information

MDPI

Article

Evaluation of Key Security Issues Associated with Mobile Money Systems in Uganda

Guma Ali [1,*], Mussa Ally Dida [1] and Anael Elikana Sam [2]

[1] Department of Information Technology Development and Management (ITDM), Nelson Mandela African Institution of Science and Technology, 447 Arusha, Tanzania; mussa.ally@nm-aist.ac.tz
[2] Department of Communication Science and Engineering (CoSE), Nelson Mandela African Institution of Science and Technology (NM-AIST), 447 Arusha, Tanzania; anael.sam@nm-aist.ac.tz
* Correspondence: gumaa@nm-aist.ac.tz

Received: 2 May 2020; Accepted: 25 May 2020; Published: 8 June 2020

Abstract: Smartphone technology has improved access to mobile money services (MMS) and successful mobile money deployment has brought massive benefits to the unbanked population in both rural and urban areas of Uganda. Despite its enormous benefits, embracing the usage and acceptance of mobile money has mostly been low due to security issues and challenges associated with the system. As a result, there is a need to carry out a survey to evaluate the key security issues associated with mobile money systems in Uganda. The study employed a descriptive research design, and stratified random sampling technique to group the population. Krejcie and Morgan's formula was used to determine the sample size for the study. The collection of data was through the administration of structured questionnaires, where 741 were filled by registered mobile money (MM) users, 447 registered MM agents, and 52 mobile network operators' (MNOs) IT officers of the mobile money service providers (MMSPs) in Uganda. The collected data were analyzed using RStudio software. Statistical techniques like descriptive analysis and Pearson Chi-Square test was used in data analysis and mean (M) > 3.0 and p-value < 0.05 were considered statistically significant. The findings revealed that the key security issues are identity theft, authentication attack, phishing attack, vishing attack, SMiShing attack, personal identification number (PIN) sharing, and agent-driven fraud. Based on these findings, the use of better access controls, customer awareness campaigns, agent training on acceptable practices, strict measures against fraudsters, high-value transaction monitoring by the service providers, developing a comprehensive legal document to run mobile money service, were some of the proposed mitigation measures. This study, therefore, provides a baseline survey to help MNO and the government that would wish to implement secure mobile money systems.

Keywords: mobile money; mobile money systems; mobile network operators; mobile money services; mobile money service providers; security issues; evaluation; Uganda

1. Introduction

The increased diffusion of powerful mobile devices like smartphones has transformed how users access mobile financial services such as mobile money. This has made many developing nations embrace mobile money as a potential payment platform. Mobile money is defined as a wide scope of financial services accessible on a mobile phone [1]. Talom and Tengeh [2] further added that mobile money is a service that allows customers to get access to financial services by using mobile devices and dialing unstructured supplementary service data (USSD) codes. According to the Global System for Mobile Communications (GSMA) [3], mobile money is now available in over 90 countries with three-quarters being lower and middle-income countries. It has thus emerged as the leading payment

platform for the digital economy, with 866 million registered accounts worldwide and $1.3 billion processed daily [3].

The evolution of the first mobile money services in the world took place in the Philippines in 2001 when Smart Communications deployed Smart Money in partnership with Banco de Oro (BDO) to subdue the problem of limited access to banking infrastructure. After the successful deployment of Smart Money, Globe Telecom later launched GCash in 2004 [4]. In the East African region, the inaugural deployment of mobile money was in Kenya when Safaricom launched M-Pesa in March 2007. In Tanzania, M-Pesa was launched by Vodacom Tanzania in April 2008 and Z-Pesa by Zantel [5,6]. For Uganda, Mobile Telephone Networks (MTN) launched its first mobile money service in 2009, following the successful launch of M-Pesa in Kenya [5].

Despite its enormous benefits in improving access to financial services, embracing the usage and acceptance of mobile money has mostly been low due to security issues and challenges associated with the system. Although few extended pieces of research have been conducted concerning mobile money security, particularly in Africa, India, and South America, the topic has not been surveyed in Uganda. The studies that were examined in this area include Mtaho [7] that investigated the security challenges associated with the mobile money authentication methods in Tanzania. Castle et al. [8] assessed the security challenges of mobile money in the developing world. Bosamia [9] identified and analyzed the different threats and vulnerabilities of a mobile wallet application. However, none of the mentioned studies evaluated the key security issues associated with mobile money systems in Uganda.

Additionally, this paper focused primarily on mobile money systems' security. Therefore, it aims to contribute to the mobile money security literature by mainly evaluating the key security issues associated with mobile money systems in Uganda. The paper adopted a descriptive research design. The findings of this study will help the mobile money operators, mobile money decision-makers, and the government to identify and evaluate the key security issues associated with mobile money systems so that novel methods or measures can be proposed to address the security gaps.

The rest of the paper is organized as follows. In the next section, the relevant literature on security issues associated with mobile money systems is covered. The third section talks about the materials and methods used in the study. The overview of the analysis of results is provided in Section 4. In Section 5, we give a detailed discussion of the results. We conclude the study with contributions, limitations, and recommendations to the relevant stakeholders.

2. Related Work

2.1. Mobile Money Evolution in Uganda

In Uganda, MTN introduced the first mobile money service in 2009, following the successful launch of M-Pesa in Kenya [5]. Other MNOs like Warid, Airtel, Uganda Telecom Limited (UTL), Orange Telecom later followed. Currently, there are seven mobile money service providers (MMSPs) in Uganda, namely MTN, Airtel, UTL, Africell, M-Cash, Ezeey Money, and Micropay, with a network of approximately 200,857 agents and 25.8 million users combined during the year of 2019 compared to approximately 13 million traditional bank accounts in 26 banks [10–12]. Bank of Uganda (BoU) annual report of 2018/19 mentioned that the total number of mobile money transactions increased from 1.35 billion to 2.51 billion and mobile money transactions were UGX 66.95 trillion during the financial year [11]. The number of smartphone connections in Uganda also magnified to approximately 6 million, around a quarter of total mobile connections [12]. These mobile money systems use USSD, short message services (SMS), and a subscriber identity module (SIM) toolkit (STK) technologies to provide access to users [13].

Mobile money platforms involve several players and stakeholders such as MNOs, banks or other financial institutions, regulatory institutions, agent networks, merchants and retailers, businesses, mobile money users, equipment manufacturers, and platform providers, who perform different roles

and in turn gain distinct benefits from the mobile money ecosystem [14]. Mobile money is now widely used in many fields, including, business, finance, health, agriculture, and education [15].

Mobile money offers an extensive range of services including deposit and withdrawal of money, transfer of money to other users, pay utility bills (like water, electricity, DStv), purchase airline tickets [16,17], pay for goods in a store, Lotto and sports betting, save money for future purchases or payment, receive a salary, take a loan, receive state aid or pension, purchase insurance, purchase airtime and data bundles, make bank transactions, pay for school fees, and taxes [1,18]. These services are rapidly deployed across emerging markets as a key instrument to further Uganda's 78% financial inclusion goal [12].

Over the past few years, several factors have driven the usage of mobile money services. They include; technology, user attitudes, product and service differentiation, supportive policy and regulation, institutional relationships, customer experience, customer expectations, quality of service, affordability, convenience, accessibility, reliability, and security [3,19–22].

Mobile Money has come out as an important innovation with potential benefits. For instance, it enhanced access to financial services for a large number of people who cannot access banks [23,24]. According to Mwangi and Kasamani [25], Murendo et al. [26], and Saxena et al. [27], mobile money provides a convenient way to send money to anyone who owns a mobile phone or has access to the mobile money agent. Nyaga [28] mentioned that mobile money services includes the reliable saving option for many low-income earners, reduction in loss of sales, good audit trail, and quicker transaction than cash at the point of sales. Kyeyune, Mayoka, and Miiro [29] assert that the system is more secure since the money is not on a user's SIM card but a central server. Marumbwa and Mutsikiwa [30] added that mobile phones have brought massive opportunities in the provision of financial services. Mobile money services have enhanced the standard of living of people who cannot access bank and has led to the stimulation of economic development [31]. Jack and Suri [32] acknowledge that mobile money systems allow people to keep their savings hidden from friends or relatives who might ask for money. Mobile money systems also greatly cut down the expenses and time lags associated with opening, operating, and maintaining a traditional bank account [27,33]. Mobile money provides the quickest mechanism for clearing unplanned domestic financial payments. Successful mobile money deployment has led to the development of mobile commerce in the developing world [34]. According to Maitai and Omwenga [20], mobile money transfer services have transformed the way the financial service industry conducts business where customers can access any time. Cisco [35] asserted that mobile money transfers are cheaper than electronic transfer services and more reliable than physically transporting money. Mobile money enables small and medium-sized enterprises (SMEs) to receive and make payments instantly through mobile phones and improves business networking [2]. Additionally, mobile money leads to economic development through increased savings and investments [21]. It also increases productiveness in the remittance service [36].

2.2. Security Issues Associated with Mobile Money Systems

Despite the vast benefits offered by mobile money in Uganda, serious security concerns have led to infringements of mobile money systems, thus, leading to low acceptance and adoption among people. The security issues associated with mobile money systems are:

i. Authentication Attack: Castle et al. [8] noted that attackers use many ways to gain access to the user's account. They take advantage of weak personal identification number (PIN) reset procedures. The present form of mobile money authentication uses a PIN to authenticate the user and requires all mobile money services to utilize the same PIN [7]. The PIN used is only four (4) or five (5) digits, making it easy for attackers to guess, smudge or snoop, and weak against brute-force attacks [7,13,37,38]. Besides, most people tend to share their PIN among friends and families, which has also added more security risks [7]. The way the customer handles mobile phones, SIM cards, and PINs affect the security of electronic money stored in a mobile money account. Bosamia [9] added that attackers who understand mobile wallet payment

applications could use reverse engineering to attack passwords or PINs and encryption keys. According to Akomea-Frimpong et al. [39], most of the mobile money systems are not properly protected giving IT fraudsters' ability to hack the systems and steal customer money.

ii. Identity Theft: Mtaho [7] observed that mobile money agents usually incorporate mobile money businesses together with other services. Most of the well-established mobile money offices have many staff members who serve distinct services. If a dishonest member of staff happens to know the PIN of a colleague in the office, he/she can carry out unauthorized transactions at the expense of the colleague. This is consistent with the submission of Trulioo [40], who noted that identity theft is usually an inside job activity through unscrupulous employees gaining unauthorized access to mobile money data that belongs to the users and then irregularly misappropriating their funds. Gwahula [37], Buku and Mazer [41] further added that identity theft results from fraudulent or offline SIM swaps by fraudsters that transfer the mobile wallet account from the customer's SIM to the fraudster's SIM, thus enabling them to have full access to the user's mobile wallet and then carry out fraudulent transactions [42,43]. According to Bosamia [9], when a customer's mobile phone is stolen, attackers can make use of any sensitive data stored in it including the PIN, and have control over the device. The mobile money PIN stored on the mobile phone will provide attackers with access to the mobile money account and then carry out fraudulent transactions [44,45].

