile money services in Ghana: An exploratory study. *Journal of Money Laundering Control*, 22(2), 300-317. https://doi.org/10.1108/JMLC-03-2018-0023

Akoramurthy, B., & Arthi, J. (2017, January). *GeoMoB: A Geo Location Based Browser for Secured Mobile Banking. In 2016 Eighth International Conference on Advanced Computing (Pp. 83-88)*. https://www.google.com

Alabdan, R. (2020). Phishing Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet*, 12(10), 1–39. https://doi.org/10.3390/fi12100168

Alamsyah, Z., Mantoro, T., Adityawarman, U., & Ayu, M. A. (2020, October). *Combination RSA With one Time Pad for Enhanced Scheme of Two-Factor Authentication. In 2020 6th International Conference on Computing Engineering and Design (ICCED) (Pp. 1-5)*. https://www.google.com

Alanezi, N. A., Alharbi, N. H., Alharthi, Z. S., & Alhazmi, O. H. (2020, November). *POSTER: A Brief Overview of Biometrics in Cybersecurity: A Comparative Analysis. 2020 First International Conference of Smart Systems and Emerging Technologies*. https://doi.org/10.1109/smart-tech49988.2020.00067

Alawida, M., Teh, J. S., Oyinloye, D. P., Alshoura, W. H., Ahmad, M., & Alkhawaldeh, R. S. (2020). A New Hash Function Based on Chaotic Maps and Deterministic Finite State Automata. *Access*, 8, 113163–113174.

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, *68*, 160–196.

Al-Gayar, S. M. S., Goga, N., Al-Habeeb, N., Ali, H. A., Marin, I., & Shubber, M. S. (2021). Testing the Usability of the MediCare System. *Turkish Journal of Computer and Mathematics Education*, 12(3), 3227–3237.

Alhassan, N. S., Yusuf, M. O., Karmanje, A. R., & Alam, M. (2018). *Salami Attacks and their Mitigation: An Overview. The 2018 5th International Conference on "Computing for Sustainable Global Development". https://scholar.google.com*

Alhothaily, A., Alrawais, A., Hu, C., & Li, W. (2018). *One-Time-Username: A Threshold-Based Authentication System. Procedia Computer Science*. https:// doi. org/ 10. 1016/j. procs. 2018.03.019

Ali, G., Dida, M. A., & Sam, A. E. (2020a). Two-Factor Authentication Scheme for Mobile Money: A Review of Threat Models and Countermeasures. *Future Internet*, 12(10), 1–27. https://doi.org/10.3390/fi12100160

Ali, G., Dida, M. A., & Sam, A. E. (2020b). Evaluation of Key Security Issues Associated with Mobile Money Systems in Uganda. *Information*, 11(6), 1–24.

Ali, G., Dida, M. A., & Sam, A. E. (2021). A Secure and Efficient Multi-Factor Authentication Algorithm for Mobile Money Applications. *Future Internet,* 13(12), 1–31.

Ali, G., Dida, M. A., & Sam, A. E. (2022). Heuristic Evaluation and Usability Testing of G-MoMo Applications. *Journal of Information Systems Engineering and Management,* 7(3), 1-14. https://doi.org/10.55267/iadt.07.12296

Al-Kadei, F. H. M. S., Mardan, H. A., & Minas, N. A. (2020). *Speed Up Image Encryption by Using RSA Algorithm. The 2020 6th International Conference on Advanced Computing and Communication Systems.* doi:10.1109/icaccs48705.2020.9074430

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, 3, 1–23. https://doi.org/10.3389/fcomp.2021.563060

Al-Kinani, M. N. H., Adetunmbi, S. B., & Hussain, A. (2020). Usability testing of mobile Flipboard application on both non-users and novice users. *International Journal of Interactive Mobile Technologies*, 14(5), 47–56.

Alliance for Financial Inclusion (AFI). (2019, July). *Uganda's Journey to Inclusive Finance through Digital Financial Services*. https://www.afi-global.org/sites/default/files/publications/2019-07/AFI_MS_Uganda_AW_digital.pdf

Al-Odat, Z., Abbas, A., & Khan, S. U. (2019). *Randomness Analyses of the Secure Hash Algorithms, SHA-1, SHA-2 and Modified SHA. The 2019 International Conference on Frontiers of Information Technology*. doi:10.1109/fit47737.2019.00066

Aloul, F., Zahidi, S., & El-Hajj, W. (2009). *Two-Factor Authentication Using Mobile Phones. 2009 IEEE/ACS International Conference on Computer Systems and Applications*, 641–644. doi:10.1109/aiccsa.2009.5069395

Alsrehin, N., & Al-Taamneh, M. A. (2020). *Face Recognition Techniques using Statistical and Artificial Neural Network: A Comparative Study. The 2020 3rd International Conference on Information and Computer Technologies.* doi:10.1109/icict50521.2020.00032

Al-Sulaiti, A., Mansour, M., Al-Yafei, H., Aseel, S., Kucukvar, M., & Onat, N. C. (2021, April). *Using Data Analytics and Visualization Dashboard for Engineering, Procurement, and*

Construction Project's Performance Assessment. 2021 IEEE 8th International Conference on Industrial Engineering and Applications.

Al-Tekreeti, N., & Ibrahim, A. A. (2020). *Speaker Voice Recognition Using a Hybrid PSO/Fuzzy Logic System. The 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies.* doi:10.1109/ismsit50672.2020.9254

Alturki, R., AlGhamdi, M. J., Gay, V., Awan, N., Kundi, M., & Alshehri, M. (2020). Analysis of an eHealth app: Privacy, security and usability. *International Journal of Advanced Computer Science and Applications,* 11(4), 209–214. 10.14569/IJACSA.2020.0110428

Altwairqi, A. F., AlZain, M. A., Soh, B., Masud, M., & Al-Amri, J. (2019). Four Most Famous Cyber Attacks for Financial Gains. *International Journal of Engineering and Advanced Technology*, 9(2), 2131–2139. https://doi.org/10.35940/ijeat.b3601.129219

Anand, A., Ramkumar, S., Akshaya Kumar, V., Vinoth, K., & Aravinth, J. (2020). *Secure Iris Recognition Using Negative Database. The 2020 International Conference on Communication and Signal Processing.* doi:10.1109/iccsp48568.2020.9182200

Arévalo, J. G., Viecco, L., & Arévalo, L. (2020, May). *Methodology to Define an Integration Process between Frameworks SCRUM, Django REST Framework y Vue.js, Implemented for Software Development, from a Quality Management Approach and Agility. IOP Conference Series: Materials Science and Engineering*. https://doi.org/10.1088/1757-899x/844/1/012022

Arief, A. T., Wirawan, W., & Suprapto, Y. K. (2019). *Authentication of Printed Document Using Quick Response (QR) Code. The 2019 International Seminar on Intelligent Technology and Its Applications.* doi:10.1109/isitia.2019.8937084

Arun-Prakash, M., & Gokul, T. (2011, February). *Network Security-Overcome Password Hacking through Graphical Password Authentication. The 2011 National Conference on Innovations in Emerging Technology*. https://doi.org/10.1109/ncoiet.2011.5738831

Australian Cyber Security Centre (ACSC). (2019). *Implementing Multi-Factor Authentication. Australian Cyber Security Centre*. https://scholar.google.com/

Awanis, A., Lowe, C., & Andersson-Manjang, S. K. (2022, March). *State of the Industry Report on Mobile Money 2022*. https://www.gsma.com

Ayala, J. (2021). *Securing Audio Using AES-based Authenticated Encryption with Python*. https://doi.org/10.20944/preprints202108.0185.v1

Ayeb, S. E., Hemery, B., Jeanne, F., & Cherrier, E. (2021, February*). Community Detection for Mobile Money Fraud Detection. The 2020 Seventh International Conference on Social Networks Analysis, Management and Security*. https://doi.org/10.1109/SNAMS52053.2020.9336578

Azimi, M., Rasoulinejad, S. A., & Pacut, A. (2019). *The Effects of Gender Factor and Diabetes Mellitus on the Iris Recognition System's Accuracy and Reliability. The 2019 Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA).* doi:10.23919/spa.2019.8936757

Badave, H., & Kuber, M. (2021). *Head Pose Estimation Based Robust Multicamera Face Recognition. The 2021 International Conference on Artificial Intelligence and Smart Systems.* doi:10.1109/icais50930.2021.93959

Baganzi, R., & Lau, A. K. W. (2017). Examining Trust and Risk in Mobile Money Acceptance in Uganda. *Sustainability*, *9*(12), 1-22. https://doi.org/10.3390/su9122233

Bai, G. (2014, December). *An Organic View of Prototyping in Information System Development. The 2014 IEEE 17th International Conference on Computational Science and Engineering*. https://doi.org/10.1109/cse.2014.333

Bai, X., Jiang, F., Shi, T., & Wu, Y. (2020). *Design of Attendance System Based on Face Recognition and Android Platform. The 2020 International Conference on Computer Network, Electronic and Automation.* doi:10.1109/iccnea50255.2020.00033

Baida, R., Andriienko, M., & Plechawska-Wójcik, M. (2020). Performance analysis of frameworks Angular and Vue.js. *Journal of Computer Sciences Institute*, *14*, 59–64. https://doi.org/10.35784/jcsi.1577

Baig, A. F., & Eskeland, S. (2021). Security, Privacy, and Usability in Continuous Authentication: A Survey. *Sensors*, 21(17), 1–26. https://doi.org/10.3390/s21175967

Balram, S., & Dragicevic, S. (2006). Modeling Collaborative GIS Processes Using Soft Systems Theory, UML and Object-Oriented Design. *Transactions in GIS*, 10(2), 199–218. doi:10.1111/j.1467-9671.2006.00253.x

Banani, S., Thiemjarus, S., Wongthavarawat, K., & Ounanong, N. (2021). A Dynamic Light-Weight Symmetric Encryption Algorithm for Secure Data Transmission via BLE Beacons. *Journal of Sensor and Actuator Networks*, 11(1), 1–19. https://doi.org/10.3390/jsan11010002

Bani-Hani, A., Majdalweieh, M., & AlShamsi, A. (2019). *Online Authentication Methods Used in Banks and Attacks against these Methods. Procedia Computer Science*, 1052–1059. https://doi.org/10.1016/j.procs.2019.04.149

Bank of Uganda (BoU). (2018, June). *Bank of Uganda Annual Report 2017/18*. Bank of Uganda.https://www.bou.or.ug/bou/bouwebsite/bouwebsitecontent/publications/Annual_Reports/All/Bank-of-Uganda-Annual-Report-2018.pdf

Bank of Uganda (BoU). (2019). *Bank of Uganda (BoU) Annual Report-2018/19*. https:// scholar. google. com

Bank of Uganda. (2021). *Bank of Uganda Annual Report 2021*. https://scholar.google.com/

Bao, X., Zhang, X., Lin, J., Chu, D., Wang, Q., & Li, F. (2019, November). *Towards the Trust-Enhancements of Single Sign-On Services. The 2019 IEEE Conference on Dependable and Secure Computing.* https://doi.org/10.1109/dsc47296.2019.8937676

Barker, E., & Barker, W. C. (2019, May). *Recommendation for Key Management: Part 2—Best Practices for Key Management Organizations* (NIST Special Publication 800–57 Part 2 Revision 1). *National Institute of Standards and Technology*. https:// doi. org/ 10. 6028/NIST.SP.800-57pt2r1

Basharzad, S. N., & Fazeli, M. (2017, December). *Knowledge-based dynamic password. The 2017 IEEE 4th International Conference on Knowledge-Based Engineering and Innovation.* https://doi.org/10.1109/kbei.2017.8325004

Basigie, A., & Mtaho, L. M. (2014). Securing Mobile Money Services in Tanzania: A Case of Vodacom M-Pesa. *International Journal of Computer Science & Network Solutions*, 2(5), 1-11.

Baskerville, R., Baiyere, A., Gregor, S., Hevner, A., & Rossi, M. (2018). Design Science Research Contributions: Finding a Balance between Artifact and Theory. *Journal of the Association for Information Systems*, 19(5), 358-376.

Bati, K. (2021). Integration of Python into Science Teacher Education, Developing Computational Problem Solving and Using Information and Communication Technologies Competencies of Pre-service Science Teachers. *Informatics in Education*, 2021, 1–16. https:// doi. org/ 10. 15388/infedu.2022.12

Baur-Yazbeck, S., Frickenstein, J., & Medine, D. (2019, November). *Cyber Security in Financial Sector Development: Challenges and potential solutions for financial inclusion.* https://scholar.google.com

Bensalem, H., Blaquiere, Y., & Savaria, Y. (2021). *Acceleration of the Secure Hash Algorithm-256 (SHA-256) on an FPGA-CPU Cluster Using OpenCL. The 2021 IEEE International Symposium on Circuits and Systems.* https://scholar.google.com

Best, J.W., & Kahn, J.V. (2006). *Research in Education* (10th Ed.). Pearson Education Inc.

Bharadi, V. A., Shah, D. N., Thapa, N. T., Pandya, B. H., & Cosma, G. (2018). *Multi-Instance Iris Recognition. The 2018 Fourth International Conference on Computing Communication Control and Automation.* https://scholar.google.com

Binbeshr, F., Mat Kiah, M., Por, L. Y., & Zaidan, A. (2021). A systematic review of PIN-entry methods resistant to shoulder-surfing attacks. *Computers & Security,* 101, 102–116. https://doi.org/10.1016/j.cose.2020.102116

Bojjagani, S., & Sastry, V. N. (2017). *VAPTAi: A Threat Model for Vulnerability Assessment and Penetration Testing of Android and iOS Mobile Banking Apps. The 2017 IEEE 3rd International Conference on Collaboration and Internet Computing.* doi:10. 1109/cic. 2017. 00022

Boonkrong, S. (2021). *Methods and threats of authentication. In: Authentication and Access Control*. Apress. https://scholar.google.com

Borah, T. R., Sarma, K. K., & Talukdar, P. H. (2015). *Retina Recognition System Using Adaptive Neuro-Fuzzy Inference System. 2015 International Conference on Computer, Communication and Control.* doi:10.1109/ic4.2015.7375663

Bornare, V., Nikam, K., Khedkar, D., & Hole, S. (2020). Data Sharing with Sensitive Information Hiding for Secure Cloud Storage. *IJSRD - International Journal for Scientific Research & Development*, *8*(3), 139–141.

Bosamia, M., & Patel, D. (2019). Wallet Payments Recent Potential Threats and Vulnerabilities with its possible security Measures. *International Journal of Computer Sciences and Engineering*, *7*(1), 810–817. https://doi.org/10.26438/ijcse/v7i1.810817

Bosamia, M. P. (2017). *MobileWallet Payments Recent Potential Threats and Vulnerabilities with its possible security Measures. The 2017 International Conference on Soft Computing and Its Engineering Applications.* https://scholar.google.com

Bouam, M., Bouillaguet, C., Delaplace, C., & Noûs, C. (2021). Computational records with aging hardware: Controlling half the output of SHA-256. *Parallel Computing*, *106*, 1–11. https://doi.org/10.1016/j.parco.2021.102804

Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, *9*(2), 27–40. https://doi.org/10.3316/qrj0902027

Bryman, A. (2012). *Social Research Methods* (4th Ed.). Oxford University Press.

Buku, M. (2017, May 25). *Innovation in Mobile Money: What Are the Risks?* CGAP. https://scholar.google.com

Buku, M., & Mazer, R. (2017). *Fraud in Mobile Financial Services: Protecting Consumers, Providers, and the System*. CGAP. https://www.cgap.org/sites/default/files/Brief-Fraud-in-Mobile-Financial-Services-April-2017.pdf

Bultel, X., Dreier, J., Giraud, M., Izaute, M., Kheyrkhah, T., Lafourcade, P., Lakhzoum, D., Marlin, V., & Mota, L. (2018, May). *Security Analysis and Psychological Study of Authentication Methods with PIN Codes. The 2018 12th International Conference On Research Challenges In Information Science*. https://scholar.google.com

Byun, D. H., Yang, H. N., & Chung, D. S. (2020). Evaluation of Mobile Applications Usability of Logistics in Life Startups. *Sustainability*, *12*(21), 1–17. https://doi.org/10.3390/su12219023

Cagiltay, N. E., Tokdemir, G., Kilic, O., & Topalli, D. (2013). Performing and analysing non-formal inspections of the entity-relationship diagram (ERD). *Journal of Systems and Software*, *86*(8), 2184–2195. https://doi.org/10.1016/j.jss.2013.03.106

Canales, C. (2020, March). *FIDO Alliance Overview* [Slides]. NovuGens. https:// novugens. com/ wp-content/uploads/2020/03/ID37-FIDO-Alliance-2.pdf

Canales, C. (2020, March). *FIDO Alliance Overview. The 2020*. Novugens. https:// scholar. google. com

Caporusso, N. (2021, September). An Improved PIN Input Method for the Visually Impaired. *The 2021 44th International Convention on Information, Communication and Electronic Technology,* Opatija, Croatia. https://doi.org/10.23919/mipro52101.2021.9597153

Caro-Alvaro, S., Garcia-Lopez, E., Garcia-Cabot, A., de-Marcos, L., & Martinez-Herraiz, J. J. (2018). Identifying Usability Issues in Instant Messaging Apps on iOS and Android Platforms. *Mobile Information Systems, 2018,* 1–19.

Carter, R. A., Anton, A. I., Dagnino, A., & Williams, L. (2001). *Evolving Beyond Requirements Creep: A Risk-Based Evolutionary Prototyping Model. Proceedings Fifth IEEE International Symposium on Requirements Engineering*. doi:10.1109/isre.2001.948548

Castle, S., Pervaiz, F., Weld, G., Roesner, F., & Anderson, R. (2016, November). *Let's Talk Money: Evaluating the Security Challenges of Mobile Money in the Developing World. Proceedings of the 7th Annual Symposium on Computing for Development.* https://doi.org/10.1145/3001913.3001919

Cayir, A. N., & Navruz, T. S. (2021). *Effect of Dataset Size on Deep Learning in Voice Recognition. The 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications. doi:10.1109/hora52670.2021.946139*

Cepheli, Z., Büyükçorak, S., & Kurt, K. G. (2016). Hybrid Intrusion Detection System for DDoS Attacks. *Journal of Electrical and Computer Engineering, 2016,* 1–8.

Chadwick, D. W., Laborde, R., Oglaza, A., Venant, R., Wazan, S., & Nijjar, M. (2019). Improved Identity Management with Verifiable Credentials and FIDO. *IEEE Communications Standards Magazine, 3*(4), 14–20.

Chaithra, T. S., & Ajay, N. (2020). P3 Search for Intellectual Processing Of Encrypted Data in Cloud. *European Journal of Molecular & Clinical Medicine*, 7(8), 2951-2971. https://ejmcm.com/pdf_4807_9c4fef8f6757c42e5e59bd0b814658d3.html

Chakraborty, M., Roy, M., Biswas, P. K., & Mitra, P. (2020). *Unsupervised Pre-Trained, Texture Aware and Lightweight Model for Deep Learning-Based Iris Recognition Under Limited Annotated Data. The 2020 IEEE International Conference on Image Processing.* doi:10.1109/icip40778.2020.919108

Chakraborty, N., Li, J., Mondal, S., Chen, F., & Pan, Y. (2019). On Overcoming the Identified Limitations of a Usable PIN Entry Method. *Access*, 7, 124366–124378.

Chang, Y. Y., Yan, S. L., Lin, P. Z., Zhong, H. B., Marescaux, J., Su, J. L., Wang, M. L., & Lee, P. Y. (2015). A mobile medical QR-code authentication system and its automatic FICE image evaluation application. *Journal of Applied Research and Technology*, *13*(2), 220–229. https://doi.org/10.1016/j.jart.2015.06.020

Chaveesuk, S., & Piyawat, N. (2021). Use of QR code technology in eastern Thailand: entrepreneur perspective. *Utopía Praxis Latinoamericana*, 26(2), 76–88.

Checkland, P. (1994). Systems Theory and Management Thinking. *American Behavioral Scientist*, *38*(1), 75–91. https://doi.org/10.1177/0002764294038001007

Checkland, P. (2000). Soft systems methodology: A thirty year retrospective. *Systems Research and Behavioral Science*, *17*(1), 11–58.

Checkland, P., & Scholes, J. (1990). *Soft Systems Methodology in Action*. Wiley. https://scholar.google.com

Chen, N. S., & Huang, S. Y. (2002). Applying the evolutionary prototyping model in developing stream-based lecturing systems. *Interactive Educational Multimedia*, 4, 62–75. http://www.ub.es/multimedia/iem

Chen, Y., & Li, S. (2020). *A High-Throughput Hardware Implementation of SHA-256 Algorithm. The 2020 IEEE International Symposium on Circuits and Systems*. doi:10. 1109/ iscas45731.2020.9181065

Chetalam, J. L. (2018). *Enhancing Security of MPesa Transactions by Use of Voice Biometrics* [Master's Thesis, The United States International University - Africa]. USIU-A Digital Repository. http://erepo.usiu.ac.ke/11732/4113.

