2019-04-29

Evaluation of Users' Knowledge and Concerns of Biometric Passport Systems

Habibu, Taban

MDPI

https://doi.org/10.3390/data4020058

data

MDPI

Article

Evaluation of Users' Knowledge and Concerns of Biometric Passport Systems

Taban Habibu [1,*], Edith Talina Luhanga [1] and Anael Elikana Sam [2]

[1] Department of Applied Mathematics and Computational Sciences (AMCS), Nelson Mandela African Institution of Science and Technology (NM-AIST), 447 Arusha, Tanzania; edith.luhanga@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: sultannubi@gmail.com; Tel.: +255-684765277

Received: 21 March 2019; Accepted: 23 April 2019; Published: 29 April 2019

Abstract: The increase in terrorism and identity fraud has forced governments worldwide to make a combined effort to enhance the security of national borders. Biometric passports are the emergent identity travel document deployed in guaranteeing the safekeeping of the entry point of the border and limiting the usage of counterfeit documents. This study analyzes users' concerns and threats to the biometric passport delivery system in Uganda, where the first biometric passports are planned for rollout in 2019. We used a mixed approach to compute and articulate the results. Factors impacting fear of technology like disclosure of personal data, improper data transmission, and data abuse were determined. Relevance knowledge of preferred technology such as the personal experience of the technology, data privacy awareness and perceived usefulness was confirmed. Threats and attacks on the technology such as counterfeit and brute-force were identified. It is important for policymakers and security expertise to understand that biometric technologies evoke fears of privacy and public liberties infringements. Therefore, end user's acceptance of biometric passports will be dependent on the degree of trust in the technology itself and in those operating the applications.

Keywords: biometric passport; technology trust; end-user; threats

1. Introduction

A biometric passport is a digitized document incorporating security features to authenticate the identity of the passport holder. The passports are aimed at strengthening border protection, enhancing privacy protection against identity theft and fraud, and securing the verification of the documents' bearer [1]. Many European countries have operationalized the infrastructure for the issuance of the new biometric passports. The International Civil Aviation Organization (ICAO) is responsible for specifying the requirements and regulations that the biometric passports should adhere to [2]. The requirements include the type of the biometric (facial image, fingerprint scan, iris image among others), the technologies to be used (Radio Frequency Identification (RFID), i.e. RFID tags) and the Public Key Infrastructure (PKI). The biometric and PKI are capable of decreasing deception and improving protection in international digital identification [3].

The East African Community (EAC) Heads of State summit in March 2016 instructed the rollout of biometric passport in all the member states (Burundi, Kenya, Rwanda, South Sudan, Tanzania, and Uganda) with each member having a 1-year phase-out of the existing national and community passports and adopting biometric passports in their place [4]. In Uganda, the rollout of the biometric passport was planned to begin in January 2019.

Despite the motivating progress in acquiring infrastructure for allowing the issuance of a biometric passport, this initiative can help facilitate faster clearance at the immigration border, guard against

multiple passport issuance as well as protect against identity theft [4]. However, users' concerns and fears, for example on disclosure of personal data and data abuse (misuse), remains a big research question. This is because a limited number of studies have explained biometric technology from the user concerns and acceptance perspective [5]. One such study found that most of the users feel worried, doubtful, or disturbance towards this technology since they regard it as a means for likely encroachments into their privacy. Understanding these users concerns as well as threats and attacks of technology is important. Individuals' feelings and opinions may increase the risk of refusal and leads to biometrics application disappointment [6,7]. A study aiming to identify users' distress and the knowledge gap of the biometric passport such as disclosure of personal data, improper data transmission, data abuse, as well as counterfeit and brute-force attack, is also likely to be a prerequisite for the development of a strategy to support the acceptance of such a ubiquitous novelty.

This study, therefore, addresses the following research questions:

- How is people's information handled during the passport issuance process?
- What are the possible security risks of the Ugandan biometric passport?
- What are people's fears and concerns regarding the biometric passport?
- What mechanisms do people suggest being used to secure the biometric data?

In addition to contributing to a more profound understanding of Ugandan users' concerns and knowledge on biometric passport security and information security during the biometric issuance process, we propose a biometric passport application system for users to control the disclosure of information and improper data transmission. The latter is against Ng-Kruelle et al.'s [8] argument which is against the infringement of state control through technologies. However, we believe that for citizens' acceptance of biometric passports regarding the privacy and security dangers they present, it is essential to propose and study alternative biometric passport application systems that either address end-user's concerns or provide an appropriate reward to users. It is safe to say that biometrics is the future of humanoid identification, however, this future will stay uncertain unless there are rigorous methods employed to protect it against any misuse or security occurrences. Therefore, the technological inventor needs to design a biometric document that is very difficult to re-produce/copy. Build the system that properly secures the template database and reference libraries in order to create and make the public acceptable of the biometric application as well as build trust in the system itself with those operating the applications.

2. Related Work

Several scholars have expressed a number of security concerns and attacks regarding the usage of biometric passports [9]. For instance, biometric passports should prevent known attacks to secure user recognition as well as sensitive information in the database. The fundamental threat experienced is the unauthorized skimming or eavesdropping of the stored information in the passport, resulting in identity theft. In this section, various threats and attacks at hardware and software levels such as eavesdropping, skimming, cloning, brute-force attack, among others are discussed.

2.1. Biometric Passport Known Attacks and Mitigation Strategies

2.1.1. Eavesdropping

This is where an attacker clandestinely listens to the communiqué link and interrupts the information by using an illegitimate RFID reader to steal the data [10]. For example, personal information or cryptography information. It has been stated that from 2 meters' away, an attacker can spy on the message path of the RFID cards. Various mitigation strategies exist to address eavesdropping attacks on biometric passports. The use of Basic Access Control (BAC) for example requires the reader to provide a key, which is obtained from the Machine-Readable Zone (MRZ) of the passport. Without knowing the key, an attacker cannot easily eavesdrop on transmitted information. Another measure is

the use of metallic materials to block Radio Frequency (RF) waves, meaning the passport must be open for an eavesdropper to gain access to the data.

2.1.2. Forging

A passport can be forged by replacing its complete chip with a different one. First, the chip is replaced with duplicated Logical Data Structure (LDS). The duplicated passport matches with the data content of the biometric passport. Second, an attacker can tamper with the LDS to create a new modified copy of credentials on the chip. Such a modified chip is fixed into a passport from which the original chip had been removed. The mitigation strategy is to build a hardware mechanism integrated with a secure chip to protect the LDS against data alteration.

2.1.3. Skimming

Skimming is where an attacker remotely reads the information of the biometric traits in the MRZ without the user's consent or notice. An invader can use an electronic storage device or unlawful reader to scan the data or unprotected contents of the biometric passport's LDS [10]. The skimmer collects sensitive traveler details such as name, age, address, among others. Of which, it modifies the data content by a far distance greater than the designed one. The data can be recovered by grinning power at the passport inside a few distances. However, if the reader newscasts the signal with high power, the time can be extended. Indeed, skimming is technologically hard to perform but gathering information from a lawful contact such as a hotel reception desk or in a tax-free shop is much easier because a passport is proof by itself. A mitigation strategy is to build a hardware device that detects, monitors, inspects and checks out the location of the card reader.

