AN INTEGRATED MOBILE IDENTITY AUTHENTICATION MODEL

ABWAO DONATUS OMONDI

A Thesis Submitted to the School of Informatics and Innovative Systems in Partial Fulfillment of the Requirements of the Degree of Masters in Information Technology Security and Audit of Jaramogi Oginga Odinga University of Science and Technology

DECLARATION AND APPROVAL

This is wholly my original work and has not been presented for an award of degree to any other university known to me

Signature ……………………………………. Date ……………………..……………….
Mr. Abwao Donatus Omondi
I152/4353/2016

APPROVAL

This thesis has been submitted for examination with our approval as university supervisors

1. **Prof: Silvance O. Abeka**
   Signature……………………………… Date…………………………………….
   School of Informatics and Innovative Systems (SIIS)

2. Dr. Joshua O. Agola
   Signature……………………………… Date…………………………………….
   School of Informatics and Innovative Systems (SIIS)

COPYRIGHT

ACKNOWLEDGEMENT

Special thanks to all individuals who played both direct and indirect contribution to its successful completion. Although this opportunity may not be adequate to recognize all persons by name, it is my sincere desire that this acknowledgment would reach to all who made significant contributions to supporting and ensuring the success of this thesis.

Special thanks to my supervisors Professor Silvance Abeka and Dr. Joshua Agola for their tireless assistance in providing guidance and supervision on the thesis. Their commitment is not only a prerequisite for the success of my project but also a lifetime inspiration to my career. I have to acknowledge their encouragement, insightful guidance and the intellectual excursion we shared during the interaction sessions we had.

To friends and family members who supported me through constructive criticism of weaknesses pointed out in the drafts during the progressive documentation process, I am humbled and very grateful. I am very grateful for your continued support until the completion of this journey and especially to its ultimate stage. It cannot be called a success without you.

May the Almighty God Bess you abundantly.

ABSTRACT

Personal identity theft is an illegal act that involves a perpetrator possessing an identity of a victim without their knowledge nor consent and in most cases for monetary gain or criminal fraudulent activities that the culprit hides in. Mobile identity has theft related cases where an identity theft criminal acquires a target person's identity for his or her own advantage. Mobile identity theft still exists with many studies reporting despite increase of security measures from the industry and other public awareness on personal mobile security. This study identified mobile identity theft as a problem in the mobile phone industry data security, orchestrated by offenders who leverage on vulnerabilities at subscriber identity module (SIM) registration and replacement processes. The study finds that vulnerability at the subscriber identity module is a type of authentication process and besides the degree of problem isolation, categorizes the authentication clusters in their operational context. The study then proposed, developed and simulated the integrated authentication model to mitigate the problem by confirming that addition of an integrated population registration records would contribute to mitigate the problem. The study used model development methodology. The developed model was tested through a simulation process using data generated from constructs of the developed model passed through a formula that determines strength of authentication score and it was observed that maximum authentication was achieved at a maximum level of authentication for all parameters. The study also noted that the introduction of the *IPRS, P* enhanced the model and prevents any weakening of authentication. The study therefore confirmed that maximum level of stable authentication could be achieved by introducing an integrated population records to the already existing authentication model with maximum level of security. The study also pointed out that the security level of "user knows" and "user is" share similar authentication behavior implying that where static biometric authentication was used, knowledge-based authentication may not make much significance.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

ACRONYMS/ ABBREVIATIONS

ATM	Automatic teller machine
IPRS	Integrated Population Registration System
KYC	Know your customer
MCC	Mobile cloud computing
MIM	Mobile identity management
MIT	Mobile identity theft
MNOs	Mobile network operators
MPIMP	Mobile phone identity management process
MPIT	Mobile phone identity theft
NFC	Near Field Communication
PIN	Personal Identification number
RFID	Radio-Frequency Identification
SIM Card	Subscriber Identifier Module Card
USSD	Unstructured supplementary services data

CHAPTER ONE

1.1 Introduction

This chapter covers the background information, problem statement, and the objectives of the study. It also covers the research questions, the significance of the study, the scope and limitations.

1.2 Background Information

Mobile identity authentication is a solution to mobile identity theft which apart from being a scholarly research affair, it is also in the public domain and has lately been on the rise. An Australian research study on a response system that mitigates identity theft reveals how overall identity response system lacks coordination and is disjointed when examines 211 theft cases related to identity reported to the National identity and cybercrime support service (Wyre, Lacey, Allan, Crime, & Justice, 2020). A survey to determine compromise types and as to whether majority of the respondents are unaware of how their details are compromised disclose that 31% of the cases are mobile number related cases (Wyre, Lacey, & Allan, 2020). Mobile Identity authentication come in complex scenarios to solve identity theft in mobile industry given the emergence of new technologies for various services to meet the demanding needs of customers in different businesses and innovative solutions. An unstructured supplementary services data (USSD), a menu based and real-time mobile based electronic service that facilities access to various services has been reportedly noted to have a number of challenges and the same service allegedly used by fraudsters to commit identity theft through subscriber identification module (SIM) swap, phone theft and kidnap, in other cases funds in the bank (Otor, Akumba, Idikwu, & Achika, 2020). The author further reports that apart from the weaknesses identified and exploited by threats within the USSD service possess a challenge to similar services used by automatic teller machine (ATM), machines used by banks to dispense money through use of PIN concludes that compromises the ATM channel and violates one of the stated guidelines for USSD operation in Nigeria (Otor et al., 2020).

A Kenyan case study that identifies various systems that support electronic means of money transfer, their effects on profitability, liquidity and the business network of financial institutions finds the main challenge to be security issues particularly theft of mobile identity, money laundering and attributes this to sophisticated technology (Wangui, Nzuki, & Management, 2021).

Efforts to address cases of identity stealing that are mobile related was first addressed in a study that develops a method of early detection and prevention of identity theft in where author argues that when use of identity is attempted, a record associated with the identity is retrieved and a request sent to the registered mobile device for location information verification (Dustin & Bruce, 2003).

A study that addresses MIT develops an enacted view on mobile identity management with an opinion that MIM play an important role in addressing usability and trust issues in mobile business growth. The author in the development has an opinion that MIM should be used to identify, acquire, access and pay for services that follow the user from device to device, location to location and context to context (Roussos, Peterson, & Patel, 2003).

Other efforts to address identity theft in developing reliable mobile identity authentication is supported by theory of human identification which the author describes as the association of verification data with a particular human being and identifies three basic means for making human identifications namely; knowledge-based identifications, token-based identifications and biometric identification (LoPucki, 2001). Despite the fact that certain constructs within this theory have been implemented in majority of MNO’s for authentication of customer identity, perpetrators of mobile phone identity theft still innovate around the weaknesses of the authentication system and are able to get away with stolen mobile phone identities.

Mobile identity authentication is achieved by variety of authentication models that uses identity parameters referred to as authentication factors in this study. The authentication process involves comparing values submitted to the model by users to the actual authentic values used during registration, the model passes the process should it find a contrary match, terminates the process and displays error message to the user. There exists a number of weaknesses besides strengths of the current mobile identity authentication models. This study was conducted to develop a mobile identity authentication model that would be used to enhance the security of mobile identity process.

1.3 Problem Statement

The problem of mobile identity theft is a challenge in a generation that have countless mitigation strategies that can be applied to help and is a major concern in the public. While several reported and non-reported cases are still observed across customers in different ways, sources indicate that those involved are changing tact and methods of mobile identity theft. In some instances, in Kenya in particular, a customer receives a call from someone claiming to be an agent of a bank or a telecommunication company and lures them to help resolve their account issues. The decoying trick usually presents itself as a coincidence to a current life problem, financial or personal challenge the customer is going through. The caller proceeds to probe the customer and obtains bank account details, their passwords, PIN in to assist them resolve their issues. Ultimately, those who fall in such pranks find themselves in surprising financial problems shortly after; their account missing money, some find loans borrowed with their details, unexplained transactions and borrowings from their phone contacts among others. Most of the mobile identity theft have been attributed to sim swapping or irregular SIM registration of someone else without their knowledge. This study identified the two processes, SIM swapping and irregular sim registration involved in the mobile identity theft problem and established that an addition of authentication factors would mitigate the problem within mobile identity authentication process.

1.4 General Objective

To develop an integrated mobile identity authentication model to mitigate mobile identity theft.

1.5 Specific Objectives

1. To assess existing mobile identity authentication models.
2. To assess mobile identity theft at subscriber identity module security processes.
3. To develop the Integrated mobile identity authentication model.
4. To simulate the model.

1.6 Research Questions

1. What are the strengths and weaknesses of the current existing mobile identity authentication models?
2. What are some of the identity theft instances that exist at subscriber identity module security processes?
3. How can a model be developed to mitigate mobile phone identity theft?
4. How can the developed model be simulated?

1.7 Significance of the Study

This study will contribute to the existing knowledge in the area of Mobile Identity theft while revealing vulnerabilities and how they need to be addressed. This study will be beneficial to a number of service providers within the mobile industry: The regulators will understand and address challenges that contribute to mobile phone identity crime and fraud. This will not only be important as an effort in revealing the gaps that still exist while trying to address the challenges but also form part of improving weaknesses in the mobile identity authentication. The Lawmakers will have the opportunity to understand the weaknesses that criminals exploit to possess mobile identities which do not belong to them and using appropriate legal structures can improve on the processes by initiating or improving laws to strengthen mobile identity. Mobile subscribers who are the major client's being addressed will also benefit from this development since the implementation of the model will reduce incidences that might victimize them since they will be weary of mitigation strategies to prevent the criminal act.

1.8 Scope of the Study

The study investigated of the security challenges of the current mobile identity authentication models, the vulnerabilities that facilitate theft, the design and development of the current mobile authentication model. Guided by the objectives of the study to determine weaknesses of the currently existing mobile identity authentication models, assess the level of mobile identity theft at SIM security processes and to determine whether the addition of IPRS would mitigate mobile identity theft.

1.9 Limitation of the Study

This study was limited to mobile phone identity theft as used by criminals, it aimed to identify vulnerabilities within the existing authentication models that have been proposed by researchers, implemented by MNOs and other efforts that try to initiate solutions in that context within the industry and academia.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

This chapter reviews literature based on the objectives in chapter one. Existing mobile identity authentication models are reviewed, their strengths and weaknesses to establish the gaps. Threats and vulnerabilities in the context of mobile identity authentication are established in the review. The chapter closes with the proposed integrated mobile authentication model.

2.2 Overview of mobile identity theft

Human identification refers to verification of characteristics owned by a human being against an access system and marks the foundation of all studies that are involved in fraud and theft of identity (Archer, Sproule, Yuan, Guo, & Xiang, 2012). Identity theft is a fraud in which someone, a perpetrator cheats the system verifying users to be someone else in order to gain access to either steal money, orchestrates a process that would have otherwise been done by the real person and other benefits (Moskovitch et al., 2009). This understanding is further expounded that in considering to overcome theft herein explained, an additional security layer in a model be introduced to mitigate challenges observed whilst addressing the gap realized which is using username and password as methods of user verification. Whereas the authors' approach introduces a continuous strategy to authentication thus considerably sealing the vulnerabilities associated with identity theft, the effort mentions nothing to do with mobile phone authentication which is the key area of this study. Knowing whether their contribution is applicable to control MIT is not clear even though the study introduces use of biometric tools as a control measure for continuous authentication.

Mobile authentication process is a sub-set for customer authentication process popularly referred to as Know Your Customer (KYC) which is the process of a business confirming the identity of its clients and evaluating potential risks of illegal intent for the business relationship (Davenport, Mule, & Lucker, 2011). Effort that are close to addressing identity theft within the mobile industry is worth considering and KYC processes that introduce authentication means reportedly addressing challenges herein described are considered further as contributory to literature while pointing out the gaps and how this study improves on the mentioned gaps.

2.3 Theory of human identification

LoPucki's (2001) study defines human identification as “the association of data with a particular human being”. The author identifies three basic means of making human identifications. First, in "knowledge-based" identification, individuals are "recognized by demonstrating that they are in possession of information which only that particular person would be expected to know". Such information includes a person's mother's maiden name, the person's social security number, or a password give to them at an earlier time. Second means of making human identification, in "token-based" identification, where persons are recognized by their possession of some items such as their national identity card, a driver’s license or a passport.

The Author argues that each of the tokens contain a description particular to an individual to be validate and that adds an additional degree of security; that an impostor might not be able to use the token because the description in the token would not match the impostor’s persona. Third means of human identification is "biometric" identification which refers to “a variety of techniques which are based on some physical and difficult-to-alienate characteristics." The Author adds that this includes descriptions of appearance, measurements of social behavior or bio-dynamics, retinal scans, DNA patterns and "imposed physical characteristics" such as brands, bracelets and anklets, embedded micro-chips and transponders.

This theory inspires the study given that its constructs are similar parameters form part of the current customer authentication. However, this theory only describes a typical current model which has challenges that the study addresses, the theory does not mention a third-party or associated database integration that mitigates the mobile identity theft as identified by the study. Some of the mentioned factors that support this theory and as used in current authentication models are elaborated in sections 2.3.1, 2.3.2 and 2.3.3.

2.3.1 Knowledge based identifications

Knowledge based identifications are authentication items used to recognize persons by demonstrating that they are in possession of information which only themselves would be expected to know (LoPucki, 2001). The author adds such examples to include the person’s mother’s maiden name, the person’s social security number or a password given to the person at an earlier time personal identifier numbers (PIN). Knowledge based identifications are used in the current mobile phone registration and SIM card replacement process by MNO's through their agents who ask for two or three popular numbers that the potential subscribers would be or call frequently, middle name of their mother to in order to authenticate these processes. Although the current authentication framework uses the same procedure, perpetrators are able to trick the agents in charge of SIM card registration and replacement and get away with forged registration details.

A comparative study evaluating the use of traditional password and personal identifier numbers (PIN) against alternative methods involving questions and answer responses and geographical representations reveal that the two mentioned methods share mutual foundation of knowledge of secrecy and depends on the user's capability to remember it to achieve authentication, (Irakleous, Furnell, Dowland, Papadaki, & Security, 2002). The investigation however concludes having learned of some bottlenecks along the way that while passwords and PIN approaches garner good ratings of their existing familiarity to the participants, other methods based upon image and cognitive questions also achieve sufficient results to suggest them as viable in certain contexts. The said proposal supports cognitive questions in addition to traditional password and personal identifier numbers to contribute significantly to knowledge-based authentication. Considering this in the context of mobile phone identity theft still leaves us with a number of desired improvements since knowledge from observation qualifies perpetrators who know the authentication aspects to manipulate the system and get away with stolen identities thus introducing a vulnerability that still needs to be addressed.

Two factor authentication has reduced incidences of fraud, including identify they, in e-commerce (Waters, 2017). The author further explains that two factor for a personal identifier number (PIN) and RSA token are force multipliers and intensely improve the security of online transactions. Finally, the Author concludes that two factor authentication originally form three basic credentialing criteria; something someone knows, something someone has and something someone IS. Which are relatively compared to PIN or password created by a user (for something you know), a National ID number or passport (for something you have) and biometric fingerprint (for something you are).

2.3.2 Token-based identification

Token-based identification in the context of mobile phone industry authentication refers to identification of a person based on what they are in possession of such as national identification card, driver’s license, and passport all which have distinct numbers. Use of one of these still poses vulnerabilities in that an impostor would pretend to have the characteristics of the holder of these documents to acquire an identity (Tiwari, Singh, & Technology, 2017). This has been realizing in a number of cases puts it that cases of mobile phone identity theft are on the rise with perpetrators leveraging on mobile money. In as much as this study supports the use of national identification documents and other applicable token-based identification, the study believes that an integration of an existing system to leverage on the mentioned tokens in providing a peer-matched identities of customers seeking to register or replace their SIM Cards would perfectly filter illegal cases.