Chinta, M., Alaparthi, J., & Koda, E. (2016). A Study on Social Engineering Attacks and Defence Mechanisms. *The International Journal of Computer Science and Information Security*, 14, 225–231.

Chishti, M. S., King, C. T., & Banerjee, A. (2021). Exploring Half-Duplex Communication of NFC Read/Write Mode for Secure Multi-Factor Authentication. *Access*, 9, 6344–6357. doi:10.1109/access.2020.3048711

Cho, J., Seo, G. W., Lee, J. S., Cho, H. K., Kang, E. M., Kim, J., Chun, D., Yi, Y., & Won, S. H. (2021). The usefulness of the QR code in orthotic applications after orthopaedic surgery. *Healthcare*, 9(3), 1–7. https://doi.org/10.3390/healthcare9030298

Chou, G. J., & Wang, R. Z. (2020). The Nested QR Code. *IEEE Signal Processing Letters*, 27, 1230–1234. https://doi.org/10.1109/lsp.2020.3006375

Cohen, L., Manion, L., & Morrison, K. R. B. (2007). *Research Methods in Education*. Routledge. https://scholar.google.com

Coneland, R., & Crespi, N. (2013, October). *Wallet-On-Wheels: Using Vehicle's Identity for Secure Mobile Money. The 2013 17th International Conference on Intelligence in Next Generation Networks.* https://doi.org/10.1109/icin.2013.6670900

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: Risks, vulnerabilities, and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research,* 6, 31–38. 10.4018/978-1-7998-6504-9.ch002

Costa, E., Soares, A. L., & de Sousa, J. P. (2020). Industrial business associations improving the internationalisation of SMEs with digital platforms: A design science research approach. *International Journal of Information Management*, 53, 102070. doi:10. 1016/j. ijinfomgt. 2020.102070

Creswell, J. W. (2005). *Educational Research: Planning, Conducting and Evaluating Quantitative and Qualitative Research* (2nd Ed.). Pearson. https://scholar.google.com

Creswell, J. W. (2011). *Educational Research: Planning, Conducting and Evaluating Quantitative and Qualitative Research* (4th Ed.). Pearson. https://scholar.google.com

Creswell, J. W., & Clark, V. P. L. (2010). *Designing and Conducting Mixed Methods Research* (Second ed.). SAGE Publications, Inc. https://scholar.google.com

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, 16, 297–334. https://doi.org/10.1007/BF02310555

Danlami, M., Jamel, S., Ramli, S. N., & Azahari, S. R. M. (2020). *Comparing the Legendre Wavelet filter and the Gabor Wavelet filter for Feature Extraction based on Iris Recognition System. The 2020 IEEE 6th International Conference on Optimization and Applications,* 1-6. doi:10.1109/icoa49421.2020.909446

Das, A., Satija, T., Zilpe, S., Kavya, J., & Kar, N. (2018). A Study of Threat Model on Mobile Wallet Based Payment System. *International Journal of Computational Intelligence & IoT*, 2(4), 760-765. file:///C:/Users/ghuma/Downloads/SSRN-id3361202.pdf

Das, I., Das, R., Singh, S., Banerjee, A., Mohiuddin, M. G., & Chowdhury, A. (2020, July). *Design and Implementation of Eye Pupil Movement Based PIN Authentication System. 2020 IEEE VLSI Device Circuit and System*. https://scholar.google.com

Dasgupta D., Roy A., & Nag A. (2017). *Biometric Authentication: Advances in User Authentication. Infosys Science Foundation Series (pp. 37-84).* Springer. https:// doi. org/ 10.1007/978-3-319-58808-7_2

Dawodi, M., Hedayati, M. H., Baktash, J. A., & Erfan, A. L. (2019). *Facebook MySQL Performance vs MySQL Performance. The 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference*. 0103-0108. doi:10.1109/iemcon. 2019.8936259

Demuyakor, J., & Demuyakor, I. (2021). Online Shopping on the Go: An assessment of QR Code Utilization among African University Students in China. *International Journal of Science and Business*, 5(5), 22–37. https://doi.org/10.5281/zenodo.4603186

Deshmukh, S. P., & Naware, A. M. (2014). Mobile Money: M-payment System for India. *International Journal of Computer Science and Information Technologies*, 5(2), 2672–2675.

Devasena, C. L. (2018). Three-Factor Authentication for Fortified Login to Ensure Privacy Preservation and Improved Security. *International Journal of Applied Engineering Research,* 13(10), 7576–7579.

Devendra, S. (2021). The Significant Role of Smartphones in Improving Consumer's Quality of Life. *International Journal of Advance Research and Innovative Ideas in Education,* 7(1), 578–586. www.ijariie.com

Dey, S., Saha, S., Singh, A. K., & McDonald-Maier, K. (2021). FoodSQRBlock: Digitizing food production and the supply chain with blockchain and QR code in the cloud. *Sustainability*, 13(6), 1–11. https://doi.org/10.3390/su13063486

Dijesh, P., Babu, S., & Vijayalakshmi, Y. (2020). Enhancement of e-commerce security through asymmetric key algorithm. *Computer Communications*, *153*, 125–134.

Din, M. M., Anwar, R. M., & Fazal, F. A. (2021). Asset tagging for library system - does QR relevant? *Journal of Physics: Conference Series*, 1860(1), 1–11.

Dornbierer, A. (2020, July). *Mobile Money and Financial Crime* (No. 18). Basel Institute on Governance. https://scholar.google.com

Downing S. M. (2004). Reliability: On the reproducibility of assessment data. *Medical Education*, *38*(9), 1006–1012. https://doi.org/10.1111/j.1365-2929.2004.01932.x

Dua, A., & Dutta, A. (2019). *A Study of Applications Based on Elliptic Curve Cryptography. The 2019 3rd International Conference on Trends in Electronics and Informatics*. doi:10.1109/icoei.2019.8862708

Dubey, P. K., Jangid, A., & Chandavarkar, B. R. (2020). *An Interdependency between Symmetric Ciphers and Hash Functions: A Survey. The 2020 11th International Conference on Computing, Communication and Networking Technologies*. doi: 10. 1109/ icccnt 49239. 2020.9225

Dubey, R., & Martin, M. V. (2021, December). *Fool Me Once: A Study of Password Selection Evolution over the Past Decade. The 2021 18th International Conference on Privacy, Security and Trust (PST)*. https://doi.org/10.1109/pst52912.2021.9647823

Dutson, J., Allen, D., Eggett, D., & Seamons, K. (2019, June). *Don't Punish all of us: Measuring User Attitudes about Two-Factor Authentication. The 2019 IEEE European Symposium on Security and Privacy Workshops*. https://doi.org/10.1109/eurospw.2019.00020

Ejaz, M. S., Islam, M. R., Sifatullah, M., & Sarker, A. (2019). *Implementation of Principal Component Analysis on Masked and Non-masked Face Recognition. The 2019 1st International Conference on Advances in Science, Engineering and Robotics Technology*. doi:10.1109/icasert.2019.8934543

ElGhanam, E., Ahmed, I., Hassan, M., & Osman, A. (2021). Authentication and Billing for Dynamic Wireless EV Charging in an Internet of Electric Vehicles. *Future Internet*, *13*(10), 1–19. https://doi.org/10.3390/fi13100257

Eliseo, M. A., Casac, B. S., & Gentil, G. R. (2017, June). *A Comparative Study of Video Content User Interfaces Based On Heuristic Evaluation. The 2017 12th Iberian Conference on Information Systems and Technologies*. https://scholar.google.com

Emanuela, E., Widyanti, A., & Pratama, G. B. (2020). *Usability Evaluation of a Fintech Lending Mobile Application for University Student: A Case Study. The 5th International Conference on Information Technology and Digital Applications*. https:// scholar. google.com

Eyada, M. M., Saber, W., El Genidy, M. M., & Amer, F. (2020). Performance Evaluation of IoT Data Management Using MongoDB Versus MySQL Databases in Different Cloud Environments. *Access*, 8, 110656–110668. doi:10.1109/access.2020.3002164

Fang, X., Yang, G., & Wu, Y. (2017). *Research on the Underlying Method of Elliptic Curve Cryptography. The 2017 4th International Conference on Information Science and Control Engineering.* doi:10.1109/icisce.2017.139

Feng, H., Li, H., Pan, X., & Zhao, Z. (2021). *A Formal Analysis of the FIDO UAF Protocol. Proceedings. The 2021 Network and Distributed System Security Symposium*. https://doi.org/10.14722/ndss.2021.24363

Feng, H., Li, H., Pan, X., Zhao, Z., & Cactilab, T. (2021). A formal analysis of the FIDO UAF protocol. *The Network and Distributed Systems Security (NDSS) Symposium, 2021*, 1–15. https://www.ndss-symposium.org/wp-content/uploads/ndss2021_4A-224363.pdf

Feng, Z. (2018). Biometric Identification Technology and Development Trend of Physiological Characteristics. *Journal of Physics: Conference Series*, 1060, 1–6. https://doi.org/10.1088/1742-6596/1060/1/012047

Fingerprints. (2017). *Biometric Technologies* [White paper]. Fingerprints. https:// www. fingerprints. com

Fishbein, M., & Ajzen, I. (1975), *Beliefs, Attitude, Intention, and Behavior: An Introduction to Theory and Research Reading*, Addison-Wesley. https://scholar.google.com

Focardi, R., Luccio, F. L., & Wahsheh, H. A. M. (2019). Usable security for QR codes. *Journal of Information Security and Applications*, 48, 1–9.

Gabriela, M. (2017). Change of Functional Requirements for Information Systems Integration with Internet of Things. *Journal of Software and Systems Development*, 2017, 1–18. https://doi.org/10.5171/2017.361662

Geetha, M., Latha, R. S., Nivetha, S. K., Hariprasath, S., Gowtham, S., & Deepak, C. S. (2021). *Design of Face Detection and Recognition System to Monitor Students during Online Examinations using Machine Learning algorithms. The 2021 International Conference on Computer Communication and Informatics.* doi:10.1109/iccci50826.2021.94025

Geetha, V., Anbumani, V., Selvi, T., Sindhuja, C. S., & Vanathi, S. (2021). IoT Based Well-organized Hostel Power Consumption and Attendance Administration System. *IOP Conference Series: Materials Science and Engineering*, *1055*(1), 1–9.

Gilman, L., & Joyce, M. (2012). *Managing the Risk of Fraud in Mobile Money*. https://scholar.google.com/

Gilmore, A. K., Davidson, T. M., Leone, R. M., Wray, L. B., Oesterle, D. W., Hahn, C. K., Flanagan, J. C., Gill-Hopple, K., & Acierno, R. (2019). Usability Testing of a Mobile Health Intervention to Address Acute Care Needs after Sexual Assault. *International Journal of Environmental Research and Public Health*, 16(17), 1-16.

Gliner, J. A., & Morgan, G. A. (2000). *Research Methods in Applied Settings: An Integrated Approach to Design and Analysis*. Lawrence Erlbaum Associates Publishers. https://scholar.google.com

Goel, N., Sharma, A., & Goswami, S. (2017). *A Way to Secure a QR Code: SQR. The 2017 International Conference On Computing, Communication And Automation.* doi:10.1109/ccaa.2017.8229850

Goldkuhl, G. (2012). Pragmatism Vs Interpretivism in Qualitative Information Systems Research. *European Journal of Information Systems*, *21*(2), 135–146. https:// doi. org/ 10.1057/ejis .2011.54

Gregor, S. (2002). Design Theory in Information Systems. *Australasian Journal of Information Systems*, *10*(1), 14–22. https://doi.org/10.3127/ajis.v10i1.439

Gregor, S. (2006). The Nature of Theory in Information Systems. *MIS Quarterly*, 30(3), 611-642. doi:10.2307/25148742

Gregor, S., & Hevner, A. R. (2013). Positioning and Presenting Design Science Research for Maximum Impact. *MIS Quarterly*, *37*(2), 337–355. https://doi.org/10.25300/misq/2013 /37.2.01

Gregor, S., & Jones, D. (2007). The Anatomy of a Design Theory. *Journal of the Association for Information Systems*, *8*(5), 312–335. https://doi.org/10.17705/1jais.00129

Guerrero-García, J. (2014). Evolutionary design of user interfaces for workflow information systems. *Science of Computer Programming*, *86*, 89–102.

Guha, R. (2021). *A Report on Automatic Face Recognition: Traditional to Modern Deep Learning Techniques. The 2021 6th International Conference for Convergence in Technology*. doi:10.1109/i2ct51068.2021.941806

Gunasekaran, E., & Muthuraman, V. (2020). *Hierarchical Convolutional Neural Network-based Iris Segmentation and Recognition System for Biometric Authentication. The 2020 International Conference on Communication and Signal Processing*. doi:10. 1109/ iccsp48568.2020.91822

Guo, C., Cai, Q., Wang, Q., & Lin, J. (2020). *Extending Registration and Authentication Processes of FIDO2 External Authenticator with QR Codes. The 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications.* doi:10.1109/trustcom50675.2020.0076

Haj-Bolouri, A., Bernhardsson, L., Bernhardsson, P., & Svensson, L. (2016). *An Information Systems Design Theory for Adaptabe E-Learning. The 2016 49th Hawaii International Conference on System Sciences*. doi:10.1109/hicss.2016.550

Hamandi, K., Salman, A., Elhajj, I. H., Chehab, A., & Kayssi, A. (2015). Messaging Attacks on Android: Vulnerabilities and Intrusion Detection. *Mobile Information Systems*, 2015, 1–13. https://doi.org/10.1155/2015/746930

Hammad, M., Pławiak, P., Wang, K., & Acharya, U. R. (2020). ResNet-Attention model for human authentication using ECG signals. *Expert Systems*, 38(6), 1–17. https:// doi. org/ 10. 1111/exsy.12547

Hamza, A., & Kumar, B. (2020). *A Review Paper on DES, AES, RSA Encryption Standards. The 2020 9th International Conference System Modeling and Advancement in Research Trends*. doi:10.1109/smart50582.2020.9336800

Han, Y. (2021). *Design of an Active Infrared Iris Recognition Device. The 2021 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers*. doi: 10. 1109/ ipec51340. 2021.942110

Han, Z., Yang, L., Wang, S., Mu, S., & Liu, Q. (2018). Efficient Multifactor Two-Server Authenticated Scheme under Mobile Cloud Computing. *Wireless Communications and Mobile Computing*, *2018*, 1–14. https://doi.org/10.1155/2018/9149730

Haq, A., & Shabbir, J. (2014). An improved estimator of finite population mean when using two auxiliary attributes. *Applied Mathematics and Computation*, 241, 14–24. https:// doi. org/10.1016/j.amc.2014.04.069

Hari, S. M. K., Pradyumna, G., Aishwarya. B., & Gayathri, C. (2021, April). *Development of Personal Identification Number Authorization Algorithm Using Real-Time Eye Tracking & Dynamic Keypad Generation. The 2021 6th International Conference for Convergence in Technology*. https://scholar.google.com

Harris, A., Goodman, S., & Traynor, P. (2013). Privacy and Security Concerns Associated with Mobile Money Applications in Africa. *Washington Journal of Law, Technology & Arts*, 8(3), 245–264. https://digitalcommons.law.uw.edu/wjlta/vol8/iss3/5/

Hassan, M. A., & Shukur, Z. (2021a). *A Secure Multi-Factor User Authentication Framework for Electronic Payment System. The 2021 3rd International Cyber Resilience Conference (CRC)*. https://doi.org/10.1109/crc50527.2021.9392564

Hassan, M. A., & Shukur, Z. (2021b). Device Identity-Based User Authentication on Electronic Payment System for Secure E-Wallet Apps. *Electronics*, 11(1), 1–29.

Hassan, M. A., Shukur, Z., & Hasan, M. K. (2020). An Efficient Secure Electronic Payment System for E-Commerce. *Computers*, 9(3), 1–13.

Haware, S., & Barhatte, A. (2017). *Retina based biometric identification using SURF and ORB feature descriptors. The 2017 International Conference on Microelectronic Devices, Circuits and Systems*. doi:10.1109/icmdcs.2017.8211697

Hayikader, S., Hanis, F.N., & Ibrahim, J. (2016). Issues and Security Measures of Mobile Banking Apps. *International Journal of Scientific and Research Publications*, 6(1), 36–41. http://www.ijsrp.org/research-paper-0116/ijsrp-p4908.pdf

He, Y., Zhang, H., Yang, E., & Fang, S. (2020, December). *Virtual Step PIN Pad: Towards Foot-input Authentication Using Geophones. The 2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems*. https://doi.org/10.1109/mass50613.2020.00084

Höhn, S., & Bongard-Blanchy, K. (2020, November). Heuristic Evaluation of COVID-19 Chatbots. *Chatbot Research and Design*, 2020, 131–144. https://doi.org/10.1007/978-3-030-68288-0_9

Hove, L., & Dubus, A. (2019). M-PESA and Financial Inclusion in Kenya: Of Paying Comes Saving? *Sustainability*, *11*(3), 1-26. https://doi.org/10.3390/su11030568

Hsiao, C. S., & Fan, C. P. (2021). *EfficientNet Based Iris Biometric Recognition Methods with Pupil Positioning by U-Net. The 2021 3rd International Conference on Computer Communication and the Internet*. doi:10.1109/iccci51764.2021.94867

Hsiao, C. S., Fan, C. P., & Hwang, Y. T. (2021). *Design and Analysis of Deep-Learning Based Iris Recognition Technologies by Combination of U-Net and EfficientNet. The 2021 9th International Conference on Information and Education Technology*. doi:10. 1109/iciet51873.2021.9419589

Hu, J. Y., Sueng, C. C., Liao, W. H., & Ho, C. C. (2012). *Android-Based Mobile Payment Service Protected By 3-Factor Authentication and Virtual Private Ad Hoc Networking. The 2012 Computing, Communications and Applications Conference*, 111–116. doi:10.1109/com comap.2012.6154013

Hu, K., & Zhang, Z. (2016). Security analysis of an attractive online authentication standard: FIDO UAF protocol. *China Communications*, *13*(12), 189–198. https://doi.org/10.1109 /cc.2016.7897543

Huang, P. C., Chang, C. C., Li, Y. H., & Liu, Y. (2020). Efficient QR Code Secret Embedding Mechanism Based on Hamming Code. *Access*, 8, 86706–86714.

Huang, X., & Zhang, Y. (2020). Indistinguishability and unextractablility of password-based authentication in the blockchain. *Future Generation Computer Systems*, 112, 561–566. https://doi.org/10.1016/j.future.2020.05.009

Huggi, S., & Jamuna, S. (2020). *Design and Verification of Memory Elements using Python. The 2020 IEEE International Conference on Electronics, Computing and Communication Technologies*. doi:10.1109/conecct50063.2020.9198470

Husny, H. R. M., Binti, N. A. N., Nizar, N. A., Abdullah, N. Y., & Ismail, W. H. W. (2017). Encrypted QR Code System. *Journal of Computing Technologies and Creative Content*, 2(1), 82–92. http://jtec.org.my/index.php/JTeC/article/view/48

Hussain, A., Barakat, M. M., & Zaaba, Z. F. (2020). Heuristic Evaluation of Stock Exchange Mobile Application in Malaysia. *International Journal of Advanced Science and Technology*, 29(6), 340–354.

