

**USING BEHAVIORAL PROFILING THROUGH
KEYSTROKES DYNAMICS AND LOCATION
VERIFICATION AUTHENTICATION AS A METHOD OF
SECURING MOBILE BANKING TRANSACTIONS**

EDWIN MBUGUA MIIRI

MASTER OF SCIENCE

(Computer Systems)

**JOMO KENYATTA UNIVERSITY OF
AGRICULTURE AND TECHNOLOGY**

2020

**Using Behavioral Profiling through Keystrokes Dynamics and Location
Verification authentication as a Method of Securing Mobile Banking
Transactions**

Edwin Mbugua Miiri

**A thesis submitted in partial fulfillment for the degree of Master of
Science in Computer Systems in the Jomo Kenyatta University of
Agriculture and Technology**

2020

DECLARATION

This Thesis is my original work and has not been presented for a degree in any other University.

Signature:
.....

Date:

Edwin Mbugua Miiri

This research has been submitted for examination with our approval as the University supervisors.

Signature:
.....

Date:

Dr. Michael Kimwele, PhD

JKUAT, Kenya.

Signature:

Date:

.....

Dr. Kennedy Ogada, PhD

JKUAT, Kenya.

DEDICATION

This work is dedicated to my parents Mr. Joseph Kibuika Miiri and Mrs. Jennifer Gaturi Miiri for the prayers and support provided all this time of research and also, to my friends, who stood by me and gave me special support during my studies.

ACKNOWLEDGMENT

I wish to acknowledge God's divine intervention while undertaking this Masters Degree, for if it weren't for His mercies and love, this could have been hard for me. I also wish to show gratitude to my parents, who always stood by me and gave me support whenever I was down, and my brothers Mr. Timothy Kibuika, Mr. Patrick Muchiri and sister Mrs. Lucy N. Kairu also my friends, relatives and my fellow work colleagues, for giving me the right encouraging words when I needed them most and understanding my schedule trying to balance work and studies, without forgetting my project supervisors, Dr. Michael Kimwele and Dr. Kennedy Ogada, for guiding me all through the research process as they dedicated their time despite their busy schedules.

TABLE OF CONTENTS

DECLARATION.....	iii
DEDICATION.....	v
ACKNOWLEDGMENT	vi
TABLE OF CONTENTS.....	vii
LIST OF APENDICES	xvi
ABBREVIATION AND ACRONYMS	xviii
ABSTRACT.....	xx
CHAPTER ONE	1
introduction	1
1.1 Introduction.....	1
1.2 Background	1
1.3 Problem statement.....	8
1.4 Research Objective.....	10
1.4.1 Main Research Objective.....	10
1.5 Specific objectives	10

1.6 Research Questions	10
1.7 Significance of the Study	11
1.8 Conclusion	12
CHAPTER TWO	13
LITERATURE REVIEW.....	13
2.1 Introduction.....	13
2.2 Information System Security	13
2.3 Threats and Vulnerabilities of mobile banking systems	16
2.3.1 Shoulder surfing.....	16
2.3.2 Key logging.....	16
2.3.3 Brute-force attack.....	17
2.3.4 Dictionary attack	17
2.3.5 Phishing.....	17
2.3.6 Guessing attack	18
2.4 Existing Techniques for Authenticating Users	18
2.4.1 Personal Identification Number (PIN)	19
2.4.2 Password Authentication.....	20

2.4.3 Recognition-based passwords Authentication	20
2.4.4 Token based authentication.....	20
2.4.5 Transparent authentication systems	21
2.5 User Profiling.....	27
2.6 Location Authentication.....	29
2.7 User Profiling and Location Authentication	30
2.8 Mobile Banking.....	32
2.9 Hindrances in the uptake of mobile banking.....	33
2.9.1 Use of a Trial Application.....	33
2.9.2 Relative advantage	33
2.9.3 Simplicity/complexity	34
2.9.4 Compatibility	34
2.9.5 Evaluation of existing authentication methods	37
2.9.6 Personal Identification Number (PIN)	37
2.9.7 Password Authentication.....	38
2.9.8 Recognition-based passwords Authentication	38
2.9.9 Token based authentication.....	38