2.1.4. Cloning

Cloning is a replication or reproducing information of a chip in the MRZ from the passport owner to an alternative chip without the knowledge of the holder. This process possesses a threat of information leakage to the chip [11]. An attacker can manipulate the chip information nearby and compromise the confidentiality of the MRZ data to create a fake LDS, because the outcome of the faked data will not be recognized as the counterfeit. Cloning requires sophisticated machinery and thus requires attackers who have the money to invest in such technology. For instance, the Israeli top-secret amenity Mossad cloned 1000 British biometric passports and the airline employee working for Mossad copied the biometric passport of Britons travelling to Israel. Therefore, biometric data leakage and alteration are possible by an imposter [10]. Personal backup software is required to protect the information on the biometric chip as well as to recover the data leakage with an exact replica of the system disk or the selected partition.

2.1.5. Man-in-the-Middle Attack

In a man-in-the-middle attack, an invader (adversary) participates in the communication between RFID readers and the biometric passport chip by intercepting most of the transferred messages, so that the whole communication process is familiar to the attacker. The invader listens to the verification of another chip and forwards the same communication to the reader acting like the genuine chip, and they can alter the communication to paralyze the message route which results in denial-of-service. To prevent the attack, there is need for forceful joint authentication composed with a complex computation process, because the attacks are hard to defend even with encryption [12]. A server need not to convey any parameter(s) in a controllable form.

2.1.6. Brute-Force Attack

A brute-force attack is one where the MRZ information (passport number, birth date, and expiry date) can be used by invaders to guess and compute the access key. The expiry data is useful for giving

the attacker a timeframe during which the attack should be accomplished. For instance, a passport with 10 years until the expiry date gives the attacker roughly 10 years to manipulate and guess the access key. Human error or bribing can also contribute to this weakness. The social engineering directly attacks the software, or blackmails or intimidates an insider who works for the passport-issuing authorities can also support the circumvention of the biometric security features [10], and are also considered forms of brute-force attack. To prevent the unauthorized reading of biometric permits via brute-force attack, one could add radio-frequency blocking material to the cover as well as secure access control like passport regulator at an airfield [13].

2.2. End User Concerns on Biometric Passport

A biometric passport has the potential to provide the security of national borders and other government organizations with increased control over individuals, thus threatening personal rights and civil liberties [14]. Privacy concerns are a significant consideration in fruitful biometric application and uptake between end users. If personal information is collected or accessed without authorization by the owner or the organization dealing with information, it can result in counterfeit of that individual information and fraudster. This would mean mistrust of the technology and noncompliance by the end-users [15], because threats to data secrecy and safety of information demand the building of trust amongst end users and government to ensure fruitful adoption levels of e-services [16]. Therefore, trust must be developed in e-services to alleviate fears that data gathered for one reason is not used for other purposes without prior authorization from the individual. One possible stratagem to form trust is to offer the end users the capability to have some control over the data kept during e-government transactions and to identify who or which government department can access it [15]. An important development in this regard is the progression of international data protection laws and guidelines that oversee the use, gathering, and storage of end user's information.

2.3. Biometric Passport Authentication Mechanism

The International Civil Aviation Organization (ICAO) [17] suggested two different approaches to validate secure chips embedded in the biometric passport: Active and Passive authentication. In active authentication, the secure regulator processes cryptographic data in the chip, while in passive authentication, only reading of the information on a tamperproof chip by a verification device is done. Therefore, passive authentication is applied to secure memory devices, while active authentication requires a processor [18].

2.3.1. Passive Authentication (PA)

The PA is aimed at detecting and averting any attempt to interfere with the pertinent information on the chip, or to counterfeit the chip inside the biometric passport. The inspection system confirms the country's security issuing data using public keys. If the autograph matches, a hash of each data group is confirmed. The credentials of a document signer can be distributed to a visited country. Classically, a visited country arrives into a contract with the issuing country to acquire the permit and dispense it at different entry checkpoints. The legitimacy of the permit is checked before the signature. This is done by checking the Certificate Revocation List (CRL) for any upkeep. The revocation lists are frequently updated in a secure but mutually agreed storage area such as a Public Key Directory (PKD).

Strengths of PA: The security of the biometric passport provides a hashing function and signature algorithms. In case an algorithm is obsolete, it can be exchanged to an alternate one. This is because the issued passport cannot be substituted again.

Weaknesses: The passive verification does not thwart the copying of chip data onto another chip. For instance, skimming or unauthorized access to contents stored in the chip. This results in an invalid certificate, because reading a permit from a secure chip to validate and confirm a signature is terrible security practice.

2.3.2. Active Authentication

The AA is aimed at averting chip cloning. It is comparatively trivial to read the chip content, extract all the information and write them to an empty chip without corrupting the autographs. It is performed using a unique cryptographic key pair KPuAA and KPrAA stored in Data Group 15 (DG15) in a secure chip. Typically, an active authentication key pair is generated inside the secure chip; however, many system designers prefer the creation of keys outside the chip to improve personalization speed. The accuracy of an AA key is confirmed by a read-through of the autograph of DG15, which is approved by the passport signer's private key and is recovered from PKD. It can also store MRZ data in a logical data structure (LDS). It detects a fake passport chip as well as a copied one.

Strength: It improves privacy since each access to the passport can be logged in the secure memory of the chip. Hence, it requires no verification devices to be online.

Weaknesses: It detects cloned passport chips which use diversified keys that do not have high entropy. It does not perform any external or terminal authentication, because it assumes all terminals are trustworthy. Thus, it holds no private biometric data.

2.3.3. Extended Access Control (EAC)

The EAC is designed to store the biometric information of the owner, such as fingerprints, face or iris images. The EAC keys are swapped bilaterally amongst the issued and visited nations. The signed certificates are offered to the verification device for reading biometric data stored on the secure chip. It consists of four (4) stages. For instance, the EAC (Mandatory) to secure the passage with diversified keys, the chip authentication (Mandatory) to replace the active authentication, the passive authentication (Primary) to perform ICAO 9303 specifications, and the terminal authentication (Mandatory) to add terminal authentication to mutual authentication. The terminal is not trusted by the passport as well as the passive one.

Security weaknesses: It is not extensively deployed and revocable because it includes the use of card-verifiable certificates, which are different from X.509 and PGP certificates. Any stealing of a verification terminal could endanger the security of all passports using the equivalent public key. It is suggested to use tamper-resistant apparatuses to secure the storage of keys and sensitive data.

3. Materials and Methods

3.1. Study Design

The study aimed at getting an impression of users' concerns and opinions about the knowledge of biometric technology and investigate potential security threats. A survey study was conducted because of its flexibility for online investigations. Written scenario-based questions were presented via questionnaires. The preliminary questionnaire was presented and discussed based on the suggestions received from the expertise, and a modified list of questions was devised, tested and validated through a small-scale field trial (pre-test). The outcomes of the pre-test were used to alter, eliminate and reformulate some questions. A mixed methods technique was employed to compute and articulate the results. The study was confirmed by the ethics review committee.

3.2. Sample Technique

The participants of the study were the individuals who owned travel documents and the issuance officers at the Ugandan immigration offices who currently issue these documents and work on the biometric systems. The stratified random sample was used to draw our target population. The formula $S_z = \sum \left[\left(\frac{N_h}{N} \right) \times P_h \right]$ was used for the sample size [19].

3.3. Data Collection and Analysis

We deployed a questionnaire organized into four parts: The social demographic characteristic of participants, such as the respondent's age, gender, level of education, knowledge of biometric technology, and type of participants. These aspects are among those that served as moderating variables. The second, concerned the factors impacting users' fear of biometric technology; the third, the security threats and challenges of the biometric technology; and lastly, the mitigation mechanisms of biometric data. Open and closed-ended questions were used for this study. The data were computed and analyzed statistically using RStudio and Statistical Package for Social Science (SPSS) version 20.0.