Ibrokhimov, S., Hui, K. L., Al-Absi, A. A., Lee, H. J., & Sain, M. (2019, May). *Multi-Factor Authentication in Cyber-Physical System: A State of Art Survey. The 2019 21st International Conference on Advanced Communication Technology*. https:// doi. org/ 10. 23919/ ICACT. 2019.8701960

Iftikhar, J., Hussain, S., Mansoor, K., Ali, Z., & Chaudhry, S. A. (2019, March). *Symmetric-Key Multi-Factor Biometric Authentication Scheme. The 2019 2nd International Conference on Communication, Computing and Digital Systems*. https://doi.org/10.1109/c-code. 2019. 8680999

Imamah. (2018, October). *One Time Password (OTP) Based on Advanced Encrypted Standard (AES) and Linear Congruential Generator (LCG). The 2018 Electrical Power, Electronics, Communications, Controls and Informatics Seminar*. https://doi.org/10.1109 /eeccis. 2018.8692931

Imario, A., Sudiharto, D. W., & Ariyanto, E. (2017). *The Validated Voice Recognition Measurement of Several Tribes in Indonesia Using Easy VR 3.0. Case Study: The Prototype of Automated Doors. The 2017 International Seminar on Application for Technology of Information and Communication,* 132-136. doi:10.1109/isemantic.2017 .825185

Islam, I., Munim, K. M., Islam, M. N., & Karim, M. M. (2019, December). *A Proposed Secure Mobile Money Transfer System for SME in Bangladesh: An Industry 4.0 Perspective. The 2019 International Conference on Sustainable Technologies for Industry*. https://doi.org/10.1109/sti47673.2019.9068075

Islam, M. S. (2015). An algorithm for electronic money transaction security (Three Layer Security): A new approach. *International Journal of Security and Its Applications*, 9(2), 203–214. http://dx.doi.org/10.14257/ijsia.2015.9.2.19

Jain, S., Dabola, S., Binjola, S., & Jindal, R. (2021, January). *AlignPIN: Indirect PIN Selection for Protection against Repeated Shoulder Surfing. The 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*. https:// doi. org/10. 1109/ confluence51648.2021.9377176

Jakhiya, M., Mittal-Bishnoi, M., & Purohit, H. (2020, February). *Emergence and Growth of Mobile Money in Modern India: A Study on the Effect of Mobile Money. The 2020 Advances in Science and Engineering Technology International Conferences*. https://doi.org/10.1109/aset48392.2020.9118375

Janakiraman, S., Sree, K. S., Manasa, V. L., Rajagopalan, S., Thenmozhi, K., & Amirtharajan, R. (2018). *OTP on Demand: An Embedded System for User Authentication. The 2018 International Conference on Computer Communication and Informatics*. doi:10. 1109/iccci.2018.8441400

Janiesch, C., Rosenkranz, C., & Scholten, U. (2020). An Information Systems Design Theory for Service Network Effects. *Journal of the Association for Information Systems*, 21, 1402–1460. doi:10.17705/1jais.00642

Jarecki, S., Krawczyk, H., Shirvanian, M., & Saxena, N. (2018). *Two-Factor Authentication with End-to-End Password Security. IACR International Workshop on Public Key Cryptography.* https://doi.org/10.1007/978-3-319-76581-5_15

Javed, M., & Lin, Y. (2018). *Iterative Process for Generating ER Diagram from Unrestricted Requirements. Proceedings of the 13th International Conference on Evaluation of Novel Approaches to Software Engineering.* https://scholar.google.com.

Jeddi, F. R., Nabovati, E., Bigham, R., & Farrahi, R. (2020). Usability evaluation of a comprehensive national health information system: A heuristic evaluation. *Informatics in Medicine Unlocked*, *19*, 1–6. https://doi.org/10.1016/j.imu.2020.100332

Jindal, P., Kaushik, A., & Kumar, K. (2020). *Design and Implementation of Advanced Encryption Standard Algorithm on 7th Series Field Programmable Gate Array. The 2020 7th International Conference on Smart Structures and Systems*. doi:10.1109/icsss4962 1.2020.9202114

Kafeero, S. (2020, October 11). *Uganda's Banks Have Been Plunged into Chaos by a Mobile Money Fraud Hack.* Quartz Africa. https://scholar.google.com/

Kairy, D., Mostafavi, M. A., Blanchette-Dallaire, C., Belanger, E., Corbeil, A., Kandiah, M., Wu, T. Q., & Mazer, B. (2021). A Mobile App to Optimize Social Participation for Individuals with Physical Disabilities: Content Validation and Usability Testing. *International Journal of Environmental Research and Public Health*, *18*(4), 1–20. https:// doi. org/10. 3390/ijerph18041753

Kammoun, M., Elleuchi, M., Abid, M., & BenSaleh, M. S. (2020). *FPGA-based Implementation of the SHA-256 Hash Algorithm. The 2020 IEEE International Conference on Design & Test of Integrated Micro & Nano-Systems)*, 1-6. doi:10.1109/dts48731. 2020.9196134

Kandhari, M. S., Zulkemine, F., & Isah, H. (2018). *A Voice Controlled E-Commerce Web Application. The 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference.* doi:10.1109/iemcon.2018.8614771

Kang, J. (2018). Mobile payment in Fintech environment: Trends, security challenges, and services. *Human-Centric Computing and Information Sciences,* 8(1), 1–16. https:// doi. org/ 10.1186/s13673-018-0155-4

Kanife, E. (2020, September 24). *MTN Rwanda to Fight Mobile Money Fraud with New USSD Code.* Technext. https://scholar.google.com/

Karrach, L., Pivarčiová, E., & Bozek, P. (2020). Recognition of perspective distorted QR codes with a partially damaged finder pattern in real scene images. *Applied Sciences*, 10(21), 1–16. https://doi.org/10.3390/app10217814

Karunanithi, D., & Kiruthika, B. (2011, November). *Single Sign-On and Single Log Out in Identity. International Conference on Nanoscience, Engineering and Technology.* https://doi.org/10.1109/iconset.2011.6168044

Kasat, O. K., & Bhadade, U. S. (2018, April). *Revolving Flywheel PIN Entry Method to Prevent Shoulder Surfing Attacks. The 2018 3rd International Conference for Convergence in Technology*. https://doi.org/10.1109/i2ct.2018.8529758

Kasemiire, C., & Bagala, A. (2020, October 7). *Thieves Use 2000 SIM cards to Rob Banks*. Daily Monitor. https://scholar.google.com/

Katsini, C., Raptis, G. E., Cen, A. J. L., Gamagedara Arachchilage, N. A., & Nacke, L. E. (2021, May). Eye-GUAna: Higher Gaze-Based Entropy and Increased Password Space in Graphical User Authentication through Gamification. *ACM Symposium on Eye Tracking Research and Applications*. https://doi.org/10.1145/3448018.3458615

Kaur, S., Sharma, S., & Singh, A. (2015). Cyber Security: Attacks, Implications, and Legitimations across the Globe. *International Journal of Computer Applications*, 114, 21–23.

Kaushik, V., & Walsh, C. A. (2019). Pragmatism as a Research Paradigm and Its Implications for Social Work Research. *Social Sciences*, *8*(9), 1–17. https://doi.org/10.3390/socsci8090255

Kebande, V. R., Awaysheh, F. M., Ikuesan, R. A., Alawadi, S. A., & Alshehri, M. D. (2021). A Blockchain-Based Multi-Factor Authentication Model for a Cloud-Enabled Internet of Vehicles. *Sensors*, 21(18), 1–20. https://doi.org/10.3390/s21186018

Keerthi, K., & Surendiran, B. (2017). *Elliptic Curve Cryptography for Secured Text Encryption. The 2017 International Conference on Circuit, Power and Computing Technologies.* doi:10.1109/iccpct.2017.8074210

Kekkonen, M., & Oinas-Kukkonen, H. (2019). *Social Comparison in Behaviour Change Support Systems: Heuristic Evaluation of a System's Usability. The Central Europe (CEUR) Workshop Proceedings.* https://scholar.google.com/

Khalid, H., Hashim, S. J., Ahmad, S. M. S., Hashim, F., & Chaudary, M. A. (2020, December). *New and Simple Offline Authentication Approach using Time-based One-time Password with Biometric for Car Sharing Vehicles. The 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering*. https://doi.org/10.1109 /csde50874. 2020. 9411569

Khalifeh, A., Alsyayid, F., Armoush, H., & Darabkh, K. A. (2020). *An Experimental Evaluation of the Advanced Encryption Standard Algorithm and its Impact on Wireless Sensor Energy Consumption. The 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies.* doi:10.1109/3ict51146.

2020.9312023

Khotimah, K., Santoso, A. B., Ma'arif, M., Azhiimah, A. N., Suprianto, B., Sumbawati, M. S., & Rijanto, T. (2020). *Validation of Voice Recognition in Various Google Voice Languages using Voice Recognition Module V3 Based on Microcontroller. The 2020 Third International Conference on Vocational Education and Electrical Engineering*. doi:10. 1109/ icvee50212.2020.92431

Kim, H., Jung, Y., & Jun, M. (2017). A Study on Secure Mobile Payment Service for the Market Economy Revitalization. *Journal of the Korea Academia-Industrial cooperation Society*, 18(3), 41–48.

Kim, H., Lee, D., & Ryou, J. (2020). *User Authentication Method using FIDO based Password Management for Smart Energy Environment. The 2020 International Conference on Data Mining Workshops, 707-710*. doi:10.1109/icdmw51313.2020.00100

Kim, S. H., Choi, D., Kim, S. H., Cho, S., & Lim, K. S. (2018). Context-Aware Multimodal FIDO Authenticator for Sustainable IT Services. *Sustainability*, *10*(5), 1–21. https:// doi. org/10. 3390/su10051656

Kiran R., Nivedha K., Pavithra Devi S., & Subha T. (2017). *Voice and Speech Recognition in the Tamil Language. The 2017 2nd International Conference on Computing and Communications Technologies.* doi:10.1109/iccct2.2017.7972293

Klieme, E., Wilke, J., van Dornick, N., & Meinel, C. (2020). *FIDOnuous: A FIDO2/WebAuthn Extension to Support Continuous Web Authentication. The 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications*. doi:10.1109/trustcom50675.2020.00254

Kosim, K. P., & Legowo, N. (2021). Factors Affecting Consumer Intention on QR Payment of Mobile Banking: A Case Study in Indonesia. *Journal of Asian Finance, Economics and Business*, 8(5), 391–401. https://doi.org/10.13106/jafeb.2021.vol8.no5.0391

Kostelidis, A., & Maniatis, M. K. (2017). *The Majesty of Vue.js 2*. Lean Publishing. https://scholar.google.com

Kothari, C. R. (2004). *Research Methodology: Methods and Techniques* (2nd Ed.). New Age International Publishers. https://scholar.google.com/

Krčadinac, O., ŠOšević, U., & Starčević, D. (2021). Evaluating the Performance of Speaker Recognition Solutions in E-Commerce Applications. *Sensors*, 21(18), 1–11. https://doi.org/10.3390/s21186231

Kuechler, W., & Vaishnavi, V. (2012). A framework for theory development in design science research: multiple perspectives. *Journal of the Association for Information Systems*, 13(6), 395 - 423. https://aisel.aisnet.org/jais/vol13/iss6/3/

Kumar, A., & Panda, S. P. (2019). *A Survey: How Python Pitches in IT-World. 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing*. doi:10.1109/comitcon.2019.8862251

Kumar, B. A., Goundar, M. S., & Chand, S. S. (2019). Usability guideline for Mobile learning applications: an update. *Education and Information Technologies*, 24(6), 3537–3553. https://doi.org/10.1007/s10639-019-09937-9

Kumar, K., Ramkumar, K. R., & Kaur, A. (2020). *A Design Implementation and Comparative Analysis of Advanced Encryption Standard (AES) Algorithm on FPGA. The 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions).* doi:10.1109/icrito48877.2020.9198033

Kunda, D., & Chishimba, M. (2018). A Survey of Android Mobile Phone Authentication Schemes. *Mobile Networks and Applications, 73,* 1–9. https://doi.org/10.1007/s11036-018-1099-7

Kurniawan, I., Sudaryanto, & Sukarno, H. (2021). The Shifting of or Code-Based Payment Method to Improve the Competitive Advantage (Ca) at Bank Jatim through Tam Model Approach. *IOSR Journal of Business and Management,* 23(3), 22–27. https:// doi. org/ 10.9790/487X-2303072227

Lakshmi, K. K., Gupta, H., & Ranjan, J. (2017). USSD: Architecture analysis, security threats, issues and enhancements. *The 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions).* doi:10.1109/ictus.2017.8286115

Lazarev, S. A., Demidov, A. V., Volkov, V. N., Stychuk, A. A., & Polovinkin, D. A. (2016, October). Analysis of Applicability of Open Single Sign-On Protocols in Distributed Information-Computing Environment. *The 2016 IEEE 10th International Conference on Application of Information and Communication Technologies.* https:// scholar. Google .com

Lee, M. B., Kang, J. K., Yoon, H. S., & Park, K. R. (2021). Enhanced Iris Recognition Method by Generative Adversarial Network-Based Image Reconstruction. *IEEE Access,* 9, 10120–10135. doi:10.1109/access.2021.3050788

Lei, Z., Nan, Y., Fratantonio, Y., & Bianchi, A. (2021). *On the Insecurity of SMS One-Time Password Messages against Local Attackers in Modern Mobile Devices. The Network and Distributed System Security Symposium 2021*. https://www.ndss-symposium.org

Lersilp, S., Putthinoi, S., Lerttrakarnnon, P., & Silsupadol, P. (2020). Development and Usability Testing of an Emergency Alert Device for Elderly People and People with Disabilities. *The Scientific World Journal, 2020,* 1–7. https://doi.org/10.1155/2020/5102849

Li, J., Hu, B., & Cao, Z. (2020, August). *A new QR Code Recognition Method using Deblurring and Modified Local Adaptive Thresholding Techniques. The 2020 IEEE 16th International Conference on Automation Science and Engineering*. https:// doi. org/ 10. 1109/ case48305. 2020.9216945

Li, N., & Zhang, B. (2021, April). *The Research on Single Page Application Front-end Development Based on Vue. Journal of Physics: Conference Series*. https://doi.org/10.1088/1742-6596/1883/1/012030

Li, Q. (2019). *An Improved Face Detection Method Based on Face Recognition Application. The 2019 4th Asia-Pacific Conference on Intelligent Robot Systems.* doi:10. 1109/ acirs. 2019. 8936020

Li, X., & Wang, Z. (2019). *Design of King Glory's Game Query System Based on Python. The 2019 3rd International Conference on Electronic Information Technology and Computer Engineering.* doi:10.1109/eitce47263.2019.9094996

Lin, Y., & Xie, H. (2020). *Face Gender Recognition based on Face Recognition Feature Vectors. The 2020 IEEE 3rd International Conference on Information Systems and Computer-Aided Education.* doi:10.1109/ICISCAE51034.2020.9236905

Liu, F. (2013). Efficient Two-Factor Authentication Protocol Using Password and Smart Card. *Journal of Computers*, 8(12), 3257–3263. https://doi.org/10.4304/jcp.8.12.3257-3263

Lone, S. A., & Mir, A. H. (2021). A novel OTP based tripartite authentication scheme. *International Journal of Pervasive Computing and Communications,* 17(3), 1–23. https://doi.org/10.1108/ijpcc-04-2021-0097

Lonie, S. (2017, July 31). *Fraud Risk Management for Mobile Money: An Overview*. Chyp. https://www.chyp.com/wp-content/uploads/2018/06/Fraud-Risk-Management-for-MM-31.07.2017.pdf

Lowe, C., Hanuman Sing, H., Browne, M., Alwashmi, M. F., Marsh, W., & Morrissey, D. (2021). Usability Testing of a Digital Assessment Routing Tool: Protocol for an Iterative Convergent Mixed Methods Study. *The Journal of Medical Internet Research Protocols*, *10*(5), 1-11. https://doi.org/10.2196/27205

Luo, M., Cao, J., Ma, X., Zhang, X., & He, R. (2021). FA-GAN: Face Augmentation GAN for Deformation-Invariant Face Recognition. *Transactions on Information Forensics and Security*, 16, 2341–2355. doi:10.1109/tifs.2021.3053460

Lv, J., Zhang, Y., Dong, W., Gao, Y., & Chen, C. (2020, June). *A General Approach to Robust QR Codes Decoding. The 2020 IEEE/ACM 28th International Symposium on Quality of Service.* https://doi.org/10.1109/iwqos49365.2020.9212963

Lynn, N. D., Islam, A., & Budiyanto, D. (2020). Increasing User Satisfaction of Mobile Commerce using Usability. *International Journal of Advanced Computer Science and Applications*, *11*(8), 300–308. https://doi.org/10.14569/ijacsa.2020.0110839

Macrae, C. (2018). *Vue.js: Up and Running: Building Accessible and Performant Web Apps* (1st ed.). O'Reilly Media. https://scholar.google.com

Maetouq, A., & Daud, S. M. (2020). HMNT: Hash Function Based on New Mersenne Number Transform. *Access*, 8, 80395–80407. doi:10.1109/access.2020.2989820

Mahajan, R., Saran, J., & Rajagopalan, A. (2015). *Mitigating Emerging Fraud Risks in the Mobile Money Industry.* Deloitte. https://scholar.google.com

Mahlangu, T. (2018, May 22). *MTN warns of SIM swap fraud*. REKORD. https:// scholar. google. com

Maina, J. (2019). Cybersecurity: *A Governance Framework for Mobile Money Providers*. https://scholar.google.com

Makulilo, A. B. (2015). Privacy in mobile money: Central banks in Africa and their regulatory limits. *International Journal of Law and Information Technology*, 23(4), 372–391. https://doi.org/10.1093/ijlit/eav014

Malakar, S., Chiracharit, W., Chamnongthai, K., & Charoenpong, T. (2021*). Masked Face Recognition Using Principal component analysis and Deep learning. The 2021 18th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology.* doi: 10. 1109/ ecti- con 51831. 2021. 9454857

Mantoro, T., Ayu, M. A., & Suhendi. (2018). *Multi-Faces Recognition Process Using Haar Cascades and Eigenface Methods. The 2018 6th International Conference on Multimedia Computing and Systems.* doi:10.1109/icmcs.2018.8525935

Markus, M. L., Majchrzak, A., & Les Gasser. (2002). A Design Theory for Systems That Support Emergent Knowledge Processes. *MIS Quarterly*, 26(3), 179–212.

Martin, A. (2019). Mobile Money Platform Surveillance. *Surveillance & Society*, 17(1/2), 213–222. https://doi.org/10.24908/ss.v17i1/2.12924

Martino, R., & Cilardo, A. (2019). A Flexible Framework for Exploring, Evaluating, and Comparing SHA-2 Designs. *Access, 7*, 72443–72456. https://doi.org/10.1109/access.2019.2920089

Maxcy, S. J. (2003). *Pragmatic threads in mixed methods research in the social sciences: The search for multiple modes of inquiry and the end of the philosophy of formalism: Handbook of Mixed Methods in Social and Behavioral Research*. https://scholar.google.com

Mbunge, E., & Rugube, T. (2018). A Robust and Scalable Four-Factor Authentication Architecture to Enhance Security for Mobile Online Transaction. *International Journal of Scientific & Technology Research*, 7(3), 139–143.

McGrath, F., & Lonie, S. (2013). *Platforms for Successful Mobile Money Services*. https://scholar.google.com

McKee, K., Kaffenberger, M., & Zimmerman, J. (2015, June). *Doing Digital Finance Right: The Case for Stronger Mitigation of Customer Risks*. https://scholar.google.com

Mega, B. (2020). *Framework for Improved Security on the Usage of Mobile Money Application based on Iris Biometric Authentication Method in Tanzania* [Master's Dissertation, The University of Dodoma]. https://scholar.google.com

Merks, P., Religioni, U., Arciszewska, K., Pankiewicz, W., Jaguszewski, M., & Vaillancourt, R. (2020). Usability testing and satisfaction of "The Patient Access": A mobile health application for patients with venous thromboembolic disease. A pilot study. *Cardiology Journal*, *27*(6), 891–893. https://doi.org/10.5603/CJ.a2020.0107

Mészárosová, E. (2015). Is Python an Appropriate Programming Language for Teaching Programming in Secondary Schools? *International Journal of Information and Communication Technologies in Education*, *4*(2), 5–14.

Mihas, P. (2019). *Qualitative Data Analysis*. Oxford Research Encyclopedia of Education. DOI:10.1093/ACREFORE/9780190264093.013.1195

Mitra, S., Jana, B., & Poray, J. (2017, December). *Implementation of a Novel Security Technique Using Triple DES in Cashless Transaction. The 2017 International Conference on Computer, Electrical & Communication Engineering*. https:// doi. org/10. 1109/iccece. 2017. 8526233

Mohammed, A., & Al-Gailani, M. F. (2019). *Developing Iris Recognition System Based on Enhanced Normalization. The 2019 2nd Scientific Conference of Computer Sciences (SCCS)*. doi:10.1109/sccs.2019.8852622

Mohit, P., Amin, R., & Biswas, G. P. (2017). Design of Secure and Efficient Electronic Payment System for Mobile Users. *Communications in Computer and Information Science*, 2017, 34–43. https://doi.org/10.1007/978-981-10-4642-1_4

Moolla, Y., De Kock, A., Mabuza-Hocquet, G., Ntshangase, C. S., Nelufule, N., & Khanyile, P. (2021). Biometric Recognition of Infants using Fingerprint, Iris, and Ear Biometrics. *Access*, 9, 38269–38286. https://doi.org/10.1109/access.2021.3062282

Morawczynski, O. (2015, March 11). *Fraud in Uganda: How Millions Were Lost to Internal Collusion*. https://scholar.google.com

Morgan, D. L. (2014). Pragmatism as a Paradigm for Social Research. *Qualitative Inquiry*, *20*(8), 1045–1053. https://doi.org/10.1177/1077800413513733

Morgan, G. A., Leech, N. L., Gloeckner, G. W., & Barrett, K. C. (2012). *IBM SPSS for Introductory Statistics: Use and Interpretation, Fifth Edition* (5th Ed.). Routledge. https://scholar.google.com

Mtaho, A. B. (2015). Improving Mobile Money Security with Two-Factor Authentication. *International Journal of Computer Applications*, 109(7), 9–15. https://doi.org/10.5120 /19198-0826

Mubeen, M., Iqbal, M. W., Junaid, M., Sajjad, M. H., Naqvi, M. R., Khan, B. A., Saeed, M. M., & Tahir, M. U. (2020). *Usability Evaluation of Pandemic Healthcare Mobile Applications. International Symposium of Geoscience, Oil & Gas Engineering, Sustainable and Environmental Technology*. https://scholar.google.com

Mudiri, J. L. (2012). *Fraud in Mobile Financial Services*. https://scholar.google.com/

Musuva-Kigen, P., Ekpeke, M., Inkoom, E., Inkoom, B., Masesa, D., Kaimba, B., Kimani, K., Mwangi, M., Munyendo, B., Mueni, F., Ndegwa, D., Wanjuki, S., Rishad, N., Keige, S., Karanja, J., Soita, H., Ngari, A. N., Nturibi, B. M., Ndegwa, D., . . . Mbae, K. (2016). *Kenya Cyber Security Report 2016*. SERIANU. https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf

Mutong'Wa, S.M., & Khaemba, S.W. (2014). A comparative study of critical success factors (CSFS) in the implementation of mobile money transfer services in Kenya. *European Journal of Engineering and Technology,* 2(2), 8–31.