2.3.3 Biometric identification

A number of physical and difficult-to-alienate characteristics that can only be associated with a single individual that if used by the MNOs then acquiring identity would mean that only one precise person gets (LoPucki, 2001). This has to be available in some database where the agencies of the mobile providers will use through a system to authenticate those seeking identity approval. It is then prudent to accommodate this aspect in an environment that is looking forward to a zero tolerance to mobile identity theft. Considering the author’s contribution in highlighting that biometric identification is one of the factors that are and can be used in human authentication gives confidence to the agents of the factor given that it gives a secure combination.

2.4 Existing mobile identity authentication model

In this section, we reviewed relevant mobile identity authentication models to establish our familiarity with and understand of current mobile identity authentication models to know whether this research had been done, to identify gaps within the study and highlight what is unknown.

2.4.1 Adversary model for mobile device authentication

A study that analyzes various mobile authentication models, classification and comparison between various mobile device authentication models reveals that a number of gaps in security of the models and that security protocols in the models lack a comprehensive security analysis. In the model analysis, user-to-device (U2D) authentication is addressed which involves a user self-authenticating before accessing mobile device functions (Mayrhofer, Mohan, & Sigg, 2020). The author acknowledges that U2D authentication is possible by one or combination of four factors, a summary of parameters used in authentication namely:

1. something a user knows this include; passwords, PIN codes, graphical patterns, among others,
2. something a user possesses that comprises of; hardware tokens, keys, and so on ,
3. something a user is or static biometric, this covers; fingerprint, face, iris, hand geometry, vein patterns, and so on and,
4. something a user does or dynamic biometric, this encompasses; gait, handwriting, speech, among others.

According to Mayrhofer et al., (2020) there is no verification that has been established as an official U2D authentication, most of user validation models either use one or a combination of factors to compare user details.

A further review of mobile authentication models and considering authentication on mobile devices in particular, the focus on the individual threats seem to match this study; hacking methods like brute-force, password guessing, installing malware and hardware-level exploits to bypass authentication are mentioned as commonly used. This study widely borrows from the adversary model for mobile authentication given that it points out explicitly the key factors that enable authentication as a combination of factors, this study is persuaded to pick the factors as the key constructs of the study even though it is supported by the theory of human identification (Funcion & Technology, 2017).

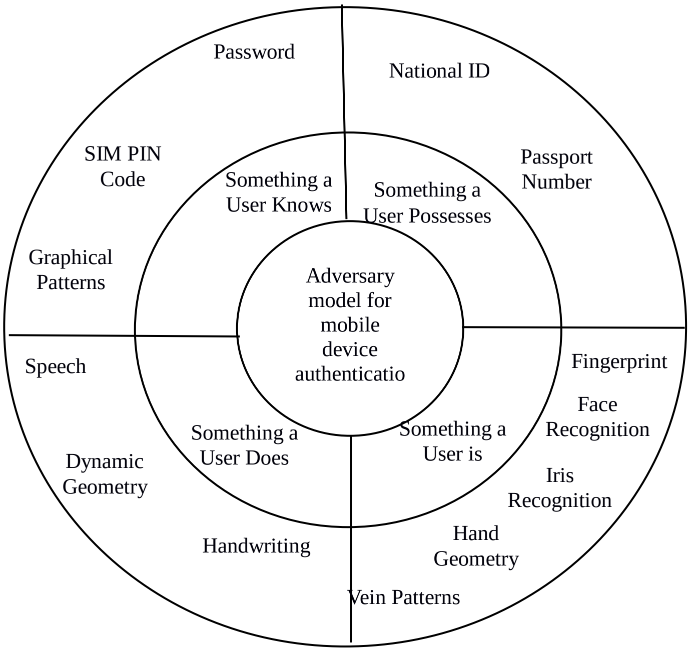


Figure 2.1: Adversary model for mobile device authentication (Mayrhofer et al., 2020).

Figure 2.1 shows how the author has categorized applicable authentication factors that can be used in any user or device validation for better understanding. This study appreciates the contribution of the authors given the conglomeration of authentication factors and leverage where one factor is inapplicable. Consequently, the strength of such a model determines resilience to threats and vulnerabilities that would break and compromise their security. While considering the application of this model, the innovativeness of threats and underlying mitigation measures, determination of the strength of any model that improves it and complements this study is a key factor in deciding whether the model will overcome the pressure and weaknesses of its construction.

The author's contribution to mitigating the mobile identity problem is applied at the vulnerable points of SIM-Card registration and replacement processes. Not only is this eminent in the combination of the collective factors considered, but also in the apparent accommodation of relevant supplementary aspects that may strengthen the security of user to device authentication. Even though the model is applicable in a user to device authentication environment, it is worth nothing that its adversity and complexity gives the considerable view that may be used and or re-used in an authentication study that may not be explored which still faces challenges as that of mobile identity theft. Given that the model bears all the constructs used in a modern authentication arena and supported by other studies, and for which reason the study considers, the study challenges or accepts a future constructive criticism that would nothing less than improve on the choice of a model in the realization of an integrated mobile authentication model. The gap in this model as explained is an integration with an external national database with one or a combination of the four factors to form a basis of cross authentication access. Whereas the registration and use of authentication of the factors mentioned in the model are critical in identifying access, cross-checking with a database that informs the validity of those factors is an initiative that this study finds fit to mitigate use of fabricated factors.

2.4.1.1 Description of authentication factors

This section describes the four main authentication factors and provides information on their appropriate vulnerability points.

2.4.1.2 Authentication by what a user knows

Table 2.1 is a summary of authentication factors of what a user knows with their vulnerability points. Authentication by that a user knows is composed of mobile PIN numbers, passwords and graphical patterns.

Table 2.1: Vulnerability points for what a user knows (Weichbroth & Łysik 2020)

#	Authentication factor	Vulnerability points
1	PIN	Shared PIN, password and graphical patterns
2	Password	PINs, passwords and graphical patterns cab be guessed
3	Graphical patterns	PIN, passwords, and graphical patterns are stolen

2.4.1.3 Authentication by what a user possesses

Table 2.2 is a summary of authentication factors of what a user possesses with corresponding vulnerability points. This study finds authentication by the user possesses to consist of national ID number and passport number.

Table 2. 2 Vulnerability points for what a user possesses (Weichbroth & Łysik 2020)

#	Authentication factor	Vulnerability points
1	National ID	Someone has (in possession of) your national ID or passport National ID or passport is cloned Someone has details in the national ID and or passport
2	Passport	

2.4.1.4 Authentication by what a user is

Table 2.3 summarizes authentication factors of what a use is with the respective vulnerability points. "User is" is the third authentication factor and comprises of fingerprint, face recognition, iris recognition, hand geometry and vein patters.

Table 2. 3 Vulnerability points for what a user is (Weichbroth & Łysik 2020)

#	Authentication factor	Vulnerability points
1	Fingerprint	Attacker has access to Fingerprint, face, iris, hand geometry and vein pattern by cloning that of a user who is registered in the mobile device. Fingerprint, face, iris, hand geometry and vein pattern spoofing
2	Face recognition	
3	Iris recognition	
4	Hand geometry	
5	Vein patterns	

2.4.1.5 Authentication by what a user does

Table 2.4 is a summary of authentication factors of "User does" with respective vulnerability points. The "user does" authentication factor is the fourth factor that consists of speech recognition, dynamic geometry and handwriting.

Table 2. 4 Vulnerability points for what a user does (Weichbroth & Łysik 2020)

#	Authentication factor	Vulnerability points
1	Speech	Fake speech synthesis or speech conversion or imitation recorded speech, cloned hand and dynamic geometry.
2	Dynamic geometry	
3	Hand geometry	

2.4.2 Mobile payment authentication model

A study admits that human behavior characteristics or how different people conduct themselves is unique and very difficult to hypothesize that none of existing research has considered the influence of user posture on users' gesture behavior authentication (Jiang & Li, 2020). The study monitors user's gesture behavior overtime and based on authentication system architecture reveals that it is possible to monitor from a user login to the entire usage process for improving the payment of mobile devices by using authentication and continuous authentication comprehensively. This model concentrates on one aspect of user and access authentication and does not consider the diversity in terms of device use and their application to scenarios for an authentication process that relies on this one factor and the population that still uses feature phones (Feng et al., 2012). Additionally, while the author apparently uses "user is" as a means of authentication token all through the study it is still falls short of three other modes of authentication contexts as identified in the base model of this study; user does, user knows and possess. Notably, the complexity of this authentication model is only workable in a smart mobile device as explained by the author, this may not be convenient for those with feature phones despite the small population that uses feature phones. According to Communications Authority report 2021, 56% of Kenyans still use feature phones (*Communications Authority of Kenya 2021 Report*, 2021).

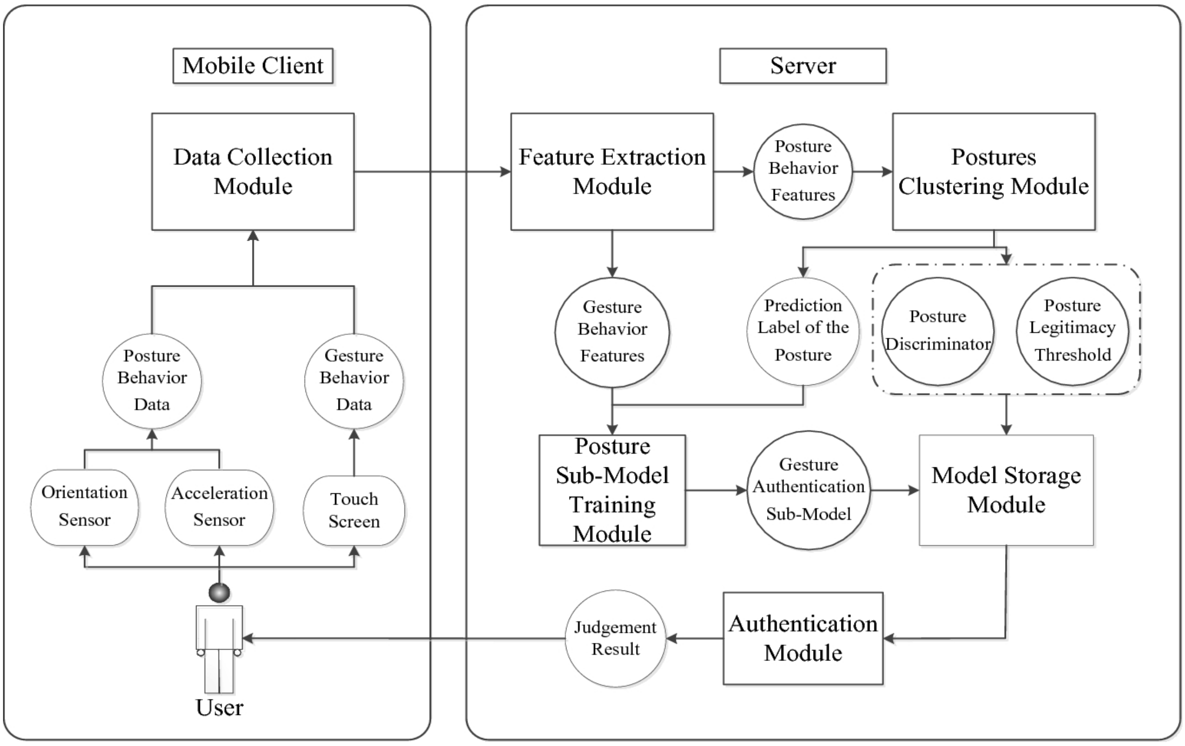

Mobile Client
Data Collection Module
Posture Behavior Data
Gesture Behavior Data
Orientation Sensor
Acceleration Sensor
Touch Screen
User
Server
Feature Extraction Module
Posture Behavior Features
Postures Clustering Module
Gesture Behavior Features
Prediction Label of the Posture
Posture Discriminator
Posture Legitimacy Threshold
Posture Sub-Model Training Module
Gesture Authentication Sub-Model
Model Storage Module
Judgement Result
Authentication Module

Figure 2.2: Mobile payment authentication model (Jiang & Li,2020)

Figure 2.2 represents the authentication factors, process modules and interactions in the mobile payment authentication model.

2.4.3 A user authentication model for online banking system

Review findings from a study that involves a critical outlook of current existing authentication access for users using online banking through mobile phones reveals that whereas current security authentication model uses biometric or PIN as authentication tokens, none of similar authentication model propose use of International Mobile Equipment Identity (IMEI) number, a factor that the author perceives to strengthen the security of user authentication (Hammood et al., 2020). As well put by the author, the IMEI number uniquely identifies mobile phone handsets while adding extra security to online banking security. Another observation by the author puts it that previous studies in the authentication arena have predominantly considered a conventional use of username and passwords, biometrics like fingerprint, facial recognition and notices that online banking authentications where mobile systems are involved would need extra security feature to enhance.

Figure 2.3 shows the interaction of authentication layers between SMS based, facial verification and user knows authentication. In as much as the author considers that addition of the IMEI number enhances the security in online banking system, this study hypothesizes that an integration of the previously mentioned authentication items mentioned by the author would make a stronger authentication. From the analysis of the adversary authentication models, Usernames and passwords are authentications used in the cluster user knows in their operation scope, finger biometrics and facial recognition are in the “user is” authentications while IMEI number is in the “user possess” cluster (Mayrhofer et al., 2020). It therefore means that is it only “user does” constructs in the authentication model for which this study is based on that the author has not considered using. This study hereby takes cognizance of the magnitude of effort the author has put in the model review however, the feeling that more authentication clusters would increase the strength of user authentication has not been fully met by this review.

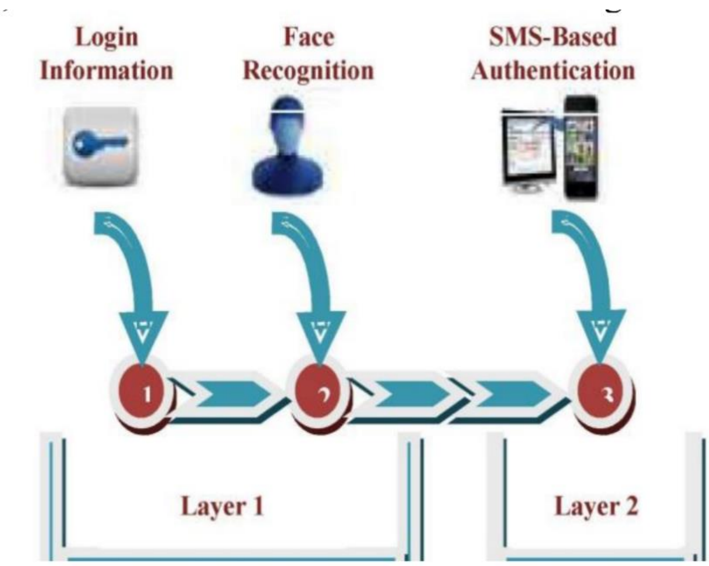


Figure 2.3: MFA using face recognition process (Hammood et al., 2020).

2.4.4 Authentication model for smart mobile devices

A comprehensive investigation that identifies open challenges of authentication schemes for mobile devices classifies authentication models involving smart mobile devices in their context of threat models and reveals five classification categories; identity based attacks, service based attacks, manipulation based attacks, eavesdropping based attacks and combined eavesdropping and identity based attacks (Amine Ferrag, Maglaras, Derhab, & Janicke, 2018). In the same study, the author reviews and gives description of multiple existing threat models to find a relevance and whether that can play a contributory element in the mobile authentication, a move that possess challenges in the authentication models as presented below. It is interesting that the model review recognizes and categorizes authentication schemes for smart mobile devices into four classes namely; biometric, channel-based, factors-based and ID-based authentication schemes.