4. Results

4.1. Social Demography Characteristic

Four-hundred-and-seventeen (n = 417) participants took part in the study. Of these, there were 384 documented owners and 33 issuance officers. Seventy-four percent of the respondents were male and 26% were female in case of the document owners; 69.7% and 30.3% were male and female in case of the officers; 65% were generally of older age, above 30; and 35% were amongst the age range of 21–30. The reason for this was to have an idea of the overall populace regarding the usage of the biometric technology. The main respondents came from the university community, who have an educational qualification higher than "Advanced" level in the case of passport owners (BSc, MSc and PhD), and officers at the regional centers in the case of issuance officers. Forty-point-six (40.6%) were students, 37.2% were teaching staff and 22.1% were employees. This was to assess if the participants were mindful and know of the new technology implemented in the biometric passport. No significant differences in participant's characteristics were observed (p-value = 0.002). The broader knowledge of the experience of biometric technology features was analyzed. The purpose was to identify if prior knowledge of the biometric characteristics had an impact on the adoption of the biometric technology. Fort-eight-point-five percent (48.5%) and 53% of the respondents have broad knowledge and experience of a fingerprint, 31.3% and 36% facial image, 9% and 4% Iris, 5% and 3% palm image, and 6.2% and 4% voice. The biometric technology was used at the workplace, nationwide identification and registration authority (NIRA) [20]. Despite broader knowledge and experience by the participants, 69.3% agreed that the biometric technology plays a great role in increasing security in the Information technology (IT) sector; 30.7% disagreed, citing that the biometric technology can be infringed and misused by an imposter. Therefore, there is a need for individual's awareness on the security and privacy of the information they give during the multiple registration in the day-to-day activities. The findings from the analysis were summarized as shown in Table 1.

Table 1. The Social demography characteristics.

Demographic Characteristic (%)		Owner/Officer	Biometric Features	Owners (%)	Issuance (%)
Gender	Male	74%/69.7%	Fingerprint	52.1%	48.5%
	Female	26%/30.3%	Facial	31.3%	36%
Age	21–30	35%	Iris	9%	4%
	30–60	65%	Palm	5%	3%
Professional	Students	40.6%	Voice	6.2%	4%
	Teaching	37.2%			
	Employees	22.2%			
Biometric Technology	Increase Security	69.3%			
	Insecurity	30.7%			

4.1.1. Factors Influencing the Adoption of Biometric Technology

This section establishes a connection between the reasons and feelings of the respondents about the perception of the biometric technology. This helps the investigator to determine the main concerns

behind the usage of the biometric technology as well as educate the scientist in understanding the preference of the general public (See Figure 1). Thirty-point-two percent (30.2%) of the respondents' agreed that the biometric passports help in protecting the individual's information from frauds and crimes such as identity theft. However, 17.4% strongly disagreed with the proclamation pointing that the biometric passport would not help in protecting frauds and crime, because the information could be counterfeited by any imposter. Two-point-four percent (2.4%) were neutral (neither agree nor disagree), although there was a mixed perception of the respondents, those who agreed considered it as a measure against crime and fraud, while those who strongly disagreed said the technology cannot help in preventing fraud and crime against humanity.

Since direct protection from frauds and crimes was not comprehensive enough, participants were questioned about the security provided by the usage of biometric passports. Twenty-eight percent (28%) disagreed. They believed that the technology does not provide any security, because the tools for protection from terrorism were not strong enough arguments to be convincing. However, 37.4% agreed and cited that the biometric passport technology provides strong authentication, prevents identity fraud and controls security at the border passage. Twelve-point-two percent (12.2%) were neutral (neither agree nor disagree). These results revealed that the provision of security innovativeness were the most important factors influencing the adoption of biometric technology.

Additionally, respondents were questioned of the biometric passport usage; 43.5% strongly agreed that the biometric passport is used to recognize and authenticate a traveler at the border control, because it uses an embedded microprocessor chip that contains the owner's biometric information for identification. Eleven-point-two percent (11.2%) strongly disagreed, they believed that using biometrics could hinder the identification process at the airports, since the process takes time to correctly identify the passport holder against his/her identifiers, hence, creating a chance for a terrorist to invade the system. Fifty-six-point-five (56.5%) believed that biometric technology is used as surveillance to constantly monitor crimes against humanity, which can help prevent a terrorist attack. Seven-point-six percent (7.6%) disagreed with the statement. Given the privacy invasion aspect of the biometric technology adoption, 41.2% of the respondents agreed that the usage of the technology could result in the invasion of privacy, because the biometric information is stored in the passports minus the owner's knowledge. Thirty percent (30%) disagreed and 7.4% neither agreed nor disagreed. Therefore, the issuance officers and technology operators should make informed decisions to recommend the adoption of the biometric technology that helps protect and guarantee user's information from fraudsters. The findings from the analysis are presented in Figure 1.

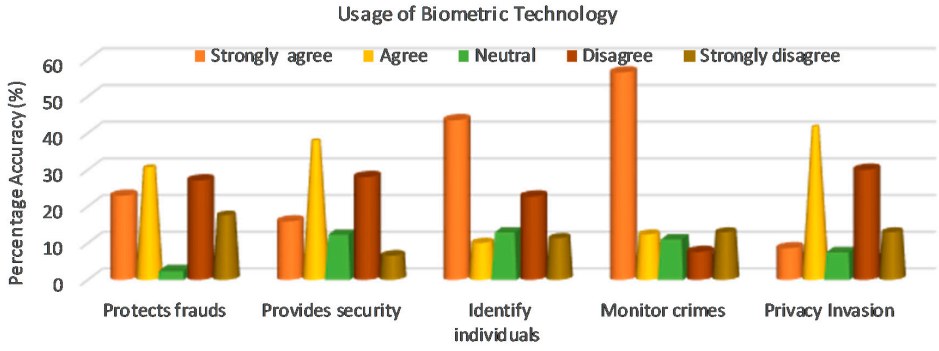


Figure 1. Usage of biometric passport technology.

4.1.2. Biometric Data Privacy

A significant effect of biometric data privacy and security compliance was investigated based on the five-point Likert scale measure, scaling from 'Strongly agree' to 'Strongly Disagree' as shown in Table 2. Data recording was done in the range of 1 to 5. The weighted average and *t*-statistics for the central tendency with *p*-values below 0.05 were computed. Eighty-point-two percent (80.2%) of the respondents showed that individual datum shouldn't be violated without the owners' consent,

because personal data are of great economic value. Therefore, one needs to know whom to share his/her information with and what would happen with his/her information. The *t*-statistics value obtained were 0.000 and had a weighted average of 1.20. Therefore, the respondent's statement was accepted and statistically significant.

Furthermore, 57.8% strongly agreed that personal data must be kept secret, because personal information is confidential and should be protected. People should learn to follow the regulations against their personal information [21]. With any information posted online in a public forum, one cannot assume it's private or safety. Our *t*-value obtained was 0.000 and had a weighted middling of 1.48. Thus, it is statistically significant.

The likely abuses of new technology by criminals were discussed by the participants for justification. Sixty-four-point-eight percent (64.8%) strongly agreed that new technologies would be abused and exploited by criminals, because identity theft, fraud, and terrorism are the real harms. Although biometrics technologies help protect against these attacks, the potential misuse is obvious. Anybody unknown can engage him/herself with strangers and exchange data files. Yet, the greatest number of users do not fully understand the threats and attacks associated with the use of new biometric technology. One should understand that a compromised biometric trait cannot be revoked once stolen. The *t*-statistics value obtained was 0.001 and had a weighted middling 1.51. Therefore, respondents' statements were accepted and statistically significant.