2.9.10	Transparent authentication systems	39
2.10	Key Research Gaps based on the Authentication Evaluation.	42
2.11	Conceptual Framework of the study.....	44
2.12	Conclusion.....	45
CHAPTER THREE		46
RESEARCH METHODOLOGY		46
3.1	Introduction.....	46
3.2	Research Methodology.....	46
3.3	Target Population	47
3.4	Sampling Technique.....	47
3.5	Research Design.....	49
3.6	Experimental Design.....	49
3.6.1	Scenario 1	49
3.6.2	Data collection procedures	50
3.6.3	Scenario 2.....	50
3.6.4	Data collection procedures	52
3.7	Sample Size.....	52
3.7.1	3.8 Data Collection Tool	53

3.7.2 Survey	54
3.7.3 Questionnaires.....	55
3.8 Conclusion	56
CHAPTER FOUR.....	57
RESULTS AND DISCUSSION	57
4.1 Introduction.....	57
4.2 General survey respondents' information.	57
4.3 Discussion and Analysis of survey questionnaire responses.	80
4.3.1 The Use of Smartphones in Mobile Banking.....	80
4.3.2 Mobile Banking Security	81
4.3.3 Mobile Banking Acceptance.....	83
4.3.4 Existing mobile banking authentication methods	84
4.3.5 Threats and vulnerabilities of mobile banking systems	84
4.3.6 Mobile Banking Application Updates.....	85
4.3.7 Change of Authentication Details	85
4.3.8 Suspicious activity on their mobile banking	86
4.3.9 Behavior profiling and location verification authentication	86

4.3.10	Enhancing security of mobile banking.....	88
4.4	Conclusion	90
CHAPTER FIVE.....		91
ALTERNATIVE METHOD FOR SECURING MOBILE TRANSACTIONS		91
5.1	Introduction.....	91
5.2	5.2 Behavior profiling and location verification authentication	92
5.3	5.3 Composition of the proposed authentication method.....	94
5.3.1	5.3.1 User Behavioral profiling.....	95
5.3.2	5.3.2 Users Location Verification	95
5.3.3	5.3.3 Keystroke Capture.....	96
5.3.4	5.3.4 Location Capture	97
5.3.5	5.3.5 Training Phase.....	98
5.4	Validation of the proposed method through an Experiment	102
5.4.1	Participant Profile.....	102
5.4.2	Experiment 1	102
5.4.3	Results	102
5.5	Discussion and Analysis	106

5.5.1 Experimental 2	112
5.5.2 Results	113
5.5.3 Discussion and Analysis	121
1) Interfaces of the proposed behavioral profiling and location verification authentication	124
5.6 Conclusion	129
CHAPTER SIX	131
SUMMARY, CONCLUSION AND RECOMMENDATIONS.....	131
6.1 Summary	131
6.2 Conclusion	132
6.3 Recommendations	134
6.3.1 User Unique Identity	134
6.3.2 User location Verification	135
6.3.3 Cost of Implication.....	135
6.4 Area of further research	135
REFERENCES.....	137
APPENDICES	162

LIST OF TABLES

Table 2.1: Authentication Evaluation Table.....	39
Table 4.1: Survey Participation	57
Table 4.2: Gender Distribution.....	58
Table 5.1: Sample user Training Results.....	110
Table 5.2: Sample user Testing Results	111
Table 5.3: The use of proposed authentication method on mobile banking.....	114
Table 5.4: Sample Data from the experiment.....	115
Table 5.5: Sample user Training Results.....	116
Table 5.6: Sample user Testing Results	117
Table 5.7: User typing and anomaly detection.....	117