Figure 2.4 shows the composition of verification factors in the authentication model for smart mobile device and the interactions. The classification of the authentication factors somehow resonates with that of adversary model for computer device authentication which this study adopts. However, the same study does not find it generic to accommodate non-smart devices in the application of its clustered authentication factors.

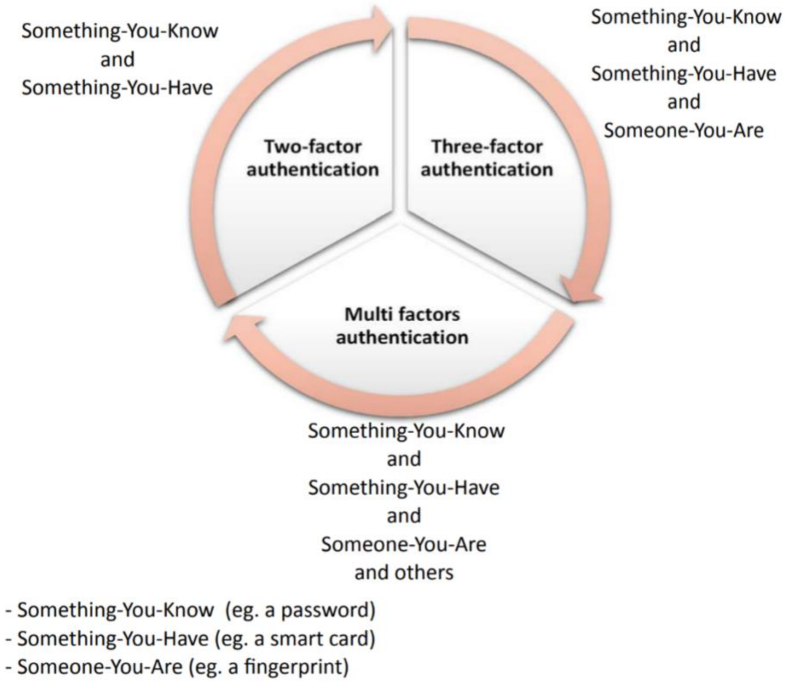

Something-You-Know
and
Something-You-Have
Something-You-Know
and
Something-You-Have
and
Someone-You-Are
Two-factor authentication
Three-factor authentication
Multi factors authentication
Something-You-Know
and
Something-You-Have
and
Someone-You-Are
and others
- Something-You-Know (eg. a password)
- Something-You-Have (eg. a smart card)
- Someone-You-Are (eg. a fingerprint)

Figure 2.4: Factors-based authentication schemes for smart mobile devices (Amine et.al.,

2.4.5 A Pseudonym based identity authentication model

A proposal that develops an unidentified authentication model that uses assumed names instead of real ones and applied in mobile crowd sensing reveals the effectiveness of the solution which is said to contribute to protection of privacy with regard to the process of authentication by means of a pseudonym (Ma, Tao, & Wu, 2017). The study develops the model by combining public key infrastructure and combined public key technology to manage key and certificates in solving challenges of large-scale key management. The study evaluates the proposed identity authentication scheme using functional testing and performance testing. The author acknowledges that security and privacy protection as a key area in mobile crowd sensing. However, the problem addressed by the author introduces a gap by putting more weight on challenges of mobile crowd sensing and not integrating the authentication factors to give a robust combined approach to solve emerging challenges of mobile identity theft at mobile authentication processes.

Figure 2.5 illustrates the pseudonym-based identity authentication process in mobile crowd sensing, it shows the interaction between user, application server and verification certificate.

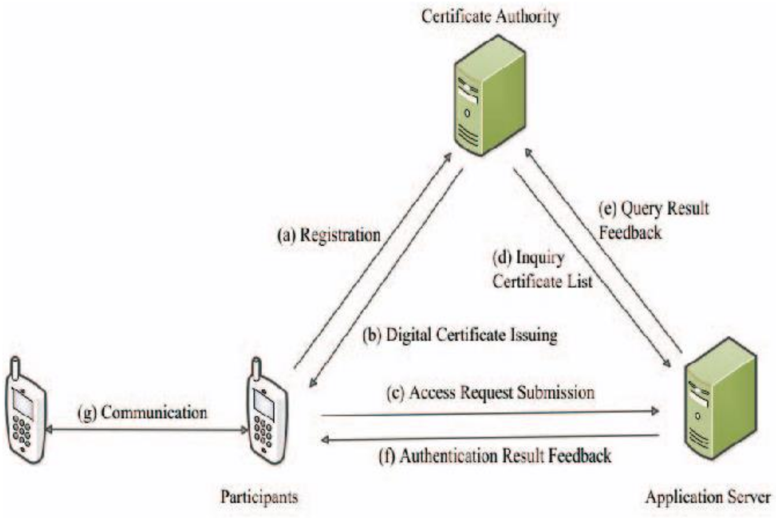

Certificate Authority
(a) Registration
(b) Digital Certificate Issuing
(c) Access Request Submission
(d) Inquiry Certificate List
(e) Query Result Feedback
(f) Authentication Result Feedback
(g) Communication
Participants
Application Server

Figure 2.5:Identity Authentication Process in mobile crowd sensing (Ma et al., 2017).

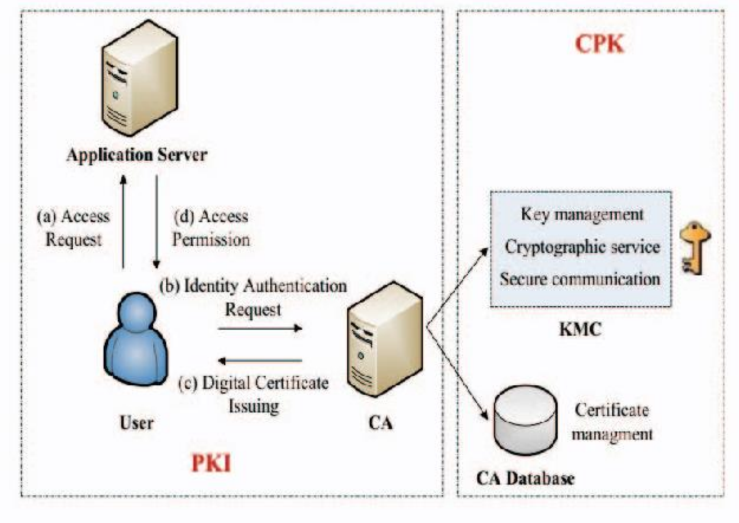


Figure 2.6: Architecture of identity authentication (Ma et al., 2017)

Figure 2.6 demonstrates identity validation architecture in the pseudonym-based identity authentication model, it also further illustrates the interaction between user, application server, certificate generation and certificate database.

2.4.6 Authentication model for android mobile phones

A model review that analyzes some of the authentication models that are used to aid authentication in mobile devices and some of the threats and technical issues faced observes that biometric authentication schemes provide the best level of security and acknowledge that complexity brought by computation and ease of use while using biometric to traditional authentication schemes gave preferences to the traditional authentication schemes which are not as secure as biometric (Kunda, Chishimba, & Applications, 2018). In the model review, authentication models discussed involve password or pin, fingerprint recognition, pattern-based authentication, facial recognition, iris and vocal based authentication. It is worth noting that the Author's focus is on device-based authentication, considering the parameters that have been discussed which still recognizes the identity of a person or user. Whereas the study described discusses mobile identity authentication at device level, this entire study is keen on authentication for identities that connect the mobile user with the service provider to access services that depend on mobile service providers which are not mentioned. While the author recognizes that biometric authentication gives the best level of security, it makes sense that the author has come out clearly that the implementation of such kind of authentication model may not work for many users due to cost and ease of use, a factor that is validated in a study of user effort, error and task disruption which considers face, voice and gesture authentication very unusable (Trewin et al., 2012).

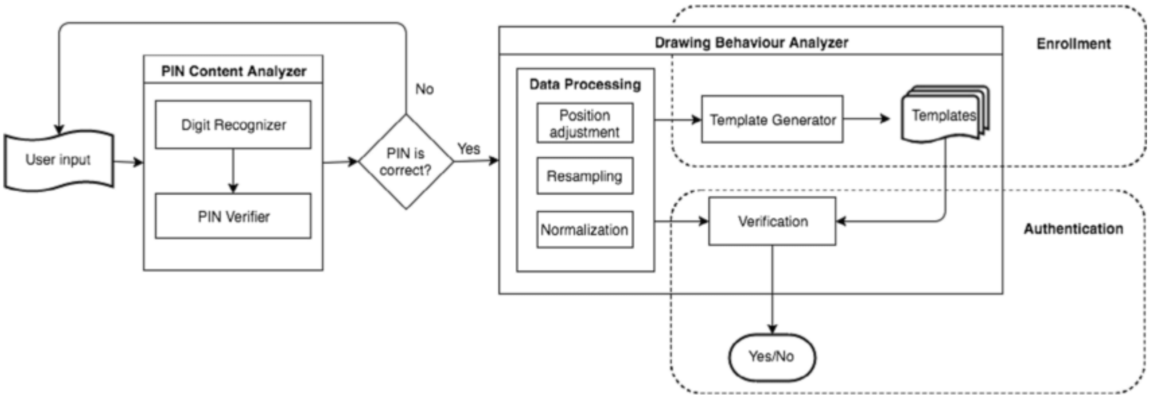
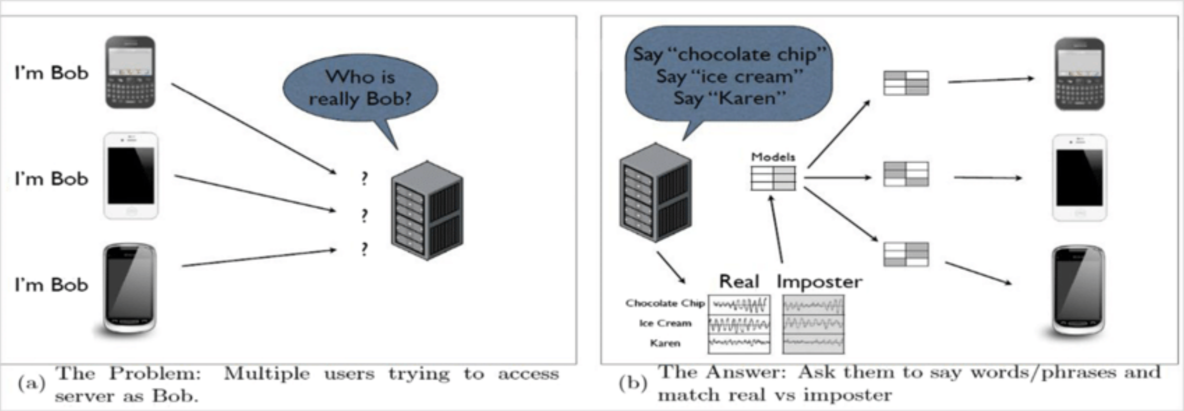


Figure 2.7: Diagram of PIN authentication phases (Kunda et al., 2018).

Figure 2.7 presents the PIN verification phases in the authentication model for android mobile phones. Figure 2.8 illustrates the setup of voice verification protocol in the authentication model for android mobile phones.



(a) The Problem: Multiple users trying to access server as Bob.

(b) The Answer: Ask them to say words/phrases and match real vs imposter

Figure 2.8: Diagram vaulted voice verification protocol (Kunda et al., 2018).

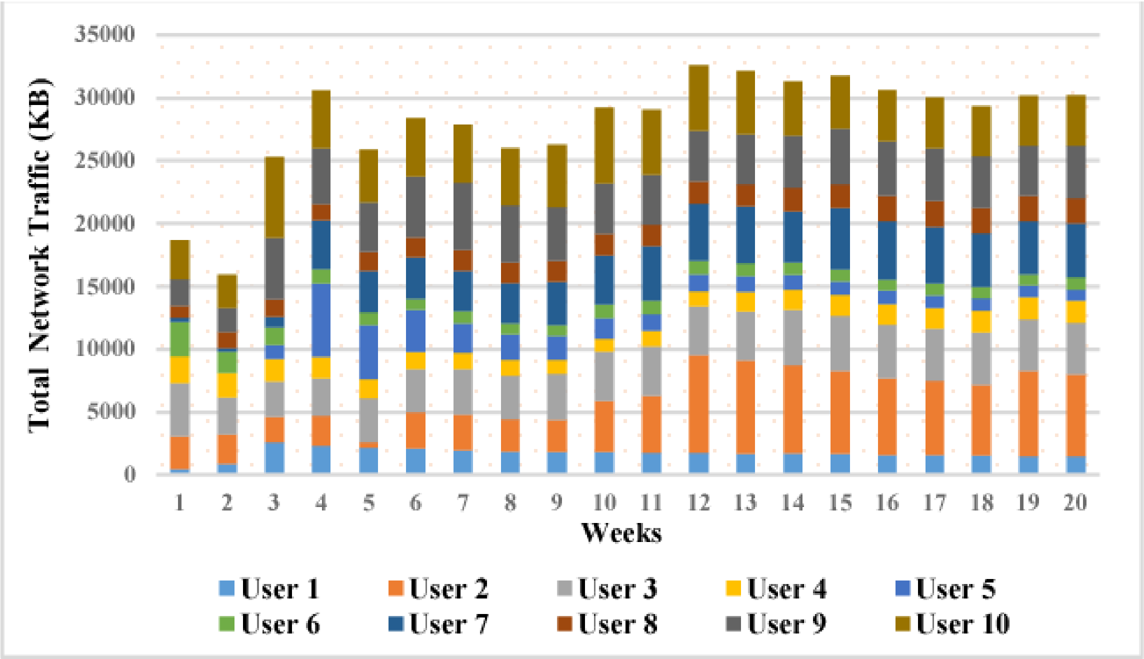


Figure 2.9: Traffic of foreground apps under both Wi-Fi and cellular networks (Ashibani & Mahmoud, 2018).

Figure 2.9 shows that network traffics of foreground apps in Wi-Fi networks increases more than that of cellular networks, a guidance that this study is likely to consider that in authentication degree needs to rise more when a user is on Wi-Fi network than when on cellular networks.

2.4.7 A secure identity-based authentication model with user anonymity for mobile devices

Analysis of a proposed development of a secure and efficient protocol that uses identity and key-agreement using elliptic curve system that uses cryptography for mobile device shows the model satisfies all security requirement despite the low computation together with the communication costs than similar models for mobile devices (Wu, Zhang, Xie, Alelaiw, & Shen, 2017). The model development is inspired by limited computing capability for mobile devices in meeting a secure efficient authentication and key agreement protocol for mobile devices. Even though the Author has made significant contributions towards model development for identity-based authentication, it is still important to consider the focus of this study that its intentions is to solve the challenge of mobile identity theft at subscribe authentication processes, a key part of the research that the author mentions least. Additionally, from the author’s insight on the study, the authentication methods used are of type “user possesses” a factor that is observed in another study that does not consider conventional use of usernames, passwords, facial recognition and biometrics as means of authentication arguing that current mobile authentications need extra security features (Hammood et al., 2020).

The study considers other authentication methods deemed to contribute to an integrated authentication model whose degree of authentication is hypothesized to mitigate the mobile identity problem. However, the author admits that mobile devices could be or have limitations in terms of their computing capability and energy, this puts more questions on the success of the model in realizing a secure authentication protocol. Efforts of solving weak authentication to mitigate threats within mobile device user identity theft, a current generation challenge despite initiatives to combat the same are still falling short of innovative methods that perpetrators use to circumvent the hardened authentication schemes and protocols to secure mobile devices. Consequently, this study finds gaps in relation to the choice of authentication factor, the authors resolution in addressing the so problem. Whereas the author uses token-based authentication factor, it is noted that the study has identified and notices that strength of authentication factors can be increased by a combination of two, three, four or more authentication factors.