Participants were asked if scanning an individual's biometric data from a template database without authorization was a privacy-infringement; 54.2% strongly agreed with the affirmation, because the infringement of one's confidential secrecy could lead to personal exposer of health issues [21]. It is suggested that transparency and good conduct of the operation and management of the biometric systems strictly be followed based on the appropriate regulations with respect to fundamental ethical principles and civil liberties. The data should be used only for the purpose specified. The *t*-statistics value obtained was 0.002 and had a weighted middling of 2.12. Therefore, the respondents' statements were statistically significant.

In addition, respondents were questioned to determine if database information used for other purposes other than the original aim is a privacy offence; 66.1% strongly agreed and cited the 2016 Uganda election as the greatest fear, because the citizen's biometric fingerprint was extracted from the national identification and registration authority (NIRA) database without owners' consent. Because most of the lawful status of biometric information is unclear, no court has addressed whether the law enforcement should allow collection of biometric data without a person's knowledge. The *t*-value obtained was 0.000 and had a weighted middling of 1.64. Therefore, respondents' statements were statistically significant. We therefore recommend the users to be extra vigilant about their privacy and personal information sharing. They should ensure that the information is encrypted with a strong authentication key before putting them on the online platform. The findings of the analysis are shown in Table 2.

Table 2. Significant effect of biometric passport.

Questions	*SA*	*A*	*N*	*D*	*SD*	*WA*	χ^2 Test
No Privacy violation	80.2	19.8	0	0	0	1.20	0.000
New technologies abuse	64.8	30.2	0	0	5.2	1.51	0.001
Personal data secrecy	57.8	39.1	0	3.1	0	1.48	0.000
Privacy infringe in Database	54.2	19.3	3.4	6.3	16.9	2.12	0.002
Function creep	66.1	24.0	0%	0	9.9	1.64	0.000

Note: *SA* = Strongly agree, *A* = agree, *N* = Neutral, *D* = Disagree, *SD* = strongly disagree. The *t*-value or *p*-value below 0.05 is significant, null hypothesis is rejected while above 0.05 is not significant, null hypothesis is accepted.

4.2. Factors Impacting Users Fear of the Biometric Technology

The study intended to understand the determinants of users' concerns and knowledge on biometric passport technology. We focused our analysis on identifying if those surveyed have been impacted with

fears of the biometric technology (See Figure 2). Thirty-eight-point-eight percent (38.8%) and 24.2% of the participants feared disclosure of personal information, because the biometric information could be used for something else other than its intended purpose. For instance, immigration officers at the airport scan the bodies of the travelers for detection against the threat and need a hard disk and internet connection to store the information, thus odours for function creep. Forty-eight-point-five percent (48.5%) and 30.5% feared improper data transmission, because the specific document of an individual could be revealed which causes the individuals to become more vulnerable to document fraud against the security linkages. Although the travel records outside the workplace may be traced, the files are provided in reaction to a data protection demand. Therefore, the data transmission needs to be monitored using a tracking scheduled and duplicated pertinent documents than issuing the original information.

Additionally, 22.9% and 9.1% showed abuse of information, because a compromised biometric data stored in the database cannot be revoked. For instance, the DNA information could reveal a person's health and exposure to disease. Suggested is a need for everybody to be vigilant on how to safeguard the identity and the storage level of the biometric database. It is safe to say that biometrics is the future of human identification, however, this future would stay uncertain unless rigorous methods are employed to protect it against any misuse or security occurrences.

Nevertheless, 18.2% and 7.8% indicated unauthorized access to individual data, because an unknown user could access the identity credentials of somebody else's information and misuse it without his/her consent. For instance, a recent case of Pharmacy2U being fined £130,000 by the data administrator for vending the clients' details to third parties without consent [22]. This situation raised fear of the citizens' secrecy and several alterations in government lawmaking. The federal government sector, IPP 1, required that personal information collection should be for lawful purposes and by lawful means. Therefore, unless awareness and user's concerns are addressed, they shall still have the fears and trust of the biometric technology acceptance. This study, therefore, helps technology developers understand the significance perception of the end-user's concerns and fears on the adoption of the biometric technology to make informed decisions.

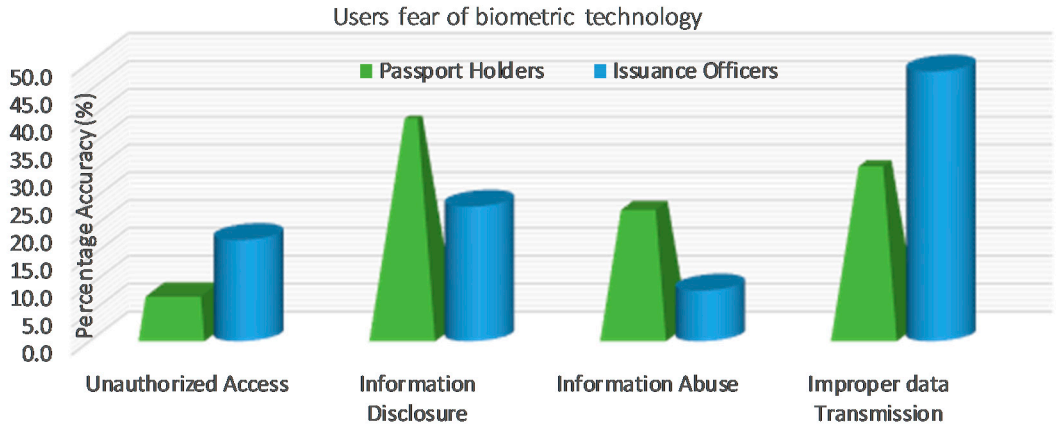


Figure 2. Factors impacting fear of the biometric technology.

4.3. The Security Threats And Challenges of the Biometric Technology

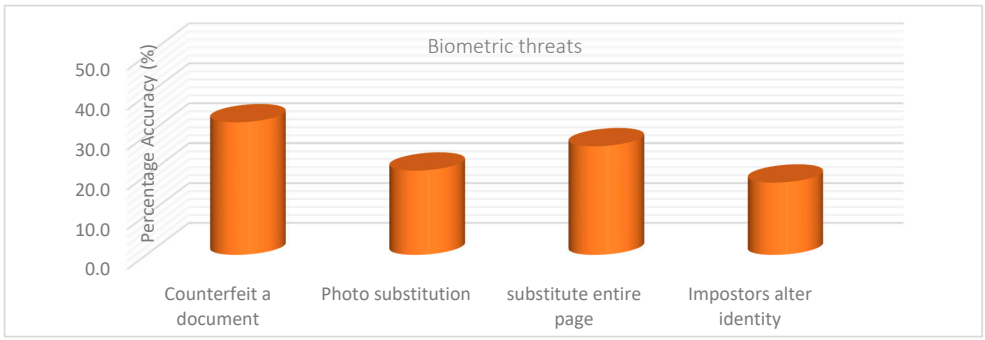
This section explains the important fundamental element of the threats experienced in issuance of the biometric passport: the attacks regarding the biometric template database. From the analysis, 33.3% of the participants stated counterfeit of their travel document as the greatest encountered threat. This is because identity fraud of travel documents are commonly experienced threats to the security of the national economy of the citizens globally It facilitates a wider range of crimes and terrorism. An imposter can make a false or fake passport to carry out unlawful fraudulent activity. The counterfeit documents comprised of unlawful duplicates of genuine permits illegally factory-made, neither issued nor verified by the authorized officer. With numerous dissimilar identity and travel documents in existence, it can

be a challenging task to differentiate amongst false and genuine documents. Therefore, INTERPOL provides several specialized tools for the law enactment to help detect fraudulent documents and works with different partners to improve the level of security of official documents.