Nair, S., Khatri, S. K., & Gupta, H. (2019). *A Model to Enhance Security of Digital Transaction. The 2019 4th International Conference on Information Systems and Computer Networks*. doi:10.1109/iscon47742.2019.9036225

Nakamura, K., Hori, K., & Hirose, S. (2021). Algebraic Fault Analysis of SHA-256 Compression Function and Its Application. *Information*, *12*(10), 1–9.

Nawal, A., Soni, H., Arewar, S., & Gangadhara, V. (2021). Secure File Storage on Cloud Using Hybrid Cryptography. *International Journal of Advanced Research in Science, Communication and Technology*, *5*(1), 79–83. https://doi.org/10.48175/ijarsct-1101

Nelson, B. (2018). *Getting to Know Vue.js: Learn to Build Single Page Applications in Vue from Scratch* (1st Ed.). Apress. https://scholar.google.com/

Ngulube, P., Mathipa, E. R., & Gumbo, M. T. (2015). *Theoretical and Conceptual Frameworks in the Social and Management Sciences. In Addressing Research Challenges: Making Headway in Developing Researchers*. Mosala-Masedi Publishers & Booksellers. https://scholar.google.com

Nielsen, J. (1994a, April 24). *10 Usability Heuristics for User Interface Design*. Nielsen Norman Group. https://scholar.google.com

Nielsen, J. (1994b, November 1). *Severity Ratings for Usability Problems: Article by Jakob Nielsen*. Nielsen Norman Group. https://scholar.google.com

Nielsen, J. (2012, June 3). *How Many Test Users in a Usability Study?* Nielsen Norman Group. https://scholar.google.com

Nielsen, J., & Mack, R. L. (1994). *Usability Inspection Methods* (1st Ed.). Wiley. https://scholar.google.com

Nyamtiga, W. B., Sam, A., & Laizer, S. L. (2013a). Enhanced Security Model for Mobile Banking Systems in Tanzania. *International Journal of Technology Enhancements and Emerging Engineering Research*, *1*(4), 4–20.

Nyamtiga, W. B., Sam, A., & Laizer, S. L. (2013b). Security Perspectives for USSD Versus SMS in Conducting Mobile Transactions A Case Study of Tanzania. *International Journal of Technology Enhancements and Emerging Engineering Research*, *1*(3), 38–43. http://paper.researchbib.com/view/paper/16520

Obaidat, M., Brown, J., Obeidat, S., & Rawashdeh, M. (2020). A Hybrid Dynamic Encryption Scheme for Multi-Factor Verification: A Novel Paradigm for Remote Authentication. *Sensors*, 20(15), 1–32. https://doi.org/10.3390/s20154212

Okpara, O. S., & Bekaroo, G. (2017, June). *Cam-Wallet: Fingerprint-Based Authentication in M-Wallets Using Embedded Cameras. The 2017 IEEE International Conference on Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe*. https://doi.org/10.1109/eeeic.2017.7977654

O'Leary, Z. (2004). *The Essential Guide to Doing Research* (1st Ed.). SAGE Publications Ltd. https://scholar.google.com

Ombiro, Z. B. H. (2016). *Mobile-Based Multi-Factor Authentication Scheme for Mobile Banking* [Master's Thesis, University of Nairobi]. University of Nairobi Research Archive. http://erepository.uonbi.ac.ke/handle/11295/99267

Ometov, A., & Bezzateev, S. (2017, November). *Multi-factor authentication: A survey and challenges in V2X applications. The 2017 9th International Congress on Ultra-Modern Telecommunications and Control Systems and Workshops (ICUMT)*. https:// doi. org/ 10. 1109/ icumt.2017.8255200

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. *Cryptography*, 2(1), 1–31.

Ongo, G., & Kusuma, G. P. (2018). *Hybrid Database System of MySQL and MongoDB in Web Application Development. The 2018 International Conference on Information Management and Technology*. doi:10.1109/icimtech.2018.8528120

Onyinyechi, O. P., Ifeanyi, O. A., Nnabuchi, E. N., & Nwakaego, I. P. (2021). Enhanced Business Marketing for Small Scale Enterprises Via the Quick Response Code Technology. *Frontiers*, 1(1), 7–13. https://doi.org/10.11648/j.frontiers.20210101.12

Osman, F., & Nakanishi, H. (2020). High Correctness Mobile Money Authentication System. *International Journal of Psychosocial Rehabilitation*, 24(4), 3544–3556.

Othman, M. K., Sulaiman, M. N. S., & Aman, S. (2018). Heuristic Evaluation: Comparing Generic and Specific Usability Heuristics for Identification of Usability Problems in a Living Museum Mobile Guide App. *Advances in Human-Computer Interaction*, *2018*, 1–13. https://doi.org/10.1155/2018/1518682

Oukili, S., & Bri, S. (2015). FPGA implementation of Data Encryption Standard using time-variable permutations. *The 2015 27th International Conference on Microelectronics*, 126-129. doi:10.1109/icm.2015.7438004

Panos, C., Malliaros, S., Ntantogian, C., Panou, A., & Xenakis, C. (2017). A Security Evaluation of FIDO's UAF Protocol in Mobile and Embedded Devices. *Communications in Computer and Information Science*, 2017, 127–142.

Paramitha, A. A., Dantes, G. R., & Indrawan, G. (2018). *The evaluation of web-based academic progress information system using heuristic evaluation and user experience questionnaire (UEQ). The 2018 Third International Conference on Informatics and Computing*. https://scholar.google.com

Pareek, A., & Khandaker, E. (2018). *Building an In-House Mobile Money Platform*. UN Capital Development Fund (UNCDF). https://amaranteconsulting.com/en/publication /building-a-mobile-money-platform

Patil, P., & Vasanth, K. (2019). *Iris Recognition Using Local and Global Iris Image Moment Features. The 2019 Innovations in Power and Advanced Computing Technologies*. doi:10.1109/i-pact44901.2019.8960219

Patra, R., & Patra, S. (2021). Cryptography: A Quantitative Analysis of the Effectiveness of Various Password Storage Techniques. *Journal of Student Research*, *10*(3), 1–14. https://doi.org/10.47611/jsrhs.v10i3.1764

Pattar, S. Y. (2019). *A Novel Approach towards Iris Segmentation and Authentication using Local Chan-Vese Method. The 2019 5th International Conference on Advanced Computing & Communication Systems.* doi:10.1109/icaccs.2019.8728441

Paul, S., Bruntha, P. M., Raj, A., Saurabh, S., & Masih, S. (2021). Anti-Spoofing Face-Recognition Technique for eKYC Application. *The 2021 3rd International Conference on Signal Processing and Communication*. doi:10.1109/icspc51351.2021.94517

Pavaloi, I., Nita, C. D., & Lazar, L. C. (2019). *Novel Matching Method for Automatic Iris Recognition Using SIFT Features. The 2019 International Symposium on Signals, Circuits and Systems.* doi:10.1109/isscs.2019.8801797

Pavani, K., & Sriramya, P. (2021). *Enhancing Public Key Cryptography using RSA, RSA-CRT and N-Prime RSA with Multiple Keys. The 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks*. doi:10. 1109/ icicv50876. 2021.9388621

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/mis0742-1222240302

Pei, Z., Wang, Y., & Han, L. (2019). *Cancelable Iris Recognition with DPL. 2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference*. doi:10.1109/iaeac47372.2019.89979

Pendurthi, H. K., Kanneganti, S. S., Godavarthi, J., Kavitha, S., & Gokarakonda, H. S. (2021). *Heart Pulse Monitoring and Notification System using Arduino. The 2021 International Conference on Artificial Intelligence and Smart Systems*. https://scholar.google.com

Petre, M. (2013). *UML in Practice. The 2013 35th International Conference on Software Engineering*. doi:10.1109/icse.2013.6606618

Phan, V. D., Pham, H. L., Tran, T. H., & Nakashima, Y. (2021). *High-Performance Multicore SHA-256 Accelerator using Fully Parallel Computation and Local Memory. 2021 IEEE Symposium in Low-Power and High-Speed Chips. https://scholar.google.com*

Phipps, R., Mare, S., Ney, P., Webster, J., & Heimerl, K. (2018, June). *ThinSIM-based Attacks on Mobile Money Systems. Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies*. https://doi.org/10.1145/3209811.3209817

Pimentel, L. J. (2010). A note on the usage of Likert scaling for research data analysis. *USM Research and Development Journal*, 18(2). 109-112.

Poltronieri, I., Zorzo, A. F., Bernardino, M., Medeiros, B., & Campos, M. D. B. (2021). *Heuristic evaluation checklist for domain-specific languages. 16th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications*. https://www.scitepress.org/Papers/2021/102394/102394.pdf

Pramusinto, W., Trya-Sartana, B., Mulyati, S., & Amini, S. (2021). Implementation of AES-192 Cryptography and QR Code to Verify the Authenticity of Budi Luhur University Student Certificate. *Jurnal Pendidikan Teknologi Kejuruan*, *3*(4), 209–215. https:// doi. org/ 10. 24036/jptk.v3i4.14823

Preethi, K., & Vodithala, S. (2021). *Automated Smart Attendance System Using Face Recognition. The 2021 5th International Conference on Intelligent Computing and Control Systems*. doi:10.1109/iciccs51141.2021.9432

Premkumar, A., Lovecchio, F. C., Stepan, J. G., Kahlenberg, C. A., Blevins, J. L., Albert, T. J., & Cross, M. B. (2018). A Novel Mobile Phone Text Messaging Platform Improves Collection of Patient-Reported Post-operative Pain and Opioid Use Following Orthopaedic Surgery. *Hospital for Special Surgery Journal, 15*(1), 37–41. https:// doi. org/ 10. 1007/s11420-018-9635-3

Pretschner, A., Lotzbeyer, H., & Philipps, J. (2001). *Model-based testing in evolutionary software development. The 12th International Workshop on Rapid System Prototyping RSP 2001*. doi:10.1109/iwrsp.2001.933854

Priya, S. P. (2017). Biometrics and Fingerprint Payment Technology. *International Journal of Advanced Research in Computer Science & Technology*, 5(1), 114–118.

Pronika, P., & Tyagi, S. S. (2021). Enhancing Security of Cloud Data through Encryption with AES and Fernet Algorithm through Convolutional-Neural-Networks (CNN). *International Journal of Computer Networks and Applications*, *8*(4), 288–299. https:// doi. org/ 10.22247/ijcna/2021/209697

Pšenák, P., & Tibenský, M. (2020). The usage of the Vue JS framework for web application creation. *Mesterséges Intelligencia*, *2*(2), 61–72. https://doi.org/10.35406/mi.2020.2.61

Purnomo, A. T., Gondokaryono, Y. S., & Kim, C. S. (2016, October). Mutual authentication in securing mobile payment system using encrypted QR code based on Public Key Infrastructure. *The 2016 6th International Conference on System Engineering and Technology*. https://doi.org/10.1109/icsengt.2016.7849649

Putra, A. H., Pramana, D., & Srinadi, N. L. P. (2019). Archives Management System Using Laravel Framework and Vue.Js (Case Study: BPKAD Bali Province). *Journal of Systems and Informatics,* 13(2), 97-104.

Putri, N. L., Maulana, A., Maryam, S. D., & Juraida, A. (2021). Improving Online Course Based on the Result of Usability Testing Methods. *Psychology and Education,* 58(1), 6373–6382. https://doi.org/10.17762/pae.v58i1.3795

Qiuyun, X., Ligang, H., Qiming, L., Shuqin, G., & Jinhui, W. (2017). The Verification of SHA-256 IP using a semi-automatic UVM platform. doi:10.1109/icemi.2017.8265733

Quan, Y. (2019, July). *Design and Implementation of E-commerce Platform based on Vue.js and MySQL. Proceedings of the 3rd International Conference on Computer Engineering, Information Science & Application Technology*. https://doi.org/ 10.2991/iccia-19.2019.69

Quiñones, D., Rusu, C., Arancibia, D., González, S., & Saavedra, M. J. (2020). SNUXH: A Set of Social Network User Experience Heuristics. *Applied Sciences*, *10*(18), 1–42. https://doi.org/10.3390/app10186547

Radojicic, T., Bozovic, M., & Blagojevic, N. (2020). *Iris Recognition on Images Reconstructed with Gradient-based Algorithm. The 2020 9th Mediterranean Conference on Embedded Computing*. doi:10.1109/meco49872.2020.913411

Rahav, A. (2018). *What Is Single-Factor Authentication (SFA)? | Security Wiki.* Secret Double Octopus. https://scholar.google.com

Rahman, M. S. (2016). The Advantages and Disadvantages of Using Qualitative and Quantitative Approaches and Methods in Language "Testing and Assessment" Research: A Literature Review. *Journal of Education and Learning,* 6(1), 102–112.

Raj, A., & D'Souza, R. (2020). Implementation of MySQL in Python. *International Journal of Research and Analytical Reviews*, *7*(1), 447–451.

Rajamanickam, S., Vollala, S., Amin, R., & Ramasubramanian, N. (2020). Insider Attack Protection: Lightweight Password-Based Authentication Techniques Using ECC. *IEEE Systems Journal*, 14(2), 1972–1983. doi:10.1109/jsyst.2019.2933464

Ramamoorthi, L. S., & Sarkar, D. (2020). Single Sign-On: A Solution Approach to Address Inefficiencies During Sign-Out Process. *Access*, 8, 195675–195691. https:// doi. org/10. 1109/ access.2020.3033570

Ramayasa, I. P., & Candrawibawa, I. G. A. (2021). Usability Evaluation of Lecturer Information Systems Using Sirius Framework and Moscow Technique. *Scientific Journal of Informatics*, *8*(1), 16–23. https://doi.org/10.15294/sji.v8i1.27126

Ramli, K., Nurhadi, R., Suryanto, Y., & Presekal, A. (2017). Performance analysis on iris recognition based on half polar iris localization and normalization method using the modified low-cost camera. *The 2017 15th International Conference on Quality in Research: International Symposium on Electrical and Computer Engineering*. doi:10.1109/qir.2017.8168441

Ramtri, G., & Patel, C. (2020). *Secure Banking Transactions Using RSA and Two Fish Algorithms. The 2020 International Conference on Emerging Trends in Information Technology and Engineering.* doi:10.1109/ic-etite47903.2020.236

Raphael, G. (2016). Risks and Barriers Associated with Mobile Money Transactions in Tanzania. *Business Management and Strategy,* 7(2), 121–139.

Rashkovits, R., & Lavy, I. (2021). Mapping Common Errors in Entity Relationship Diagram Design of Novice Designers. *International Journal of Database Management Systems*, *13*(1), 1–19. https://doi.org/10.5121/ijdms.2021.13101

Ravitch, S. M., & Riggan, M. J. (2016). *Reason & Rigor: How Conceptual Frameworks Guide Research* (2nd Ed.). SAGE Publications, Inc. https://scholar.google.com

Ray, S., Biswas, G. P., & Dasgupta, M. (2016). Secure Multi-Purpose Mobile-Banking Using Elliptic Curve Cryptography. *Wireless Personal Communications,* 90(3), 1331–1354. https://doi.org/10.1007/s11277-016-3393-7

Reaves, B., Bowers, J., Scaife, N., Bates, A., Bhartiya, A., Traynor, P., & Butler, K. R. B. (2017). Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications. *ACM Transactions on Privacy and Security*, 20(3), 1–31. https://doi.org/10.1145/3092368

Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (2019, August). A Usability Study of Five Two-Factor Authentication Methods. *SOUPS'19: Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*, 357–370. https://dl.acm.org/doi/10.5555/3361476.3361502

Reyad, O., Mansour, H. M., Heshmat, M., & Zanaty, E. A. (2021). *Key-Based Enhancement of Data Encryption Standard for Text Security. The 2021 National Computing Colleges Conference.* doi:10.1109/nccc49330.2021.9428818

Reyes, A. R. L., Festijo, E. D., & Medina, R. P. (2018). Securing One Time Password (OTP) for Multi-Factor Out-of-Band Authentication through a 128- bit Blowfish Algorithm. *International Journal of Communication Networks and Information Security*, 10(1), 242–247. https://www.ijcnis.org/index.php/ijcnis/article/view/3188

Reynolds, J., Samarin, N., Barnes, J., Judd, T., Mason, J., Bailey, M., & Egelman, S. (2020). Empirical Measurement of Systemic 2FA Usability. The *29th USENIX Security Symposium.* https://scholar.google.com

Ribeiro, E., Uhl, A., & Alonso-Fernandez, F. (2019). *Super-Resolution and Image Re-projection for Iris Recognition. The 2019 IEEE 5th International Conference on Identity, Security, and Behavior Analysis.* doi:10.1109/isba.2019.8778581

Rodrigues, B., Chaudhari, A., & More, S. (2016). Two-factor verification using QR-code: A unique authentication system for Android smartphone users. *The 2016 2nd International Conference on Contemporary Computing and Informatics.* doi:10.1109/ic3i. 2016.7918008

Ryan, G. (2018). Introduction to positivism, interpretivism and critical theory. *Nurse Researcher, 25*(4), 41 - 49. https://oro.open.ac.uk/49591/17/49591ORO.pdf

Saad, N. A. M., & Muniandi, M. (2020). The Reflections on using Oracle Data Modeler in Creating Entity Relationship Diagram (ERD). *International Journal of Research Publications*, *66*(1), 20–26. https://doi.org/10.47119/ijrp1006611220201601

Sabri, P. N. A., Abas, A. B., & Din, R. B. (2021). Enhancing Data Storage of Colored QR Code Using C3M Technique. *European Journal of Molecular & Clinical Medicine*, 7(8), 3805-3813. https://ejmcm.com/article_6709.html

Sadekin, S. M. & Shaikh, H. M. (2016). Security of E-Banking in Bangladesh. *Journal of Finance and Accounting,* 4(1), 1–8. doi: 10.11648/j.jfa.20160401.11

Sadeq, M. J., Rayhan, K. S., Akter, M., Forhat, R., Haque, R., & Akhtaruzzaman, M. (2020). Integration of blockchain and remote database access protocol-based database. *Fifth International Congress on Information and Communication Technology*, 2020, 533–539. https://doi.org/10.1007/978-981-15-5859-7_53

Sadikoglu, F., & Uzelaltinbulat, S. (2016). Biometric Retina Identification Based on Neural Network. *Procedia Computer Science*, 102, 26–33. doi:10.1016/j.procs.2016.09.365

Saha, A., Saha, J., & Sen, B. (2019). *An Expert Multi-Modal Person Authentication System Based on Feature Level Fusion of Iris and Retina Recognition. The 2019 International Conference on Electrical, Computer and Communication Engineering*. https://scholar.google.com

Sahu, M., & Dash, R. (2020). *Study on Face Recognition Techniques. The 2020 International Conference on Communication and Signal Processing,* 0613-0616. doi:10.1109/iccsp 48568.2020.91823

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, 11(4), 1–17. https://doi.org/10.3390/fi11040089

Salim, A., Sagheer, A. M., & Yaseen, L. (2020). Design and Implementation of a Secure Mobile Banking System Based on Elliptic Curve Integrated Encryption Schema. *Communications in Computer and Information Science*, 2020, 424–438. https://doi.org/10. 1007/978-3-030-38752-5_33

Salman, H. M., Wan-Ahmad, W. F., & Sulaiman, S. (2018). Usability Evaluation of the Smartphone User Interface in Supporting Elderly Users From Experts' Perspective. *IEEE Access*, *6*, 22578–22591. https://doi.org/10.1109/access.2018.2827358

Salman, M., Li, Y., & Wang, J. (2019, July). A Graphical PIN Entry System with Shoulder Surfing Resistance. *The 2019 IEEE 4th International Conference on Signal and Image Processing.* https://doi.org/10.1109/siprocess.2019.8868388

Santesteban-Echarri, O., Tang, J., Fernandes, J., & Addington, J. (2020). Development and Usability Testing of SOMO, a Mobile-Based Application to Monitor Social Functioning for Youth at Clinical High-Risk for Psychosis. *Digital Psychology,* 1(1), 4–19.