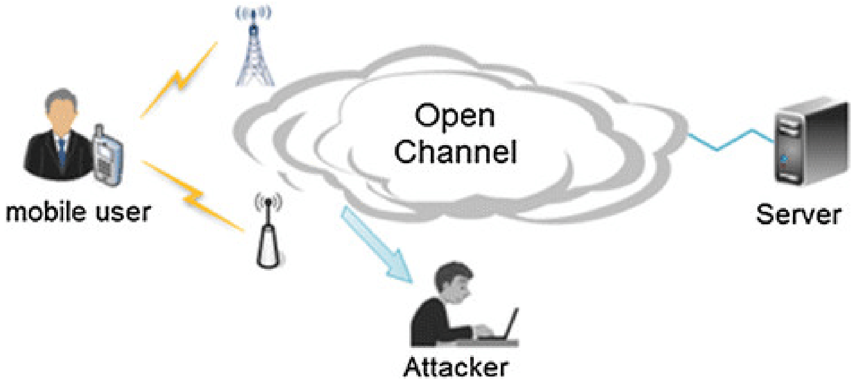


Figure 2.10: Authentication and key agreement protocol for mobile user (Wu et al., 2017).

Figure 2.10 shows a mobile user interacting with a network that is potentially predisposed to an attacker. The author maintains that the protocol provides an active secure communication between one and more mobile users and servers.

2.4.8 Two factor authentication model for mobile money.

A study that analyzes threat models and their mitigation measures in an authentication model that uses two-factor in mobile money identity verification classifies threat models into; attacks against privacy, attacks against authentication, attacks against confidentiality, attacks against integrity and attacks against availability (Ali et al., 2020a). The author further reveals that there exists a gap to be addressed that amounts from use of personal identification number and subscriber identity module (SIM) to authenticate users which according to the research are susceptible to attacks. The study profiles the processes involved in the authentication scheme and elaborates categorically the enrollment processes, the authentication processes, the vulnerabilities involved and what attack points and goes ahead to provide the mitigation measures of the attack types for the susceptible attack points.

The author’s work generates an output from a review of 97 papers with several related mobile authentication models, revealing the weak points, designing the appropriate vindication measures whilst summarizing the gaps existing, there is no integration with external databases containing information that is used by attackers for counterchecking especially during authentication.

Figure 2.11 shows threat model categories that provide a clear understanding of grouping various threats with respective security types.

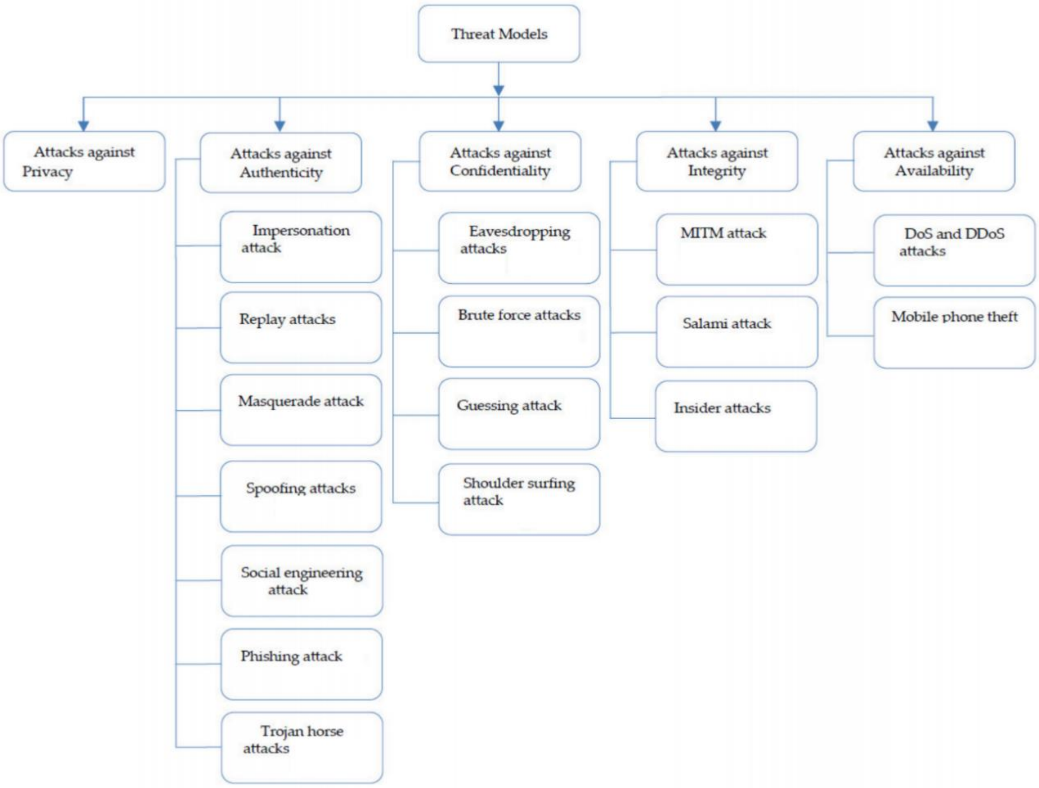


Figure 2.11: A classification of threat models in the mobile money's two factor authentication scheme (Ali et al., 2020a).

Figure 2.12 is a summary of countermeasures for attacks that the mobile money two factor authentication with their respective mitigation measures, a classification that is further categorized into cryptographic functions and personal identification.

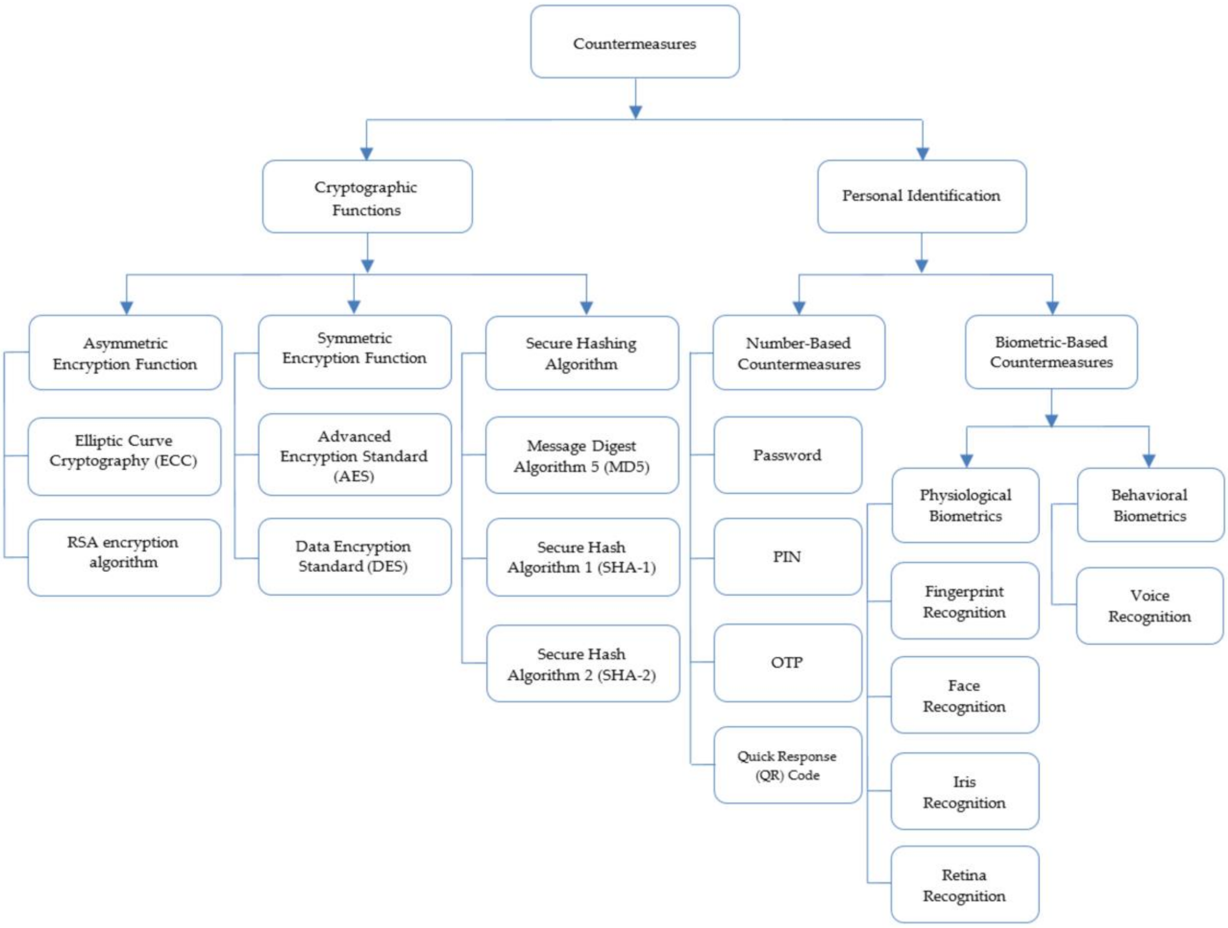

Countermeasures
Cryptographic Functions
Personal Identification
Asymmetric Encryption Function
Symmetric Encryption Function
Secure Hashing Algorithm
Number-Based Countermeasures
Biometric-Based Countermeasures
Elliptic Curve Cryptography (ECC)
Advanced Encryption Standard (AES)
Message Digest Algorithm 5 (MD5)
Password
Physiological Biometrics
Behavioral Biometrics
RSA encryption algorithm
Data Encryption Standard (DES)
Secure Hash Algorithm 1 (SHA-1)
PIN
Fingerprint Recognition
Voice Recognition
Secure Hash Algorithm 2 (SHA-2)
OTP
Face Recognition
Quick Response (QR) Code
Iris Recognition
Retina Recognition

Figure 2.12: Countermeasures against attacks in mobile money's two factor authentication scheme (Ali et al., 2020a).

Table 2.5 : Mobile authentication models study matrix

#	Model name	Constructs extracted	Classification
1.	Adversary model for mobile device authentication	User is, user does, user knows, user possess	Knowledge based, token based, biometric authentication
2.	Mobile payment authentication model	User knows, user is	Token and knowledge-based authentications
3.	A user authentication model for online banking system	User knows, user is and biometrics	Token based, knowledge based and biometric authentication
4.	Authentication model for smart mobile devices	User knows and biometric	Token based, knowledge based, and biometric authentication.
5.	A Pseudonym based identity authentication model	User possesses	Token based authentications
6.	Authentication model for android mobile phones	User knows, user possesses	Token based and biometric
7.	A secure identity-based authentication model with user anonymity for mobile devices.	User possesses and user is	Token based and biometric authentications
8.	Two factor authentication model for mobile money	User knows, user is and biometric	Knowledge based, token based, biometric authentication.

Table 2.5 represents mobile authentication models study matrix, a composition of classification of their factors and constructs extracted. The profiling gives the particular constructs and factors of each of the related mobile authentication models while providing an overview of their difference.

2.5 Integrated population management records (IPRS)

This section details integrated population records, a database of the population with details about birth registration, civil registration and national death registrations. The integrated population records as considered by this study has details that when counter-checked during user validation may reveal information on validity of records.

2.5.1 Danish civil registration system (CRS)

A civil registration system established in 1968 in Denmark to record details of citizens in a central database where easy tracking for medical purposes and other information tracking uses be used (Pedersen, 2011). The system apart from name, gender, date and place of birth, citizenship, parents' details with continuous update on place of residence, the Danish CRS records details of unique identification number of all citizens, immigrants and emigrants. Other details of the system also include complete information of children, family among others. Although the described system gives a better platform for authentication with users but this has not come out clear on the author's comments as majority of the application or use of the database is for epidemiological purposes, tracking the number of death versus those alive and perhaps budgeting. Having touched little to do with supporting relevant systems needed to mitigate mobile identity theft, this database still has a gap precisely within its area of application.

2.5.2 Kenya integrated population registration records (K-IPRS)

A digital national population register referred to as Integrated population registration system is a central database that brings together over a dozens of databases held by various government agencies on population recording, national identification records among others (Chege, 2015). The author further explains that IPRS combines data from birth and death register, citizenship register, ID card register, aliens register, passport register, and the marriage and divorce register. The birth and death register has all the information of the registration details on births and deaths in Kenya. Contribution of Integrating this component into an authentication model will filter any attempts by perpetrators to acquire irregular identities through SIM registration and replacement. This would then play a very important role in authenticating wrong information within the process of acquiring mobile phone identity thus making sure that legitimate owners have the so said identities.

Additionally, the provided information is very relevant for a more secure mobile customer identity validation for a player who is out for a precise validation process and if telecommunication companies will integrate its databases with the integrated population registry in Kenya, then it is undisputed that Kenya will successfully mitigate mobile identity theft and online fraudsters by ensuring that only those validated against the integrated system, IPRS acquire identity profiles with the MNOs and that nobody can illegally or unlawfully own and use a mobile phone identity of someone else. This would be applied on SIM SWAP as well, another process that is used by criminals to steal mobile phone identities for illegal activities.

2.6 The proposed model

Figure 2.13 displays the proposed integrated mobile identity model that borrows from adversary model for mobile device authentication which is supported by the theory of human identification. In addition, the proposed model includes the Integrated Population Records, which, which we propose to have a contributory factor in the integrated mobile authentication model to mitigate the problem of mobile phone identity theft.

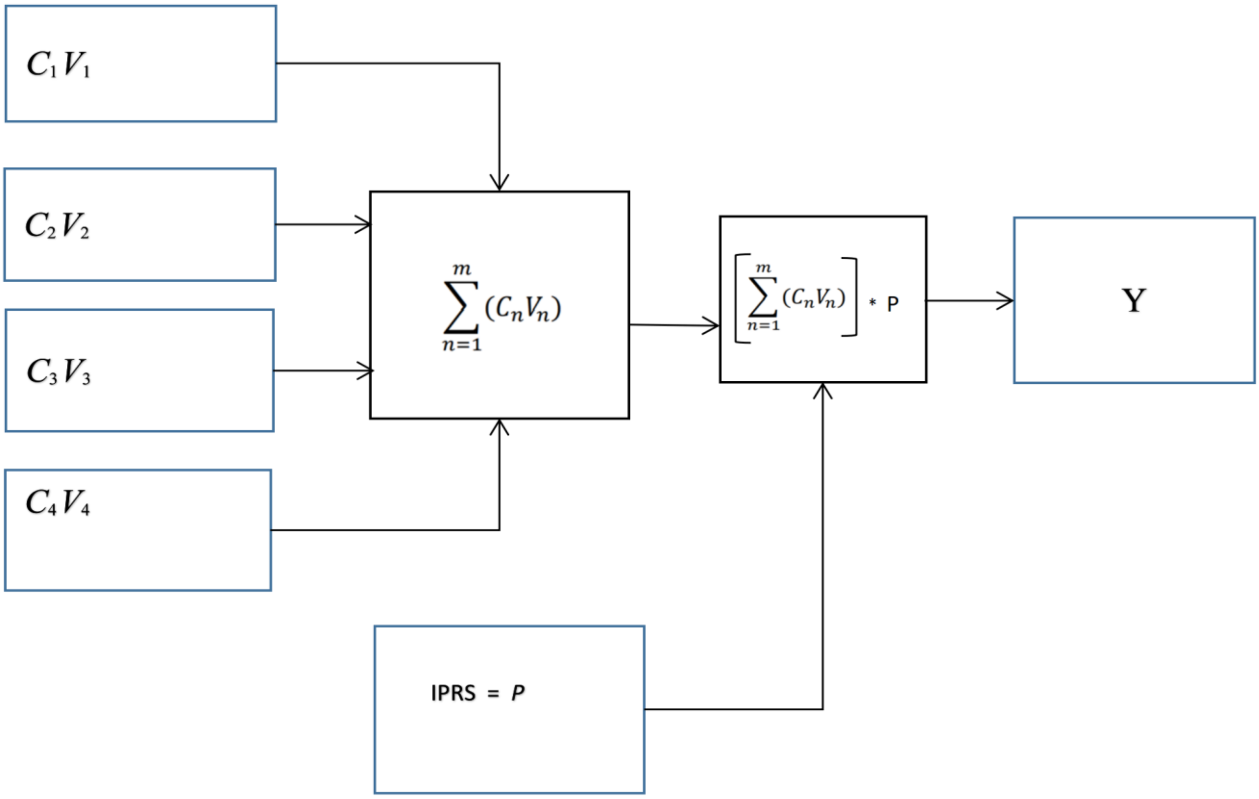


Figure 2.13: The proposed integrated mobile identity authentication model.