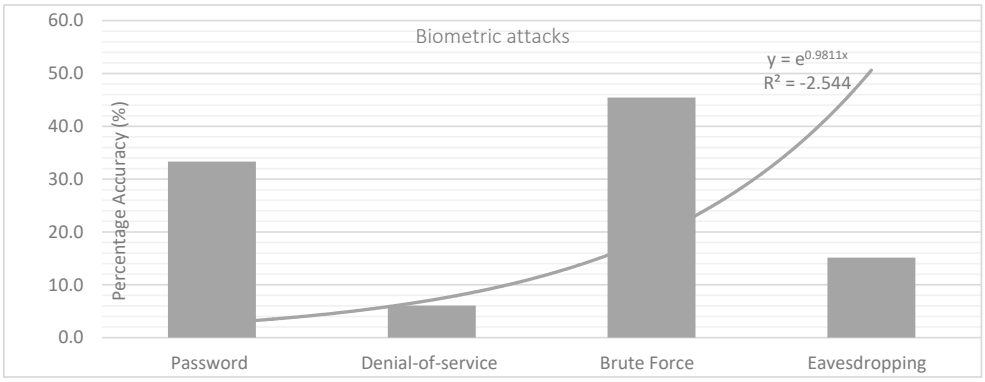
Additionally, 27.3% revealed the elimination and substitution of passport pages. These threats were related to the fraudsters seeking to tamper with legitimate passport data pages of the genuine document owners at the production stage. Rules should be followed by the public authorities to make the biometric passport pages harder for the fraudsters not to predict where, when, how, and by whom the identity should be checked.

Furthermore, 21.2% presented threats related to photo substitution. Photo substitution is removing the biometric data image from the genuine individual's document and exchanging it with an imposter's biometric data image. Likewise, 18.2% revealed an imposters alteration of their identity as another threat, because the impostor can modify the biometric features to change the data in a genuine document to obtain high verification scores. For instance, modification of the biographical data in the optical or MRZ.

Additionally, attacks to the biometric template database were discussed. Foty-five-point-five percent (45.5%) of the respondents revealed brute force attack as the greatest vulnerability, because the imposter can attack the server system to acquire the biometric template database. Thirty-three-point-three percent (33.3%) showed password recovering, because an imposter can crack and recovers password from the stored system to access unauthorized files. Fifteen-point-two percent (15.2%) showed eavesdropping. Eavesdropping is where an invader clandestinely listens to the communiqué link and interrupts the message using digital devices such as the RFID chips. Six-point-one percent (6.1%) revealed denial-of-service. This is because an attacker tried to prevent genuine users from obtaining access to the server system. These exposures in the technology can permit an invader to remotely spy on a user's information. Therefore, three-factor authentication is required to generate a pre-determined pin code to prevent an attacker from compromising an individual account. The findings of the analysis are presented in Figure 3a,b.



(**a**)



(**b**)

Figure 3. (**a**) Graphical representation of the biometric threats. (**b**) Graphical representation of the biometric attacks.

Several types of individual information connected to bodily, biological or behavioral features of end-user's acceptance were discussed. Fingerprint and face identifiers received the highest preference from the respondents with 44% and 32%, respectively. The fingerprints have been used as an additional identification mechanism in many national ID systems, and thus, are found to be more acceptable. They are used in an indoor access control, workers' identification, gate pass attendance, and customer identification. They do not need the user to stay firm, which is different from the iris or retina. The person simply needs to touch the sensor screen of the authentication device and is done. The face modalities for recognition and verification were the most acceptable modality by travelers. We recognize and verify our family, friends, colleagues, and neighbors by looking at their face on an everyday basis. Ten percent (10%) preferred iris recognition, because the iris system is the most reliable, secure to use, and is hard to forge. The modality has been installed in many countries and no record has shown its data breach. Six percent (6%) preferred the signature scan, because the digital signatures are much more difficult to forge than normal handwriting and protect the integrity of one's official documents. Four percent (4%) preferred a voice scan, because they are used remotely unlike other types of biometrics that could not remotely be used, such as fingerprints, retina biometrics or iris biometrics. Four percent (4%) preferred Hand Scan.

The modalities parameters were compared for the acceptance–rejection of the biometric technology. For instance, the false acceptance rate, false rejection rate, crossover error rate, receiver capture characteristics, and the sensor subject distance. The false rejection rate is the degree of possibility that the biometric technology would mistakenly refuse access to a lawful individual. In other words, the likelihood that biometric technology would fail to identify an enrollee or confirm the lawful claimed identity of an enrollee. It is estimated as FRR = NFR ÷ NEVA (NIA). Where FRR is the false rejection rate, NFR is the number of false rejections, NEVA is the number of enrollee verification attempts, and NIA is the number of identification attempts. The estimate assumed that the enrollee identification/verification attempts are symbolic of those entire enrollees of the people. The false rejection rate excludes "failure to acquire" errors. Nevertheless, the false acceptance rate is the degree of probability that the biometric system would wrongly agree with the unlawful user. In other words, the possibility that a biometric system would mistakenly identify a person or fail to reject a fraud. The ratio assumed passive impostor attempts. It is projected as FAR = NFA ÷ NIIA (NIVA). The FAR is the false acceptance rate, NFA is the number of false acceptances, NIIA is the number of impostor identification attempts, and NIVA is the number of impostor verification attempts. The findings of the analysis are shown in Table 3.

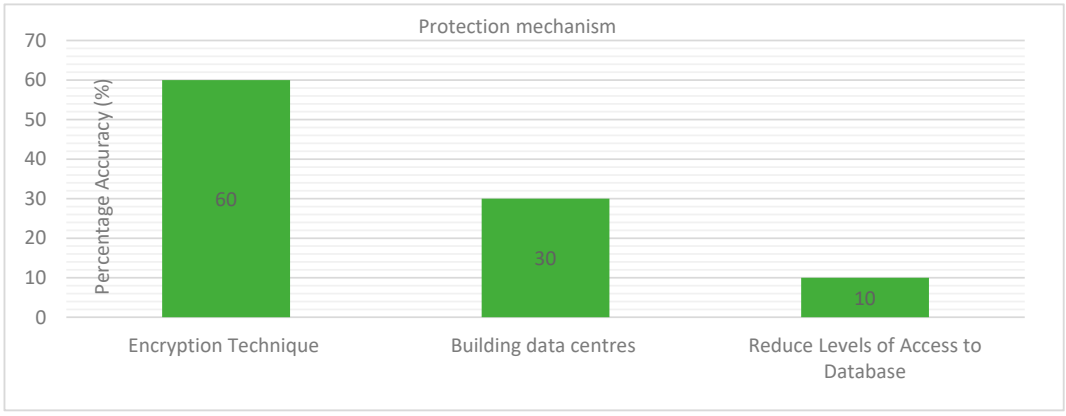
Table 3. Biometric modality comparison.