LIST OF FIGURES

Figure 2.1: Biometric Authentication Types	23
Figure 2.2 : Conceptual Framework.....	44
Figure 4.1: Age distribution.....	58
Figure 4.2: Educationlevel distribution.....	59
Figure 4.3: Smartphone ownership.....	60
Figure 4.4 Bank account ownership.....	61
Figure 4.5 Mobile banking subscription	62
Figure 4.6 Mobile banking usage.....	63
Figure 4.7: Interval of mobile banking usage	64
Figure 4.8 : Reasons that hinder adoption.....	65
Figure 4.9 : Concerns in mobile banking adoption.....	66
Figure 4.10: Smart phone skills and expertise	68
Figure 4.11: Mobile banking experience	69
Figure 4.12: Security in mobile banking service	70
Figure 4.13: Securitfeatureomobile banking.....	72
Figure 4.14: Mobilebanking service update.....	73
Figure 4.15: Change of authentication details	74
Figure 4.16: Suspicious activity on mobile banking account detected.....	75
Figure 4.17: Capturing user behavior and location verification to secure mobile banking transactions	
Figure 4.18: Using behavior and location verification to secure mobile banking transactions	78
Figure 4.19: Using behavior and location verification to secure mobile banking transactions	79
Figure 5.1 : User Profiling	95

Figure 5.2 : Proposed alternative authentication method.....	101
Figure 5.3 : `Respondents' Authentication complexity	103
Figure 5.4: PIN/Password as a strong authentication method	104
Figure 5.5: Respondents regular change of PINs	105
Figure 5.6: Respondents view on location of the transaction	106
Figure 5.7: Use of user profiling and location verification.....	113
Figure 5.8: Mobile Banking Authentication Using Behavioral Profiling and Location Verification.....	120
Figure 5.9: Respondents Concern in using the proposed authentication method	121
Figure 5.10: User Registration	125
Figure 5.11: User Account Confirmation	125
Figure 5.12: User Authentication.....	126
Figure 5.13: User Profiling Authentication.....	127
Figure 5.14: User Location Verification	128
Figure 5.15: :Successful Login	128
Figure 5.16: Unsuccessful Login	129

LIST OF APPENDICES

Appendix A Survey Questionnaire	162
Appendix B: Letter of introduction.....	170

ABBREVIATION AND ACRONYMS

APT	Advanced Persistent Threats
ATM	Automated Teller Machines
CBK	Central Bank of Kenya
CCB	China Construction Bank
DNA	Deoxyribonucleic acid
EER	Equal Error Rate
FAR	False Acceptance Rate
FRR	False Rejection Rate
GPS	Global Positioning System
GSMA	Global System for Mobile Communications
ICBC	Industrial and Commercial Bank of China
ICSIRT	Industry Computer Security and Incident Response Team
ICT	Information and Communication Technology
ID	Identity document
IEC	International Electro technical Commission
IP	Internet Protocol address
IS	Information Systems
ISO	International standard organization
IT	Information technology
KCB	Kenya Commercial Bank
MAC	Media access control address
M-banking	Mobile banking
M-pesa	Mobile money

OTP	One time password
PIN	Personal Identification Number
SIM	Subscriber identification module
SMS	Short Message Service
SVM	Support vector machines
TESPOK	Technology Service Providers of Kenya
USA	United States of America

ABSTRACT.