CHAPTER THREE: RESEARCH METHODOLOGY

3.0 Introduction

This chapter elaborates the methodology used in the study, the design and the procedures that were accomplished in the development of the model. The study used simulation research procedure in developing the integrated authentication model, code was developed with web2.0 development tools. The simulation was done by increasing and decreasing the authentication strength of the developed simulator at various vulnerability points to determine threat mitigation strengths. Ethical considerations are also provided to clarify issues to pertaining to knowledge, mutual respect, fairness and support important social and moral values.

3.1 Research design

The study aimed at developing a simulation integrated mobile authentication model for mobile authentication based on reviewed literature, identified a model which the study adopted to add components of integrated population records and computed by a formula that determines strength of authentication factor. The model was then implemented by an algorithm derived from the mathematical equation in two comparisons. The algorithm produced a visual output when coded to yield bar graphs that showed the strength factor as a measure for each authentication parameter, a cumulative reading for the two scenarios comparatively gave direction on the best composition factor that overcome the vulnerabilities.

3.2 Model development tools

The implementation of the model was developed to include of an algorithm coded using java that ran on a web-server environment. The java source code involved the instruction that determined the authentication strength factor, a combination of weighing system C_n and scoring mitigation strategy for each vulnerability point V_n. The web server that operated the model ran Apache tomcat and provided the necessary environment for simulations. Tested on unit by unit to check if the model would run, the artifact was then deployed on the web-server for simulations process. Since the development of the constructed model involved code development, the tools were not collecting data but implementing the equation 4.1 for determining the strength of authentication factor. The variation of the artifact produced results that were graphical presentations from arbitrary data loaded with the arguments, these arbitrary data were integer ranging from $0 \ldots 1$ and so the tools did not anticipate nor collect any information that needed validation. The validity of the tools was taken care of during implementation of the equation 4.3 in the algorithm in figure 4.5 and 4.6, this was done by testing the algorithm. The actual implementation of determination of authentication strength by the expression for various factors validated the tools used in research methodology, having ensured that the data produced by the model was a result of the functions that determined the strength of authentication and so ensure no data was produced with unwanted entries.

3.3 Model simulation and procedure

The model simulation process followed with each of the two scenarios being tested separately and recording. The first strength factor computation was implemented considering the model with parameters before addition of the integrated population records. Whereas literature review identified vulnerabilities as social engineering, client-side injection, poor authorization and authentication, side channel data leakage, broken cryptography and sensitive information disclosure. Our study addressed a poor authentication problem to find an improved authentication scheme that needs to overcome the threats that are associated with it, a higher authentication score would mitigate the mentioned threats that exploit poor validations. The first authentication strength factor was derived by using the four major authentication features namely: user knows (passwords, PIN codes, graphical patterns), user possesses (hardware tokens, keys), user is (static biometric which include; fingerprint, face, iris, hand geometry, and vein patterns among others) and user does (dynamic biometric which include; gait, handwriting, and speech among others). The computation was done using individual features and a combination of the rest of the features too.

A second level of computation was done considering an addition of the integrated population registration records: ID/ Citizenship register, Passport register and Death register. The results of the computation with the three features added produced a score that by comparison formed a basis to determine the model’s effectiveness. The higher the authentication score, the stronger the model and the effective the scheme to overcome vulnerability threats. The computation formula was then used to develop an algorithm that was implemented using tools; Java development kit, and html5 to produce a graphical display of the score. To provide an optimum and fair score that the model operates on, the developed model produced test results and a weighing scale that was loaded with significant values. The scale was increased and decreased to determine the strength of the model at various vulnerability points. The computation from the current models was modified and different sets of computation made to produce comparisons drawn would be referred to as old and new models. The old model refers to the current model that the study picks on before addition of any authentication features whereas the new model refers to the model with new authentication factors.

3.4 Ethical Review

This research study apart from following the due process of ethical review and considering the acceptable morals in the model development, it considered informed practice within model and code development, simulation and deduction that does not harm, respects confidentiality and privacy as elaborated by the ethical review board of Jaramogi Oginga Odinga University of Science and technology. A copy of the approval attached in the appendix section and entitled “Ethical review clearance letter”.

CHAPTER FOUR: MODEL DEVELOPMENT

4.0 Introduction

This section gives a description of development of the model while considering the two aspects of the model. At the same time, an explanation how the adversary mobile authentication model works is also provided to give a foundational understanding of the construction of the integrated model.

The next part of this section follows with the process of the algorithm development and includes the integrated model explanation as well.

4.1 Determination of strength of authentication

$$Authentication\ strength = \sum_{n=1}^{m} C_n V_n \quad \#4.1$$

Equation 4.1 was used as a framework for determining the authentication strength of biometric authentication by determining their scores and it was constructed by Information Technology Laboratory, a department of National Information of Standards and Technology (NIST) (Information Technology Laboratory, 2015). The formula helps to determine authentication score by and details a weighing system C_n and scoring mitigation strategies for each vulnerability point V_n in the quest to understand the strength of authentication technologies as used identity management systems. This was discussed in an "advanced identity workshop" which provided a methodology for comparing other authentications. In the workshop, the focus area of the formula was used to measure functional strength of biometric authentication mechanisms and the purpose was to yield a generally applicable and exceedingly extensible framework upon which other needs of diverse communities and sectors of authentication would be met.

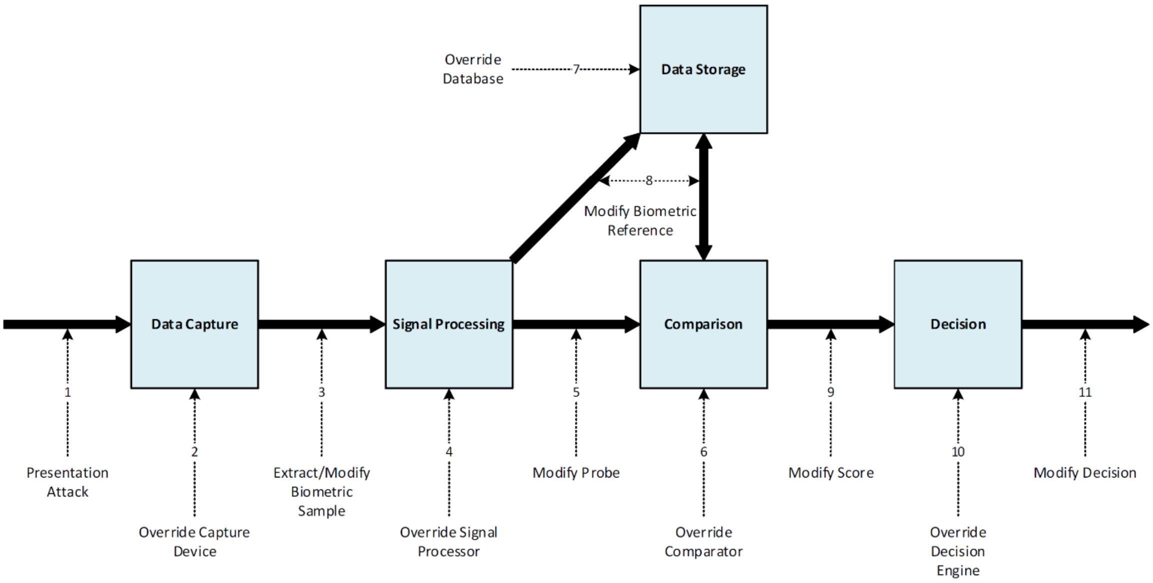


Figure 4.1: Biometric system attack diagram (Information Technology Laboratory, 2015).

Figure 4.1 shows the process chain flow of attack map in a biometric system. The development considers attack scenarios in a biometric authentication arena to produce different vulnerability points. Some of the mentioned vulnerability and attack points in biometric authentication include biometric spoofing attacks. Biometric patterns that are predisposed to such attacks include; facial images on social media companies and finger biometrics. On presentation attacks, methods like presentation attack detection present higher mitigation factors to combat attacks that might exploit their vulnerability points. A vulnerability point refers to a weakness given a perpetrator is aware of the authentication value. Other methods presented to mitigate biometric attacks include biometric capture device, biometric sampling and comparison and decision. All these mentioned methods of biometric authentication have a score calculation that computes their score factor to give their strength.

Score aggregation is recommended while computing scores for distributed entities, this ensures authentication system integrity for relying parties. The former refers to authenticating factors that rely on each other in an authentication scenario, this would be particularly possible where one, two or more factors are used.

4.1.1 Preliminary definitions

The notations that will be used in describing the model are as follows:

Y: the output, which is the prediction of the level of authentication.

C – the weighing constant score for each authentication factor.

V – will be representing the mitigation score for each vulnerability point and

n: a number bounded by the set $\{1,2,3,4\}$ with each number representing different authentication types as follows;

$\{1\}$ – user knows

$\{2\}$ – represents user possesses

$\{3\}$ – represents user is

$\{4\}$ – represents user does

V: presence of a vulnerability bounded by the values 0 (absent) or 1 (present).

4.2 Adaptation of the adversary model for mobile authentication

Considering the formula that we adapted to develop our algorithm, value of C with T where C denotes the threat weighing constant for each authentication factor at vulnerability points V_n. We introduce the value of P in the equation to produce 4.2.

$$Y = \left[\sum_{n=1}^{m} C_n V_n\right] * P \ \ \#4.2$$

Equation 4.2 demonstrates the mathematical statement that provides prediction of the value of authentication strength. In the adoption of the equation in the determination of authentication strengths of the adversary model for mobile computing and the integrated identity authentication model, we take cognizance of the introduced values in the equation and explain the values as used in the Equation 4.2 in the Table 4.1.

Table 4.1: Authentication factors, their global vulnerability statistics and weighing factor

#	Authentication factor clusters	Individual authentication factors	Nominated authentication factor	Global vulnerability statistics	Vulnerability weighing factor	Source
1	User knows	PIN code Passwords Graphical patterns	PIN	12%	0.12	Weichbroth & Łysik 2020
2	User possesses	National ID number Passport number	National ID	13%	0.13	DESAI et al., 2018
3	User is	Fingerprint Face recognition Iris recognition Hand geometry Vein patterns	Fingerprint	53.3%	0.533	Weichbroth & Łysik 2020
4	User does	Dynamic geometry Handwriting Speech	Speech	51%	0.51	Enge, 2019

Table 4.1 presents a summary of authentication factors against their respective C_n. According to Weichbroth & Łysik (2020), global statistic from a study on mobile security threats and best statistics reveal that 12.6% of mobile users use PIN as an authentication method to secure their phones. We denote the weighing system C_1 value for PIN authentication factor to 0.126 which presents the likelihood of using PIN in mobile authentication. This forms the basis of determination of authentication score for other factors within the user knows cluster.

DESAI et al., (2018) revealed that one billion people globally do not have registered identities which is a representative of 13%. This provides a constant factor of 0.13, a weighing system value for national ID as a representative of other authentication factors within "user possesses" cluster in determining strength of authentication.

Similarly, global statistics on use of speech recognition and fingerprint validation for mobile users represent 53.3% and 51% respectively reflecting a constant weighing factor for both 0.533 and 0.51 respectively (Weichbroth & Łysik 2020; Enge, 2019). Applying this constant in the strength of authentication factor formula provides an opportunity for their use as a basis in the authentication strength determination for other similar authentication factors like face recognition, iris recognition, hand geometry, vein patterns, handwriting and dynamic geometry. Global statistics on countries that register mortality statistics have it that only 26% of the world population is registered with Africa at 7%, this is way below the registration of births (CDC, 2015).

However, registration of citizens through their appropriate systems notes that in the countries with civil registration, 97% of adults have been registered which inspires those governments in their service provision. Kenya has maintained a birth information registration of 67% for the last 20 years from 2000 - 2020 (World Bank, 2021). The percentages as revealed from the global statics make 0.26 for birth registration weighing factor, 0.97 for civil registration constant that consider national unique identification and 0.67 constant that register birth information.

4.3 Computing the authentication strength for the authentication factors

Equation 4.2 represent the formula for computing the strength of the integrated identity authentication model. For user knows, considering notations C_1V_1 which is adapted to C_1V_1 for values C_nV_{1n}... C_nV_m where C_n and C_m denotes constant weighing factor for different vulnerability points for each authentication factors.

Applying this for user possesses, user is and user does, we have C_1V_1, C_2V_2, C_3V_3, C_4V_4

Figure 4.3 is the integrated mobile identity authentication model that implements the formula for determining strength of authentication score.

4.4 The Integrated mobile identity authentication model

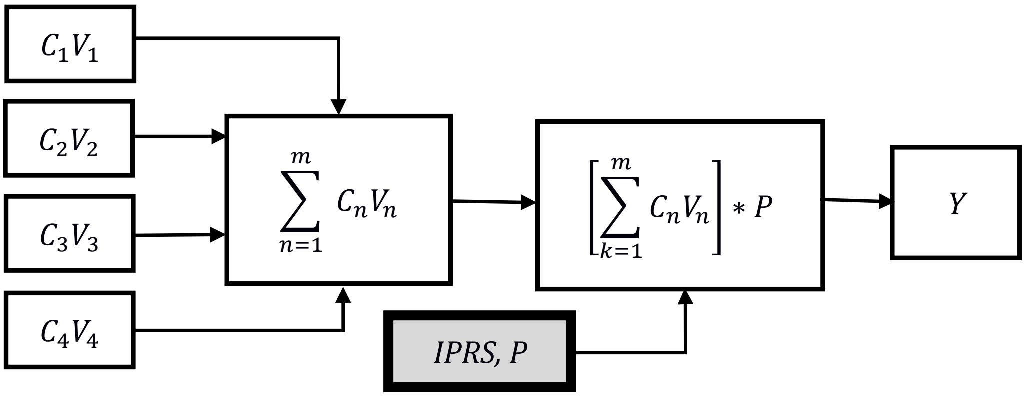


Figure 4.2: Integrated mobile identity authentication model

Figure 4.2 displays the composition of the integrated mobile identity authentication model, the factors, the equation used to compute various components and the prediction result.

4.5 Algorithm Development

The algorithm that implements the model which integrates the current model that works based on theory of human identification with the integrated population registration records to produce an integrated mobile identity authentication model.