Modalities	Accuracy	Ease to Use	User Acceptance	Speed	FAR (%)	FRR (%)
Facial	Medium	High	High	Medium	1%	20%
Iris	High	Medium	Medium	Medium	2%	2%
Fingerprint	High	High	High	High	0.94%	0.99%
Voice	Medium	High	medium	High	2%	10%
Signature	Medium	Medium	Medium	High	-	-
Hand scan	Medium	High	Medium	High	2%	2%

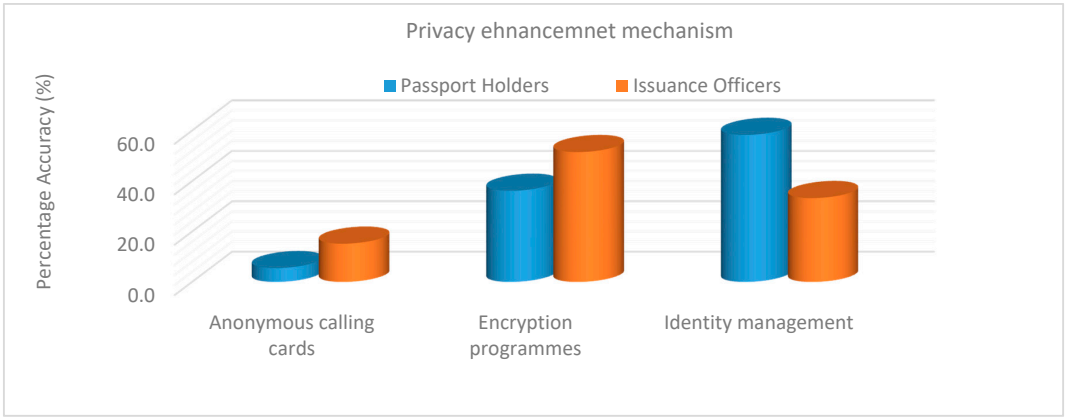
4.4. The Protection Mechanism of the Biometric Data

Despite the increasing attacks and threats to biometric technology, the best mechanisms to secure and enhance the privacy of the user's information were discussed. The encryption techniques and encryption program were the recommended techniques with 60% and 51.5%, respectively. The encryption technique helped protect biometric private information and sensitive data and enhanced the security of the server's communication. The respondents suggested the encryption

program to enhance the privacy. This is because the encryption program binds the digital key to securely encrypt the sensitive biometric information. Then, the information is saved in the database that makes it harder for the imposter to break into. If this mechanism could be put in practice, then most of the respondents would be likely to apply for a biometric passport. Thirty percent recommended building data centers. Because the data center would provide centralized services. For instance, the data storage, the backup-recovery, and data management to run either online or offline. Fifty-eight-point-three percent (58.3%) and 33.3% commended identity management, because it facilitates role-based access control that would allow the system administrators to control and oversee access to the organization's critical systems and guarantees access to the specific application for which they are authorized. Ten percent (10%) of the participant recommended reduction level of database access, because security is a significant issue in database management. We, therefore, recommend that civil policy for biometric data gathering and handling should be based on lawful ideologies and should include the input of diverse actors such as civil society organizations, industry associations, privacy-security experts, government officials, as well as intelligence expertise. The findings of the analysis are presented in Figure 4a,b.



(**a**)



(**b**)

Figure 4. (**a**) Graphical representation of the biometric protection mechanism. (**b**) Graphical representation of the biometric privacy-enhancing mechanism.

4.5. Implementation of the Proposed Biometric Passport System

The python flash framework was used for the development, because it facilities for designing web applications and built-in development servers, and provides simplicity, flexibility and fine-grained control as well as a fast debugger. It allows one to quickly add common security mechanisms to the application such as Session-based authentication, Role management password hashing, Basic

hypertext transfer protocol (HTTP), and Token-based authentication. Five steps were involved in the application system. Step 1: Create login credentials and choose the regional center. Step 2 and Step 3: Auto generate the regional code and fill the form. The regional code is a unique code for each center and applicant. For instance, [AR33200031920] code for Arua region and [MB66200011920] for Mbale region. The application identification (ID) helped identify the region/center of the applied applicant. It included the regional code, year, month, and personal unique ID. This guaranteed the security of the personal information to track the record. Step 4: Adding documents. The passport photo was automatically encrypted once uploaded into the system and decrypted upon verifying and approving the applicant document. This helped to prevent the data linkage and fraudster from infringing on personal information and counterfeiting the document. Step 5: Declaration statement and submission. This generated individual data entry to print a copy of the submission form and send it to the regional officer. The verified and approved form were automatically sent to the headquarter. The Small Message Service (SMS) notification was then received by the applicant. For instance, (Hello John [AR33200031920] your application has been verified and has been forwarded to headquarters, we shall contact you to come for biometric scans).

The regional officer from the headquarter can view the applicant's details, decrypt the passport photo to verify the applicant, and then invite the applicant for the biometric scan. Immediately after a click of the application button, an automatic SMS reaches the applicant. For example, "Hello John (AR3320003192), we are inviting you for a biometric scan. Please come to our office Kampala (Headquarter)". The integrated biometric features such as the face image and fingerprint were captured to generate two encrypted template files. For instance, the byte file and the text file. These files were saved securely into a central database. Several authentication processes were involved. *Windows Authentication*: to validate and permit resources. *Forms Authentication:* creates username and password. *Biometric feature authentication*: to encrypt the biometric data and storage database with security privileges. This successful deployment and operation depended highly upon the present existing technology and the resources in place. Many countries are adopting a biometric passport application program with the combination of a paper and electronic passport system to store biometric data in the central server. The system is designed to be non-traceable by the imposter, it also contains protection mechanisms to avoid hacking and despicable attacks that can compromise the user's information and individual rights to privacy during the personal information transmission.

As biometric technologies are not designed fully with security or privacy capabilities, technology inventors need to address the provisions of the deployed application. The user populace needs to talk in the planning process to guarantee and reassure the end-user's acceptance. Our proposed application system involved security tools such as Jinja2, Wtforms, Cryptography, and Twilio programmable sms among others. Jinja2 were used as a template engine that contained variables and tags to control the logic of the information flow. It provides a protection framework for automation of testing the application and helps prevent cross-site scripting (XSS) attacks. The Wtforms were used to generate a passport applicant's form, instead of writing Hypertext Markup Language (HTML) directly. This provided protection from Cross Site Reference Forgery (CSRF) through Wtforms CSRF module. The cryptography modules were used to encrypt the face scan and the fingerprint image based on Fernet instance. The Fernet ensured that the message encrypted would not be read lacking the key. The Twilio programmable sms was used to alert users and authority through sms messages in case of unauthorized access to the system and the database template of the application. With these security tools implemented, we were able to address users' concerns of privacy and security of the biometric information. Of the concerned addressed were, the passport was issued by the correct person who applied and followed the procedures. The individual information was secured and encrypted with Twilio sms notification that assured the person of his/her information safety. Two encrypted files were produced that make it computationally complex for any impostor to break into the template database server to access any individual data. The digital data on the passport were only readable by an authorized officer. The application could detect, monitor, signal, and report illegal attempts of the

template database linkage. The proposed system provided faster, more reliable and easier processing of biometric documents. The system was able to control the individual information and provided feedback immediately as well as increased accuracy and efficiency. The system was able to reduce fraud and forgery of documents. Thus, it could build public acceptance, confidence and trust in the system itself and in those operating the applications. The proposed framework for the biometric passport application system is presented in Figure 5.