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2015). *Research Methods for Business Students* (7th Ed.). Pearson. https://scholar.google.com

Saunders, M., Lewis, P., & Thornhill, A. (2007). *Research Methods for Business Students* (4th Ed.). Pearson. https://scholar.google.com

Saxena, N., & Payal, A. (2011). Enhancing Security System of Short Message Service for M-Commerce in GSM. *International Journal of Computer Science & Engineering Technology,* 2(4), 126–133.

Saxena, S., Vyas, S., Kumar, B. S., & Gupta, S. (2019, February). Survey on Online Electronic Payments Security. *The 2019 Amity International Conference on Artificial Intelligence*. https://doi.org/10.1109/aicai.2019.8701353

Schorr, F., & Hvam, L. (2018). *Design Science Research: A Suitable Approach to Scope and Research I.T. Service Catalogs. The 2018 IEEE World Congress on Services*. doi:10.1109/services.2018.00026

Sefotho, M. M. (2015). A Researcher's Dilemma: Philosophy in Crafting Dissertations and Theses. *Journal of Social Sciences*, *42*(1–2), 23–36. https://doi.org/10.1080/09718923.2015.11893390

Sghaier, A., Zeghid, M., Massoud, C., & Mahchout, M. (2017). Design and Implementation of Low Area/Power Elliptic Curve Digital Signature Hardware Core. *Electronics*, *6*(2), 1–23. https://doi.org/10.3390/electronics6020046

Shahid, M., & Tasneem, K. A. (2017). Impact of Avoiding Non-functional Requirements in Software Development Stage. *American Journal of Information Science and Computer Engineering*, 3(4), 52–55. http://files.aiscience.org/journal/article/pdf/70080086.pdf

Shahriar, H., Klintic, T., & Clincy, V. (2015). Mobile Phishing Attacks and Mitigation Techniques. *Journal of Information Security*, 06(03), 206–212. https://doi.org/10.4236/jis.2015.63021

Shaik, C. (2021). Preventing Counterfeit Products using Cryptography, QR Code and Webservice. *Computer Science & Engineering: An International Journal*, 11(1), 1–11.

Shaikh, J. R., Nenova, M., Iliev, G., & Valkova-Jarvis, Z. (2017). *Analysis of standard elliptic curves for the implementation of elliptic curve cryptography in resource-constrained E-commerce applications. The 2017 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems*. https://scholar.google.com

Shamshad, S., Mahmood, K., Kumari, S., & Khan, M. K. (2020). Comments on "Insider Attack Protection: Lightweight Password-Based Authentication Techniques Using ECC." *IEEE Systems Journal*, 2020,1–4. doi:10.1109/jsyst.2020.2986377

Shang, J., & Wu, J. (2020, March*). LightDefender: Protecting PIN Input using Ambient Light Sensor. The 2020 International Conference on Pervasive Computing and Communications.* https://doi.org/10.1109/percom45495.2020.912736

Sharma, L., & Mathuria, M. (2018, January). *Mobile banking transactions using fingerprint authentication. The 2018 2nd International Conference on Inventive Systems and Control*. https://doi.org/10.1109/icisc.2018.8399016

Sharma, M. K., & Nene, M. J. (2020). Two-factor authentication using biometric-based quantum operations. *Security and Privacy*, 3(3), 1–21. https://doi.org/10.1002/spy2.10

Sharma, N., & Bohra, B. (2017, February). Enhancing online banking authentication using a hybrid cryptographic method. *The 2017 3rd International Conference on Computational Intelligence & Communication Technology*. https://doi.org/10.1109/ciact.2017. 7977275

Sharma, P. (2019). *A Contemplate on Multifactor Authentication. The 2019 6th International Conference on Computing for Sustainable Global Development (Indiacom)*. https://scholar.google.com

Sharma, S. K., & Al-Muharrami, S. (2018). Mobile Banking Adoption: Key Challenges and Opportunities and Implications for a Developing Country. *Emerging Markets from a Multidisciplinary Perspective*. doi:10.1007/978-3-319-75013-2_7

Sharmila, S. R., Kumar, D., Puranik, V., & Gautham, K. (2019). *Performance Analysis of Human Face Recognition Techniques. The 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU).* doi:10.1109/iot-siu.2019.8777610

Shavetov, S., & Sivtsov, V. (2020). *Access Control System Based on Face Recognition. The 2020 7th International Conference on Control, Decision and Information Technologies*. doi:10.1109/codit49905.2020.9263894

Sherrell, L. (2013). Evolutionary Prototyping. *Encyclopedia of Sciences and Religions*, 803–803. doi:10.1007/978-1-4020-8265-8_201039

Shi, C., Liu, J., Liu, H., & Chen, Y. (2021). WiFi-Enabled User Authentication through Deep Learning in Daily Activities. *ACM Transactions on Internet of Things*, 2(2), 1–25. https://doi.org/10.1145/3448738

Shi, X., & Chen, Y. (2020). New Teaching Method of Python Programming for Liberal Arts Students. *International Journal of Innovation and Research in Educational Sciences*, *7*(3), 261–271.

Shilpa, S., & Panchami V. (2016, November). *BISC Authentication Algorithm: An Efficient New Authentication Algorithm Using Three-Factor Authentication for Mobile Banking. 2016 Online International Conference on Green Engineering and Technologies*. https://doi.org/10.1109/get.2016.7916852

Shin, Y. J. (2018). Review of the suitability to introduce new identity verification means in South Korea: Focused on Block Chain and FIDO. *Journal of Convergence for Information Technology*, 8(5), 85–93. https://doi.org/10.22156/CS4SMB.2018.8.5.085

Sholichah, R. J., Imrona, M., & Alamsyah, A. (2020). *Performance Analysis of Neo4j and MySQL Databases using Public Policies Decision Making Data. The 2020 7th International Conference on Information Technology, Computer, and Electrical Engineering*. doi:10.1109/icitacee50144.2020.9239206

Shruti, M. I., Pratiksha, M. K., Jyoti, M. M., Snehal, M. N., & Vaibhav, P. D. (2020). Designing Security Framework for Secure Exam System based on QR Code. *International Journal for Research in Applied Science & Engineering Technology,* 8(6), 1692–1697. https://www.ijraset.com

Silverman, B. W. (2017). *Density Estimation for Statistics and Data Analysis* (1st Ed.). Taylor & Francis. https://doi.org/10.1201/9781315140919

Singh, A. S., & Masuku, M. B. (2014). Sampling Techniques & Determination of Sample Size in Applied Statistics Research: An Overview. *International Journal of Economics, Commerce and Management*, 2(11), 1–22.

Singh, A., & Raj, S. (2019). Securing passwords using dynamic password policy generator algorithm. *Journal of King Saud University: Computer and Information Sciences*, 2019, 1–5. https://doi.org/10.1016/j.jksuci.2019.06.006

Singh, B., & Jasmine, K. S. (2015). Secure End-To-End Authentication for Mobile Banking. *Advances in Intelligent Systems and Computing, 2015*, 223–232. doi:10.1007/978-3-319-18473-9_22

Singh, L. J., & Imphal, N. (2018). A Survey on Phishing and Anti-Phishing Techniques. *International Journal of Computer Science Trends and Technology*, 6(2), 62–68. http://www.ijcstjournal.org/volume-6/issue-2/IJCST-V6I2P13.pdf

Sinha, B. R., Dey, P. P., Amin, M. N., & Romney, G. W. (2013). Database modeling with Object Relationship Schema. *The 2013 12th International Conference on Information Technology Based Higher Education and Training.* doi:10.1109/ithet.2013.667102

Sithara, R., & Rajasree, R. (2019). A survey on Face Recognition Technique. *The 2019 IEEE International Conference on Innovations in Communication, Computing and Instrumentation*. doi:10.1109/icci46240.2019.940438

Song, J., Zhang, M., & Xie, H. (2019). Design and Implementation of a Vue.js-Based College Teaching System. *International Journal of Emerging Technologies in Learning, 14*(13), 59–69. https://doi.org/10.3991/ijet.v14i13.10709

Srivastava, S., & Sivasankar, M. (2016, August). *On the generation of Alphanumeric One-time Passwords. The 2016 International Conference on Inventive Computation Technologies*. https://doi.org/10.1109/inventive.2016.7823287

Suebtimrat, P., & Vonguai, R. (2021). An Investigation of Behavioral Intention towards QR Code Payment in Bangkok, Thailand. *Journal of Asian Finance, Economics and Business*, 8(1), 939–950. https://doi.org/10.13106/jafeb.2021.vol8.no1.939

Suhaili, S., & Watanabe, T. (2017, November). *Design of high-throughput SHA-256 hash function based on FPGA. The 2017 6th International Conference on Electrical Engineering and Informatics*. https://doi.org/10.1109/iceei.2017.8312449

Sukmasetya, P., Setiawan, A., & Arumi, E. R. (2020). Usability evaluation of university website: a case study. *Journal of Physics: Conference Series*, *1517*(1), 7–12.

Sultan, S., & Ghanim, M. F. (2020). Human Retina Based Identification System Using Gabor Filters and GDA Technique. *Journal of Communications Software and Systems*, 16(3), 243–253. https://doi.org/10.24138/jcomss.v16i3.1031

Sun, L., Liang, S., Chen, P., & Chen, Y. (2021). Encrypted digital watermarking algorithm for quick response code using discrete cosine transform and singular value decomposition. *Multimedia Tools and Applications*, 80(7), 10285–10300.

Sürücü, L., & Maslakçı, A. (2020). Validity And Reliability in Quantitative Research. *Business & Management Studies: An International Journal*, 8(3), 2694-2726, doi: http://dx.doi.org/10.15295/bmij.v8i3.1540

Suwera, N. F. (2021, May 28). *Mobile Money (Momo) Fraud: Two-Factor Authentication, an Algorithm to End This Menace. Modern Ghana*. https://scholar.google.com

Szalachowski, P. (2021). Password-Authenticated Decentralized Identities. *Transactions on Information Forensics and Security*, 16, 4801–4810.

Szymkowski, M., Saeed, E., Omieljanowicz, M., Omieljanowicz, A., Saeed, K., & Mariak, Z. (2020). A Novelty Approach to Retina Diagnosing using Biometric techniques with SVM and clustering algorithms. *Access*, 8, 125849 - 125862. doi:10.1109/access. 2020.3007656

Taher, K. A., Nahar, T., & Hossain, S. A. (2019, January). *Enhanced Cryptocurrency Security by Time-Based Token Multi-Factor Authentication Algorithm. The 2019 International Conference on Robotics, Electrical and Signal Processing Techniques*. https://doi.org/10.1109/icrest.2019.8644084

Talom, F. S. G., & Tengeh, R. K. (2019). The Impact of Mobile Money on the Financial Performance of the SMEs in Douala, Cameroon. *Sustainability*, 12(1), 1-17. https://doi.org/10.3390/su12010183

Tanseer, I., Kanwal, N., Asghar, M. N., Iqbal, A., Tanseer, F., & Fleury, M. (2020). Real-Time, Content-Based Communication Load Reduction in the Internet of Multimedia Things. *Applied Sciences*, *10*(3), 1–30. https://doi.org/10.3390/app10031152

Tao, Y., Cai, F., Zhan, G., Zhong, H., Zhou, Y., & Shen, S. (2021). Floating quick response code based on structural black color with the characteristic of privacy protection. *Optics Express*, 29(10), 1–11. https://doi.org/10.1364/oe.423923

Tashakkori, A. M., & Teddlie, C. B. (1998). *Mixed Methodology: Combining Qualitative and Quantitative Approaches (Applied Social Research Methods)* (1st Ed.). SAGE Publications, Inc. https://scholar.google.com

Teddlie, C., & Tashakkori, A. (2009). *Foundations of Mixed Methods Research*. SAGE Publications. https://scholar.google.com

Thenerve. (2019, April 2). *Coins.ph, GCash, GrabPay, PayMaya: Who's Leading the Mobile Payments War in PH?* Rappler. https://scholar.google.com

Thomas, P. A., & Mathew, K. P. (2021). A broad review on non-intrusive active user authentication in biometrics. *Journal of Ambient Intelligence and Humanized Computing*, 2021, 1–22. https://doi.org/10.1007/s12652-021-03301-x

Thomas, R. (2021). Face recognition from image patches using an ensemble of CNN-local mesh pattern networks. *The 2021 6th International Conference for Convergence in Technology*. doi:10.1109/i2ct51068.2021.941813

Thomas, T., V, S., Sobhana, N., & Koolagudi, S. G. (2020, December). *Speaker Recognition in Emotional Environment using Excitation Features. The 2020 Third International*

Conference on Advances in Electronics, Computers and Communications. https://doi.org/10.1109/icaecc50550.2020.9339501

Tran, Q. N., Turnbull, B. P., & Hu, J. (2021). Biometrics and Privacy-Preservation: How Do They Evolve? *Open Journal of the Computer Society*, 2, 179–191.

Tran, T. H., Pham, H. L., & Nakashima, Y. (2021). A High-Performance Multimem SHA-256 Accelerator for Society 5.0. *Access*, 9, 39182–39192. doi:10.1109/access.2021. 3063485

Tremoulet, P. D., Shah, P. D., Acosta, A. A., Grant, C. W., Kurtz, J. T., Mounas, P., Kirchhoff, M., & Wade, E. (2021). Usability of Electronic Health Record: Generated Discharge Summaries: Heuristic Evaluation. *Journal of Medical Internet Research*, 23(4), 1–13.

Trulioo. (2015). *Emerging Fraud Risk in the Mobile Wallet Ecosystem*. Trulioo. https://scholar.google.com

Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information & Management*, 52(4), 506–517. https://doi.org/10.1016/j.im.2015.03.002

Tyas, S. S., & Khairunisa, Y. (2020). *Usability Testing for Student Academic Information System in State Polytechnic of Creative Media. The 5th International Conference on Computing and Applied Informatics*. https://scholar.google.com

Tymchenko, O., Havrysh, B., Tymchenko, O. O., Khamula, O., Kovalskyi, B., & Havrysh, K. (2020). *Person Voice Recognition Methods. The 2020 IEEE Third International Conference on Data Stream Mining & Processing*. doi:10.1109/dsmp47368. 2020.920402

Uganda Bureau of Statistics. (2021). *COVID-19 and Beyond: A Spotlight on Uganda's Adolescent Reproductive Health*. https://scholar.google.com

Uganda Communications Commission. (2019). *Telecommunications, Broadcasting and Postal Markets Industry Report Q2 (April–June)*. UCC. https://www.ucc.co.ug

Uganda Communications Commission. (2021, September). *Market Performance Report 3Q21*. UCC. https://scholar.google.com

Ugwu, C., & Mesigo, T. (2015). A Novel MobileWallet Based on Android OS and Quick Response Code Technology. *International Journal of Advanced Research in Computer Science & Technology,* 3(1), 85–89. http://www.ijarcst.com/

Vangala, A., Das, A. K., & Lee, J. (2021). Provably secure signature-based anonymous user authentication protocol in an Internet of Things-enabled intelligent precision agricultural environment. *Concurrency and Computation: Practice and Experience*, 2021, 1–27. https://doi.org/10.1002/cpe.6187

Venable, J. (2006). *The role of theory and theorising in design science research. Proceedings of the 1st International Conference on Design Science in Information Systems and Technology*. https://scholar.google.com

Venable, J. R., Pries-Heje, J., & Baskerville, R. (2017). Choosing a Design Science Research Methodology. *Australasian Conference on Information Systems*, 2017, 1–11.

Vincent, O. R., Okediran, T. M., Abayomi-Alli, A. A., & Adeniran, O. J. (2020). An Identity-Based Elliptic Curve Cryptography for Mobile Payment Security. *Computer Science*, *1*(2), 1–12. https://doi.org/10.1007/s42979-020-00122-1

Vingen, D., Andrews, E. J., & Ferati, M. (2020). Usability in Patient-Oriented Drug Interaction Checkers: A Scandinavian Sampling and Heuristic Evaluation. *Informatics*, *7*(4), 1–27. https://doi.org/10.3390/informatics7040042

Vishwakarma, N., & Patel, V. (2019). Biometric Iris Recognition using Sobel Edge Detection for Secured Authentication. *The 2019 2nd International Conference on Intelligent Communication and Computational Techniques.* doi:10.1109/icct46177.2019.896904

Vorakulpipat, C., Pichetjamroen, S., & Rattanalerdnusorn, E. (2021). Usable comprehensive-factor authentication for a secure time attendance system. *PeerJ Computer Science*, 7, 1–22. https://doi.org/10.7717/peerj-cs.678

Vyas, H. A., & Virparia, P. V. (2020). Template-Based Transliteration of Braille Character to Gujarati Text: The Application. *Rising Threats in Expert Applications and Solutions*, *1187*, 437–446. https://doi.org/10.1007/978-981-15-6014-9_50

Waheed, Z., Waheed, A., & Akram, M. U. (2016). *A robust non-vascular retina recognition system using structural features of the retinal image. The 2016 13th International Bhurban Conference on Applied Sciences and Technology*. doi:10.1109/ibcast.2016.7429862

Wahsheh, H. A. M., & Luccio, F. L. (2020). Security and privacy of QR code applications: A comprehensive study, general guidelines and solutions. *Information*, 11(4), 1–23. https://doi.org/10.3390/INFO11040217

Walliman, N. S. R. (2016). *Social Research Methods: The Essentials* (2nd Ed.). SAGE Publications Ltd. https://www.google.com

Walls, J. G., Widmeyer, G. R., & El Sawy, O. A. (1992). Building an Information System Design Theory for Vigilant EIS. *Information Systems Research*, *3*(1), 36–59. https://doi.org/10.1287/isre.3.1.36

Wang, C. (2020). *A Brief Introduction of Python to Freshman Engineering Students Using Multimedia Applications. The 2020 IEEE Frontiers in Education Conference*. doi:10.1109/fie44824.2020.9273894

Wang, C., Muhammad, J., Wang, Y., He, Z., & Sun, Z. (2020). Towards Complete and Accurate Iris Segmentation Using Deep Multi-Task Attention Network for Non-Cooperative Iris Recognition. *Transactions on Information Forensics and Security*, 15, 2944–2959. doi:10.1109/tifs.2020.2980791

Wang, J., Liu, G., Chen, Y., & Wang, S. (2021). Construction and Analysis of SHA-256 Compression Function Based on Chaos S-Box. *Access*, *9*, 61768–61777. https:// doi. org/ 10. 1109/access.2021.3071501

Wang, K., & Kumar, A. (2020). Periocular-Assisted Multi-Feature Collaboration for Dynamic Iris Recognition. *IEEE Transactions on Information Forensics and Security*, 14(8), 1–14. doi:10.1109/tifs.2020.3023289

Wang, M. J., & Li, Y. Z. (2015). Hash Function with Variable Output Length. *The 2015 International Conference on Network and Information Systems for Computers*, 190-193. doi:10.1109/icnisc.2015.22

Wang, X., Yan, Z., Zhang, R., & Zhang, P. (2021). Attacks and defenses in user authentication systems: A survey. *Journal of Network and Computer Applications*, 188, 1–21. https://doi.org/10.1016/j.jnca.2021.103080

Wazid, M., Zeadally, S., & Das, A. K. (2019). Mobile Banking: Evolution and Threats: Malware Threats and Security Solutions. *Consumer Electronics Magazine*, 8(2), 56–60. doi:10.1109/mce.2018.2881291

Widaningsih, S., & Suheri, A. (2021). Design of Waste Management System Using QR Code for Effective Management in Wastebank. *Journal of Physics*, 1764(1), 1–6. https://doi.org/10.1088/1742-6596/1764/1/012066

Wimberly, H., & Liebrock, L. M. (2011, May). *Using Fingerprint Authentication to Reduce System Security: An Empirical Study. The 2011 IEEE Symposium on Security and Privacy, 32–46*. https://doi.org/10.1109/sp.2011.35

Wong, A. K. L., Morgan, M., & Butler, M. (2012). *Designing a Technology Enhanced Collaborative Space for Learning Entity-Relationship Modeling. The 2012 IEEE 12th International Conference on Advanced Learning Technologies*. doi:10.1109/ icalt.2012.240

Wu, L., Cai, H. J., & Li, H. (2021). SGX-UAM: A Secure Unified Access Management Scheme with One-Time Passwords via Intel SGX. *Access*, 9, 38029–38042.