iii. USSD Technology Vulnerabilities: Nyamtiga, Anael, and Loserian [46] define USSD as a session-based, real-time communication technology used by the GSM network to provide additional services between a mobile client and an application server. Talom and Tengeh [2] further expanded the definition as a communications protocol for mobile communication technology used to send text between mobile phones and an application program in a mobile network without having access to the internet. The greatest risk of USSD is that information carried within the communication channel is not encrypted, thus making USSD data vulnerable to attacks [2,14,46]. This is consistent with the submission of Mtaho [7] who noted that during the verification process, the client enters the PIN that passes through the USSD system to the server in a plain text; thus, attackers using network sniffer software such as Wireshark can intercept it. Phipps et al. [47] further reported that there is also a threat to the redirection of USSD by attackers. This is by using ThinSIM, which can leverage the call control to redirect the USSD connection to a server owned by the attacker.

iv. SMiShing and Vishing Attacks: According to Maseno, Ogao, and Matende [48], a smishing attack is where fraudsters use an emotional delusional SMS to trick users to reveal their mobile money PIN. When used, an attacker can send SMS to the user(s) to "confirm" a payment when no money has been transferred. Vishing attack, on the other hand, is where attackers use anonymous phone calls or false promotions to trick users into disclosing their PINs or other sensitive personal information that is used to steal from their mobile money accounts [27,48]. This is in line with the submissions of Gilman and Joyce [44], Buku and Mazer [41], Lonie [45], Akomea-Frimpong et al. [39], who reported that phishing or social engineering frauds such as fraudsters impersonating as employees of service providers are common with mobile money. They added that the fraudsters send false promotions to users that they have won prizes and to claim those prizes, they need to send money to the fraudster's number. Mudiri [42] also noted that fraudsters call or send fake SMS using either their mobile phones or computers to customers or agents and then guide them through various steps that later result in the transfer of money from their account to the fraudsters' account. According to a report by Kigen et al. [49], social engineering was Kenya's second-largest cyber-security concern in 2015 and vishing was the widely used method of launching attacks on mobile money platforms in Kenya, where individuals were tricked to provide sensitive information such as mobile money PIN, which led to fraudulent transactions. With the rise of vishing attacks on many Kenyan mobile platforms, no substantial research has been undertaken to offer a remedy, thus affecting the integrity

of mobile transactions [48]. Kisekka [50] also confirmed that "according to MTN Uganda, some suspicious individuals have obtained PINs from customers under pretenses and have subsequently withdrawn funds from mobile money accounts of customers".

v. Brute-Force (Guessing) Attack: The brute-force attack is where attackers can predict and calculate the key required for accessing the system by using the machine-readable zone information [27,51]. Lately, the brute force attack has become common in mobile money were attackers utilize many channels to gain access to the user's mobile money account [44]. Reaves et al. [38] added that most mobile money applications use poor authentication such as numeric PINs that are proven ineffective against brute-force attacks.

vi. Denial-of-Service (DoS) Attack: This is where attackers are targeting a network link with fake traffic to block requests from mobile money users to access the database [8]. Buku and Mazer [41] noted that the disruption of the network creates opportunities for fraud, mainly through offline SIM swaps and over-the-counter (OTC) transactions. When a DoS attack occurs, the organization loses revenue and the mobile money account becomes inaccessible to customers [8,9,36,37].

vii. Man-in-the-Middle Attack: According to Taban, Luhanga, and Anael [51], in a man-in-the-middle attack, the intruder intercepts a message in transit and becomes familiar with the messaging system, thereby transmitting fake data to either party. Fraudsters hack or control the traffic into the mobile money platform and manipulate accounts to perform transactions or gain benefit [38,52]. This attack may include full root exploits as well as access to partial server logs, database records, or proprietary source code [8].

viii. Salami Attack: According to Balasubramanian [53], a salami attack is where a bank employee installs a program on the bank's server to steal or deducts a small sum of money from customers' accounts and deposits them into the attacker's account without the customers realizing. Salami attacks are difficult to detect or trace because the money deducted is small. Alhassan et al. [54] also observed that attackers could hack mobile wallets by inserting a program into the wallet server to deduct a small sum of money from each wallet and deposit them into the attacker's account.

ix. Replay Attack: According to Paik [55], SMS-based services such as GCASH are prone to interception and replay attacks. In developing nations, weak algorithms such as A5 protect SMS. Attackers with scanning software can easily get these messages while in transit, modify them and then, later on, resend them to the designated receivers. The SMS originating address is also spoofable, so there is no guarantee that messages sent are safe from alteration [44].

x. Insider Threat: Findings from Serianu research indicate that over 80% of fraud within remote systems has been borne out through facilitation by insiders and employees due to inside access [56]. Organizations have lost huge amounts of money to the tune of billions of shillings because of employee fraud within companies or institutions [56]. This assertion is consistent with the submission of Gilman and Joyce [44], Trulioo [40] who observed that less scrupulous employees abuse their privileges by accessing and stealing money from customers' wallets. Various instances of mobile money fraud have been reported by Morawczynski in the press, including the Ugandan newspaper, Daily Monitor, citing a fraud incident in MTN Uganda that resulted in the theft of 10 billion (US$ 3.83 million) and USh 15 billion ($900,000) from the company, and the crime was committed by senior MTN Uganda staff [45,57]. Similarly, the same scenario also occurred in Rwanda when Tigo lost more than 495 million francs ($170,000) to staff after they conspiried to manipulate the mobile money system [57].

xi. Agent-driven fraud: Many people, because of illiteracy or a general fear of making a mistake, trust agents who conduct transactions on their behalf [58]. Agents now take advantage of such people by stealing their money intended for a deposit and charges an additional amount compared to the company charge [59]. In some incidences, agents also defraud their depositors and abscond with the money [60]. According to Buku and Mazer [41], some other common

frauds related to agents include, float loss in the agent's account resulting from unauthorized use, misuse of PINs, and fraudsters impersonating MNO staff to gain unauthorized access to an agent's float account [45]. Gilman and Joyce [44] added that some mobile money agents also transfer customer money into their accounts. Akomea-Frimpong et al. [39] noted that some mobile money agents operate in open spaces like under trees, open market, under umbrellas, building with weak locks where they are attacked and robbed of their physical money. Customers also commit fraud against agents by giving a wrong mobile phone number repeatedly to get the agent's PIN, fake currency deposits, and physical force [8,41,45]. The 2015 surveys of the Helix Institute indicated that fraud is the primary concern of many agents [41]. The surveys found that 53% of mobile money agents in Uganda and 42% in Tanzania had experienced fraud, and Uganda recorded the highest rate of fraud and crime rates in the region [41].

xii. Malware: According to Castle et al. [8] and Chen et al. [61], software developers often include third-party libraries in their applications and such libraries can introduce unintended vulnerabilities. Musuva-Kigen et al. [56] observed that communication networks sometimes deliver malware to mobile phones. This malware spread in several ways, such as attaching to received SMS, internet downloads, and received Bluetooth messages. This malware then eavesdrops on user input and steals sensitive information stored on the mobile phone, such as mobile money PIN, and grant access to the intruder at will [9,62]. According to Bosamia [9], attackers often install malware through malware attachments that give them the exclusive right to redirect the users to the malicious uniform resource locator (URL), insecure Wi-Fi hotspots, fake websites, and access points so that users can avail their details to them, which they later use for mobile wallet payment without user's consent.

xiii. Mobile Phones Vulnerabilities: Mtaho [7] emphasized that a mobile phone has many security features that were left by the manufacturer without being disabled. Some of these features allow encryption of the data, but the task is left to the user. If users do not enable such features, attackers can intercept sensitive information stored in them like users' mobile money PIN. Previous studies have shown that technically skilled attackers take advantage of poor security design inside mobile money applications by creating a backdoor that allows them to login or simply circumvent poorly implemented encryption [9,62]. In addition to compromising data, mobile phones with active services, such as mobile money systems, could be accessed without approval, resulting in the stealing of money from mobile wallets [9].

xiv. Unauthorized SIM Swap: SIM swapping occurs when a fraudster uses social engineering techniques to obtain the mobile user's credentials to take control of the victim's SIM card. With this stolen information about the victim, the fraudster can use false documents to register the SIM and take over the victim's mobile money account [9,42,44]. The fraudster can directly receive incoming calls and text messages, including access to the victim's mobile money account, thus having full access to the funds in the account [40].

2.3. Hypothesis Development

To assess the relationship between demographic variables and mobile money systems' security challenges in Uganda, we considered five (5) constructs: gender, age, education level, duration of mobile money usage, and mobile money transactions in a month. No study has ever been carried out to assess the relationship between these constructs and mobile money systems' security challenges.

3. Materials and Methods

3.1. Study Design

A descriptive research design was employed in the study because both the quantitative and qualitative data are collected from the study area concerning the status of the phenomena [63]. The population for this study included registered MM users, registered MM agents, and MNO IT

officers of the seven mobile money service providers in Uganda. The study targeted a population of 25,800,000 registered MM users, 200,857 registered MM agents, and 100 MNO IT officers. This is because they possess experience with mobile money systems.

3.2. Sampling Technique

A stratified random sampling technique was employed for the study. This was used to group the population into strata of registered MM users, registered MM agents, and MNO IT officers. This is because each stratum is more homogeneous than the total population, thus giving the researchers confidence to select samples from each stratum to constitute the total sample size for the study [64]. The survey questionnaires were administrated for a period of nine weeks, from February 2020 to April 2020.

The sample size for the study was determined using Krejcie and Morgan's formula [65]. A number of 1614 respondents were selected using Krejcie and Morgan's formula below from a population of 26,000,957.

$$s = \frac{X^2 NP(1-P)}{d^2(N-1) + X^2 P(1-P)}$$

3.3. Validity and Reliability of the Questionnaires

Validity refers to the extent to which the instrument used for data collection accurately measures what it is intended to measure [66]. A credible research design is one that maximizes validity, that is to say, it provides a clear explanation of the phenomenon under study and controls all plausible biases or mistakes that could distort the research findings [67]. The validity of the instrument for this study was determined using the content validity index (CVI) [63]. According to Amin [63], Polit and Beck [68], A CVI of 0.78 and above is considered satisfactory for the study.