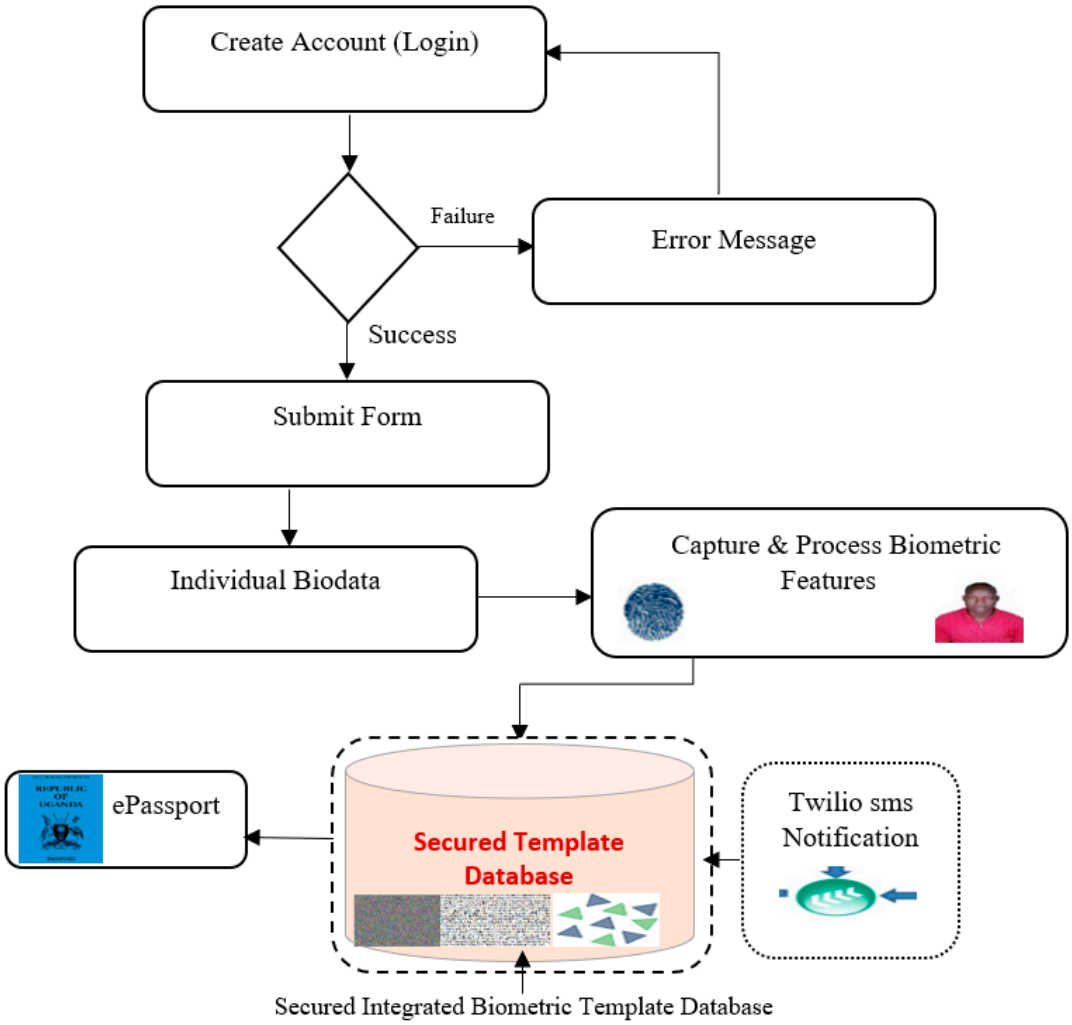


Figure 5. A Proposed framework for biometric passport application system.

5. Discussion

Despite the factors impacting fears of biometric technology, the study found three dependent features that do have an impact on the users' concerns of the biometric technologies. These were the disclosure of personal data, improper data transmission, and abuse of information. This was because of perpetrator workers and third-party suppliers (insider threats) at the organization who could potentially misuse the personal data for another purpose. It is suggested that an appropriate policymaker craft a privacy policy that guards against the exposure of personal information without jeopardizing the benefits of the new technologies. Although organizations do not actively attempt to disclose personal data, it is actually very hard in practice for them to ensure privacy, because information resides anywhere in the IT infrastructure and can be elusive by an imposter in the present-day information system. For instance, when the 15,277 million Uganda voters' fingerprints meant for National Identity Cards (NIC) were extracted from the NIRA database, it raised serious anxiety for the citizens [23]. Such a situation should be prevented and maintained. The cultures

throughout the world recognize a multitude of treaties to protect and respect privacy to control who has access to data. Therefore, there is a need to facilitate the server database with extra protection coding such as hash functions to disallow data queries transfer. Additionally, a mandatory strategy for implementing comprehensive privacy strategies and regulations that set out training and awareness program to all agents at the beginning of the employment with the custodian is an important element before being granted access to personal information.

In addition to impacting fears, counterfeiting documents was another threat attested, because an imposter could make a false document to carry out and commit unlawful fraud activities. Therefore, secure worldwide law set-ups, allowing member countries to demeanor first-line authorizations and second-line inspection at airfields, marine ports and borders as well as forensic laboratories, were required to detect fraudulent documents. Furthermore, partner countries in different sectors need to design a document that is very hard to copy, re-produce and personalize by an imposter. The information should be linked with security features for fraudsters to reach, alter and display perfect and detection traces of changes and the replication of the individual information so that automated detection of a fraudster can be identified. Nevertheless, brute-force and password were other attacks experienced, because an imposter can try a mixture of usernames and passwords to break into the server. Protecting the biometric data server is very important. One needs to install firewalls and Norton security to block malevolent attacks to safeguard the server database. The long and complicated encrypted key hashed and three factor authentications can also help defend the account and deny a user access after a pre-defined number of attempts. A recent study has indicated that there is an exponential increase in Internet of Things (IoT) malware and ransomware attack [24]. These attacks emerged from multiple countries around the globe and they are getting more sophisticated with each passing day. Therefore, the system administrator or server controller needs to be more vigilant in protecting the database information.

The findings suggested encryption techniques as the most favorable method of protecting the biometric database, because the encryption generates a secret key to securely protect data where no one else has access to in the template database. For instance, espionage uses encryption to securely protect content folders which contain emails, chat histories, tax information, credit card numbers, and other sensitive information. The study also recommends the implementation of the biometric passport application system that would enhance individual identity control, because it discoursed privacy and builds users' trust in the delivery of e-passport services. In addition, it increases the accuracy of personal identification measures and effective communication amongst the user and state in the secure handling and execution of individual information. Thus, it eliminates de-facto standard for authentication and user's perceptions towards potential infringements. Additionally, the study provided valuable information for all stakeholders (governments, private enterprise) that are anticipating offering users these security features in their everyday applications.

Our study contributes to the knowledge gap of users' concerns for privacy and security implication, specifically on biometric system acceptance. Firstly, because non-technical issues such as factors prompting the acceptance of the biometric technology as well as the end-users' future anticipated fears and perceived benefits were discussed. Secondly, we have proposed a framework for biometric passport application to guarantee individual data privacy. The proposed architecture presents a valuable tool for every organization considering new technology to improve its functionality. It is a good companion to the administration by suggesting different implementation ideas to safeguard the social benefits from biometrics. Thirdly, we develop a model that is more focused and technology-specific. This is significant since some organizations are already involved in adopting the technology because of its perceived helpfulness but eventually can decline to operate it due to the high risk of security and privacy. Therefore, the end-user's concern can be effectively combated only if the application system makes sure that the fraudster does not know where, when and how he/she would be caught.