Wu, R., Zhang, X., Wang, M., & Wang, L. (2020). *A High-Performance Parallel Hardware Architecture of SHA-256 Hash in ASIC. The 2020 22nd International Conference on Advanced Communication Technology*. doi:10.23919/icact48636.2020.906145

Xiaoshuan, Z., Zetian, F., Wengui, C., Dong, T., & Jian, Z. (2009). Applying evolutionary prototyping model in developing FIDSS: An intelligent decision support system for fish disease/health management. *Expert Systems with Applications*, 36(2), 3901–3913. doi:10.1016/j.eswa.2008.02.049

Ximenes, A. M., Sukaridhoto, S., Sudarsono, A., Ulil Albaab, M. R., Basri, H., Hidayat Yani, M. A., Chang Choon, C., & Islam, E. (2019, September). *Implementation QR Code Biometric Authentication for Online Payment. The 2019 International Electronics Symposium*. https://doi.org/10.1109/elecsym.2019.8901575

Xing, Y., Huang, J., & Lai, Y. (2019). Research and Analysis of the Front-end Frameworks and Libraries in E-Business Development. *Proceedings of the 2019 11th International Conference on Computer and Automation Engineering*. https://doi.org/10.1145/3313991.3314021

Xinyuan, M., Tao, W., & Kaigang, M. (2020). Application of Python Parallel Computing in Online Identification of Thevenin Equivalent Parameters. The *2020 IEEE 3rd Student Conference on Electrical Machines and Systems.* doi:10.1109/scems48876.2020 .9352354

Xu, H. J., Ku, W. C., & Dan, Y. X. (2016, May). An observation attacks resistant PIN-entry scheme using localized haptic feedback. *The 2016 IEEE Region 10 Symposium*. https://doi.org/10.1109/tenconspring.2016.7519378

Yamane, T. (1973). *Statistics: An Introductory Analysis* (3rd Ed.). Harper and Row. https://www.google.com

Yang, W., Wang, S., Hu, J., Zheng, G., & Valli, C. (2019). Security and Accuracy of Fingerprint-Based Biometrics: A Review. *Symmetry*, 11(2), 1–19.

Yang, W., Wang, S., Sahri, N. M., Karie, N. M., Ahmed, M., & Valli, C. (2021). Biometrics for Internet-of-Things Security. *Sensors*, 21(18), 1–26.

Ye, F., & Yang, J. (2021). A Deep Neural Network Model for Speaker Identification. *Applied Sciences*, 11(8), 1–18. https://doi.org/10.3390/app11083603

Yu, J. H., Ku, G. C. M., Lo, Y. C., Chen, C. H., & Hsu, C. H. (2021). Identifying the Antecedents of University Students' Usage Behaviour of Fitness Apps. *Sustainability*, *13*(16), 1–13. https://doi.org/10.3390/su13169043

Yu, J., Zhao, Y., Zhu, S., Wang, A., & Wang, Y. (2018). *A Bibliometric Analysis on Face Recognition Technology Research. The 2018 IEEE International Conference of Safety Produce Informatization.* doi:10.1109/iicspi.2018.8690483

Yuan, X., Gu, L., Chen, T., Elhoseny, M., & Wang, W. (2018). *A Fast and Accurate Retina Image Verification Method Based on Structure Similarity. The 2018 IEEE Fourth International Conference on Big Data Computing Service and Applications (BigDataService),* 181-185. doi:10.1109/bigdataservice.2018.00034

Yuen, A. H., Cheng, M., & Chan, F. H. (2019). Student satisfaction with learning management systems: A growth model of belief and use. *British Journal of Educational Technology*, 50(5), 2520-2535. https://doi.org/10.1111/bjet.12830

Yusoh, S., & Matayong, S. (2017). *Heuristic evaluation of online satisfaction survey system for public healthcare service: Applying analytical hierarchical process. The 2017 2nd International Conferences on Information Technology, Information Systems and Electrical Engineering*. https://www.google.com

Zadeh, M. J., & Barati, H. (2019, October). *Security Improvement in Mobile Banking Using Hybrid Authentication. Proceedings of the 2019 3rd International Conference on Advances in Artificial Intelligence.* https://doi.org/10.1145/3369114.3369151

Zaidi, A. Z., Chong, C. Y., Jin, Z., Parthiban, R., & Sadiq, A. S. (2021). Touch-based continuous mobile device authentication: State-of-the-art, challenges and opportunities. *Journal of Network and Computer Applications,* 191, 1–29.

Zakaria, N., Wahabi, H., & Qahtani, M.A. (2020). Development and usability testing of Riyadh Mother and Baby Multi-center cohort study registry. *Journal of Infection and Public Health*, 13(10), 1473–1480.

Zamanzadeh, V., Ghahramanian, A., Rassouli, M., Abbaszadeh, A., Alavi-Majd, H., & Nikanfar, A. R. (2015). Design and Implementation Content Validity Study: Development of an instrument for measuring Patient-Centered Communication. *Journal of Caring Sciences*, 4(2), 165–178. https://doi.org/10.15171/jcs.2015.017

Zhang, H., Xiao, X., Ni, S., Dou, C., Zhou, W., & Xia, S. (2021). Smartwatch User Authentication by Sensing Tapping Rhythms and Using One-Class DBSCAN. *Sensors*, 21(7), 1–16. https://doi.org/10.3390/s21072456

Zhang, J., Tan, X., Wang, X., Yan, A., & Qin, Z. (2018). T2FA: Transparent Two-Factor Authentication. *Access*, 6, 32677–32686.

Zhang, L., Ning, H.-Y., & Yang, Y. (2016). A New Type MySQL Integrated Mutual Authentication Security Model. *The 2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control*. doi:10.1109/imccc.2016.14

Zhang, X., Zeng, H., & Zhang, X. (2017). *Mobile Payment Protocol based on Dynamic Mobile Phone Token. The 2017 IEEE 9th International Conference on Communication Software and Networks.* doi:10.1109/iccsn.2017.8230198

Zhang, Y., He, Z., Wan, M., Zhan, M., Zhang, M., Peng, K., Song, M., & Gu, H. (2021). A New Message Expansion Structure for Full Pipeline SHA-2. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *68*(4), 1553–1566.

Zhao, Y., Yoshigoe, K., Bian, J., Xie, M., Xue, Z., & Feng, Y. (2016). A Distributed Graph-Parallel Computing System with Lightweight Communication Overhead. *IEEE Transactions on Big Data,* 2(3), 204–218. doi:10.1109/tbdata.2016.2532907

Zhiqi, Y. (2021). *Face recognition based on Improved VGGNET Convolutional Neural Network. The 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference*, 2530-2533. doi:10.1109/iaeac50856.2021.93908

Zhuang, Y., Chuah, J. H., Chow, C. O., & Lim, M. G. (2020). *Iris Recognition using Convolutional Neural Network. The 2020 IEEE 10th International Conference on System Engineering and Technology*. doi:10.1109/icset51301.2020.92653

Zin, M. Z. M., Saidi, R. M., Sappar, F., & Arshad, M. A. (2019). Multi-factor Authentication to Authorizing Access to an Application: A Conceptual Framework. *Journal of Advanced Research in Computing and Applications,* 16(1), 1–9.

Žukauskas, P., Vveinhardt, J., & Andriukaitienė, R. (2018). Philosophy and Paradigm of Scientific Research. In J. Vveinhardt, & R. Andriukaitienė (Eds.), *Management Culture and Corporate Social Responsibility* (pp. 121–139). IntechOpen. https:// www. google. com

APPENDICES

Appendix 1: Introduction letter from the school of CoCSE

THE NELSON MANDELA
AFRICAN INSTITUTION OF SCIENCE AND TECHNOLOGY
(NM-AIST)
School of Computational and Communication Science and Engineering

Direct Line: +255 272970001
Fax: +255272970016
Email: dean-cocse@nm-aist.ac.tz

Tengeru
P. O. Box 447
Arusha, TANZANIA
Website: www.nm-aist.ac.tz

OUR Ref. No. NM-AIST/P.072/UG.18 **Date**: 3rd February,2020

To Whom It May Concern

Dear Sir/ Madam

RE: INTRODUCTION TO MR.GUMA ALI

Kindly refer to the above heading.

I wish to introduce Mr. Guma Ali with registration No. NM-AIST/P.072/UG.18, a PhD student at Nelson Mandela African Institution of Science and Technology in the school of Computational and Communication Science Technology.

As part of the requirement for PhD degree, Mr. Guma Ali is undertaking a research entitled "***Development of secured Multi-Factor Authentication Algorithm Using PIN, OTP, and Biometric Fingerprint for Money Systems***".

In order to accomplish his research objectives, he would like to collect some information from your institution/office. The information to be collected will be used for research purposes only and will help the student to develop an electronic system that will help to solve security challenges associated with mobile money systems.

It is my sincere hope that you will assist the student in accomplishing his study.

Looking forward to your cooperation.

Sincerely,

Shubi Kaijage *PhD*

Ag. Dean, School of Computational and Communication Science and Engineering (CoCSE)

Appendix 2: Questionnaire for MNO IT officers

Dear respondent,

This questionnaire is for **Mr. Guma Ali**, a PhD student at The Nelson Mandela African Institution of Science and Technology, Arusha – Tanzania. He is researching "***Evaluation of Key Security Issues associated with Mobile Money Systems in Uganda***" and will value your input by obliging to fill out this questionnaire. As an MNO IT officer, your opinion is critical in this study. We would be most grateful if you may spare your precious time to answer all the questions before you. All the information provided will be treated with confidentiality. Therefore, feel free to avail all the necessary information to the best of your knowledge.

Thanks for your cooperation and participation.

Section A: Demographic Information

Instruction: *Where applicable, please mark with a tick [✓] inside the box provided for your appropriate option or by adding information in the space provided with solid lines.*

Question One

A1 What is your Gender? Male ☐ Female ☐

A2 How old are you?

Less than 18 years ☐ Between 18-30 years ☐ Between 31-50 years ☐

More than 50 Years ☐

A3 What is your marital status?

Single ☐ Married ☐ Divorced ☐ Widowed ☐ Widower ☐

A4 What is your highest level of Education?

Certificate ☐ Diploma ☐ Bachelors ☐ Masters ☐ PhD ☐

Section B: Mobile Money Services

Question Two

B1 Which mobile money service provider do you work for?

MTN Mobile Money ☐ Airtel Money ☐ Africell Money ☐ M-Sente ☐

Ezeey Money ☐ M-Cash ☐ Micropay ☐ Others: _____

B2 How long have you been working with the mobile money services provider?

Less than 1 year ☐ Between 1-5 years ☐ Between 6-10 years ☐

More than 10 years ☐

B3 How do you access mobile money services?

☐ By dialling the USSD code, e.g., *144#, *165#, *185#, etc.

☐ Through downloaded apps, e.g., MTN MyApp, My Airtel, Xente, EasyPay, etc.

☐ Using mobile web browsers, e.g., Chrome, Firefox, Opera, etc.

B4 How many times in a month do you perform mobile money transactions?

Not at all ☐ 1 – 5 ☐ 6 – 10 ☐

11 – 15 ☐ 16 – 20 ☐ 21 and above ☐

B5 Which of the following services are performed using mobile money?

- ☐ Send and receive the money within Uganda.
- ☐ International money transfer.
- ☐ Withdrawing money.
- ☐ Save and borrow money, e.g. Using MTN MoKash.
- ☐ Mobile banking.
- ☐ Buy insurance.
- ☐ Receive pension.
- ☐ Buy goods and services.
- ☐ Paying for telecom network services, like data bundles, airtime, etc.
- ☐ Paying for utilities like NWSC, UMEME, DStv & GOtv, Fees, Taxes, etc.

B6 The table below is about the benefits of using mobile money. Rate the benefits of mobile money based on your experience as an MNO IT officer by using the scale of **1** - Strongly Disagree, **2** - Disagree, **3** - Neutral, **4** - Agree, and **5** - Strongly Agree.

S/No	Benefits of using mobile money	1	2	3	4	5
1	It offers convenience in terms of sending and receiving money.					
2	More reliable than physically sending money.					
3	It saves time.					
4	It is trustworthy.					
5	Quicker and easier to do transactions.					
6	Increases access to financial services.					
7	Reduces the time and costs spent on maintaining bank accounts.					
8	Mobile money results in economic growth.					
9	It provides mobile financial services.					
10	Improves the standard of living of the subscribers.					
11	Boosts the diffusion of banking services.					

Section C: Mobile Money Security Issues

Question Three

C1 Rate your agreement with each of the statements about mobile money security challenges by ticking the suitable option provided in the table.

S/No	Mobile money security challenges	1	2	3	4	5
1	I received a complaint that a customer lost his phone and heard someone use it to request money from his friends and relatives.					
2	Customers confess that they have ever revealed their mobile money PIN to friends and relatives and later lost money from their mobile money account.					
3	Customers complain that they receive calls from people claiming to be customer care representatives asking them to update their mobile money PIN, Birthdate, names, phone number.					
4	I have received complaints from clients that they got messages from someone claiming they have sent money wrongly to their mobile money account.					
5	I have received complaints from customers that they received calls informing them that if they send money to a given number, the balance in their mobile money account will double.					
6	Customers confess that when sick or occupied, they ask their friends or relatives to use their phones to withdraw money.					
7	I have received complaints from customers that a certain amount is always deducted at certain intervals without their mobile money account authorisation.					
8	When they deposit money to their mobile money account, customers confess that they receive strange calls from people claiming they accidentally sent money to their money account.					
9	I have received complaints from clients that their phone sometimes goes temporarily out of service and later receive information from friends or relatives that they had requested them to send money to their phone.					
10	Some customers confess that they do not know how to use their mobile money accounts, so they always request the mobile money agents to withdraw money on their behalf.					

C2 The table below has statements about the different ways to alleviate security challenges. Rate your agreement with each information about the different ways to alleviate security challenges by ticking the suitable option using the scale of **1** - Not A Priority, **2** - Low Priority, **3** - Neutral, **4** - Medium Priority, and **5** - High Priority.

S/No	Ways to alleviate the security challenges	1	2	3	4	5
1	Use of multi-factor authentication for better access controls.					
2	There should be an increase in customer awareness campaigns.					
3	Training mobile money agents on standard practice.					
4	Mobile money service providers must have a comprehensive legal document to guide mobile money service.					
5	Severe punishment of the offenders.					
6	Know your customer Controls.					
7	The victims of mobile money fraud should report the cases to regulators and security agencies.					
8	The mobile money service providers must monitor high-value transactions.					
9	There is a need for mobile money service providers and the government to publish all the reported incidences.					
10	There is a need for mobile money service providers and the government to develop a portal where mobile money subscribers can anonymously share their incidents.					

Thanks

Appendix 3: Questionnaire for mobile money agents

Dear respondent,

This questionnaire is for **Mr. Guma Ali**, a PhD student at The Nelson Mandela African Institution of Science and Technology, Arusha – Tanzania. He is researching "***Evaluation of Key Security Issues associated with Mobile Money Systems in Uganda***" and will value your input by obliging to fill out this questionnaire. As a mobile money agent, your opinion is critical in this study. We would be most grateful if you may spare your precious time to answer all the questions before you. All the information provided will be treated with confidentiality. Therefore, feel free to avail all the necessary information to the best of your knowledge.

Thanks for your cooperation and participation.

Section A: Demographic Information

Instruction: *Where applicable, please mark with a tick [✓] inside the box provided for your appropriate option or by adding information in the space provided with solid lines.*

Question One

A1 What is your Gender? Male ☐ Female ☐

A2 How old are you?

Less than 18 years ☐ Between 18-30 years ☐ Between 31-50 years ☐

More than 50 Years ☐

A3 What is your marital status?

Single ☐ Married ☐ Divorced ☐ Widowed ☐ Widower ☐

A4 What is your highest level of Education?

Primary School ☐ Ordinary Level ☐ Advanced Level ☐ Certificate ☐

Diploma ☐ Bachelors ☐ Masters ☐ PhD ☐

Section B: Mobile Money Services

Question Two

B1 Which mobile money service provider(s) do you use or operate?

MTN Mobile Money ☐ Airtel Money ☐ Africell Money ☐ M-Sente ☐

Ezeey Money ☐ M-Cash ☐ Micropay ☐ Others: _____

B2 How long have you been operating mobile money services?

Less than 1 year ☐ Between 1-5 years ☐ Between 6-10 years ☐

More than 10 years ☐

B3 How do you access mobile money services?

☐ By dialling the USSD code, e.g., *144#, *165#, *185#, etc.

☐ Through downloaded apps, e.g., MTN MyApp, My Airtel, Xente, EasyPay, etc.

☐ Using mobile web browsers, e.g., Chrome, Firefox, Opera, etc.

B4 How many times in a month do you perform mobile money transactions?

Not at all ☐ 1 – 5 ☐ 6 – 10 ☐

11 – 15 ☐ 16 – 20 ☐ 21 and above ☐

B5 Which of the following services do you perform using mobile money?

- ☐ Send and receive the money within Uganda.
- ☐ International money transfer.
- ☐ Withdrawing money.
- ☐ Save and borrow money, e.g. Using MTN MoKash.
- ☐ Mobile banking.
- ☐ Buy insurance.
- ☐ Receive pension.
- ☐ Buy goods and services.
- ☐ Paying for telecom network services, like data bundles, airtime, etc.
- ☐ Paying for utilities like NWSC, UMEME, DStv & GOtv, Fees, Taxes, etc.

B6 The table below is about the benefits of using mobile money. Rate the benefits of mobile money based on your experience as an MNO IT officer by using the scale of **1** - Strongly Disagree, **2** - Disagree, **3** - Neutral, **4** - Agree, and **5** - Strongly Agree.

S/No	Benefits of using mobile money	1	2	3	4	5
1	It offers convenience in terms of sending and receiving money.					
2	More reliable than physically sending money.					
3	It saves time.					
4	It is trustworthy.					
5	Quicker and easier to do transactions.					
6	Increases access to financial services.					
7	Reduces the time and costs spent on maintaining bank accounts.					
8	Mobile money results in economic growth.					
9	It provides mobile financial services.					
10	Improves the standard of living of the subscribers.					
11	Boosts the diffusion of banking services.					

Section C: Mobile Money Security Issues

Question Three

C1 Rate your agreement with each of the statements about mobile money security challenges by ticking the suitable option provided in the table.

S/No	Mobile money security challenges	1	2	3	4	5
1	I have lost my agent phone and heard someone use it to request money from customers and mobile money service providers.					
2	I have revealed my mobile money agent PIN to someone, and I lost some money from my account.					
3	I have received a call or a message from a person claiming to be from the customer care centre asking me about my birth date, name, phone number and agent PIN to update my information.					
4	I have received a call or SMS from someone claiming they have sent money wrongly to my mobile money account.					
5	I have received a call or SMS informing me that if I send a certain amount of money to another number, the balance in my mobile money account will double.					
6	If I am sick or occupied, I request people to use my agent phone to withdraw and send money on my behalf.					
7	I noticed my phone was temporarily out of service, and later I received information from customers that I had requested them to send money to my phone.					
8	When I deposit money into my mobile money agent account, a certain amount is always deducted at certain intervals without my authorization.					
9	When I deposit money to my mobile money agent account, I get a strange call from someone claiming to have accidentally sent the money.					
10	When depositing money into my mobile money agent account, sometimes the bank teller claims the cash at hand to be banked less than the cash handed over to the teller.					

C2 The table below has statements about the different ways to alleviate security challenges. Rate your agreement with each information about the different ways to alleviate security challenges by ticking the suitable option using the scale of **1** - Not A Priority, **2** - Low Priority, **3** - Neutral, **4** - Medium Priority, and **5** - High Priority.

S/No	Ways to alleviate the security challenges	1	2	3	4	5
1	Use of multi-factor authentication for better access controls.					
2	There should be an increase in customer awareness campaigns.					
3	Training mobile money agents on standard practice.					
4	Mobile money service providers must have a comprehensive legal document to guide mobile money service.					
5	Severe punishment of the offenders.					
6	Know your customer Controls.					
7	The victims of mobile money fraud should report the cases to regulators and security agencies.					
8	Mobile money service providers must monitor high-value transactions.					
9	There is a need for mobile money service providers and the government to publish all the reported incidents.					
10	There is a need for mobile money service providers and the government to develop a portal where mobile money subscribers can anonymously share their incidents.					

Thanks

Appendix 4: Questionnaire for mobile money customers

Dear respondent,

This questionnaire is for **Mr. Guma Ali**, a PhD student at The Nelson Mandela African Institution of Science and Technology, Arusha – Tanzania. He is researching "***Evaluation of Key Security Issues associated with Mobile Money Systems in Uganda***" and will value your input by obliging to fill out this questionnaire. As a mobile money customer, your opinion is critical in this study. We would be most grateful if you may spare your precious time to answer all the questions before you. All the information provided will be treated with confidentiality. Therefore, feel free to avail all the necessary information to the best of your knowledge.

Thanks for your cooperation and participation.

Section A: Demographic Information

Instruction: *Where applicable, please mark with a tick [✓] inside the box provided for your appropriate option or by adding information in the space provided with solid lines.*

Question One

A1 What is your Gender? Male ☐ Female ☐

A2 How old are you?

Less than 18 years ☐ Between 18-30 years ☐ Between 31-50 years ☐

More than 50 Years ☐

A3 What is your marital status?

Single ☐ Married ☐ Divorced ☐ Widowed ☐ Widower ☐

A4 What is your highest level of Education?