4.5.1 Algorithm

```
Algorithm 1: compute the strength of authentication score

Input: = {$C_1,C_2,C_3,C_4$}, {$V_1,V_2,V_3,V_4$}
Output: scoRes
step 1: read $C_1,V_1,C_2,V_2,C_3,V_3,C_4,V_4$
Step 2:   Let userKnows = $C_1*V_1$
Step 3:   Let userPossesses = $C_2*V_2$
Step 4:   Let userIs = $C_3*V_3$
Step 5:   Let userDoes = $C_4*V_4$
Step 6:   Let scoRes = userKnows + userPossesses + userIs + userDoes
Step 7: return scoRes
Step 8: Stop
```

Figure 4.3 shows the details of the algorithm for computing strength of authentication score, values of $C_1,V_1,C_2,V_2,C_3,V_3,C_4,V_4$ are initialized and computed.

```
Algorithm 2:  compute the integrated mobile authentication score

Input: $scoRes$ , $P$
Output: $newscoRes$
step 1:   Read $scoRes$ , $P$
Step 2:   Let $newscoRes = scoRes *P$
Step 3: return $newscoRes$
Step 5: Stop
```

Figure 4.4 displays the steps of the algorithm for computing integrated of authentication score.

4.6 Code Development

After the algorithm development, code is developed using java and run on the JRE to produce results which are displayed on a web platform. The results indicate strength levels on a scale from 0…1, for each authentication cluster, these readings are summed up to give an overall strength indication of the models for both integrated and current.

```
Function computecvScores(){
Var     userKnows, userPossesses, userIs,  userDoes = 0;
Var vulPointC;
Calculate the products
For vupoints in range(1,4) {
  userKnows =     $C_1 *V_1$;
  userPossesses = $C_2 * V_2$;
  userIs =            $C_3* V_3$;
  userDoes =       $C_4 * V_4$;
    }
return userKnows, userPossesses, userIs, userDoes;

}
```

Figure 4.5 details the source code that implements the computation of strength of authentication score.

```
Function computeIngscore(){
computecvScores();
Var p,y=0;
Calculate the products
 y = (userKnows +userPossesses +userIs +userDoes) * p;

 return y;

}
```

Figure 4. 6 details the source code that implemented the algorithm for computing the integrated authentication score.

CHAPTER FIVE: RESULTS AND DISCUSSION

5.0 Introduction

This chapter gives a summary of simulation results of the adversary model for mobile authentication referred to herein s current model, simulation of the integrated mobile authentication model and their discussions for each scenario.

5.1 Model simulation parameters

The technical simulation process considered testing for the strengths of the adversary model for mobile device authentication vis-à-vis the integrated mobile identity authentication model. The results of each test were presented and further discussions about the test were made in the discussions section. Tests were made to determine the strength of the model in two scenes to reveal the ability to overcome threats and vulnerabilities. The two scenarios each are tested with $V_{n=0}$ and $V_{n=1}$. This is also referred to authentication factors at nominal and authentication values at maximum. The results of each scenario provide a deduction for the simulation on aggregate factors.

Figure 2.1 provides details of the constructs of the adversary model for mobile authentication model.

5.2 Strength of authentication of the model at nominal without integrated records

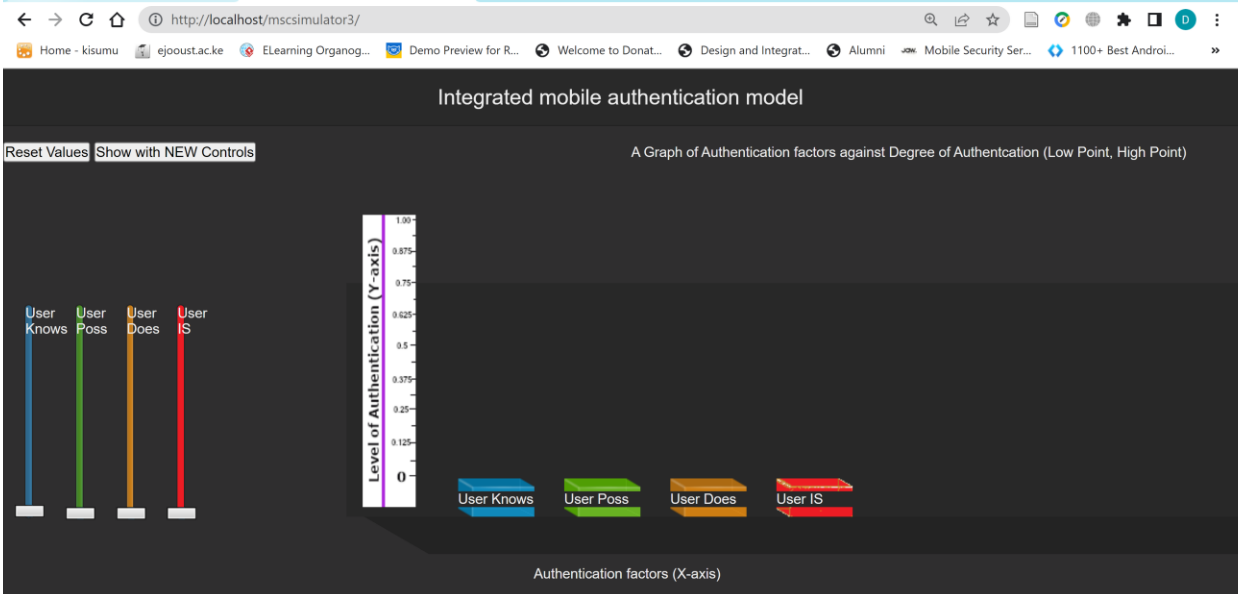


Figure 5. 1: Simulation of the adversary model for mobile device authentication model with $V_{n=0}$.

Figure 5.1 with values $V_{n=0}$, is an initialization of authentication factors with values : V_1 = 0, V_2 = 0, V_3 = 0, V_4 = 0, and C_1 = *0.12*, C_2 = *0.13*, C_3 = *0.533*, C_4 = *0.51* and produces C_1V_1 = 0.12*0, C_2V_2 = 0.13*0, C_3V_3 = 0.533*0, C_4V_4 = 0.51*0 to give an authentication strength value = **0**.

The simulation of the authentication process to predict the score value happens when all $C_{n=0}V_{n=0}$are The computation could be explained as determining strength of the model considering that scoring mitigation strategies were all null,

5.3 Strength of adversary model with all maximum values

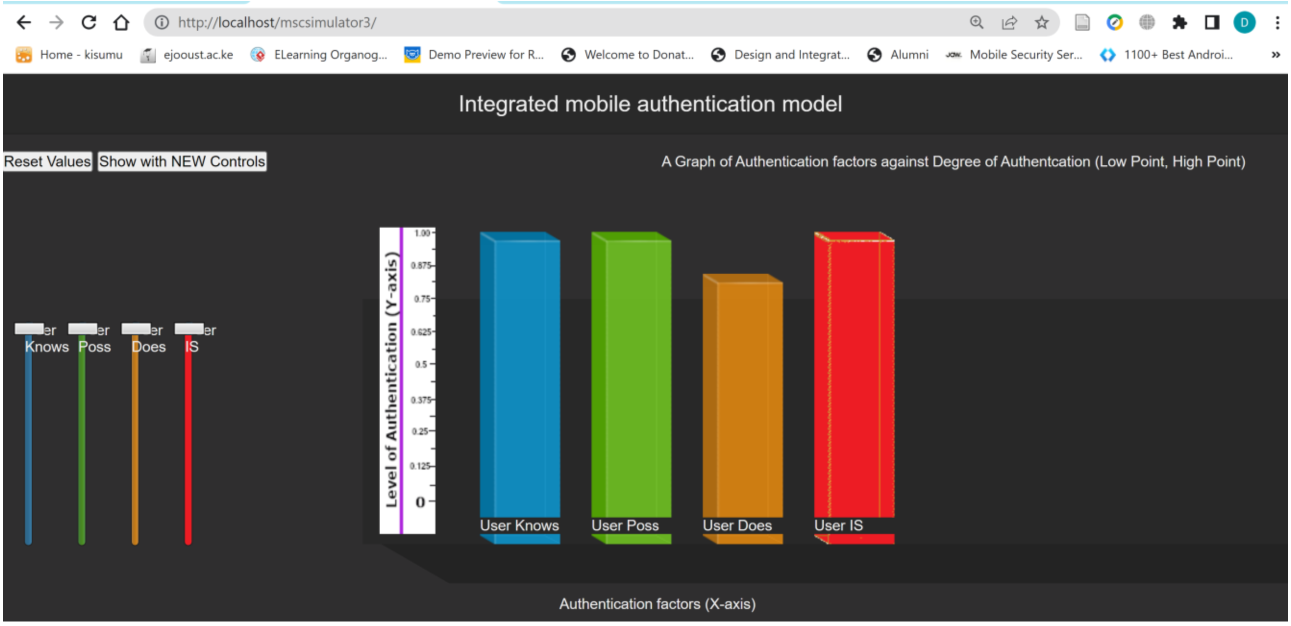


Figure 5. 2: Simulation of the adversary model for mobile device authentication model with $V_{n=1}$.

Figure 5.2 with $V_{n=1}$, is an initialization of authentication factors with the values: V_1 = 1, V_2 = 1, V_3 = 1, V_4 = 1, C_1 = *0.12*, C_2 = *0.13*, C_3 = *0.533*, C_4 = *0.51* and produces [C_1V_1 = 0.12*1, C_2V_2 = 0.13*1, C_3V_3= 0.533*1, C_4V_4 = 0.51*1]/4 To give an authentication strength value = **0.3233**

5.4 Simulating the integrated mobile identity authentication model

This simulation simulated the integrated model with additional value *P* in the formula that compute the authentication strengths against vulnerability points.

5.5 Strength of authentication of the integrated mobile identity authentication model at nominal

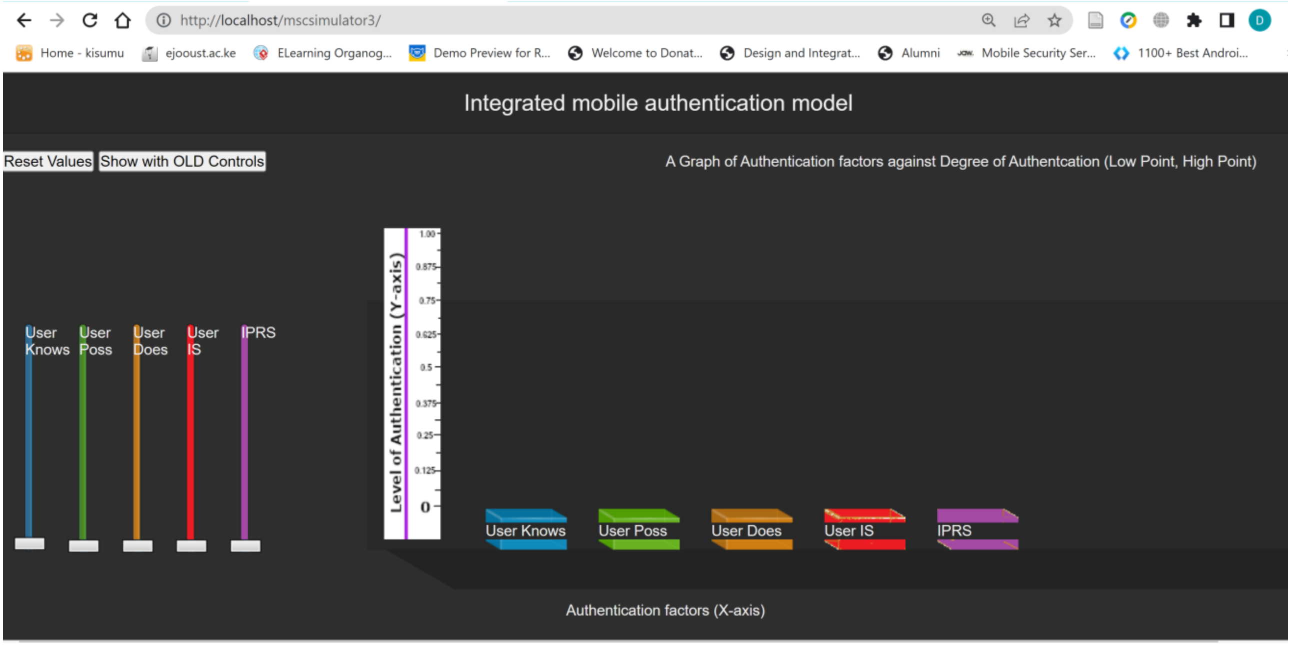


Figure 5.3: A simulation of the integrated mobile authentication model with $V_{n=0}$

The introduction of the IPRS, *P* introduces a new factor in the computation of the authentication strength and produces the following:

Figure 5.3 with values $V_{n=0}$, is an initialization of authentication factors with values: V_1 = 0, V_2 = 0, V_3 = 0, V_4 = 0, P = 0, C_1 = *0.12*, C_2 = *0.13*, C_3 = *0.533*, C_4 = *0.51* and produces [C_1V_1 = 0.12*0, C_2V_2 = 0.13*0, C_3V_3 = 0.533*0, C_4V_4 = 0.51*0]* To give an authentication strength value = **0**.

The result 0 from the computation of the authentication score denote the strength of the model at the lowest, borrowing from the computation formula in Equation 4. 2 imply that scores of the model were calculated without any mitigation strategy. This simulation was done to predict the scores when the model had no mitigation strategies.

5.6 Strength of authentication of the integrated mobile identity authentication model when all values are maximum, $V_{n=1}$

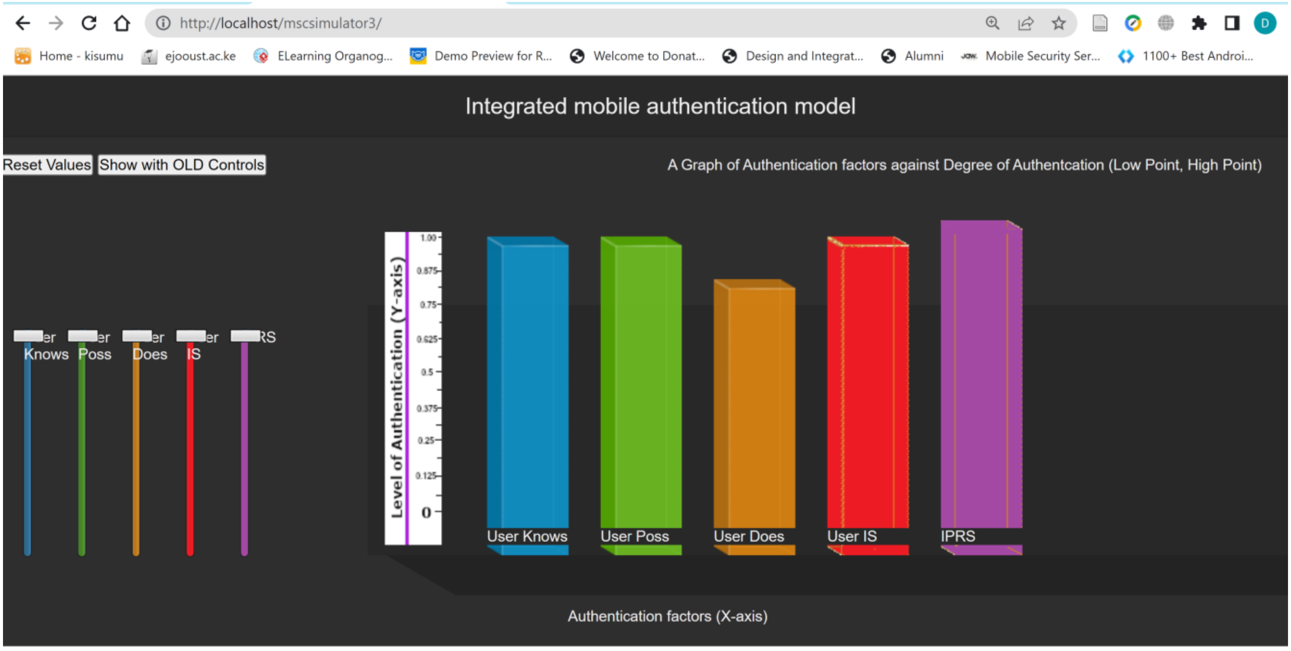


Figure 5. 4: Simulation is a simulation of the integrated mobile identity authentication model with $V_{n=1}$

When the level of authentication for all the factors are increased to their maximum against each vulnerability points, the strength is computed as below noting that *P value = 0.97:*

Figure 5.4 with values $V_{n=1}$ is an initialization of authentication factors with values: V_1 = 1, V_2 = 1, V_3 = 1, V_4 = 1, While C_1 = *0.12*, C_2 = *0.13*, C_3 = *0.533*, C_4 = *0.51*, *P* = *0.97* and produces [(C_1V_1 = 0.12*1) + (C_2V_2 = 0.13*1) + (C_3V_3 = 0.533*1) + (C_4V_4 = 0.51*1)]*0.97/4 To give an authentication strength value = **0.3136**

5.7 Interpretation of results

The results in the fours scenarios in Figure 5.1, 5.2, 5.3 and 5.4 give directions on how the models perform in cases where authentication factors were minimum or maximum. It is evident that maximum authentication score was achieved when an extra factor that performs cross-validations was introduced. The model strength was calculated to give predictions when the mitigation strategies employed were at their maximum. In particular, before the introduction of the new parameter, the sum of the authentication score was 1.293 giving an average strength factor of 0.32325 whereas when the new factor *P* was introduced, the value of the sum of authentication became 1.25421. The integrated result is expected to improve the strength of the model, the negative changed in the resultant value was an indication that the P value had significance.