Reliability is "the consistency with which a measuring instrument yields certain results when the entity being measured has not changed" [66,69]. The reliability of the research instrument was ascertained through pre-testing to crosscheck the consistency and accuracy of the questions and answers obtained. A Cronbach alpha coefficient test was conducted to establish the reliability of the variables. The four (4) variables, along with their respective Cronbach alpha scores are summarized in Appendix A, Table A1. According to Cronbach [70], if Alpha coefficient values are above 0.7, then the variables are considered satisfactory for the research.

3.4. Data Collection and Analysis

The study used structured questionnaires to gather quantitative data from registered MM users, registered MM agents, and qualitative data from MNO IT officers. The questionnaires were designed and divided into four parts. The first part covered demographic information; the second part covered mobile money services; the third part contained questions regarding the opinions of the respondents on the security issues associated with mobile money systems in Uganda; and, the last part had suggestions on different ways or measures to mitigate the security challenges associated with mobile money systems. The questionnaires contained direct questions of yes/no, multiple choice items, and five-point Likert scale. Questionnaires were pretested with ten registered MM users, six registered MM agents, and four MNO IT officers in Uganda. Some questions were reviewed based on the responses from the pilot test.

Evidence-based questionnaires were used in this study to obtain quantitative information to serve the research questions: (a) What are the key security issues associated with mobile money systems in Uganda?; (b) What is the relationship between demographic variables (like gender, age, education level, duration of mobile money usage, mobile money transactions in a month) and the mobile money systems' security challenges?; (c) What are the different ways or measures to mitigate the security challenges associated with mobile money systems?

Out of 1614 administered questionnaires, 1240 (76.8%) fully completed questionnaires were returned, of which 741 (59.8%) were filled by registered MM users, 447 (36.0%) by registered MM agents, and 52 (4.2%) by MNO IT officers respectively, with a response rate of 76.8%.

The collected data were analyzed using RStudio software. Statistical techniques like descriptive analysis (percentages, means, and standard deviations), graph, and Pearson Chi-Square tests were used in the data analysis. For a five-point Likert scale data, results for the means (M) > 3.0 and p-value < 0.05 were considered statistically significant [71,72].

4. Results

4.1. Respondents' Social Demography Characteristics

From Table 1, the respondents' gender, age, marital status, and level of education were analyzed.

Table 1. Respondents' social demography characteristic i.e., gender, age, marital status, and level of education.

No	Variable	MM Users No. (%)	MM Agents No. (%)	MNO IT Officers No. (%)
1	**Gender**			
	Male	422 (57.0%)	244 (54.6%)	29 (55.8%)
	Female	319 (43.0%)	203 (45.4%)	23 (44.2%)
2	**Age**			
	Less than 18 years	44 (5.9%)	22 (4.9%)	0 (0.0%)
	Between 18–30 years	497 (67.1%)	330 (73.8%)	46 (88.5%)
	Between 31–50 years	175 (23.6%)	90 (20.1%)	5 (9.6%)
	More than 50 Years	25 (3.4%)	5 (1.1%)	1 (1.9%)
3	**Marital Status**			
	Single	534 (72.1%)	290 (64.9%)	35 (67.3%)
	Married	184 (24.8%)	137 (30.6%)	16 (30.8%)
	Divorced	16 (2.2%)	14 (3.1%)	1 (1.9%)
	Widowed	7 (0.9%)	6 (1.3%)	0 (0.0%)
4	**Level of Education**			
	Primary School	27 (3.6%)	14 (3.1%)	0 (0.0%)
	Ordinary Level	77 (10.4%)	59 (13.2%)	0 (0.0%)
	Advanced Level	179 (24.2%)	113 (25.3%)	3 (5.8%)
	Certificate	37 (5.0%)	60 (13.4%)	4 (7.7%)
	Diploma	75 (10.1%)	43 (9.6%)	4 (7.7%)
	Bachelors	260 (35.1%)	151 (33.8%)	37 (71.2%)
	Masters	70 (9.4%)	7 (1.6%)	4 (7.7%)
	PhD	16 (2.2%)	0 (0.0%)	0 (0.0%)

No—Numbers, **MM**—Mobile Money, **MNO**—Mobile Network Operator, **IT**—Information Technology, **PhD**—Doctor of Philosophy.

4.1.1. Mobile Money Service Characteristic

Table 2 depicts the distributions of the responses of the respondents regarding mobile money service characteristic, i.e., mobile money service providers, the duration of mobile money service usage, access to mobile money services, and mobile money transactions in a month. This was aimed at determining whether they contribute to mobile money security issues.

Table 2. Respondents' mobile money service characteristic, i.e., mobile money service providers, duration of mobile money service usage, access to mobile money services, and mobile money transactions in a month.

No	Variable	MM Users No. (%)	MM Agents No. (%)	MNO IT Officers No. (%)
	Mobile Money Service Providers			
1	MTN Mobile Money	480 (45.1%)	390 (45.3%)	29 (46.8%)
	Airtel Money	540 (50.7%)	361 (41.9%)	27 (43.5%)
	Africell Money	23 (2.2%)	62 (7.2%)	3 (4.8%)
	M-Sente	9 (0.8%)	7 (0.8%)	2 (3.2%)
	Ezeey Money	4 (0.4%)	28 (3.3%)	1 (1.6%)
	M-Cash	4 (0.4%)	8 (0.9%)	0 (0.0%)
	Others	5 (0.5%)	5 (0.6%)	0 (0.0%)
	Duration of Mobile Money Service Usage			
2	Less than 1 year	66 (8.9%)	66 (14.8%)	5 (9.6%)
	Between 1–5 years	349 (47.1%)	228 (51.0%)	37 (71.2%)
	Between 6–10 years	237 (32.0%)	133 (29.8%)	8 (15.4%)
	More than 10 years	89 (12.0%)	20 (4.5%)	2 (3.8%)
	Access to Mobile Money Services			
3	By dialing USSD code	718 (89.8%)	431 (87.6%)	51 (72.9%)
	Through downloaded apps	76 (9.5%)	50 (10.2%)	19 (27.1%)
	Through a mobile phone web browser	6 (0.8%)	11 (2.2%)	0 (0.0%)
	Mobile Money Transactions in a Month			
4	Not at all	13 (1.8%)	2 (0.4%)	0 (0.0%)
	1–5	209 (28.2%)	31 (6.9%)	4 (7.7%)
	6–10	159 (21.5%)	41 (9.2%)	5 (9.6%)
	11–15	74 (10.0%)	27 (6.0%)	2 (3.8%)
	16–20	115 (15.5%)	43 (9.6%)	1 (1.9%)
	21 and above	171 (23.1%)	303 (67.8%)	40 (76.9%)

MTN—Mobile Telephone Network, **USSD**—Unstructured Supplementary Service Data.

4.1.2. Services Performed Using Mobile Money

Figure 1 shows the findings on services performed using mobile money. Respondents were asked which services they performed using mobile money and 24.6% of the respondents use mobile money to send and receive the money within Uganda, followed by withdrawing money (21.0%), paying for telecom network services (like airtime, data bundles) (16.5%), paying for utilities (like NWSC, UMEME, DStv) (15.8%), save and borrow money (8.1%), buy goods and services (5.6%), mobile banking (4.8%), international money transfer (2.7%), buy insurance (0.6%), and receive a pension (0.3%).

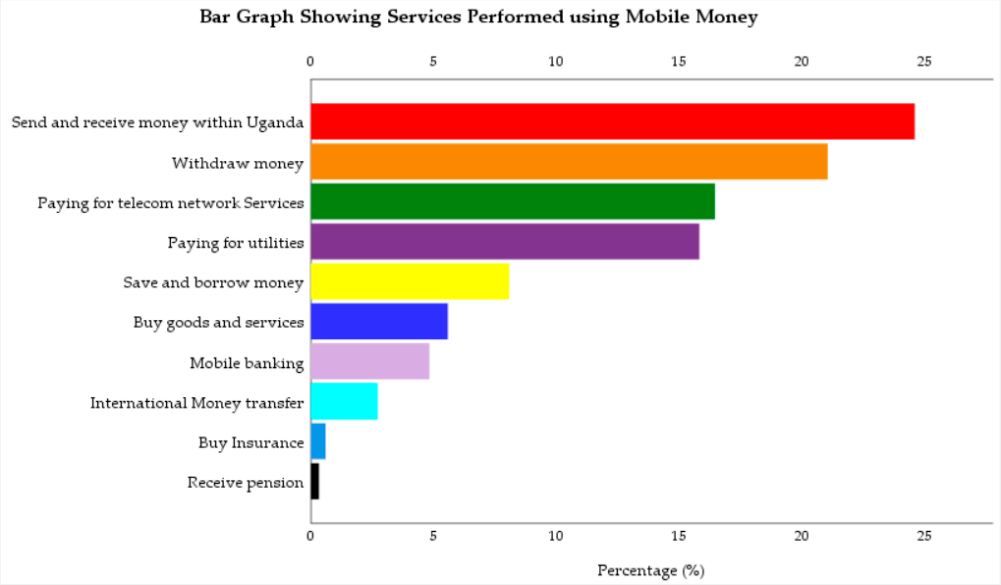

Figure 1. Opinion of respondents regarding the services performed using mobile money services.

4.1.3. Benefits of Using Mobile Money Services

Table 3 shows the responses of the participants according to a 5-point Likert scale concerning the benefits of using mobile money services. Percentages, means (M), standard deviations (Std Dev), and Chi-square tests (χ^2) were computed to assist the research conclusion.

Table 3. Opinion of respondents regarding the benefits of using mobile money services.