With the current rise of security attacks existing authentication methods on mobile phones such as PINs and passwords are becoming ineffective. Researchers have suggested various alternative authentication solutions such as the use of multi-level authentication, graphical password or biometric password. Behavioral profiling refers to distinguishing users based on their unique activities such as walking, voice or typing. Location authentication is a method of providing authorization to users based on the verification of their location. The objective of this research was to evaluate the limitations of existing authentication methods that have been proposed recently by researchers in their literature and to propose an alternative authentication method based on user behavioral profiling and location based verification characteristics. This research identified the threats and vulnerabilities of mobile banking systems and examined where these authentication methods had been applied. Traditional authentication mechanisms like PINs and passwords being the most widely used authentication techniques suffer from limitations and drawbacks such as shoulder surfing, brute force, guessing attack and phishing attacks. Over a period of 30 days a study was conducted to examine the use of PINS and their limitations and the use of PINs incorporated with behavioral and location authentication in mobile banking and an analysis of the data collected from a sample size of 153 out of 247 through experiments and online surveys who comprised of staffs from Kenya Commercial Bank (KCB) head office branch at Kencom. This study evaluated existing authentication methods and their performance summarized. To address the limitations of PINs this work proposed an alternative authentication method that uses behavioral profiling using Keystroke dynamics and location data. To evaluate the proposed authentication method experiments were done through use of a prototype android mobile banking application that captured the typing behavior while logging in and location data from 60 users. The experiment results were lower compared to the previous studies provided in this paper with a False Rejection Rate (FRR) of 5.33% which is the percentage of access attempts by legitimate users that have been rejected by the system and a False Acceptance Rate (FAR) of 3.33% which is the percentage of access attempts by imposters that have been accepted by the system incorrectly, giving an Equal Error Rate (EER) of 4.3%. The outcome of this study demonstrated keystroke dynamics and location verification on PINs as an alternative authentication of mobile banking transactions building on current smartphones features with less implementation costs with no additional hardware compared to other biometric methods

CHAPTER ONE

INTRODUCTION

1.1 Introduction

This chapter gives an overview of the security of information systems and their authentication. It starts by highlighting the most widely used techniques of user authentication and their limitations. It further explores on the need to have a reliable user authentication. Current existing biometric user authentication techniques are also discussed together with their categories and how they are gaining popularity in giving an extra level of security compared to the traditional PIN and Passwords. A look into how the information systems have extended into the emerging developments of mobile technology are given focusing in the banking sector and the security concerns. Towards the end of the chapter the problem statement of this research is also covered as well as the research objective followed by the intended research questions from the specific research objectives. This research also gives the significance of the problem and proposes suggested authentication alternative.

1.2 Background

The need to secure private or sensitive information in mobile devices is one of the main challenges in information security. However, usual methods such as passwords and tokens fail to keep up with the challenges presented due to many drawbacks (Alariki & Manaf, 2014). A report by Javelin Strategy & Research (2017) showed that 15.4 million consumers were victims of identity theft or fraud in 2016 this was up by 16 percent from 2015, and the highest figure recorded since the firm began tracking fraud instances in 2004. Account takeover fraud where thieves used stolen login information to access a

consumer's accounts rose 31 percent. Access to information is not limited to personal information only. Users increasingly need to access information for business reasons. Access to business data from mobile devices requires secure authentication, but traditional password schemes based on a mix of alphanumeric and symbols are cumbersome and unpopular, leading some users to avoid accessing business data on their personal devices altogether (Trewin et al., 2012). Security in computer systems aim to provide Confidentiality, Integrity and Availability in Information Systems in order to serve the information technology user. Solms & Niekerk (2013) defined Information security as the protection of information, which is an asset, from possible harm resulting from various threats and vulnerabilities.

The concept of information security and its relevant practices and procedures is constantly evolving to suit the fluid business environment (Reid & Niekerk, 2014). User authentication is a prerequisite for meeting basic security requirements like access control through use of PINS, passwords, tokens and biometric as methods of authenticating users in information systems are gaining in popularity.

Currently the most widely used authentication techniques including PINs and patterns for mobile devices are vulnerable to attacks such as shoulder surfing, key logging, brute force, guessing attack and phishing attacks (Alzubaidi & Kalita, 2016). Classification of these limitations fall into two categories: external factors and internal factors. The external factors refer to impostors and malware techniques. The authentication scheme like password or PIN based have proven to be vulnerable to different forms of observation attacks such as, video-recording, key logging or shoulder surfing attacks

(Joy & Jyothi, 2016). While internal factors mainly refer to users' habits like unsafe behaviors.