Primary School ☐ Ordinary Level ☐ Advanced Level ☐ Certificate ☐

Diploma ☐ Bachelors ☐ Masters ☐ PhD ☐

Section B: Mobile Money Services

Question Two

B1 Which mobile money service provider(s) do you use?

MTN Mobile Money ☐ Airtel Money ☐ Africell Money ☐ M-Sente ☐

Ezeey Money ☐ M-Cash ☐ Micropay ☐ Others: _____

B2 How long have you been using mobile money services?

Less than 1 year ☐ Between 1-5 years ☐ Between 6-10 years ☐

More than 10 years ☐

B3 How do you access mobile money services?

☐ By dialling the USSD code, e.g., *144#, *165#, *185#, etc.

☐ Through downloaded apps, e.g., MTN MyApp, My Airtel, Xente, EasyPay, etc.

☐ Using mobile web browsers, e.g., Chrome, Firefox, Opera, etc.

B4 How many times in a month do you perform mobile money transactions?

Not at all ☐ 1 – 5 ☐ 6 – 10 ☐

11 – 15 ☐ 16 – 20 ☐ 21 and above ☐

B5 The table below is about the benefits of using mobile money. Rate the benefits of mobile money based on your experience as an MNO IT officer by using the scale of **1** - Strongly Disagree, **2** - Disagree, **3** - Neutral, **4** - Agree, and **5** - Strongly Agree.

S/No	Benefits of using mobile money	1	2	3	4	5
1	It offers convenience in terms of sending and receiving money.					
2	More reliable than physically sending money.					
3	It saves time.					
4	It is trustworthy.					
5	Quicker and easier to do transactions.					
6	Increases access to financial services.					
7	Reduces the time and costs spent on maintaining bank accounts.					
8	Mobile money results in economic growth.					
9	It provides mobile financial services.					
10	Improves the standard of living of the subscribers.					
11	Boosts the diffusion of banking services.					

Section C: Mobile Money Security Issues

Question Three

C1 Rate your agreement with each of the statements about mobile money security challenges by ticking the suitable option provided in the table.

S/No	Mobile money security challenges	1	2	3	4	5
1	I have lost my phone and heard someone use it to request money from my friends and family members.					
2	I have revealed my mobile money PIN to someone, and I lost some money from my mobile money account.					
3	I have received a call or SMS from a person from the customer care centre asking me about my birth date, name, phone number and PIN to update my information.					
4	I have received a call or SMS from someone claiming they have sent money wrongly to my mobile money account.					
5	I have received a call or SMS informing me that if I send a certain amount of money to another number, the balance in my mobile money account will double.					

6	If I am sick or occupied, I request people to use my phone to withdraw money for me.					
7	I noticed that my phone was temporarily out of service and later received information from friends and relatives that I requested them to send money to my phone.					
8	When I deposit money into my mobile money account, a certain amount is always deducted at certain intervals without my authorization.					
9	When I deposit money into my mobile money account, I get a strange call from someone claiming to have accidentally sent the money.					
10	When depositing money into my mobile money account, sometimes the agent claims the cash at hand to be banked less than the cash handed over to the agent.					
11	I do not know how to use mobile money services, so I always request the help of a mobile money agent to withdraw money from my mobile money wallet.					

C2 The table below has statements about the different ways to alleviate security challenges. Rate your agreement with each information about the different ways to alleviate security challenges by ticking the suitable option using the scale of **1** - Not A Priority, **2** - Low Priority, **3** - Neutral, **4** - Medium Priority, and **5** - High Priority.

S/No	**Ways to mitigate mobile money security challenges**	**1**	**2**	**3**	**4**	**5**
1	Use of multi-factor authentication for better access controls.					
2	There should be an increase in customer awareness campaigns.					
3	Training mobile money agents on standard practice.					
4	Mobile money service providers must have a comprehensive legal document to guide mobile money service.					
5	Severe punishment of the offenders.					
6	Know your customer Controls.					
7	The victims of mobile money fraud should report the cases to the regulators and security agencies.					

8	The mobile money service providers must monitor high-value transactions.					
9	There is a need for mobile money service providers and the government to publish all the reported incidences.					
10	There is a need for mobile money service providers and the government to develop a portal where mobile money subscribers can anonymously share their incidences.					

Thanks

Appendix 5: Heuristic evaluation post-test questionnaire for evaluation experts

Dear evaluation experts,

This questionnaire is for **Mr. Guma Ali**, a PhD student at The Nelson Mandela African Institution of Science and Technology, Arusha – Tanzania. He is researching "***Heuristic evaluation of native G-MoMo applications***" and will value your input by obliging to give feedback by filling in this post-test questionnaire after performing tasks using the G-MoMo applications. As an expert, your opinion is critical in this study. We would be most grateful if you may spare your precious time to answer all the questions before you. All the information provided will be treated with confidentiality. Therefore, feel free to avail all the necessary information to the best of your knowledge.

Thanks for your cooperation and participation.

Section A: Demographic Information

Instruction: *Where applicable, please mark with a tick [✓] inside the box provided for your appropriate option or by adding information in the space provided with solid lines.*

Question One

A1 What is your Gender? Male ☐ Female ☐

A2 How old are you?

Less than 20 years ☐ Between 20-29 years ☐ Between 30-39 years ☐

More than 39 Years ☐

A3 What is your marital status?

Single ☐ Married ☐ Divorced ☐ Widowed ☐ Widower ☐

A4 What is your highest level of Education?

Certificate ☐ Diploma ☐ Bachelors ☐ Masters ☐ PhD ☐

A5 What is your employment status?

Self-Employed ☐ Worker ☐ Employee ☐ Others: _____

A6 What kind of smartphone(s) are you using to run the G-MoMo applications?

_____

A7 For how long have you been performing heuristic evaluations on software products?

_____

Section B: Usability Testing of Native G-MoMo Applications

Question Two

B1 Rate your agreement with each statement about the Heuristic evaluation of the native G-MoMo applications by ticking the suitable option provided in the table. The options are: **0** - Not a problem at all (I do not agree that this is a usability problem at all), **1** - Cosmetic problem (Need not be fixed unless extra time is available on project), **2** - Minor problem (Fixing this should be given low priority), **3** - Major problem (Important to fix, so should be given high priority), and **4** - Catastrophic problem (Imperative to fix this before the product can be released).

S/No	Usability heuristics and sub heuristics	Expert Ratings				
		0	1	2	3	4
H1	**Visibility of system status**					
H1.1	Each page of the G-MoMo applications has a title or header describing the content on that page.					
H1.2	Every page of the G-MoMo application has a consistent icon and design.					
H1.3	The colour-coding scheme used in the G-MoMo applications can quickly and easily be understood.					
H1.4	The G-MoMo applications logo is meaningful, identifiable, and sufficiently visible.					
H1.5	When subscribers click or select a button, they get different visual responses.					
H1.6	The data entry fields of G-MoMo applications are large enough to show all of the entered data without scrolling.					
H1.7	The user is informed about what is going on through constructive and timely feedback when using the G-MoMo applications.					
H2	**Match between the system and the real world**					
H2.1	The G-MoMo applications have icons that are usable and understandable.					
H2.2	The language used in the G-MoMo applications is understandable to the users.					
H2.3	The selected theme colours are appropriate.					
H2.4	The information is organised at each level of the G-MoMo application to show a clear, consistent and logical structure to typical users.					
H2.5	The terms used are consistent with the G-MoMo application function.					
H2.6	There is consistency in naming the menu related to the user's task domain.					
H3	**User control and freedom**					
H3.1	The G-MoMo applications wait for the user's signal after completing the user's task.					

H3.2	Users control the G-MoMo applications.					
H3.3	The word "Logout" is marked on the G-MoMo applications.					
H3.4	The G-MoMo applications have search field options.					
H3.5	Users can move forward and backwards between fields or dialogue box options of G-MoMo applications.					
H3.6	Users can exit the G-MoMo applications even when they have made mistakes.					
H4	**Consistency and standards**					
H4.1	Each page of the G-MoMo application has a consistent information section.					
H4.2	Menu titles of the G-MoMo applications are either cantered or left-justified.					
H4.3	The buttons, textboxes, and labels used in G-MoMo applications comply with international standards.					
H4.4	Fonts or styles look the same on every page of G-MoMo applications, and font sizes are appropriate.					
H4.5	The number of colours used in G-MoMo applications is constrained to two or three.					
H4.6	The same actions always have the same results when using G-MoMo applications.					
H5	**Error prevention**					
H5.1	G-MoMo applications request confirmation before actions with significant implications.					
H5.2	There is always a notification or pop-up when an input error is in G-MoMo applications.					
H5.3	The G-MoMo applications' designs stop users from making severe usability errors.					
H5.4	The G-MoMo applications display error messages when the user makes an error.					
H5.5	The instructions contained in the navigation are clear.					
H6	**Recognition rather than recall**					
H6.1	The G-MoMo applications are easy to use for the first time.					
H6.2	The visual page space is well used, and there are "white" areas between informational objects for visual relaxation.					

H6.3	There is suitable colour and brightness contrast between the image and background colours.					
H6.4	There is no need for the user to recall all the dialogue information.					
H6.4	Font size, boldface, colour, and typography show the importance of different screen items.					
H6.5	The instructions on using the G-MoMo applications are visible and accessible.					
H7	**Flexibility and efficiency of use**					
H7.1	G-MoMo applications always keep the user busy without unnecessary delays.					
H7.2	G-MoMo applications design adapts to the changes in screen resolution.					
H7.3	G-MoMo applications can be used on a variety of devices with fingerprint sensors.					
H7.4	The information displayed on each menu is appropriate and sufficient for the user. Each menu of the G-MoMo applications displays appropriate and sufficient information for the user.					
H7.5	The G-MoMo applications cater to different users, from novices to experts.					
H7.6	The navigation menu is per the classification.					
H7.7	G-MoMo applications have a search box on the applications' homepage.					
H8	**Aesthetic and minimalist design**					
H8.1	G-MoMo applications dialogues are concise and only contain relevant information.					
H8.2	It is easy for novice users to understand the information display and navigation menu.					
H8.3	Each icon used in the G-MoMo applications stands out from its background.					
H8.4	The pop-up or pull-down menus are well-defined.					
H8.5	Layout formats used in the G-MoMo applications are all the same.					

H8.6	Each data entry screen of the G-MoMo applications has a short, simple, straightforward, distinctive title.					
H8.7	The visual layout in the G-MoMo applications is well-designed.					
H9	**Help users recognise, diagnose, and recover from errors**					
H9.1	G-MoMo applications indicate that an error has occurred.					
H9.2	G-MoMo applications use plain language to explain the error.					
H9.3	G-MoMo applications explain the actions needed for recovery.					
H9.4	The information displayed on each page of G-MoMo applications allows the user to decide.					
H9.5	There is consistency and uniformity in each G-MoMo application's page structure.					
H10	**Help and documentation**					
H10.1	The G-MoMo applications have help and documentation to support the users' needs.					
H10.2	The information in the help and documentation are accessible, aimed at the user's tasks, and details the steps to accomplish a task.					
H10.3	The G-MoMo applications have messages that give instructions for the operation.					
H10.4	The G-MoMo applications contain a panel of tips and tricks or orientation screens for the app.					
H10.5	G-MoMo applications provide a clear description of their capabilities.					

Appendix 6: Usability testing post-test questionnaire for selected participants

Dear evaluation participants,

This questionnaire is for **Mr. Guma Ali**, a PhD student at The Nelson Mandela African Institution of Science and Technology, Arusha – Tanzania. He is researching "***Usability testing of native G-MoMo applications***" and will value your input by obliging to give feedback by filling in this post-test questionnaire after performing tasks using the G-MoMo applications. As a participant, your opinion is critical in this study. We would be most grateful if you may spare your precious time to answer all the questions before you. All the information provided will be treated with confidentiality. Therefore, feel free to avail all the necessary information to the best of your knowledge.

Thanks for your cooperation and participation.

Section A: Demographic Information

Instruction: *Where applicable, please mark with a tick [✓] inside the box provided for your appropriate option or by adding information in the space provided with solid lines.*

Question One

A1 What is your Gender? Male ☐ Female ☐

A2 How old are you?

Less than 20 years ☐ Between 20-29 years ☐ Between 30-39 years ☐

More than 39 Years ☐

A3 What is your marital status?

Single ☐ Married ☐ Divorced ☐ Widowed ☐ Widower ☐

A4 What is your highest level of Education?

Certificate ☐ Diploma ☐ Bachelors ☐ Masters ☐ PhD ☐

A5 What is your employment status?

Self-Employed ☐ Worker ☐ Employee ☐ Others: _____

A6 What kind of smartphone(s) are you using to run the G-MoMo applications?

_____

Section B: Usability Testing of Native G-MoMo Applications

Question Two

B1 Rate your agreement with each statement about the usability testing of native G-MoMo applications by ticking the suitable option provided in the table. The options are: **1** - Strongly Disagree, **2** - Disagree, **3** - Neutral, **4** - Agree, and **5** - Strongly Agree.

S/No	System usability statements	1	2	3	4	5
1	It is easy to learn how to use G-MoMo applications.					
2	I believe I can effectively complete my task using G-MoMo applications with minimal time and effort.					
3	The algorithm's security and transaction goals are efficiently achieved with G-MoMo applications.					
4	I can easily remember the appearance and procedure of using the G-MoMo applications.					
5	I get a response when an error occurs while using G-MoMo applications.					

6	I felt delighted, confident and satisfied with the ease of using the G-MoMo applications.					
7	I do not need technical support to use the G-MoMo applications.					
8	The G-MoMo applications are attractive and aesthetically designed.					
9	G-MoMo applications are useful regarding authentication and transaction performance.					
10	I found the various components of G-MoMo applications well integrated.					
11	There is an instruction menu on using the G-MoMo applications to prevent errors in the operation of the application.					
12	The information provided with the G-MoMo applications is easy to understand.					

Thanks

Appendix 7: Python code for registering new mobile money customers

```
from models.utils import(
   dbConfig
   )
from models import(
   UserCustomer
   )
from api.common import(
   custom_fields as custom_fields_common
   )
from cryptography.fernet import Fernet
key=custom_fields_common.EncryptionKey()
KEY=key()
FT = Fernet(KEY)
import uuid
class CreateCustomer(object):
   """docstring for CreateCustomer"""

   def __init__(self, **kwargs):
      self.first_name =FT.encrypt(kwargs['first_name'].encode()).decode()
      self.last_name=FT.encrypt(kwargs['last_name'].encode()).decode()
      self.mobile=FT.encrypt(kwargs['mobile'].encode()).decode()

   def __call__(self):
      session=dbConfig.Session()
      mobile_uuid=self.generate_mobile_uuid()
      user_customer=UserCustomer(
                  first_name=self.first_name,
                  last_name=self.last_name,
                  mobile=self.mobile,
                  mobile_uuid=mobile_uuid
                  )
      session.add(
         user_customer
         )
      session.commit()
      session.close()
      return mobile_uuid
```

```
def generate_mobile_uuid(self):
    session2=dbConfig.Session()
    while True:
        mobile_uuid=str(uuid.uuid4())
        user_customer=session2.query(
                        UserCustomer
                        ).filter_by(
                            mobile_uuid=mobile_uuid
                            )
        if user_customer.count()==0:
            session2.close()
            break
    return mobile_uuid
```

Appendix 8: Vue JS code for registering the phone number and smartphone and creating the UUID

```
check_mobile_uuid:function() {
        var vm =this
        alert({
          title: "Warning",
          message: "This smartphone and phone number is not registered. Select 'Ok' to register them",
          okButtonText: "OK"
        }).then(() => {
          const dialogs = require('@nativescript/core/ui/dialogs')
          prompt({
              title: "Enter your phone number",
              message: "We shall send OTP to this number. Ensure that the number is on this smartphone",
              okButtonText: "OK",
              cancelButtonText: "Cancel",
              defaultText: "256779597131",
              inputType: dialogs.inputType.text
            }).then(result => {
              if (result.text.length!==12) {
                  alert({
                    title: "Error",
                    message: "The phone number must be of 12 digits",
                    okButtonText: "OK"
                  }).then(() => {
                    vm.check_mobile_uuid()
                  })
              } else{
                var url1=`${BASE_URI}/api/customer/check_mobile/${APP_ID}`
                console.log(url1)
                console.log(result.text)
                var content=JSON.stringify({
                  mobile: result.text
                })
                console.log("Content",content)
                Http.request({
                  url: url1,
```

```
  method: "POST",
  headers: { "Content-Type": "application/json" },
  content: content,
}).then(function (response1) {
    console.log(response1)
    var response1_json = response1.content.toJSON();
    console.log(response1_json)
    if (response1_json.request_detail.data!==true) {
        alert({
          title: "Verification failed",
          message: `Reason: ${response1_json.request_detail.reason}`,
          okButtonText: "OK"
        }).then(() => {
          console.log("Alert dialog closed");
        });
    } else{
        // call the api send otp
        var url2=`${BASE_URI}/api/customer/send_otp/${APP_ID}`
        console.log(url2)
        Http.request({
          url: url2,
          method: "POST",
          headers: { "Content-Type": "application/json" },
          content: JSON.stringify({
            mobile_uuid: response1_json.mobile_uuid
          }),
        }).then(function (response2) {
            var response2_json = response2.content.toJSON();
            console.log(response2_json)
            if (response2_json.request_detail.data!==true) {
                alert({
                  title: "Error",
                  message: `Reason: ${response2_json.request_detail.reason}`,
                  okButtonText: "OK"
                }).then(() => {
                  console.log("Alert dialog closed");
                });
            } else{
                prompt({
```

```
                    title: "Enter the OTP",
                    message: "We sent an OTP to your phone number. Enter it to
verify your number",
                    okButtonText: "OK",
                    cancelButtonText: "Cancel",
                    inputType: dialogs.inputType.text
                  }).then(result2 => {
                   var
                url3=`${BASE_URI}/api/customer/verify_otp/${APP_ID}`
                   // console.log(url1)
                   Http.request({
                    url: url3,
                    method: "POST",
                    headers: { "Content-Type": "application/json" },
                    content: JSON.stringify({
                     mobile_uuid: response1_json.mobile_uuid,
                     otp:result2.text
                    }),
                   }).then(function (response3) {
                      var response3_json = response3.content.toJSON();
                      console.log(response3_json)
                      if (response3_json.request_detail.data!==true) {
                          alert({
                            title: "Error",
                            message:`Reason:
${response3_json.request_detail.reason}`,
                            okButtonText: "OK"
                          }).then(() => {
                            console.log("Alert dialog closed");
                          });
                      } else{
                        vm.register_new_device(
                          response1_json.mobile_uuid,
                          result.text
                          )
                      }
                   }).catch(function (error) {
                      console.log(error)
                    })
```

```
                        })
                    }
                }).catch(function (error) {
                    console.log(error)
                })
            }
        }).catch(function (error) {
            console.log(error)
        })
    }
});
},
register_new_device:function(mobile_uuid,mobile){
    var vm=this

permissions.requestPermission(permissions.PERMISSIONS.WRITE_EXTERNAL_STORAGE
)
        .then( () => {
            console.log("Woo Hoo, I have the power!");

permissions.requestPermission(permissions.PERMISSIONS.READ_EXTERNAL_STORAGE)
            .then( () => {
                console.log(mobile_uuid,mobile)
                const documents = fileSystemModule.knownFolders.documents();
                const folder = documents.getFolder("keystore");
                const path = fileSystemModule.path.join(folder.path, "mobile_uuid.txt");
                console.log(path)
                const file = fileSystemModule.File.fromPath(path);
                file.writeText(mobile_uuid)
                .then((result) => {
                    console.log("result",result)
                    file.readText()
                        .then((res) => {
                            console.log("successMessage", `Successfully saved in${file.path}`);
                            console.log("writtenContent", res);
                            console.log("isItemVisible", true);
                            alert({
```

```
                                title: "Success",
                                message: `Your device has been successfully registered with phone number ${mobile}. We are going to exit this app, and you will have to open it again`,
                                okButtonText: "OK"
                            }).then(() => {
                                if (application.android) {
                                    application.android.foregroundActivity.finish();
                                } else {
                                    exit(0);
                                }
                            });
                        });
                    }).catch((err) => {
                        console.log(err);
                    });
                    // var exists = fileSystemModule.File.exists("/data/user/0/org.nativescript.gmomo/files/keystore/mobile_uuid.json");
                })
                .catch( () => {
                    console.log("Uh oh, no permissions - plan B time!");
                });
            })
            .catch( () => {
                console.log("Uh oh, no permissions - plan B time!");
            });
        },
```

Appendix 9: Python code for setting the mobile money PIN

```
from models.utils import(
   dbConfig
   )
from models import(
   UserCustomer
   )
from passlib.hash import sha256_crypt

class CreatePin(object):
   """docstring for CreatePin"""

   def __init__(self, **kwargs):
      self.pin = sha256_crypt.encrypt(kwargs['pin'])
      self.mobile_uuid=kwargs['mobile_uuid']

   def __call__(self):
      session=dbConfig.Session()
      user_customer=session.query(
                  UserCustomer
                  ).filter_by(
                     mobile_uuid=self.mobile_uuid
                     ).one()
      user_customer.pin=self.pin
      session.commit()
      session.close()
      return True
```