The simulation process of the model considered two scenarios that predicted the strength of authentication to give a clear understanding of the objectives of the study. The simulation of the adversary model for computer device authentication presented the first scenario, the authentication parameters were initialized with one of the values equal to 1 and in another instance one of the values equal to 0. When authentication parameters were initialized in a case when one of the values equal to 0, the readings gave a strength of 0 whereas 1.293 an average strength factor of 0.32325 with one of the values equal to 1. Module identity theft would likely take place in an environment that authentication mitigation strategy does not qualify to validate factors requested, this imply that the model would be vulnerable to identity theft when one of the authentication parameters were a factor of 0. This was a similar case in the integrated authentication model where model simulation gave a reading of 0 having been factored with 0 value inputs $C_{n=x}V_{n=0}$ for all factors.

In the case when the factor P was introduced, there was a significant change in the strength of the authentication with a difference, indicating a -0.03879 factor of improvement. The introduction of P was to initiate a cross authentication in the adversary model to improve the validation of factors in the security process and a difference of -0.03879 is an indication that truly P was in deed a factor of consequence.

CHAPTER SIX: RECOMMENDATIONS AND FURTHER WORK

6.0 Introduction

This section gives reference to the results and commends the appropriate next course of action in terms of shaping the study to overcome the vulnerabilities and most importantly to contribute to solving the study problem which is mobile identity theft.

6.1 Testing for strengths and weaknesses of current mobile identity authentication model.

Desktop research from the literature review reveals a number of strengths and weaknesses of the current mobile identity authentication models. To validate the existence of weaknesses of the current mobile identity authentication models, the authentication score was computed at different vulnerability points for each of the factors, the difference from the determined score from 1 tells how far the model is from attaining maximum strength. The strengths were determined at the following scenarios; test conducted with the current model when parameters were loaded at nominal, significant and maximum values. The determined strength of authentication score realized in various scenarios noted the following: That current mobile identity authentication model had an overall strength factor of 0.3233, an average authentication strength that is earned from a combination of the four factors. It's it worth noting however that the model produces a score of zero factor when simulated at $C_{n=0}$ which produces a total and average authentication score of 0.

6.2 Testing the strength of the integrated authentication model

This test apart from computing the strength of authentication level of the integrated mobile identity model to find whether there is significance in the introduction of the *IPRS*, P in the model. The introduction of P in the determination of the authentication strength of the integrated model produces a value 0.3136 which is quite different from the previous value 0.3233 implying that generally there is less reduction in the authentication strength of the mobile authentication.

6.3 To develop and simulate the integrated mobile identity authentication model.

The development of the integrated model was built from the first and second objectives and was inspired by theory of human identification which was actualized in the current model and integrated population registration records that introduced new parameters to validate the feasibility of the integrated model.

Considering the two tests for the current and integrated mobile authentication model at nominal and maximum levels, an authentication strength of 0.3233 and 0.3136 factors respectively are produced. The second result shows a difference of 0.0097 which tells us that with the introduction of the *IPRS*, P there would be very little interference with the model given the current situation which has risen cases of attacks that manipulate the pointed vulnerabilities. The study however notes a relationship between the values of C_1V_1 and C_3V_3 such that an increase in values of C_1V_1 causes a rise in C_3V_3 and vise visor implying that where knowledge-based authentication factors are used, biometric values may have similar effect.

6.4 Effectiveness of the authentication in an integrated environment

The study hereby confirms that maximum level of authentication can only be achieved by ensuring that values of authentication factors are maximum as possible. Whereas the study also notes that introduction of the *IPRS*, P makes the model stronger since the strength do not have much reduction.

6.5 Conclusion

The study hereby confirms that maximum level of mobile authentication can be achieved by increasing the values of authentication factors, this can be attributed to increasing the size, amount or complexity of various authentication factors. The study also notes that addition of *IPRS*, P adds more strength and reduces cases or instances that reduce the strength of the authentication.

While the study also notes that PIN, passwords and graphical patterns provide similar authentication strength as fingerprint, face recognition, iris recognition, hand geometry and veins patters only when their complexity is highest and may not be used at the same time. The study however poses this as future study area to answer the observation.

REFERENCES

Ali, G., Ally Dida, M., & Elikana Sam, A. (2020a). Two-Factor authentication scheme for mobile money: A review of threat models and countermeasures. *Future Internet, 12*(10), 160.

Ali, G., Ally Dida, M., & Elikana Sam, A. (2020b). Evaluation of key security issues associated with mobile money systems in Uganda. *Information, 11*(6), 309.

Alizadeh, M., Abolfazli, S., Zamani, M., Baharun, S., Sakurai, K. (2016). Authentication in mobile cloud computing: A survey. *Journal of Network and Computer Applications*, *61*, 59-80.

Anwar, M., & Imran, A. (2015, April). A Comparative Study of Graphical and Alphanumeric Passwords for Mobile Device Authentication. In *MAICS* (pp. 13-18).

Ferrag, M. A, Maglaras, L., Derhab, A., & Janicke, H. (2020). Authentication schemes for smart mobile devices: Threat models, countermeasures, and open research issues. *Telecommunication Systems*, *73*(2), 317-348.

Archer, N., Sproule, S., Yuan, Y., Guo, K., & Xiang, J. (2012). *Identity Theft and Fraud: Evaluating and managing risk*: University of Ottawa Press.

Ashibani, Y., & Mahmoud, Q. H. (2018, November). A user authentication model for IoT networks based on app traffic patterns. In *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)* (pp. 632-638). IEEE.

CDC. (2015, November 6). Global Program for Civil Registration and Vital Statistics (CRVS) Improvement. Retrieved February 3, 2023, from https://www.cdc.gov/nchs/isp/isp_crvs.htm

Chege, A. M. (2015). *Implementation of the national population registry system in Kenya.* (Doctoral dissertation, University of Nairobi).

Chen, D., Ding, Z., Yan, C., & Wang, M. (2019). A behavioral authentication method for mobile based on browsing behaviors. *IEEE/CAA Journal of Automatica Sinica*, *7*(6), 1528-1541.

Chen, S., Wen, H., Wu, J., Xu, A., Jiang, Y., Song, H., & Chen, Y. (2019). Radio frequency fingerprint-based intelligent mobile edge computing for internet of things authentication. *Sensors 19*(16), 3610.

Communications Authority of Kenya 2021 Report. (2021, December 16). Communications Authority of Kenya. Retrieved January 6, 2022, from https://www.ca.go.ke/59-million-mobile-phone-devices-connected-to-mobile-networks-as-at-september-2021-ca-report-shows/

Cui, Z., Fei, X.U.E, Zhang, S., Cai, X., Cao, Y., Zhang, W., & Chen, J. (2020). A hybrid BlockChain-based identity authentication scheme for multi-WSN. *IEEE Transactions on Services Computing*, *13*(2), 241-251.

Davenport, T. H., Mule, L. D., & Lucker, J. (2014). Know What Your Customers Want Before They Do.

DESAI, V. T., DIOFASI, A., & LU, J. (2018, May 25). *The global identification challenge: Who are the 1 billion people without proof of identity?* WORLD BANK BLOGS. Retrieved December 12, 2022, from https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity

Enge. (2019, March 5). *31 Must Know Voice Usage Trends for 2019*. Perficient. Retrieved January 17, 2023, from https://blogs.perficient.com/2019/03/05/31-must-know-voice-usage-trends-for-2019/

Feng, T., Liu, Z., Kwon, K.-A., Shi, W., Carbunar, B., Jiang, Y., & Nguyen, N. (2012, November). Continuous mobile authentication using touchscreen gestures. In *2012 IEEE conference on technologies for homeland security (HST)* (pp. 451-456). IEEE.

Funcion, D. G. (2017). Content Analysis of Online Documents on Identity Theft Using Latent Dirichlet Allocation Algorithm. *Journal of Science, Engineering and Technology (JSET)*, *5*, 56-68.

Hammood, W. A., Abdullah, R., Hammood, O. A., Asmara, S. M., Al-Sharafi, M. A., & Hasan, A. M. (2020, February). A review of user authentication model for online banking system based on mobile IMEI number. In *IOP Conference Series: Materials Science and Engineering* (Vol. 769, No. 1, p. 012061). IOP Publishing.

Garcia, M. E., Garcia, M. E., & Grassi, P. A. (2016). Measuring Strength of Authentication. In *Advanced Identity Workshop, on Applying Measurement Science in the Identity Ecosystem: Summary and Next Steps*. US Department of Commerce, National Institute of Standards and Technology.

Information Technology Laboratory, N. (2015). *Measuring Strength of Authentication*. Paper presented at the Advanced Identity Workshop, Gaithersburg, Maryland.

Workshop retrieved from https://www.nist.gov/system/files/nstic-strength-authentication-discussion-draft.pdf

Irakleous, I., Furnell, S. M., Dowland, P. S., & Papadaki, M. (2002). An experimental comparison of secret-based user authentication technologies. *Information Management & Computer Security*.

Jia, Y.-B. (2020). Linear programming.

Jiang, C., & Li, Z. (2020). Mobile Payment Authentication. In *Mobile Information Service for Networks* (pp. 207-242): Springer, Singapore.

Kim, J., & Park, N. (2019). Lightweight knowledge-based authentication model for intelligent closed circuit television in mobile personal computing. *Personal and Ubiquitous Computing*, 1-9.

Kunda, D., & Chishimba, M. (2018). A survey of android mobile phone authentication schemes. *Mobile Networks and Applications*, 1-9.

Li, Y., Cheng, Q., Liu, X., & Li, X. (2020). A secure anonymous identity-based scheme in new authentication architecture for mobile edge computing. *IEEE Systems Journal*, *15*(1), 935-946.

LoPucki, L. M. (2001). Human identification theory and the identity theft problem. *Tex. L. Rev.*, *80*, 89.

Ma, P., Tao, D., & Wu, T. (2017, August). *A pseudonym based anonymous identity authentication mechanism for mobile crowd sensing.* In *2017 3rd International Conference on Big Data Computing and Communications (BIGCOM)* (pp. 10-14). IEEE.

Mayrhofer, R., Mohan, V., & Sigg, S. (2021). Adversary Models for Mobile Device Authentication. *ACM Computing Surveys (CSUR)*, *54*(9), 1-35.

Moskovitch, R., Feher, C., Messerman, A., Kirschnick, N., Mustafic, T., Camtepe, A., . . . Elovici, Y. (2009, June). Identity theft, computers and behavioral biometrics. In *2009 IEEE International Conference on Intelligence and Security Informatics* (pp. 155-160). IEEE.

Mufandaidza, M., Ramotsoela, T., & Hancke, G. P. (2018). "Continuous user authentication in smartphones using gait analysis." In *IECON 2018-44th Annual Conference of the IEEE Industrial electronics society* (pp. 4656-4661). IEEE.

Otor, S. U., Akumba, B. O., Idikwu, J. S., & Achika, I. P. (2020). An Improved Security Model for Nigerian Unstructured Supplementary Services Data Mobile Banking Platform. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *6*(3), 974-987.

Pedersen, C. B. (2011). The Danish civil registration system. *Scandinavian journal of public health*, *39*(7_suppl), 22-25.

Roussos, G., Peterson, D., & Patel, U. (2003). Mobile identity management: An enacted view. *International Journal of Electronic Commerce*, *8*(1), 81-100.

Tiwari, D., Singh, S. (2017). A Fusion Based Authentication Technique. *Advances in Computational Sciences and Technology, 10*(8), 2337-2342.

Trewin, S., Swart, C., Koved, L., Martino, J., Singh, K., & Ben-David, S. (2012, December). Biometric authentication on a mobile device: a study of user effort, error and task disruption. In *Proceedings of the 28th Annual Computer Security Applications Conference* (pp. 159-168).

Wangui, M., & Nzuki, D. (2021). THE EFFECT OF ELECTRONIC MONEY TRANSFER SYSTEMS ON THE FINANCIAL PERFORMANCE OF FINANCIAL INSTITUTIONS IN KENYA (CASE STUDY OF SUMAC DEPOSIT TAKING MICROFINANCE LTD). *International Research Journal of Business and Strategic Management*, *2*(1).

Weichbroth, P., & Łysik, Ł. (2020). Mobile security: Threats and best practices. *Mobile Information Systems*, *2020*, 1-15.

Waters, T. (2017). Multifactor authentication–a new chain of custody option for military logistics. *The Cyber Defense Review*, *2*(3), 139-148.

World Bank. (2018, September). Identification for Development. Retrieved February 2, 2023, from https://documents1.worldbank.org/curated/en/921761542144309171/pdf/132011-REVISED-PUBLIC-ID4D-Uganda-Diagnostic-12282018.pdf

World Bank. (2021, June.). Completeness of Birth Registration. Retrieved June 2021, from https://data.worldbank.org/indicator/SP.REG.BRTH.ZS

Wu, L., Zhang, Y., Xie, Y., Alelaiw, A., & Shen, J. (2017). An efficient and secure identity-based authentication and key agreement protocol with user anonymity for mobile devices. *Wireless Personal Communications*, *94*(4), 3371-3387.