No	Benefits of Using Mobile Money Services	SD	D	U	A	SA	Mean	Std Dev	χ^2	Sig. Value
1	It provides a convenient way to send and receive money to anyone who owns a mobile phone or has access to a mobile money agent.	0.4	1.3	2.8	25.1	70.4	4.64	0.643	2229.177	0.000
2	More reliable than physically transporting money.	0.3	1	6.4	30.4	61.9	4.45	0.756	1522.274	0.000
3	Mobile money services save time.	1	1	6.8	34.3	56.9	4.33	0.850	1214.411	0.000
4	Mobile money services are trustworthy.	0.8	3.4	10.1	33.6	52.1	4.09	0.949	761.935	0.000
5	Faster and easier market transactions.	0.6	2.2	11.4	38.1	47.7	4.27	0.841	1050.355	0.000
6	Improves access to financial services for a large number of people.	0.7	1.8	15.9	33.5	48.1	4.30	0.804	1154.847	0.000
7	Reduces the expenses and delays associated with opening, operating, and maintaining bank accounts.	0.8	6.6	16.2	31.9	44.4	4.13	0.964	806.944	0.000
8	Mobile money leads to economic growth and development through increased savings and investments.	1	5.3	18.5	33.5	41.7	3.90	1.059	518.798	0.000
9	It offers many services such as money transfers, mobile payment, mobile banking, and mobile financial services.	1.5	4.8	18.3	37.1	38.4	4.53	0.688	1737.234	0.000
10	Enhances the standard of living for the unbanked population.	2.4	6.9	19.8	34.3	36.5	3.96	1.028	593.250	0.000
11	Increases the banking penetration/untapped market at a low acquisition cost.	2.5	8.9	20.2	33.4	35.1	4.06	0.941	749.960	0.000

SD—Strongly Disagree, **D**—Disagree, **U**—Uncertain, **A**—Agree, and **SA**—Strongly Agree, **M** = Mean, **Std Dev**—Standard Deviation, χ^2—Chi-Square, **Sig. Value**—Significance Value.

The significant majority (70.4%) of the respondents strongly agreed that mobile money provides a convenient way to send and receive money to anyone who owns a mobile phone or has access to a mobile money agent. The mean (M) is 4.64 ($4.64 \geq 4.5$), which strongly agrees that mobile money provides a convenient way to send and receive money to anyone who owns a mobile phone or has access to a mobile money agent while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that mobile money provides

a convenient way to send and receive money to anyone who owns a mobile phone or has access to a mobile money agent, χ^2 (df = 4, N = 1240) = 2229.177, p = 0.000.

It was reported that 61.9% of the respondents strongly agreed that mobile money is more reliable than physically transporting money. The mean (M) is 4.45 (4.45 ≥ 4.0), which agrees with the notion that mobile money is more reliable than physically transporting money while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that mobile money is more reliable than physically transporting money, χ^2 (df = 4, N = 1240) = 1522.274, p = 0.000.

The consensus of 56.9% of the respondents strongly agreed that mobile money services save time. The mean (M) is 4.33 (4.33 ≥ 4.0), which agrees that mobile money services save time while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that mobile money services save time, χ^2 (df = 4, N = 1240) = 1214.411, p = 0.000.

It was reported that 52.1% of the respondents strongly agreed that mobile money services are trustworthy. The mean (M) is 4.09 (4.09 ≥ 4.0), which agrees that mobile money services are trustworthy while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that mobile money services are trustworthy, χ^2 (df = 4, N = 1240) = 761.935, p = 0.000.

Besides, 47.7% of the respondents strongly agreed that mobile money services are faster and easier market transactions. The mean (M) is 4.27 (4.27 ≥ 4.0), which agrees that mobile money services are faster and easier market transactions while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that mobile money services are faster and easier market transactions, χ^2 (df = 4, N = 1240) = 1050.355, p = 0.000.

It was reported that 48.1% of the respondents strongly agreed that mobile money services improve access to financial services for a large number of people. The mean (M) is 4.30 (4.30 ≥ 4.0), which agrees that mobile money services improve access to financial services for a large number of people while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that mobile money services improve access to financial services for a large number of people, χ^2 (df = 4, N = 1240) = 1154.847, p = 0.000.

A similar majority (44.4%) of the respondents strongly agreed that mobile money services reduce the expenses and delays associated with opening, operating, and maintaining bank accounts. The mean (M) is 4.13 (4.13 ≥ 4.0), which agrees with the notion that mobile money services reduce the expenses and delays associated with opening, operating, and maintaining bank accounts while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that mobile money services reduce the expenses and delays associated with opening, operating, and maintaining bank accounts, χ^2 (df = 4, N = 1240) = 806.944, p = 0.000.

It was reported that 41.7% of the respondents strongly agreed that mobile money services lead to economic growth and development through increased savings and investments. The mean (M) is 3.90 (3.90 ≥ 3.5), which agrees with the notion that mobile money services lead to economic growth and development through increased savings and investments while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that mobile money services lead to economic growth and development through increased savings and investments, χ^2 (df = 4, N = 1240) = 518.798, p = 0.000.

Still, 38.4% of the respondents strongly agreed that mobile money services offer many services such as money transfers, mobile payment, mobile banking, and mobile financial services. The mean (M) is 4.53 (4.53 ≥ 4.5), which strongly agrees with the notion that mobile money services offer many services such as money transfers, mobile payment, mobile banking, and mobile financial services while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that mobile money services offer many

services such as money transfers, mobile payment, mobile banking, and mobile financial services, χ^2 (df = 4, N = 1240) = 1737.234, p = 0.000.

It was reported that 36.5% of the respondents strongly agreed that mobile money services enhance the standard of living for the unbanked population. The mean (M) is 3.96 (3.96 ≥ 3.5), which agrees with the notion that mobile money services enhance the standard of living for the unbanked population while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that mobile money services enhance the standard of living for the unbanked population, χ^2 (df = 4, N = 1240) = 593.250, p = 0.000.

The significant majority (35.1%) of the respondents strongly agreed that mobile money services increase banking penetration/untapped market at a low acquisition cost. The mean (M) is 4.06 (4.06 ≥ 4.0), which agrees that mobile money services increase banking penetration/untapped market at a low acquisition cost while the chi-square test was performed with the sig. value of 0.000 which is less than 0.05. This means that it was statistically significant to say that mobile money services increase banking penetration/untapped market at a low acquisition cost, χ^2 (df = 4, N = 1240) = 749.960, p = 0.000.

4.2. Security Issues Associated with Mobile Money Systems

This study mainly focuses on the evaluation of key security issues associated with mobile money systems. Table 4 depicts the opinion of respondents regarding the security issues associated with mobile money systems. Percentages, means (M), standard deviations (Std Dev), and Chi-square tests (χ^2) were computed to assist the research conclusion.

Table 4. Opinion of respondents regarding the security issues associated with mobile money systems.

No.	Security Challenges of Mobile Money Systems	SD	D	U	A	SA	Mean	Std Dev	χ^2	Sig. Value
1	Identity theft	8.7	18.1	9.4	29	34.7	3.63	1.347	334.508	0.000
2	Authentication attack	6.5	18.3	9.6	31	34.5	3.69	1.290	387.661	0.000
3	Phishing attack	14.9	24.1	10.9	19.7	30.4	3.27	1.477	145.145	0.000
4	Vishing attack	6.2	12.7	9.6	21.6	49.8	3.96	1.289	771.298	0.000
5	Smishing attack	14	22.7	14.3	16.9	32.1	3.30	1.467	143.927	0.000
6	PIN sharing	7.6	16.2	10.4	32.4	33.4	3.68	1.291	368.379	0.000
7	Agent-driven fraud	16.6	26	14.1	22.3	21	3.05	1.410	54.524	0.000

SD—Strongly Disagree, **D**—Disagree, **U**—Uncertain, **A**—Agree, and **SA**—Strongly Agree, **M**—Mean, **Std Dev**—Standard Deviation, **χ^2**—Chi-Square, **Sig. Value**—Significance Value.

It was reported that 34.7% of the respondents strongly agreed that identity theft is one of the security challenges of mobile money systems. The mean (M) is 3.63 (3.63 ≥ 3.5), which agrees that identity theft is a key security challenge experienced by the users while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that identity theft is a key security challenge to mobile money systems, χ^2 (df = 4, N = 1240) = 334.508, p = 0.000.

34.5% of the respondents strongly agreed that an authentication attack is a security challenge to mobile money systems. The mean (M) is 3.69 (3.69 ≥ 3.5), which agrees that the authentication attack is a key security challenge experienced by the users while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that the authentication attack is a key security challenge to mobile money systems, χ^2 (df = 4, N = 1240) = 387.661, p = 0.000.

A similar majority (30.4%) of the respondents strongly agreed that a phishing attack is a security challenge to mobile money systems. The mean (M) is 3.27 (3.27 ≥ 3.0), which agrees with the notion that a phishing attack is a key security challenge while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that a phishing attack is a security challenge to mobile money systems, χ^2 (df = 4, N = 1240) = 145.145, p = 0.000.

It was reported that 49.8% of the respondents strongly agreed that a vishing attack is a common security challenge to mobile money systems. The mean (M) is 3.96 (3.96 ≥ 3.5), which agrees with the notion that a vishing attack is a security challenge experienced by the users while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that a vishing attack is a key security challenge to mobile money systems, χ^2 (df = 4, N = 1240) = 771.298, p = 0.000.

The consensus of 32.1% of the respondents strongly agreed that a smishing attack is a security challenge to mobile money systems. The mean (M) is 3.30 (3.30 ≥ 3.0), which agrees that a smishing attack is a key security challenge experienced by the users while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that a smishing attack is a key security challenge to mobile money systems, χ^2 (df = 4, N = 1240) = 143.927, p = 0.000.

Besides, 33.4% of the respondents strongly agreed that PIN sharing is one of the security challenges of mobile money systems. The mean (M) is 3.68 (3.68 ≥ 3.5), which agrees with the notion that PIN sharing is a key security challenge experienced by the users while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that PIN sharing is a key security challenge to mobile money systems, χ^2 (df = 4, N = 1240) = 368.379, p = 0.000.

Lastly, 22.3% of the respondents agreed that agent-driven fraud is a common security challenge to mobile money systems. The mean (M) is 3.05 (3.05 ≥ 3.0), which agrees with the notion that agent-driven fraud is a key security challenge experienced by the users while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that agent-driven fraud is a key security challenge to mobile money systems, χ^2 (df = 4, N = 1240) = 54.524, p = 0.000.

4.3. The Relationship between Demographic Variables (Like Gender, Age, Education Level, Duration of Mobile Money Usage, Mobile Money Transactions in a Month) and Mobile Money Systems' Security Challenges

Hypothesis 1 (H1). *There is no significant relationship between gender and mobile money systems' security challenges.*

From Table 5, a Pearson chi-square test suggests that there is no statistically significant relationship between gender and identity theft (χ^2 (4) = 0.625, p = 0.804), authentication attack (χ^2 (4) = 6.312, p = 0.177), phishing attack (χ^2 (4) = 1.109, p = 0.893), vishing attack (χ^2 (4) = 8.405, p = 0.078), smishing attack (χ^2 (4) = 4.626, p = 0.328), PIN sharing (χ^2 (4) = 1.214, p = 0.876), and agent-driven fraud (χ^2 (4) = 4.383, p = 0.357) because the p-values are greater than 0.05, then we accept the null hypothesis.