Limitations and Future Work

Our study focused only on users' knowledge and concerns of biometric passport and security measures. It is possible that the results may have been marginally altered had biometric national identification and driving permit been considered for the large study. Additionally, we concentrated on university students, teaching staff and issuance officers as the target sample, because other categories are sometimes portrayed as more suspicious of such invasive technologies and this may be an obstacle to the generalization of our results. This research is also limited to statistical data collected since the security issue is a complicated task to perform, only beginning to be collated and released on request, justification and approval. Future studies could consider the conceptual framework to be tested on other samples (East African Countries) and the whole population (not only universities) to confirm all the hypotheses postulated. Second, they could explore other different biometric technologies (Driving permit and National identification) to see if users' concerns portray the same fears.

6. Conclusions

In this study, we aimed to assess Ugandans' readiness and concerns regarding biometric passports. We conducted a survey study with 384 passport holders and 33 issuance officers. Our findings revealed that users have privacy and security concerns such as the disclosure of personal data, improper data transmission, abuse of personal information, counterfeiting, and brute-force attacks. The encryption mitigation strategies were felt to be the best security approach. We proposed the biometric passport (e-passport) application system for users to integrate the biometric information with a combination of biodata. Not one form of prevention measure was required to protect biometric templates against adversary attacks. The integrated Twilio programmable sms notification with a cryptography module was paramount to the system. This reduced the exposure to frauds and protected the biometric passport information stored in the database. These findings also lay the basis for the continued study of biometric technology end-users' concerns as the technologies are developed further and see increased adoption, as well as the technology designers and the researchers for where to focus future efforts.

Author Contributions: Data curation, T.H.; Formal analysis, E.T.L.; Investigation, T.H.; Methodology, T.H.; Supervision, E.T.L. and A.E.S.; Writing—review & editing, T.H., E.T.L. and A.E.S.

Funding: This research received no external funding.

Acknowledgments: The authors thanked the participants as well as the unremarkable commentators for their feedback and useful suggestions. The authors are also grateful to Muni University and The Nelson Mandela African Institution of Science and Technology.

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

References

1. Kundra, S.; Dureja, A.; Bhatnagar, R. The study of recent technologies used in E-passport system. In Proceedings of the 2014 IEEE Glob Humanit Technol Conference—South Asia Satell GHTC-SAS 2014, Trivandrum, India, 26–27 September 2014; Volume 3, pp. 141–146. Available online: http://bensmyth.com/research.php%5Cnhttp://bensmyth.com/publications/10thesis/%5Cnhttps://vsm.cs.utwente.nl/~{}mostowskiwi/papers/nluug2008.pdf%5Cnhttp://ink.library.smu.edu.sg/etd_coll/52/%5Cnhttp://dx.doi.org/10.1016/j.enconman.2015.12.039%5Cnhttp://arxiv (accessed on 27 September 2014).
2. Ntungwe, V.N. ILO Convention 185 on Seafarers' Identity Document Thirteen Years after Entering Into Force: Analysing Implementation Challenges and Future Outlook. Master's Thesis, World Maritime University, Malmö, Sweden, 2018.
3. Caviedes, A. European integration and the governance of migration. *J. Contemp. Eur. Res.* **2016**, *12*, 552–565.
4. East African Community. *Ministry of East African Community Affairs in Conjunction with the Directorate of Citizenship and Immigration Control M of IA*; East African Community: Kampala, Uganda, 2012.
5. Morosan, C. Customers' adoption of biometric systems in restaurants: An extension of the technology acceptance model. *J. Hosp. Mark. Manag.* **2011**, *20*, 661–690. [CrossRef]

6. Pons, A.P.; Polak, P. Understanding user perspectives on biometric technology. *Commun. ACM* **2008**, *51*, 115–118. [CrossRef]
7. Miltgen, C.L.; Popovič, A.; Oliveira, T. Determinants of end-user acceptance of biometrics: Integrating the "big 3" of technology acceptance with privacy context. *Decis. Support Syst.* **2013**, *56*, 103–114. [CrossRef]
8. Ng-Kruelle, G.; Swatman, P.A.; Hampe, J.F.; Rebne, D.S. Biometrics and e-identity (e-passport) in the European Union: End-user perspectives on the adoption of a controversial innovation. *J. Theor. Appl. Electron. Commer. Res.* **2006**, *1*, 12–35.
9. Habibu, T.; Sam, A.E. Assessment of vulnerabilities of the biometric template protection mechanism. *Int. J. Adv. Technol. Eng. Explor.* **2018**, *5*, 243–254. [CrossRef]
10. Hancke, G.P. Practical eavesdropping and skimming attacks on high-frequency RFID tokens. *J. Comput. Secur.* **2011**, *19*, 259–288. [CrossRef]
11. Calderoni, L.; Maio, D. Cloning and tampering threats in e-passports. *Expert Syst. Appl.* **2014**, *41*, 5066–5070. [CrossRef]
12. Jannati, H. Analysis of relay, terrorist fraud and distance fraud attacks on RFID systems. *Int. J. Crit. Infrastruct. Prot.* **2015**, *11*, 51–61. [CrossRef]
13. Nixon, M.S.; Carter, J.N.; Bustard, J.D.; Hadid, A. Measuring and mitigating targeted biometric impersonation. *IET Biom.* **2014**, *3*, 55–61.
14. Carpenter, D.; McLeod, A.; Hicks, C.; Maasberg, M. Privacy and biometrics: An empirical examination of employee concerns. *Inf. Syst. Front.* **2018**, *20*, 91–110. [CrossRef]
15. Gudavalli, M.; Kumar, D.S.; Raju, S.V. Securing e-governance services through biometrics. *Int. J. Secur. Appl.* **2014**, *8*, 103–112. [CrossRef]
16. Antoni, D.; Herdiansyah, M.I.; Akbar, M. Critical factors of transparency and trust for evaluating e-government services for the poor. In Proceedings of the 2017 Second International Conference on IEEE Informatics and Computing (ICIC), Jayapura, Indonesia, 1–3 November 2017; pp. 1–6.
17. Sinha, A. A survey of system security in contactless electronic passports. *J. Comput. Secur.* **2011**, *19*, 203–226. [CrossRef]
18. Chaabouni, R.; Vaudenay, S. The extended access control for machine readable travel documents. *BIOSIG* **2009**, *155*, 93–103.
19. Shalabh, K. Chapter 4 stratified sampling. *Sampling Theory*. Available online: http://home.iitk.ac.in/~{}shalab/sampling/chapter4-sampling-stratified-sampling.pdf (accessed on 26 April 2019).
20. NIRA-Uganda. *Mass Registration of Pupils and Students*; NIRA-Uganda: Kampala, Uganda, 2015.
21. Singh, S.C. Confidentiality and disclosure in the practice of medicine and healthcare services. *Inst. Dev. Manag.* **2014**, *1*, 313.
22. NPA. *Pharmacy2U Is NOT Your Local Pharmacy and Has Nothing to Do with Us*; NPA: Washington, DC, USA, 2017.
23. Vava, R.C. *Biometric Voter Registration: Lessons from Ugandan Polls*; ZESN: Harare, Zimbabwe, 2016.
24. McLean, A. IoT Malware and Ransomware Attacks on the Incline: Intel Security. Available online: https://www.zdnet.com/article/iot-malware-and-ransomware-attacks-on-the-incline-intel-security/ (accessed on 25 April 2019).