Appendix 10: Python code for enrolling biometric fingerprints

```
from models.utils import(
   dbConfig
   )
from models import(
   User
   )
from api.common import(
   custom_fields as custom_fields_common
   )
from cryptography.hazmat.primitives.asymmetric import rsa
from cryptography.hazmat.primitives import serialization
from cryptography.fernet import Fernet
key=custom_fields_common.EncryptionKey()
KEY=key()
FT = Fernet(KEY)
private_encryption_key=custom_fields_common.PrivateEncryptionKey()

class RegisterBiometric(object):
   """docstring for RegisterBiometric"""

   def __init__(self, **kwargs):
      self.device_id =FT.encrypt(kwargs['device_id'].encode()).decode()
      self.device_name =FT.encrypt(kwargs['device_name'].encode()).decode()
      self.mobile_uuid=kwargs['mobile_uuid']

   def __call__(self):
      private_key = rsa.generate_private_key(public_exponent=65537,key_size=2048)
      private_key_pem = private_key.private_bytes(
            encoding=serialization.Encoding.PEM,
            format=serialization.PrivateFormat.PKCS8,
            encryption_algorithm=serialization.BestAvailableEncryption(
                  private_encryption_key()
                  )
            )
      private_key_pem=private_key_pem.decode()
      public_key = private_key.public_key()
```

```
        public_key_pem =
public_key.public_bytes(encoding=serialization.Encoding.PEM,format=serialization.PublicFor
mat.SubjectPublicKeyInfo)
        public_key_pem=public_key_pem.decode()
        session=dbConfig.Session()
        user=User(
                mobile_uuid=self.mobile_uuid,
                public_key=public_key_pem,
                device_id=self.device_id,
                device_name=self.device_name
                )
        session.add(
           user
           )
        session.commit()
        session.close()
        return private_key_pem
```

Appendix 11: Python code for authenticating the mobile money customer's PIN

```
from models.utils import(
   dbConfig
   )
from models import(
   UserCustomer
   )
from passlib.hash import sha256_crypt
class AuthenticateWithPin(object):
   """docstring for AuthenticateWithPin"""

   def __init__(self, **kwargs):
      self.pin = kwargs['pin']
      self.mobile_uuid=kwargs['mobile_uuid']

   def __call__(self):
      session=dbConfig.Session()
      user_customer=session.query(
               UserCustomer
               ).filter_by(
                  mobile_uuid=self.mobile_uuid
                  ).one()
      if sha256_crypt.verify(self.pin,user_customer.pin):
         session.close()
         return True
      session.close()
      return False
```

Appendix 12: Python code for sending OTP

```
from models.utils import(
   dbConfig
   )
from models import(
   UserCustomer,
   OTPCustomer
   )
from passlib.hash import sha256_crypt
from twilio.rest import Client
import random
from api.common import(
   custom_fields as custom_fields_common
   )
from cryptography.fernet import Fernet
key=custom_fields_common.EncryptionKey()
KEY=key()
FT = Fernet(KEY)
class SendOTP(object):
   """docstring for SendOTP"""

   def __init__(self, **kwargs):
      self.mobile_uuid=kwargs['mobile_uuid']

   def __call__(self):
      session=dbConfig.Session
      # print(self.mobile_uuid)
      user_customer=session.query(
                  UserCustomer
                  ).filter_by(
                     mobile_uuid=self.mobile_uuid
                     ).one()
      otp=""
      for i in range(5):
         otp+=str(random.randrange(10))
      account_sid = 'ACbd7afbc90628207cad756ada46d2f11b'
      auth_token = '5a28dc186fbef81510e1015968ec87eb'
      client = Client(account_sid, auth_token)
```

```
        mobile=FT.decrypt(user_customer.mobile.encode()).decode()
        # print(mobile)
        # to=f"+256{mobile[1:]}"
        to=f"+{mobile}"
        message = client.messages.create(
                        body=f"<#> Your G-MoMo App OTP is:{otp}. Be Safe. Do NOT SHARE
this code with anybody. N/RywfrtlZL",
                        from_="+13363447508",
                        to=to
                    )
        message.sid
        otps_customer=session.query(
            OTPCustomer
            ).filter_by(
               user_id=user_customer.user_id
               ).filter_by(
                  otp_state="active"
                  )
        for otp_customer_ in otps_customer:
           otp_customer_.otp_state="expired"
           session.commit()
        otp_value=otp
        otp=FT.encrypt(otp.encode()).decode()
        otp_customer=OTPCustomer(
                    otp=otp,
                    user_customer=user_customer
                    )
        session.add(
           otp_customer
           )
        session.commit()
        session.close()
        return otp_value
```

Appendix 13: Python code for verifying the OTP

```
from models.utils import(
   dbConfig
   )
from models import(
   UserCustomer,
   OTPCustomer
   )
from api.common import(
   custom_fields as custom_fields_common
   )
from cryptography.fernet import Fernet
key=custom_fields_common.EncryptionKey()
KEY=key()
FT = Fernet(KEY)

class VerifyOTP(object):
   """docstring for VerifyOTP"""

   def __init__(self, **kwargs):
      self.mobile_uuid=kwargs['mobile_uuid']
      self.otp=kwargs['otp']

   def __call__(self):
      session=dbConfig.Session()
      user_customer=session.query(
                  UserCustomer
                  ).filter_by(
                     mobile_uuid=self.mobile_uuid
                     ).one()
      otp_customer=session.query(
            OTPCustomer
            ).filter_by(
               user_id=user_customer.user_id
               ).filter_by(
                  otp_state="active"
                  )
      if otp_customer.count()==1:
```

```
    otp_customer=otp_customer.one()
    print(FT.decrypt(otp_customer.otp.encode()).decode()==self.otp)
    print(FT.decrypt(otp_customer.otp.encode()).decode(),self.otp)
    if FT.decrypt(otp_customer.otp.encode()).decode()==self.otp:
        otp_customer.otp_state='expired'
        session.commit()
        session.close()
        return True
# otp_customer.otp_state='expired'
session.commit()
session.close()
return False
```

Appendix 14: Python code for verifying the customer's biometric fingerprint

(i) Signing the challenge

```
from models.utils import(
   dbConfig
   )
from models import(
   User,
   Challenge
   )
from api.common import(
   custom_fields as custom_fields_common
   )
from cryptography.fernet import Fernet
from cryptography.hazmat.primitives import serialization
from cryptography.hazmat.primitives import hashes
from cryptography.hazmat.primitives.asymmetric import padding
import base64
import string
import random
key=custom_fields_common.EncryptionKey()
KEY=key()
FT = Fernet(KEY)
private_key_password=custom_fields_common.PrivateEncryptionKey()

class SignChallenge(object):
   """docstring for SignChallenge"""

   def __init__(self, **kwargs):
      self.mobile_uuid=kwargs['mobile_uuid']
      # challenge_decode=base64.b64decode(kwargs['challenge'].encode())
      self.challenge=kwargs['challenge']
      self.private_key=kwargs['private_key']

   def __call__(self):
      session=dbConfig.Session()
```

```
        user=session.query(
                User
                ).filter_by(
                    mobile_uuid=self.mobile_uuid
                    ).filter_by(
                        account_state="active"
                        )
        if user.count()==0:
            session.close()
            return False, ""
        user=user.one()

        private_key = serialization.load_pem_private_key(
                        self.private_key.encode(),
                        password=private_key_password()
                        )
        signature = private_key.sign(
                    self.challenge.encode(),
                    padding.PSS(
                        mgf=padding.MGF1(hashes.SHA256()),
                        salt_length=padding.PSS.MAX_LENGTH
                        ),
                    hashes.SHA256()
                    )
        encoded = base64.b64encode(signature)
        decoded=encoded.decode()
        session.close()
        return True,decoded
```

(ii) Verify the public key

```
from models.utils import(
    dbConfig
    )
from models import(
    User,
    Challenge
```

```
    )
from api.common import(
    custom_fields as custom_fields_common
    )
from cryptography.fernet import Fernet
from cryptography.hazmat.primitives import serialization
from cryptography.hazmat.primitives import hashes
from cryptography.hazmat.primitives.asymmetric import padding
import base64
import string
import random
key=custom_fields_common.EncryptionKey()
KEY=key()
FT = Fernet(KEY)

class VerifySignature(object):
    """docstring for VerifySignature"""

    def __init__(self, **kwargs):
        self.mobile_uuid=kwargs['mobile_uuid']
        # self.challenge=FT.decrypt(kwargs['challenge'].encode())
        self.signature=kwargs['signature']

    def __call__(self):
        session=dbConfig.Session()
        user=session.query(
                User
                ).filter_by(
                    mobile_uuid=self.mobile_uuid
                    ).filter_by(
                        account_state="active"
                        )
        if user.count()==0:
            session.close()
            return False, ""
        user=user.one()
        public_key = serialization.load_pem_public_key(
                        user.public_key.encode()
                        )
```

```
decoded=base64.decodebytes(self.signature.encode())
try:
    public_key.verify(
        decoded,
        self.challenge.encode(),
        padding.PSS(
            mgf=padding.MGF1(
                hashes.SHA256()
                ),
            salt_length=padding.PSS.MAX_LENGTH
            ),
        hashes.SHA256()
    )
    # check_challenge=check_challenge.one()
    # check_challenge.challenge_state="inactive"
    # session.commit()
    session.close()
    return True
except:
    session.close()
    return False
```

Appendix 15: Vue JS code for confirming money withdrawal using biometric fingerprints and QR codes

(i) Biometric fingerprint confirmation

```
verifyWithFingerPrint: function(){
    var vm=this
    vm.busy=true
    fingerprintAuth.available().then(
      function(avail) {
        console.log("Available? " + JSON.stringify(avail));
        if (avail.biometrics==true){
          fingerprintAuth.verifyFingerprint(
            {
            message: "Scan with your finger",
            fallbackTitle: "Enter PIN"
          }).then(
              () => {
                console.log("Fingerprint was OK");
                // vm.navigateToHome()
                const documents = fileSystemModule.knownFolders.documents();
                const folder = documents.getFolder("keystore");
                const path = fileSystemModule.path.join(folder.path, "key.txt");
                const file = fileSystemModule.File.fromPath(path);
                file.readText()
                  .then((res) => {
                    console.log("writtenContent", res);
                    if (res=="None"){
                      alert({
                        title: "Authorization failed",
                        message: `Dear ${vm.user_detail.first_name}, you have already
authorized another device, consider verifying that device.`,
                        okButtonText: "OK"
                      }).then(() => {
                        // console.log("Alert dialog closed");
                      });
                      vm.busy=false
                    } else {
```

```
                    var
url1=`${BASE_URI_FIDO_SDK}/api/customer/biometric_auth_challenge/${APP_ID}`
                    Http.request({
                     url: url1,
                     method: "POST",
                     headers: { "Content-Type": "application/json" },
                     content: JSON.stringify({
                      mobile_uuid: vm.mobile_uuid
                     }),
                    }).then(function (response1) {
                      var response1_json = response1.content.toJSON();
                      console.log("response1_json",response1_json)
                      if (response1_json.request_detail.data!==true) {
                       console.log(response1_json.request_detail.reason)
                       alert({
                        title: "Transaction failed",
                        message: `Reason: ${response1_json.request_detail.reason}`,
                        okButtonText: "OK"
                       }).then(() => {
                       });
                      }else{
                          var
url2=`${BASE_URI_FIDO_SDK}/api/customer/sign_challenge/${APP_ID}`
                          Http.request({
                            url: url2,
                            method: "POST",
                            headers: { "Content-Type": "application/json" },
                            content: JSON.stringify({
                              mobile_uuid: vm.mobile_uuid,
                              private_key:res,
                              challenge:response1_json.challenge
                            }),
                           }).then(function (response2) {
                            console.log(response2)
                            vm.currentProgress=99
                            var response2_json = response2.content.toJSON();
                            console.log("response2_json",response2_json)
                            if (response2_json.request_detail.data!==true) {
                              console.log(response2_json.request_detail.reason)
```

```
                                    alert({
                                      title: "Transaction failed",
                                      message: `Reason: ${response2_json.request_detail.reason}`,
                                      okButtonText: "OK"
                                    }).then(() => {
                                    });
                                   }else{
                                     var
url3=`${BASE_URI_FIDO_SDK}/api/customer/verify_signature/${APP_ID}`
                                     Http.request({
                                        url: url3,
                                        method: "POST",
                                        headers: { "Content-Type": "application/json" },
                                        content: JSON.stringify({
                                         mobile_uuid: vm.mobile_uuid,
                                         challenge:response1_json.challenge,
                                         signature:response2_json.signature
                                        }),
                                       }).then(function (response3) {
                                         console.log(response3)
                                         var response3_json = response3.content.toJSON();
                                         console.log("response3_json",response3_json)
                                         if (response3_json.request_detail.data!==true) {
                                          alert({
                                             title: "Transaction failed",
                                             message: `Reason:
${response3_json.request_detail.reason}`,
                                              okButtonText: "OK"
                                           }).then(() => {
                                           });
                                           vm.busy=false
                                         }else{
                                           console.log("Things are perfect")
                                           vm.scan_qr()
                                           vm.currentProgress=50
                                         }
                                       }).catch(function (error) {
                                         console.log(error)
                                       })
```

```
                                    }
                                   }).catch(function (error) {
                                    console.log(error)
                                   })
                                 }
                                }).catch(function (error) {
                                 console.log(error)
                                })
                               }
                             });
                        },
                        error => {
                         console.log("Fingerprint NOT OK. Error code: " + error.code + ". Error
message: " + error.message);
                        }
                    );
                }
               }
            )
           },
```

(ii) Scanning QR code

```
scan_qr:function(){
        var vm=this
        if(vm.amount<500 || vm.amount==null || vm.amount==""){
         alert({
            title: "Transaction failed",
            message: `Reason: The withdraw money should not be less than UGX 500`,
            okButtonText: "OK"
          }).then(() => {
            // console.log("Alert dialog closed");
          });
         vm.busy=false
        } else {
         vm.currentProgress=10
         barcodescanner.requestCameraPermission().then(
            function() {
              console.log("Camera permission requested 1");
```

```
            barcodescanner.scan({
                formats: "QR_CODE,PDF_417",   // Pass in of you want to restrict scanning to certain types
                cancelLabel: "EXIT. Also, try the volume buttons!", // iOS only, default 'Close'
                cancelLabelBackgroundColor: "#333333", // iOS only, default '#000000' (black)
                message: "Use the volume buttons for extra light", // Android only, default is 'Place a barcode inside the viewfinder rectangle to scan it.'
                showFlipCameraButton: true,   // default false
                preferFrontCamera: false,     // default false
                showTorchButton: true,        // default false
                beepOnScan: true,             // Play or Suppress beep on scan (default true)
                fullScreen: true,             // Currently only used on iOS; with iOS 13 modals are no longer shown fullScreen by default, which may be actually preferred. But to use the old fullScreen appearance, set this to 'true'. Default 'false'.
                torchOn: false,               // launch with the flashlight on (default false)
                closeCallback: function () { console.log("Scanner closed"); }, // invoked when the scanner was closed (success or abort)
                resultDisplayDuration: 500,   // Android only, default 1500 (ms), set to 0 to disable echoing the scanned text
                // orientation: "landscape",     // Android only, optionally lock the orientation to either "portrait" or "landscape"
                openSettingsIfPermissionWasPreviouslyDenied: true // On iOS you can send the user to the settings app if access was previously denied
              }).then(
                function(result) {
                  vm.currentProgress=40
                  console.log("Scan format: " + result.format);
                  console.log("Scan text:   " + result.text);
                  vm.verify_qr(result.text)
                },
                function(error) {
                  console.log("No scan: " + error);
                  alert({
                    title: "Transaction failed",
                    message: `Reason: We couln't scan the QR of the G-momo Agent`,
                    okButtonText: "OK"
                  }).then(() => {
                  });
                  vm.busy=false
```

```
                }
              );
            }
          );
        }
    },
```

(iii) QR code confirmation

```
verify_qr:function(qr){
        var vm=this
        var url2=`${BASE_URI}/api/customer/verify_qr/${APP_ID}`
        Http.request({
         url: url2,
         method: "POST",
         headers: { "Content-Type": "application/json" },
         content: JSON.stringify({
          mobile_uuid: vm.mobile_uuid,
          qr:qr
         }),
        }).then(function (response2) {
            vm.currentProgress=50
            console.log(response2)
            var response2_json = response2.content.toJSON();
            console.log("response2_json",response2_json)
            if (response2_json.request_detail.data!==true) {
              alert({
                title: "Transaction failed",
                message: `Reason: Agent not found! Please report this to 256-779-597131 in case you suspect a fraudster.`,
                okButtonText: "OK"
              }).then(() => {
                // console.log("Alert dialog closed");
              });
              vm.busy=false
            }else{
              vm.currentProgress=60
              vm.withdrawMoney()
```

```
        }
      }).catch(function (error) {
        console.log(error)
      })
  },
```

Appendix 16: Python code for changing the mobile money PIN

```
from models.utils import(
   dbConfig
   )
from models import(
   UserCustomer
   )
from passlib.hash import sha256_crypt

class CreatePin(object):
   """docstring for CreatePin"""

   def __init__(self, **kwargs):
      self.pin = sha256_crypt.encrypt(kwargs['pin'])
      self.mobile_uuid=kwargs['mobile_uuid']

   def __call__(self):
      session=dbConfig.Session()
      user_customer=session.query(
                  UserCustomer
                  ).filter_by(
                     mobile_uuid=self.mobile_uuid
                     ).one()
      user_customer.pin=self.pin
      session.commit()
      session.close()
      return True
```

Appendix 17: Python code for changing the biometric fingerprint

```
from models.utils import(
   dbConfig
   )
from models import(
   User
   )
from api.common import(
   custom_fields as custom_fields_common
   )
from cryptography.hazmat.primitives.asymmetric import rsa
from cryptography.hazmat.primitives import serialization
from cryptography.fernet import Fernet
key=custom_fields_common.EncryptionKey()
KEY=key()
FT = Fernet(KEY)
private_encryption_key=custom_fields_common.PrivateEncryptionKey()
class RegisterNewDeviceBiometric(object):
   """docstring for RegisterNewDeviceBiometric"""

   def __init__(self, **kwargs):
      self.device_id =FT.encrypt(kwargs['device_id'].encode()).decode()
      self.device_name =FT.encrypt(kwargs['device_name'].encode()).decode()
      self.mobile_uuid=kwargs['mobile_uuid']

   def __call__(self):
      private_key = rsa.generate_private_key(public_exponent=65537,key_size=2048)
      private_key_pem = private_key.private_bytes(
            encoding=serialization.Encoding.PEM,
            format=serialization.PrivateFormat.PKCS8,
            encryption_algorithm=serialization.BestAvailableEncryption(
                        private_encryption_key()
                        )
            )
      private_key_pem=private_key_pem.decode()
      public_key = private_key.public_key()
```

```
        public_key_pem =
public_key.public_bytes(encoding=serialization.Encoding.PEM,format=serialization.PublicFor
mat.SubjectPublicKeyInfo)
        public_key_pem=public_key_pem.decode()
        session=dbConfig.Session()
        user=session.query(
                User
                ).filter_by(
                    mobile_uuid=self.mobile_uuid
                    ).one()
        user.public_key=public_key_pem
        user.device_id=self.device_id
        user.device_name=self.device_name
        session.commit()
        session.close()
        return private_key_pem
from models.utils import(
    dbConfig
    )
from models import(
    UserCustomer
    )
class AddNewBiometricDevice(object):
    """docstring for AddNewBiometricDevice"""
    def __init__(self, **kwargs):
        self.mobile_uuid=kwargs['mobile_uuid']
    def __call__(self):
        session=dbConfig.Session()
        user_customer=session.query(
                    UserCustomer
                    ).filter_by(
                        mobile_uuid=self.mobile_uuid
                        ).one()
        user_customer.public_key_state="set"
        session.commit()
        session.close()
        return False
```

RESEARCH OUTPUTS

(i) Publications

Ali, G., Dida, M. A., & Sam, A. E. (2020). Two-factor authentication scheme for mobile money: A review of threat models and countermeasures. *Future Internet*, *12*(10), 160.

Ali, G., Dida, M. A., & Sam, A. E. (2020). Evaluation of key security issues associated with mobile money systems in Uganda. *Information*, *11*(6), 309.

Ali, G., Dida, M. A., & Sam, A. E. (2021). A Secure and Efficient Multi-Factor Authentication Algorithm for Mobile Money Applications. *Future Internet*, 13(12), 299.

Ali, G., Dida, M. A., & Sam, A. E. (2022). Heuristic Evaluation and Usability Testing of G-MoMo Applications. *Journal of Information Systems Engineering and Management*, *7*(3), 1-14.

(ii) Poster presentation