Table 5. Relationship between gender and mobile money systems' security challenges.

No	Mobile Money Systems' Security Challenges	df	χ^2	*p*-Value
1	Identity theft	4	1.625	0.804
2	Authentication attack	4	6.312	0.177
3	Phishing attack	4	1.109	0.893
4	Vishing attack	4	8.405	0.078
5	Smishing attack	4	4.626	0.328
6	PIN sharing	4	1.214	0.876
7	Agent-driven fraud	4	4.383	0.357

df—degrees of freedom, χ^2—Chi-Square, ***p*-Value**—calculated probability.

Hypothesis 2 (H2). *There is no significant relationship between age and mobile money systems' security challenges.*

As shown in Table 6, a Pearson chi-square test suggests that there is no statistically significant relationship between age and identity theft (χ^2 (12) = 8.956, p = 0.707), authentication attack

(χ^2 (12) = 20.086, p = 0.065), smishing attack (χ^2 (12) = 20.359, p = 0.061), PIN sharing (χ^2 (12) = 17.476, p = 0.133), agent-driven fraud (χ^2 (12) = 18.766, p = 0.094) because the p-values are greater than 0.05, then we accept the null hypothesis. However, there is a statistically significant relationship between age and phishing attack (χ^2 (12) = 31.544, $p < 0.05$), vishing attack (χ^2 (12) = 41.697, $p < 0.05$) because the p-values are less than 0.05, then we reject the null hypothesis for the two security challenges.

Table 6. Relationship between age and mobile money systems' security challenges.

No	Mobile Money Systems' Security Challenges	df	χ^2	p-Value
1	Identity theft	12	8.956	0.707
2	Authentication attack	12	20.086	0.065
3	Phishing attack	12	31.544	0.002
4	Vishing attack	12	41.697	0.000
5	Smishing attack	12	20.359	0.061
6	PIN sharing	12	17.476	0.133
7	Agent-driven fraud	12	18.766	0.094

Hypothesis 3 (H3). *There is no significant relationship between education level and mobile money systems' security challenges.*

From Table 7, a Pearson chi-square test suggests that there is statistically significant relationship between education level and identity theft (χ^2 (28) = 62.972, $p < 0.05$), phishing attack (χ^2 (28) = 61.796, $p < 0.05$), vishing attack (χ^2 (28) = 56.076, $p < 0.05$), smishing attack (χ^2 (28) = 52.370, $p < 0.05$), PIN sharing (χ^2 (28) = 49.025, $p < 0.05$), agent-driven fraud (χ^2 (28) = 42.564, $p < 0.05$) because the p-values are less than 0.05, then we reject the null hypothesis. However, there is no statistically significant relationship between education level and authentication attack (χ^2 (28) = 40.446, p = 0.060) because the p-values are greater than 0.05, then we accept the null hypothesis for this security challenge.

Table 7. Relationship between education level and mobile money systems' security challenges.

No	Mobile Money Systems' Security Challenges	df	χ^2	p-Value
1	Identity theft	28	62.972	0.000
2	Authentication attack	28	40.446	0.060
3	Phishing attack	28	61.796	0.000
4	Vishing attack	28	56.076	0.001
5	Smishing attack	28	52.370	0.003
6	PIN sharing	28	49.025	0.008
7	Agent-driven fraud	28	42.564	0.038

Hypothesis 4 (H4). *There is no significant relationship between the duration of mobile money usage and mobile money systems' security challenges.*

As shown in Table 8, a Pearson chi-square test suggests that there is statistically significant relationship between duration of mobile money usage and identity theft (χ^2 (12) = 26.785, $p < 0.05$), phishing attack (χ^2 (12) = 24.192, $p < 0.05$), vishing attack (χ^2 (12) = 25.792, $p < 0.05$), smishing attack (χ^2 (12) = 40.608, $p < 0.05$), PIN sharing (χ^2 (12) = 21.734, $p < 0.05$), agent-driven fraud (χ^2 (12) = 38.095, $p < 0.05$) because the p-values are less than 0.05, then we reject the null hypothesis. However, there is no statistically significant relationship between duration of mobile money usage and authentication attack (χ^2 (12) = 12.757, p = 0.387) because the p-values are greater than 0.05, then we accept the null hypothesis for this security challenge.

Table 8. Relationship between mobile money usage duration and mobile money systems' security challenges.

No	Mobile Money Systems' Security Challenges	df	χ^2	*p*-Value
1	Identity theft	12	26.785	0.005
2	Authentication attack	12	12.757	0.387
3	Phishing attack	12	24.192	0.019
4	Vishing attack	12	25.792	0.011
5	Smishing attack	12	40.608	0.000
6	PIN sharing	12	21.734	0.041
7	Agent-driven fraud	12	38.095	0.000

Hypothesis 5 (H5). *There is no significant relationship between the number of mobile money transactions in a month and mobile money systems' security challenges.*

From Table 9, a Pearson chi-square test suggests that there is no statistically significant relationship between number of mobile money transactions in a month and authentication attack (χ^2 (20) = 21.641, p = 0.360), vishing attack (χ^2 (20) = 21.209, p = 0.385), smishing attack (χ^2 (20) = 15.540, p = 0.745), PIN sharing (χ^2 (20) = 29.827, p = 0.073), agent-driven fraud (χ^2 (20) = 25.778, p = 0.173) because the p-values are greater than 0.05, then we accept the null hypothesis. However, there is a statistically significant relationship between the number of mobile money transactions in a month and identity theft (χ^2 (20) = 42.570, $p < 0.05$), phishing attack (χ^2 (20) = 33.884, $p < 0.05$) because the p-values are less than 0.05, then we reject the null hypothesis for these security challenges.

Table 9. Relationship between number of mobile money transactions in a month and mobile money systems' security challenges.

No	Mobile Money Systems' Security Challenges	df	χ^2	*p*-Value
1	Identity theft	20	42.570	0.002
2	Authentication attack	20	21.641	0.360
3	Phishing attack	20	33.884	0.027
4	Vishing attack	20	21.209	0.385
5	Smishing attack	20	15.540	0.745
6	PIN sharing	20	29.827	0.073
7	Agent-driven fraud	20	25.778	0.173

4.4. The Different Ways or Measures to Mitigate the Mobile Money Systems Security Challenges

From Table 10, the responses of the participants regarding the different measures to mitigate the security challenges associated with mobile money systems are presented in the form of percentages, means (M), standard deviations (Std Dev), and Chi-square tests (χ^2) to assist in research conclusion.

There was a significant majority (64.7%) of the respondents who strongly agreed that the use of better access controls like, PIN, one-time password, and Biometric fingerprint altogether is a high priority. The mean (M) is 4.41 (4.41 ≥ 4.0), which agrees with the notion that the use of better access controls can mitigate mobile money systems' security challenges while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that the use of better access controls is a priority in mitigating mobile money systems' security challenges, χ^2 (df = 4, N = 1240) = 1698.427, p = 0.000.

It was reported that 60.9% of the respondents strongly agreed that customer awareness campaigns to increase customer education and protection is a high priority. The mean (M) is 4.47 (4.47 ≥ 4.5), which strongly agrees with the notion that customer awareness campaigns to increase customer education and protection is a high priority while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that customer

awareness campaigns to increase customer education and protection is a high priority in mitigating mobile money systems' security challenges, χ^2 (df = 4, N = 1240) = 1603.621, p = 0.000.

Table 10. Opinion of respondents regarding the different ways or measures to mitigate the security challenges of mobile money systems.

No	Measures to Mitigate the Security Challenges Associated with Mobile Money Systems	NP	LP	U	MP	HP	Mean	Std Dev	χ^2	Sig. Value
1	Use of better access controls like PIN, One-time password, and Biometric fingerprint altogether.	2.7	5.2	5.1	22.3	64.7	4.41	0.994	1698.427	0.000
2	Customer awareness campaigns to increase customer education and protection.	0.8	1.8	8.1	28.5	60.9	4.47	0.784	1603.621	0.000
3	Agent training on acceptable practices.	1	3	10.5	25.1	60.4	4.41	0.870	1486.452	0.000
4	Comprehensive legal document to guide mobile money service.	1.5	5.3	13.6	28.5	51	4.22	0.970	1015.024	0.000
5	Strict measures against fraudsters.	1.2	3.7	9.5	17	68.5	4.48	0.899	1918.411	0.000
6	Know Your Customer (KYC) Controls.	1.9	4.7	14.9	29	49.4	4.19	0.984	951.669	0.000
7	Mobile users should report any security incidence/fraud to the regulators and security agencies.	0.8	2.9	8.2	23.6	64.4	4.48	0.828	1727.944	0.000
8	High-Value transaction monitoring from the service providers	2.3	2.9	11.3	26.9	56.5	4.32	0.949	1278.927	0.000
9	The government and mobile money service providers should publish any reported incidences.	2.1	5	10.2	27.7	54.9	4.28	0.980	1190.427	0.000
10	The government and mobile money service providers should come up with a portal where victims can share their incidences anonymously.	3.8	5.7	11.7	28.3	50.5	4.16	1.080	950.935	0.000

NP—Not A Priority, **LP**—Low Priority, **U**—Uncertain, **MP**—Medium Priority, and **HP**—High Priority, **M**—Mean, **Std Dev**—Standard Deviation χ^2—Chi-Square, **Sig. Value**—Significance Value.

Besides, 60.4% of the respondents strongly agreed that agent training on acceptable practices is a higher priority. The mean (M) is 4.41 (4.41 ≥ 4.0), which agrees with notion that agent training on acceptable practices is necessary while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that agent training on acceptable practices is a priority in mitigating the security challenges, χ^2 (df = 4, N = 1240) = 1486.452, p = 0.000.

It was reported that 51.0% of the respondents strongly agreed that a comprehensive legal document to guide mobile money service is a high priority. The mean (M) is 4.22 (4.22 ≥ 4.0), which agrees with the notion that comprehensive legal document to guide mobile money service is necessary for mobile money service providers and the government while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that a comprehensive legal document to guide mobile money service is necessary for successful implementation of mobile money services, χ^2 (df = 4, N = 1240) = 1015.024, p = 0.000.

The consensus of 68.5% of the respondents strongly agreed that strict measures against fraudsters are a high priority. The mean (M) is 4.48 (4.48 ≥ 4.0), which agrees with the notion that strict measures against fraudsters are a priority while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that strict measures against fraudsters are a high priority in mitigating mobile money systems' security challenges, χ^2 (df = 4, N = 1240) = 1918.411, p = 0.000.