Wyre, M., Lacey, D., & Allan, K. (2020). *Australia's Identity Theft Response System: Addressing the Needs of Victims*. Australian Institute of Criminology

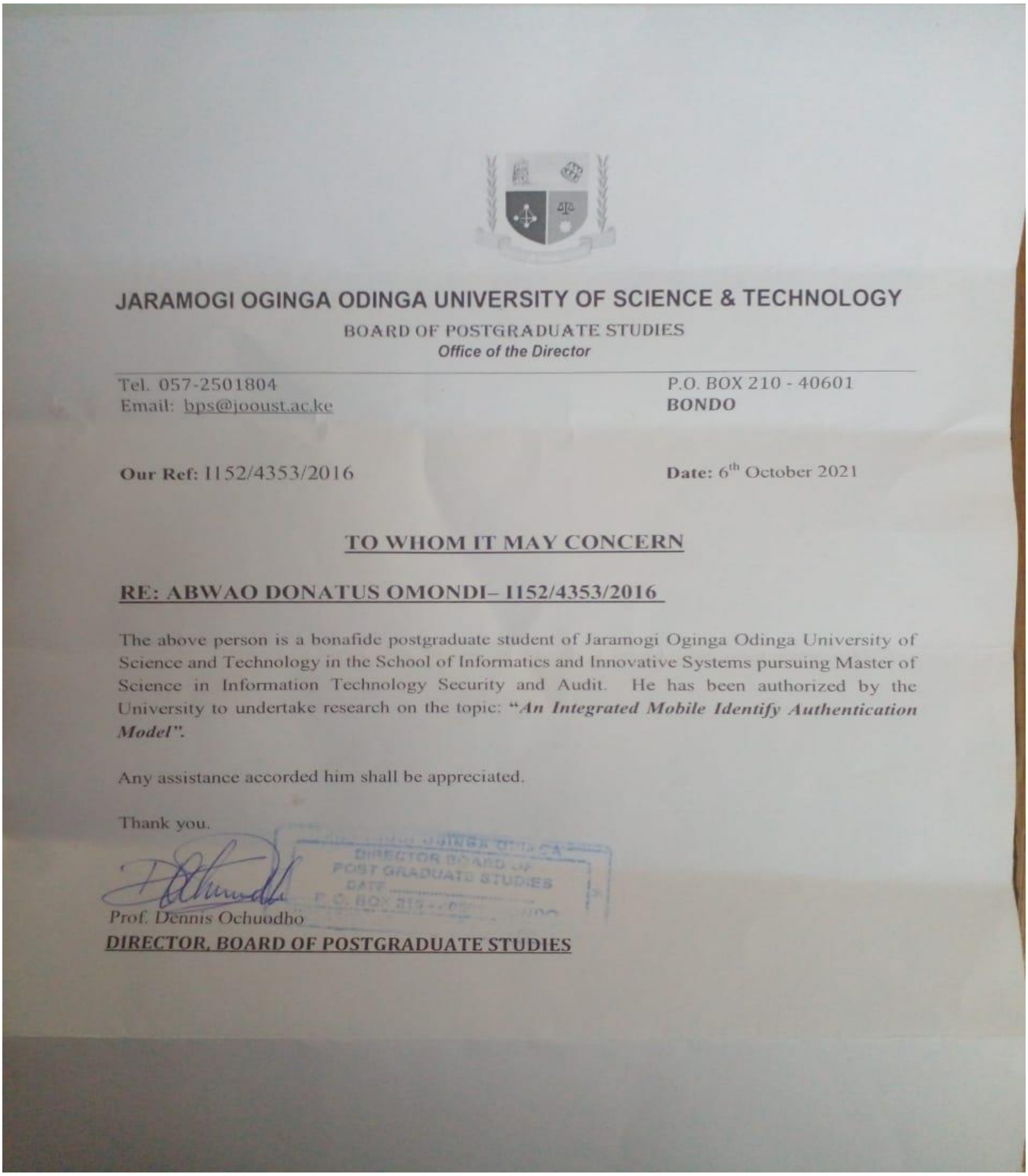
Wyre, M., Lacey, D., & Allan, K. (2020). The identity theft response system. *Trends and Issues in Crime and Criminal Justice*, (592), 1-18.

Xu, J., Xue, K., Tian, H., Hong, J., Wei, D. S., & Hong, P (2020). An identity management and authentication scheme based on redactable blockchain for mobile networks. *IEEE Transactions on Vehicular Technology*, *69*(6), 6688-6698.

Xue, K., Hong, P., Ma, C, & Sciences, S. (2014). A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture. *Journal of Computer and System Sciences,80*(1), 195-206.

APPENDICES

Appendix I: Postgraduate Clearance Letter



JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE & TECHNOLOGY

BOARD OF POSTGRADUATE STUDIES

Office of the Director

Tel. 057-2501804
Email: bps@jooust.ac.ke

P.O. BOX 210 - 40601
BONDO

Our Ref: I152/4353/2016

Date: 6th October 2021

TO WHOM IT MAY CONCERN

RE: ABWAO DONATUS OMONDI– I152/4353/2016

The above person is a bonafide postgraduate student of Jaramogi Oginga Odinga University of Science and Technology in the School of Informatics and Innovative Systems pursuing Master of Science in Information Technology Security and Audit. He has been authorized by the University to undertake research on the topic: ***"An Integrated Mobile Identify Authentication Model".***

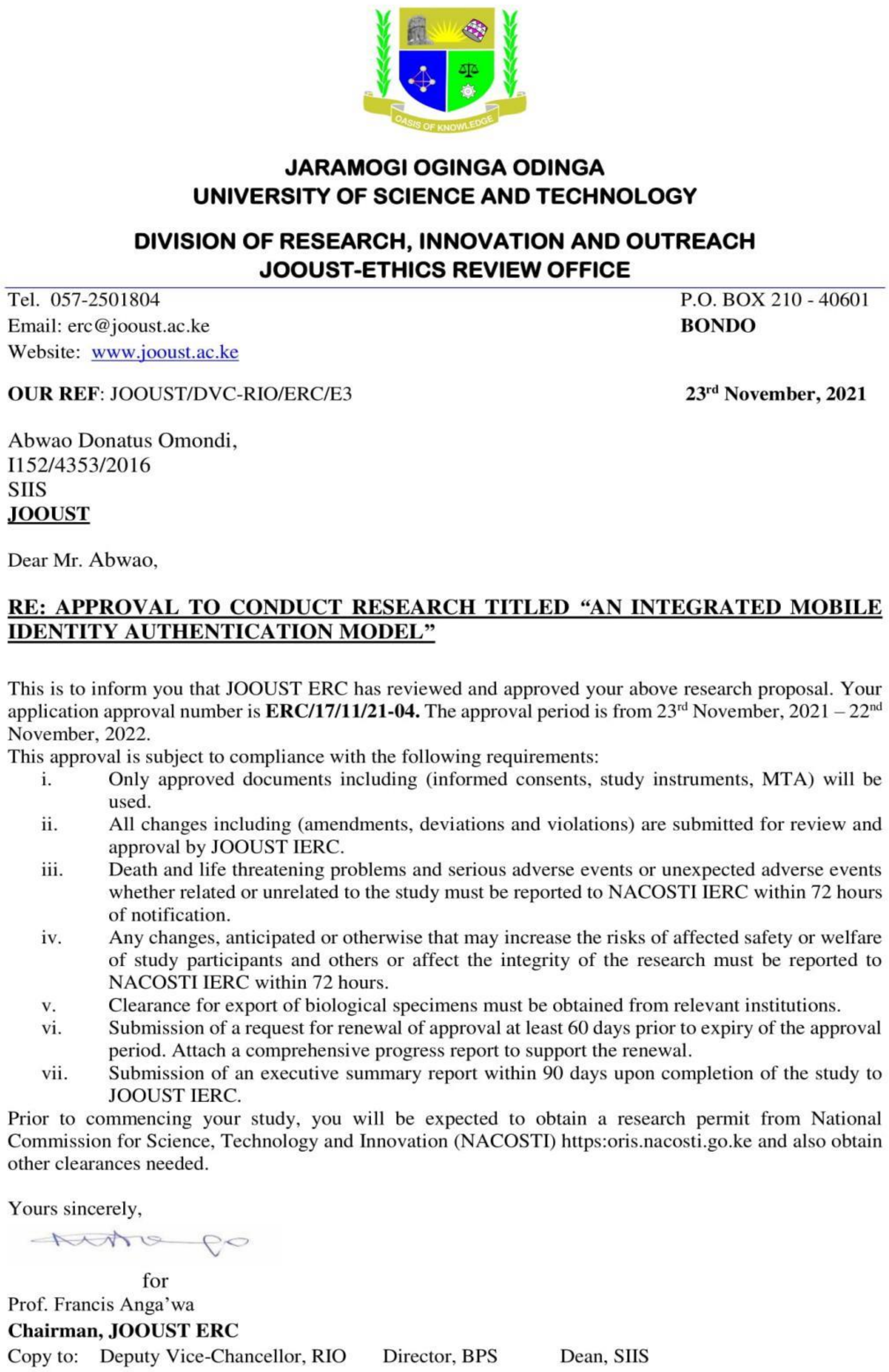
Any assistance accorded him shall be appreciated.

Thank you.

JARAMOGI OGINGA ODINGA
DIRECTOR BOARD OF
POST GRADUATE STUDIES
DATE ....
P.O. BOX 210 - 40601 BONDO

Prof. Dennis Ochuodho
DIRECTOR, BOARD OF POSTGRADUATE STUDIES

Appendix II: Ethical Review Clearance Letter



JARAMOGI OGINGA ODINGA
UNIVERSITY OF SCIENCE AND TECHNOLOGY

DIVISION OF RESEARCH, INNOVATION AND OUTREACH
JOOUST-ETHICS REVIEW OFFICE

Tel. 057-2501804
Email: erc@jooust.ac.ke
Website: www.jooust.ac.ke

P.O. BOX 210 - 40601
BONDO

OUR REF: JOOUST/DVC-RIO/ERC/E3

23rd November, 2021

Abwao Donatus Omondi,
I152/4353/2016
SIIS
JOOUST

Dear Mr. Abwao,

RE: APPROVAL TO CONDUCT RESEARCH TITLED "AN INTEGRATED MOBILE IDENTITY AUTHENTICATION MODEL"

This is to inform you that JOOUST ERC has reviewed and approved your above research proposal. Your application approval number is **ERC/17/11/21-04.** The approval period is from 23rd November, 2021 – 22nd November, 2022.

This approval is subject to compliance with the following requirements:

i. Only approved documents including (informed consents, study instruments, MTA) will be used.
ii. All changes including (amendments, deviations and violations) are submitted for review and approval by JOOUST IERC.
iii. Death and life threatening problems and serious adverse events or unexpected adverse events whether related or unrelated to the study must be reported to NACOSTI IERC within 72 hours of notification.
iv. Any changes, anticipated or otherwise that may increase the risks of affected safety or welfare of study participants and others or affect the integrity of the research must be reported to NACOSTI IERC within 72 hours.
v. Clearance for export of biological specimens must be obtained from relevant institutions.
vi. Submission of a request for renewal of approval at least 60 days prior to expiry of the approval period. Attach a comprehensive progress report to support the renewal.
vii. Submission of an executive summary report within 90 days upon completion of the study to JOOUST IERC.

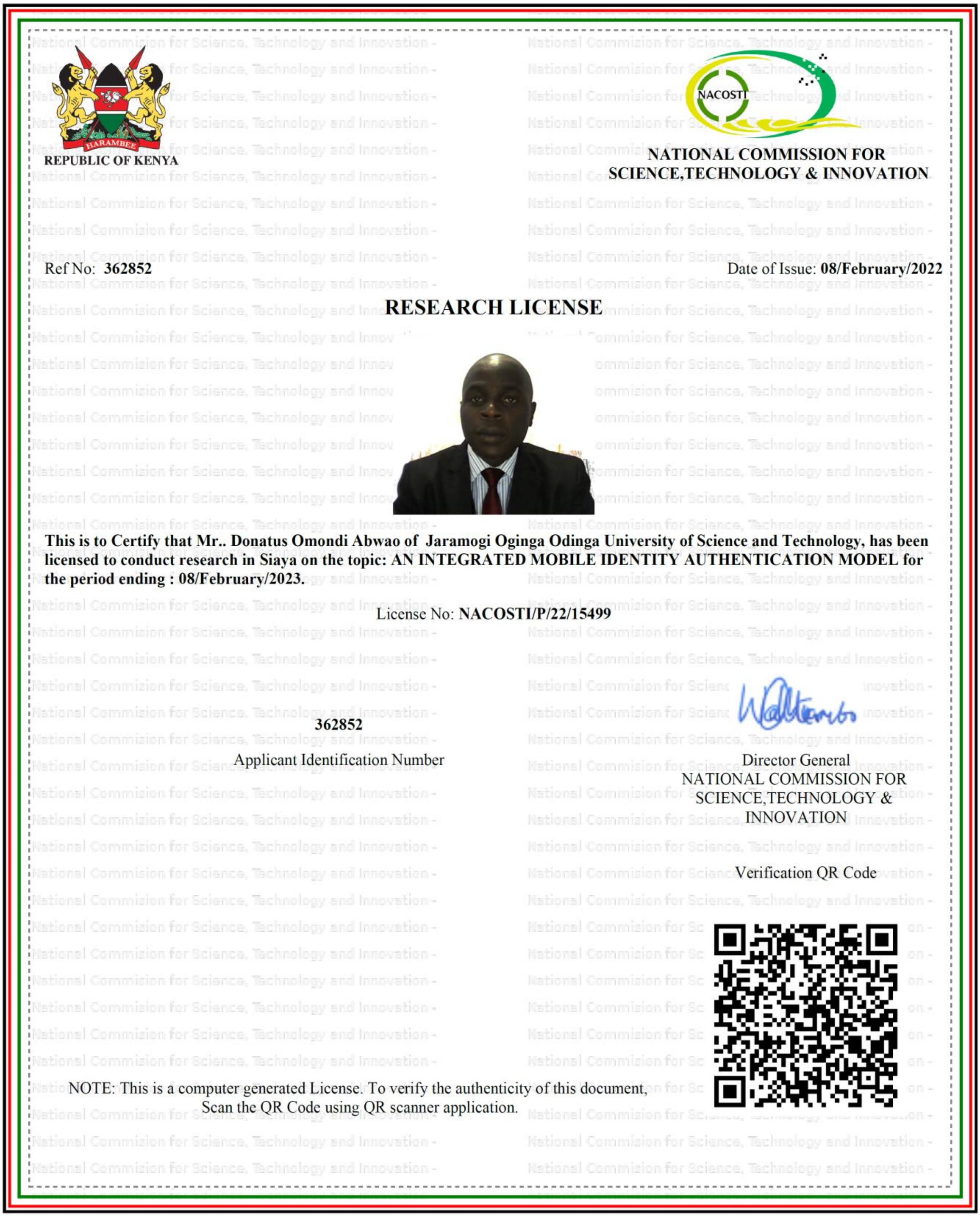
Prior to commencing your study, you will be expected to obtain a research permit from National Commission for Science, Technology and Innovation (NACOSTI) https:oris.nacosti.go.ke and also obtain other clearances needed.

Yours sincerely,

for
Prof. Francis Anga'wa
Chairman, JOOUST ERC

Copy to: Deputy Vice-Chancellor, RIO Director, BPS Dean, SIIS

Appendix III: National Commission for Science, Technology & Innovation License



REPUBLIC OF KENYA

NATIONAL COMMISSION FOR
SCIENCE,TECHNOLOGY & INNOVATION

Ref No: **362852**

Date of Issue: **08/February/2022**

RESEARCH LICENSE

This is to Certify that Mr.. Donatus Omondi Abwao of Jaramogi Oginga Odinga University of Science and Technology, has been licensed to conduct research in Siaya on the topic: AN INTEGRATED MOBILE IDENTITY AUTHENTICATION MODEL for the period ending : 08/February/2023.

License No: **NACOSTI/P/22/15499**

362852

Applicant Identification Number

Director General
NATIONAL COMMISSION FOR
SCIENCE,TECHNOLOGY &
INNOVATION

Verification QR Code

NOTE: This is a computer generated License. To verify the authenticity of this document,
Scan the QR Code using QR scanner application.