It was reported that 49.4% of the respondents strongly agreed that knowing your customer controls during registration is necessary. The mean (M) is 4.19 (4.19 ≥ 4.0), which agrees that knowing and verifying customer credentials during registration is a priority while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that know your customer controls during registration is necessary for mitigating the security challenges, χ^2 (df = 4, N = 1240) = 951.669, p = 0.000.

Furthermore, 64.4% of the respondents strongly agreed that mobile users should report any security incidence/fraud to the regulators and security agencies. The mean (M) is 4.48 (4.48 ≥ 4.0), which agrees with the notion that mobile users reporting any security incidence/fraud to the regulators and security agencies is a priority while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that reporting any security incidence/fraud to the regulators and security agencies by mobile users is necessary for mitigating mobile money systems' security challenges, χ^2 (df = 4, N = 1240) = 1727.944, p = 0.000.

It was reported that 56.5% of the respondents strongly agreed that high-value transaction monitoring from the service providers is a high priority. The mean (M) is 4.32 (4.32 ≥ 4.0), which agrees with the notion that high-value transaction monitoring from the service providers is a must while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that high-value transaction monitoring from the service providers is a priority in mitigating the security challenges, χ^2 (df = 4, N = 1240) = 1278.927, p = 0.000.

A similar majority (54.9%) of the respondents strongly agreed that the government and mobile money service providers should publish any reported incidences. The mean (M) is 4.28 (4.28 ≥ 4.0), which agrees with the notion that the government and mobile money service providers should publish any reported incidences while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that the government and mobile money service providers should publish any reported incidences to mitigate the security challenges, χ^2 (df = 4, N = 1240) = 1190.427, p = 0.000.

Lastly, 50.5% of the respondents strongly agreed that the government and mobile money service providers should come up with a portal where victims can share their incidences anonymously. The mean (M) is 4.16 (4.16 ≥ 4.0) which strongly agrees with the notion that it is a priority for the government and mobile money service providers to come up with a portal where victims can share their incidences anonymously while the chi-square test was performed with the sig. value of 0.000, which is less than 0.05. This means that it was statistically significant to say that the government and mobile money service providers should come up with a portal where victims can share their incidences anonymously to mitigate the security challenges associated with mobile money systems, χ^2 (df = 4, N = 1240) = 950.935, p = 0.000.

5. Discussion

The opinion of MM users, MM agents, and MNO IT officers remain paramount in the implementation of secured mobile money systems. Therefore, the main aim of this study was to evaluate the key security issues associated with mobile money systems in Uganda. The crucial objective of the survey was for MM users, MM agents, and MNO IT officers to identify and evaluate the key security challenges associated with mobile money systems, assess the relationship between demographic variables and mobile money systems' security challenges in Uganda, and suggest mitigation measures for the security challenges to improve the mobile money technology. Before evaluating the key security challenges, there is a need to establish the services and benefits offered by mobile money.

The results in Figure 1 shows some of the services performed using mobile money. They include sending and receiving money within Uganda, withdrawing money; paying for telecom network services (like data bundles, airtime, etc.); paying for utilities (like NWSC, UMEME, DStv); saving and borrowing money; buying goods and services; mobile banking; international money transfer; buying insurance, and receiving a pension. This outcome is consistent with the studies conducted by Lwanga and Adong [17], BoU [1], Afi [18], who identified depositing and withdrawing of money, transfer of money to other users, paying utility bills, paying for goods in a store, saving money for future purchases or payment, receiving a salary, taking a loan, receiving state aid or pension, buying insurance, purchasing airtime and data bundle, and making bank transactions as the services performed using mobile money.

The findings presented in Table 3, mentioned convenient means to transport and receive money to anyone who has a mobile phone or has access to a mobile money agent, improved access to financial services for a large number of people, more reliability than physically transporting money, and that it saves time as some of the benefits of mobile money services. This is in line with the submissions of Kikulwe, Fischer, and Qaim [23], Mugambi, Njunge, and Yang [24], Saxena et al. [27], Marumbwa and Mutsikiwa [30], Kanobe et al. [33], Cisco [35], who identified a convenient way to send money to anyone who owns a mobile phone, enhance access to financial services for a large number of people who are effectively excluded from banks, transfer money through mobile phones without physically visiting the bank, and cut down time lags associated with opening, operating, and maintaining a traditional bank account as some of the benefits. Furthermore, faster and easier market transactions, increased banking penetration, enhanced standard of living for the unbanked population, and economic growth and development are some of the mentioned benefits. These findings conform with the studies of Lonergan et al. [31], Hu et al. [34], who stated that mobile money provides the quickest mechanism for clearing unplanned domestic financial payments, enhances the standard of living for the unbanked population, and stimulates economic development.

From Table 4, respondents identified the following as the security issues associated with mobile money systems:

Identity theft: This is a form of mobile money crime committed by a friend, relative, or a fraudster who steals the owners' financial information such as PIN for performing transactions. According to Bosamia [9], when a customer's mobile phone is stolen, attackers make use of any sensitive data stored in it, including the PIN, and have control over the device. The mobile money PIN stored on the mobile phone will provide them with access to the mobile money account enabling them to carry out fraudulent transactions [45,46]. This is in line with the work of Trulioo [40], Mtaho [7], who noted that identity theft is usually an inside job activity through unscrupulous employees gaining unauthorized access to mobile money data that belongs to the users and then irregularly misappropriating their funds. This is affirmed by Gwahula [37], Buku and Mazer [41], who observed that identity theft results from fraudulent or offline SIM swaps by fraudsters that transfer the mobile wallet account from the customer's SIM to the fraudster's SIM, enabling them to have full access to the user's mobile wallet to carry out fraudulent transactions [42,43].

Authentication attack: This is a mobile money crime where attackers target and try to exploit the mobile money authentication process by an applying brutal-force attack or weak PIN attack. This is in line with the findings of Mtaho [7], Castle et al. [8], Mtaho and Mselle [13], Gwahula [37], Reaves et al. [38], who found out that attackers use many ways to gain access to users' account and take advantage of weak PIN reset procedures, making it easy to guess, smudge, or snoop. This outcome is consistent with the study conducted by Bosamia [9], Akomea-Frimpong et al. [39], who reported that most of the mobile money systems are not properly protected, giving IT fraudsters the ability to apply reverse engineering to attack hardcoded passwords or PINs, encryption keys, and steal customer money.

Phishing attack: This is a form of mobile money crime where fraudsters masquerade as employees of the mobile money service provider by calling or sending SMS messages to mobile money users and agents to reveal their data including a PIN for an update. This is in line with the submissions of Bosamia [9], who also found out that fraudsters carry out sophisticated attacks by sending either email messages, SMSs, or calls to mobile money users to disclose their personal and financial information.

Vishing attack: This is a form of mobile money fraud where fraudsters use voice calls to trick mobile money users and agents into revealing their critical financial information like a PIN. This reaffirms the findings of earlier studies by Saxena et al. [27], Maseno, Ogao, and Matende [48] who observed that attackers use anonymous phone calls or false promotions to trick users into disclosing their PINs or other sensitive personal information that is then used to steal from their mobile money accounts. It was further supported by Kigen et al. [49], who added that vishing is a widely used method of launching

attacks on mobile money platforms in Kenya, where individuals have been tricked to provide sensitive information such as mobile money PINs, which have led to fraudulent transactions.

Smishing attack: This is a form of mobile money fraud where fraudsters send emotional delusional SMS messages to lure mobile money users and agents into revealing their mobile money account information, including the PIN. This finding is described in other earlier studies conducted by Mudiri [42], Maseno, Ogao, and Matende [48], where fraudsters send fake SMS using their mobile phones to mobile money users and mobile money agents, and then take them through various steps, which later result in the transfer of money from their account to the fraudsters' account. It is also consistent with the studies of Akomea-Frimpong et al. [39], Buku and Mazer [41], Gilman and Joyce [44], Lonie [45] who reported that fraudsters impersonating as employees of mobile money service providers send fake SMS messages to customers that they have won a promotion prize, and for them to claim the price they should send money to the fraudster's number.

PIN sharing: Many mobile money users and agents tend to share their mobile money PIN(s) among relatives, friends, which makes their account vulnerable to identity theft, brute-force attack, and authentication attacks. This finding is reported in other earlier studies conducted by Mtaho [7], who observed that most people tend to share their mobile money PIN among friends and families, which has also added more security risks to the platform.

Agent-driven fraud: mobile money agents also experience fraud from both mobile money attackers/fraudsters, employees of the MNO, and users, thus threatening the security of the platform. This result is logical with the work conducted by Buku and Mazer [41], Lonie [45], in which they found that the common acts of fraud that agents experience include float loss in the agent's account resulting from unauthorized use, misuse of PINs, and fraudster impersonating MNO staff to gain unauthorized access to the agent's float account. Buku and Mazer [41] reported that the 2015 surveys of the Helix Institute indicate that fraud was the primary concern of many agents, and found that 53% of mobile money agents in Uganda and 42% in Tanzania had experienced fraud. Uganda recorded the highest rate of fraud and crime rates in the region. Castle et al. [8], Gilman, and Joyce [44] added that customers also commit fraud against agents by giving wrong mobile phone numbers repeatedly to get the agent's PIN.

Tables 5–9 analyzed the relationships between demographic variables (like gender, age, education level, duration of mobile money usage, mobile money transactions in a month) and mobile money systems' security challenges. Respondents observed that:

There is no statistically significant relationship between gender and identity theft, authentication attack, phishing attack, vishing attack, smishing attack, PIN sharing, and agent-driven fraud. There is a statistically significant relationship between age and phishing attack or vishing attack. Furthermore, there is a statistically significant relationship between education level and identity theft, phishing attack, vishing attack, smishing attack, PIN sharing, agent-driven fraud. Besides, there is a statistically significant relationship between duration of mobile money usage and identity theft, phishing attack, vishing attack, smishing attack, PIN sharing, agent-driven fraud. Finally, there is a statistically significant relationship between the number of mobile money transactions in a month and identity theft, phishing attacks.

The findings presented in Table 10 are regarding the different ways and measures to mitigate the security challenges associated with mobile money systems, respondents agreed that:

Use of better access controls such as multi-factor authentication (i.e., PIN, one-time password, and biometric fingerprint). These findings are similar to the studies of Bosamia [9], Gilman and Joyce [44], Lonie [45], who found out that there is a need for control access rights to protect customer information, and that all interactions between servers must be logged, secured, and strongly authenticated using two-factor authentication. Lonie [45] further pointed out that there is a need to enforce high-security standard measures for payment processing systems and encryption should occur at the earliest possible point in the messaging flow where all external messages between customer and partner activities are encrypted.

Customer awareness campaigns to increase customer education and protection. This finding is reported in other earlier studies conducted by Bosamia [9], Gwahula [37], Akomea-Frimpong et al. [39], Mudiri [42], Gilman and Joyce [44], who added that financial education, customer awareness campaigns, security awareness, and risk awareness need to be carried out to increase customer education, protection and encourage their participation in this industry.

Agent training on acceptable practices. It is also consistent with the study of Gilman and Joyce [44], who argued that agent training is needed on acceptable practices, terms, and conditions.

Need for a comprehensive legal document to guide mobile money service. This is in line with the work of Akomea-Frimpong et al. [39], Lonie [45], Alhassan et al. [54], who stated that detailed legal code, internal fraud policy, and an efficient and robust user and security policy should be developed and used by mobile money merchants and partner banks.

Mobile money service providers should monitor high-value transactions. This outcome is consistent with the study conducted by Gilman and Joyce [44], who argued that there is a need for threshold limits to reduce the risk associated with anti-money laundering/combating the financing of terrorism (AML/CFT). Mudiri [42], Gilman, and Joyce [44], further added that monitoring and supervision of mobile money agents are imperative.

Some other measures to mitigate the security challenges of mobile money systems include: taking strict measures against fraudsters; reporting any security incidences or fraud to the regulators and security agencies; publishing any reported incidences by the government and mobile money service providers; the government and mobile money service providers should come up with a portal where victims can share their incidences anonymously.

6. Conclusions

Mobile money systems have come out as the primary payment platform for the digital economy, thus bettering the standard of living of many people who have limited access to the banking infrastructure in developing nations like Uganda. By enabling access to cashless payment infrastructure, these systems allow citizens of developing nations to decrease the physical security risks associated with hard currency transactions. However, the security of most of the mobile money systems remains a big challenge. In this article, the researchers evaluated the security challenges of mobile money systems. They found significant security challenges with the current mobile money systems such as identity theft, authentication attack, phishing attack, vishing attack, SMiShing attack, PIN sharing, and agent-driven fraud. The study also found significant relationships between constructs and mobile money systems' security challenges in Uganda. Several mitigation measures were recommended for successful implementation of secure mobile money systems such as the use of better access controls, customer awareness campaigns, agent training on acceptable practices, developing a comprehensive legal document to run mobile money service, KYC controls, high-value transaction monitoring by the service providers, but to mention a few.

The findings of this study contribute to the theoretical literature in the following ways. First, this paper extends the theoretical knowledge of security challenges in mobile money systems. To our best knowledge, no empirical study has been conducted to evaluate the key security issues associated with mobile money systems in Uganda. Second, our study contributes to the literature by empirically testing the relationship between constructs (gender, age, education level, duration of mobile money usage, and mobile money transactions in a month) and mobile money systems' security challenges. Most of these constructs have never been used in studies focusing on mobile money systems' security challenges. The study also offers useful managerial contributions. Firstly, the study suggests that identifying and improving the security issues and challenges of mobile money systems are an important factor in the implementation of secure mobile money services. Thus, to encourage the successful implementation of secure mobile money systems, MMSPs need to evaluate the current system so that proper mitigation measures can be proposed and implemented to increase service delivery. Secondly, mobile money systems' security challenges are a threat to the implementation of

mobile money services. By assessing the relationship between constructs and mobile money systems' security challenges in Uganda, MNOs can emphasize measures to counter those challenges. Lastly, the study can be useful to the Bank of Uganda concerning financial inclusion, which is important to achieve a sustainable development goal.

This study encountered some limitations that create an opportunity for future research on mobile money systems' security challenges. Firstly, the survey was restricted to only Uganda and the survey data were mainly used for descriptive analysis regarding the key security issues associated with mobile money systems. The study did not investigate the views of other stakeholders, such as banks or other financial institutions and regulatory institutions. Thus, the findings from this study may not fully represent the opinions of all the stakeholders in Uganda. Secondly, the respondents' involvement in answering the questionnaires were primarily voluntary, which might make some bias towards the sample. Thus, future research involving an online survey is encouraged to embrace the views of all the mobile money stakeholders who did not take part in the study. Thirdly, the research is limited to statistical data gathered from the few participants since mobile money security is a complicated issue, and data can only be availed on request and approval. Finally, the data used for empirical analysis were gathered from respondents in Uganda who have characteristics differing from respondents in other parts of the world. Future research could focus on repeating a similar topic in other regions of the world like Kenya, Tanzania, Rwanda, Burundi, Somalia, Nigeria, Ghana, South Africa, Haiti, India, Pakistan, Colombia, Philippines, Mexico, Brazil, and so on. This would help in the evaluation of the validity of the proposed measures across different countries. This study, therefore, provides a baseline survey to help MNO and the government that would wish to implement secure mobile money systems.

Author Contributions: Data curation, G.A.; formal analysis, M.A.D. and A.E.S.; investigation, G.A.; methodology, G.A.; supervision, M.A.D. and A.E.S.; writing—review and editing, G.A., M.A.D., and A.E.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: The authors thanked the participants who sacrificed their time to take part in the survey. The authors would like to extend their appreciation to anonymous reviewers for their valuable remarks, Muni University and NM-AIST for the conducive working and research environment.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Table A1. Reliability Scores for Each Variable.

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 ways or measures to mitigate the mobile money systems security challenges	0.729	10

Source: authors.

References

1. Bank of Uganda (BoU). *Bank of Uganda Annual Report 2017/18*; Bank of Uganda: Kampala, Uganda, 2018; Available online: https://www.bou.or.ug/bou/media/statements/Bank-of-Uganda-releases-Annual-Report-2017-2018.html (accessed on 18 April 2019).
2. Talom, F.S.G.; Tengeh, R.K. The Impact of Mobile Money on the Financial Performance of the SMEs in Douala, Cameroon. *Sustainability* **2019**, *12*, 183. [CrossRef]

3. Global System for Mobile Communications (GSMA). The Mobile Economy Sub-Saharan Africa 2018. 2018. Available online: www.gsma.com/mobilemoney (accessed on 20 July 2018).
4. Thenerve. Coins.ph, GCash, GrabPay, PayMaya: Who's Leading the Mobile Payments War in PH? 2019. Available online: https://www.rappler.com/brandrap/data-stories/225782-mobile-payments-leading-philippines (accessed on 10 May 2019).
5. Baganzi, R.; Lau, A.K. Examining Trust and Risk in Mobile Money Acceptance in Uganda. *Sustainability* **2017**, *9*, 1–22.
6. Hove, L.V.; Dubus, A. M-PESA and Financial Inclusion in Kenya: Of Paying Comes Saving? *Sustainability* **2019**, *11*, 568. [CrossRef]
7. Mtaho, A.B. Improving Mobile Money Security with Two-Factor Authentication. *Int. J. Comput. Appl.* **2015**, *109*, 9–15.
8. Castle, S.; Pervaiz, F.; Weld, G.; Roesner, F.; Anderson, R. Let's talk money: Evaluating the security challenges of mobile money in the developing world. In Proceedings of the 7th Annual Symposium on Computing for Development (ACM DEV'16), New York, NY, USA, 18–20 November 2016; pp. 1–10.
9. Bosamia, M.P. Mobile Wallet Payments Recent Potential Threats and Vulnerabilities with its possible security Measures. In Proceedings of the 2017 International Conference on Soft Computing and its Engineering Applications (icSoftComp-2017), Changa, India, 1–2 December 2017; pp. 1–7.
10. Uganda Communications Commission (UCC). *Telecommunications, Broadcasting and Postal Markets Industry Report Q2 (April–June) 2019*; UCC: Kampala, Uganda, 2019.
11. Bank of Uganda (BoU). *Bank of Uganda (BoU) Annual Report-2018/19*; Bank of Uganda: Kampala, Uganda, 2019.
12. Okeleke, K. *Uganda: Driving Inclusive Socio-Economic Progress through Mobile-Enabled Digital Transformation*; GSMA: London, UK, 2019.
13. Mtaho, A.B.; Mselle, L. Securing Mobile money services in Tanzania: A Case of Vodacom M-Pesa. *Int. J. Comput. Sci. Netw. Solut.* **2014**, *2*, 1–11.
14. United Nations. *Mobile Money for Business Development in the East African Community*; United Nations: Geneva, Switzerland, 2012.
15. Kiconco, R.I.; Rooks, G.; Solano, G.; Matzat, U. A skills perspective on the adoption and use of mobile money services in Uganda. *Inf. Dev.* **2018**, *35*, 724–738. [CrossRef]
16. Kumar, G.R.; Joan, N. Mobile Money: M-Pesa in Uganda. *Intercont. J. Financ. Res. Rev.* **2016**, *4*, 45–65.
17. Lwanga, M.M.; Adong, A. A Pathway to Financial Inclusion: Mobile Money and Individual Savings in Uganda. *Econ. Policy Res. Centre EPRC* **2016**, *127*, 1–32.
18. Alliance for Financial Inclusion (AFI). *Uganda's Journey to Inclusive Finance through Digital Financial Services*; Alliance for Financial Inclusion: Kuala Lumpur, Malaysia, 2019.
19. Nyaga, J.N.; Ogollah, K. Challenges Facing Penetration of New Mobile Money Transfer Services in Nairobi. *IOSR J. Econ. Financ. IOSR-JEF* **2015**, *6*, 2321–5933.
20. Maitai, J.; Omwenga, J. Factors Influencing the Adoption of Mobile Money Transfer Strategy in Telecommunication Industry in Kenya: A Case of Safaricom–Kenya Ltd. *IOSR J. Bus. Manag. IOSR-JBM* **2016**, *18*, 84–94. [CrossRef]
21. Bank of Uganda (BoU). *State of the Industry Report on Mobile Money. Decade Edition: 2006–2016*; Bank of Uganda: Kampala, Uganda, 2017.
22. Ismail, L.; Moya, M.B.; Bwiino, K.; Ismael, K. Examining Determinants of Behavioral Intention in Adoption of Mobile Money Transfer Services in Uganda. *ICTACT J. Manag. Stud.* **2017**, *3*, 433–439. [CrossRef]
23. Kikulwe, E.M.; Fischer, E.; Qaim, M. Mobile money, smallholder farmers, and household welfare in Kenya. *PLoS ONE* **2014**, *9*, e109804. [CrossRef] [PubMed]
24. Mugambi, A.; Njunge, C.; Yang, S.C. Mobile-Money Benefits and Usage: The Case of M-PESA. *IT Prof.* **2014**, *16*, 16–21. [CrossRef]
25. Mwangi, K.K.; Kasamani, B.S. A Universal Mobile Money Transfer Platform. *Int. J. Comput. Appl.* **2017**, *175*, 40–47.
26. Murendo, C.; Wollni, M.; De Brauw, A.; Mugabi, N. Social Network Effects on Mobile Money Adoption in Uganda Social Network Effects on Mobile Money Adoption in Uganda. *J. Dev. Stud.* **2018**, *388*, 1–17.
27. Saxena, S.; Vyas, S.; Kumar, B.S.; Gupta, S. Survey on Online Electronic Payments Security. In Proceedings of the 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, 4–6 February 2019; pp. 746–751.

28. Nyaga, K.M. The Impact of Mobile Money Services on the Performance of Small and Medium Enterprises in an Urban Town in Kenya. Master's Thesis, KCA University, Nairobi, Kenya, 2013.
29. Kyeyune, R.; Mayoka, K.G.; Miiro, E. ICT Infrastructure, Mobile Money Systems and Customer Satisfaction in Uganda. *Int. Sci. Res. J.* **2012**, *1*, 1–8.
30. Marumbwa, J.; Mutsikiwa, M. An Analysis of the Factors Influencing Consumers' Adoption of Mobile Money Transfer Services (MMTs) in Masvingo Urban Zimbabwe. *Br. J. Econ. Manag. Trade* **2013**, *3*, 498–512. [CrossRef]
31. Dharmapalam, J.; Lonergan, N.; Price, K.; Pilorge, P. *Mobile Money: An Overview for Global Telecommunication Operators*; Ernst & Young Global Ltd.: London, UK, 2009; pp. 1–44.
32. Jack, W.; Suri, T. *Mobile Money: The Economics of M-PESA*; NBER Working Paper; Georgetown University: Washington, DC, USA, 2011.
33. Kanobe, F.; Alexander, P.M.; Bwalya, K.J. Policies, Regulations and Procedures and Their Effects on Mobile Money Systems in Uganda. *Electron. J. Inf. Syst. Dev. Ctries.* **2017**, *83*, 1–15. [CrossRef]
34. Hu, X.; Li, W.; Hu, Q.; Hu, X. Are Mobile Payment and Banking the Killer Apps for Mobile Commerce? In Proceedings of the 41st Hawaii International Conference on System Sciences, Waikoloa, HI, USA, 7–10 January 2008.
35. CISCO. *MTN Mobile Money Services*; CISCO: San Jose, CA, USA, 2012; pp. 1–4.
36. Mutong'Wa, S.M.; Khaemba, S.W. A comparative study of critical success factors (csfs) in implementation of mobile money transfer services in Kenya. *Eur. J. Eng. Technol.* **2014**, *2*, 8–31.
37. Gwahula, R. Risks and Barriers Associated with Mobile Money Transactions in Tanzania. *Bus. Manag. Strategy* **2016**, *7*, 121–139.
38. Reaves, B.; Bowers, J.; Scaife, N.; Bates, A.; Bhartiya, A.; Traynor, P.; Butler, K.R.B. Mo(bile) money, mo(bile) problems: Analysis of branchless banking applications. *ACM Trans. Priv. Secur.* **2017**, *20*, 1–31. [CrossRef]
39. Akomea-Frimpong, I.; Andoh, C.; Akomea-Frimpong, A.; Dwomoh-Okudzeto, Y. Control of Fraud on Mobile money services in Ghana: An exploratory study. *J. Money Laund. Control* **2018**, *22*, 300–317. [CrossRef]
40. Trulioo. Emerging Fraud Risk in the Mobile Wallet Ecosystem. 2015. Available online: https://www.trulioo.com/blog/emerging-fraud-risk-in-the-mobile-wallet-ecosystem/ (accessed on 23 May 2019).
41. Buku, M.; Mazer, R. Fraud in Mobile Financial Services: Protecting Consumers, Providers, and the System. 2017. Available online: http://www.cgap.org/publications/fraud-mobile-financial-services (accessed on 18 December 2019).
42. Mudiri, L.J. Fraud in Mobile Financial Services. 2013. Available online: http://www.microsave.net/files/pdf/RP151_Fraud_in_Mobile_Financial_Services_JMudiri.pdf (accessed on 18 April 2019).
43. Taban, H.; Anael, S.E. Assessment of vulnerabilities of the biometric template protection mechanism. *Int. J. Adv. Technol. Eng. Explor.* **2018**, *5*, 243–254.
44. Gilman, L.; Joyce, M. Managing the Risk of Fraud in Mobile Money. 2012. Available online: http://www.gsma.com/mmu (accessed on 18 January 2020).
45. Lonie, S. Fraud Risk Management for Mobile Money: An Overview. 2017. Available online: https://www.chyp.com/wp-content/uploads/2018/06/Fraud-Risk-Management-for-MM-31.07.2017.pdf (accessed on 25 October 2019).
46. Nyamtiga, B.W.; Anael, S.; Loserian, L.S. Enhanced Security Model for Mobile Banking Systems in Tanzania. *Int. J. Technol. Enhanc. Emerg. Eng. Res.* **2013**, *1*, 4–19.
47. Phipps, R.; Mare, S.; Ney, P.; Webster, J.; Heimerl, K. ThinSIM-based Attacks on Mobile Money Systems. In Proceedings of the COMPASS '18: ACM SIGCAS Conference on Computing and Sustainable Societies (COMPASS), New York, NY, USA, 20–22 June 2018; pp. 1–11.
48. Maseno, E.M.; Ogao, P.; Matende, S. Vishing Attacks on Mobile Platform in Nairobi County Kenya. *Int. J. Adv. Res. Comput. Sci. Technol.* **2017**, *5*, 73–77.
49. Kigen, P.M.; Kimani, C.; Mwangi, M.; Shiyayo, B.; Ndegwa, D.; Kaimba, B.; Shitanda, S. *Kenya Cyber Security Report 2015*; Serianu Ltd.: Nairobi, Kenya, 2015.
50. Kisekka, J.I. MTN Uganda Issues a Statement on Mobile Money Fraudulent Withdrawals. 2019. Available online: https://www.dignited.com/45203/mtn-statement-mobile-money-fraud-withdrawals/ (accessed on 10 June 2019).
51. Taban, H.; Luhanga, E.T.; Anael, S.E. Evaluation of Users' Knowledge and Concerns of Biometric Passport Systems. *Data* **2019**, *4*, 58.

52. Mahajan, R.; Saran, J.; Rajagopalan, A. *Mitigating Emerging Fraud Risks in the Mobile Money Industry*; Deloitte: Mumbai, India, 2015.
53. Balasubramanian, S. Study of Cybercrime in Banking and Financial Sectors. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.* **2018**, *3*, 1205–1212.
54. Alhassan, N.S.; Yusuf, M.O.; Karmanje, A.R.; Alam, M. Salami Attacks and their Mitigation—An Overview. In Proceedings of the 2018 5th International Conference on Computing for Sustainable Global Development, New Delhi, India, 14–16 March 2018; pp. 4639–4642.
55. Paik, M. Stragglers of the herd get eaten: Security concerns for GSM mobile banking applications. In Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications, New York, NY, USA, 22–23 February 2010.
56. Musuva-Kigen, P.; Ekpeke, M.; Inkoom, E.; Inkoom, B.; Masesa, D.; Kaimba, B.; Mbae, K. *Kenya Cyber Security Report 2016*; Serianu Ltd.: Nairobi, Kenya, 2016.
57. Morawczynski, O. Fraud in Uganda: How Millions Were Lost to Internal Collusion. 2015. Available online: https://www.cgap.org/blog/fraud-uganda-how-millions-were-lost-internal-collusion (accessed on 10 June 2019).
58. McKee, K.; Kaffenberger, M.; Zimmerman, J. Doing Digital Finance Right: The Case for Stronger Mitigation of Customer Risks. 2015. Available online: https://www.cgap.org/sites/default/files/researches/documents/Focus-Note-Doing-Digital-Finance-Right-Jun-2015.pdf (accessed on 10 January 2020).
59. Mudiri, J.L. *Fraud in Mobile Financial Services*; MicroSave: New Delhi, India, 2012.
60. Lake, A.J. *Risk Management in Mobile Money: Observed Risks and Proposed Mitigants for Mobile Money Operators*; World Bank: Washington, DC, USA, 2013.
61. Chen, K.; Wang, X.; Chen, Y.; Wang, P.; Lee, Y.; Wang, X.; Ma, B.; Wang, A.; Zhang, Y.; Zou, W. Following Devil's Footprints: Cross-Platform Analysis of Potentially Harmful Libraries on Android and iOS. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016; pp. 357–376.
62. Harris, A.; Goodman, S.; Traynor, P. Privacy and Security Concerns Associated with Mobile Money Applications in Africa. *Wash. J. Law Technol. Arts* **2013**, *8*, 246–264.
63. Amin, M.E. *Social Science Research: Conception, Methodology and Analysis*; Makerere University Printery: Kampala, Uganda, 2005.
64. Kothari, C.R. *Research Methodology: Methods and Techniques*, 2nd ed.; New Age International Publishers: New Delhi, India, 2004.
65. Krejcie, R.V.; Morgan, D.W. Determining Sample Size for Research Activities. *Educ. Psychol. Meas.* **1970**, *30*, 607–610. [CrossRef]
66. Sekaran, U.; Bougie, R. *Research Methods for Business: A Skill-Building Approach*, 5th ed.; John Wiley and Sons Inc.: Hoboken, NJ, USA, 2009.
67. Shadish, W.R.; Cook, T.; Campbell, D.T. *Experimental and Quasi-Experimental Designs for Generalized Causal Inference*; Houghton Mifflin: Boston, MA, USA, 2002.
68. Polit, D.F.; Beck, C.T. *Nursing Research: Principles and Methods*, 7th ed.; Lippincott Williams & Wilkins: Philadelphia, PA, USA, 2003.
69. Leedy, P.; Ormrod, J. *Practical Research: Planning and Design*; Prentice-Hall, Inc.: Upper Saddle River, NJ, USA, 2001.
70. Cronbach, L.J. Coefficient alpha and the internal structure of tests. *Psychometrika* **1951**, *16*, 297–334. [CrossRef]
71. Morgan, G.A.; Leech, N.L.; Gloeckner, G.W.; Barrett, K.C. *IBM SPSS for Introductory Statistics: Use and Interpretation*, 5th ed.; Routledge: New York, NY, USA, 2013.
72. Landau, S.; Everitt, B.S. *A Handbook of Statistical Analyses Using SPSS*; Chapman & Hall/CRC Press LLC: Boca Raton, FL, USA, 2004.