In the traditional authentication scheme, the user provides the username and static password to service provider, but there are some inherent shortcomings of this method static passwords maybe forgotten users have difficulty in remembering complex and random passwords. Regarding user authentication on mobile phones, the challenges of passwords and PINs still exist (Liu et al., 2013). To overcome these challenges of passwords and PINs based authentication, research is being done on biometrics based methods for authenticating users. The essential reason of biometric verification is that everybody is unique. Biometric recognition is very important for security purposes as researchers Gundecha and Mohan (2016) found out in their study that it was used for variety of applications. Currently biometric user authentication techniques can be categorized into two categories namely: physiological and behavioral approaches. Physical biometric traits based on physiological characteristics of people also include iris or face recognition. Behavioral modalities in contrast to fingerprint recognition require subjects to perform a behavior over time, like gait or keystroke recognition (Shih et al., 2015).

The main goal of applying biometrics to user authentication is to authenticate legitimate users and detect impostors in terms of users' physiological or behavioral characteristics. Unlike passwords, for which only an exact match is acceptable, biometrics typically

seek a good but not necessarily perfect match for authentication. Smartphones have become one of our daily necessities. They are used to store personal data and handle private communication. Unfortunately, there are some privacy and security issues along with the use of smartphones; for example, a user's private data, e.g., photo, contacts, and bank details, can be compromised, if his/her smartphone without any protection is stolen or lost. Secret knowledge-based approaches, e.g., password or PIN, are commonly used for authentication. However poor use of password or PIN may lead to great security breaches (Spolaor et al., 2016).

The main advantage of biometric technologies is that users don't have to remember or carry anything at the time of authentication. Another advantage of using biometric is that biometrics provide highest level of security and very hard to forge. Biometric technologies are gaining popularity these days because they provide an extra level of security when these technologies are used in conjunction with traditional methods for authentication. Although Physiological biometrics are considered to be more robust and secure, they are expensive to use because specialized hardware is needed to detect the features.

On the other hand, behavioral characteristics are cheaper than physiological characteristics because additional hardware is not required. Behavioral biometrics rely on data captured as the user naturally interacts with the device. As a result, behavioral biometrics provide cost-effective and intuitive access control (Al Abdulwahid et al., 2016). Addition of location information in authentication helps in making sure that only

the authorized individual accesses secured information and guarantee that only devices positioned in specific zone can receive secured information (Shivhare et al., 2014). User location cannot be used for authentication on its own, but combining it with any of the other authentication factors can boost security and create Multi-Factor Authentication (MFA). MFA is the process of authenticating a user after successfully presenting several evidences to an authentication system through an active authentication process, which consists of user credentials, passwords, biometrics, cognitive behavior metrics, software and hardware devices among others (Dasgupta et al., 2017).

A study by Ponemon Institute (2015) indicates that many organizations have lost billions of dollars as a result of information breaches or information violations. These breaches have also had some negative effects on customer trust. Organization investing in security measures can be able to reduce the frequency and intensity of computer security related losses. Security measures, such as an improved access control system, may significantly reduce the loss. The development of mobile technology has allowed the potential of information systems to extend information access to mobile phones. With the growing adoption of smart mobile devices, such as smartphones and tablets, is fundamentally changing the way how business is conducted. New mobile technologies exert a significant influence on individuals, organizations, and society at large (Fischer & Smolnik, 2013). Over the past decade the application of mobile devices such as smartphones and tablets are explosively growing.

The smart mobile devices currently being available in the market are having much more computing powers and turning into powerful general purpose computing platform (You, et al., 2015). As the mobile platform becomes extremely popular, the mobile privacy and

security issues are also increasing; mobile flaws and threats are rapidly growing (Aldhaban et al., 2015). Widespread usage of mobile devices in conjunction with malicious software attacks calls for the development of mobile-device-oriented mechanisms aiming to provide strong authentication and transaction security (Ortiz-Yepes et., 2014). After the point-of-entry authentication stage at the beginning of a session, using modalities such as a PIN or password, the user of the device can perform almost all tasks without having to periodically re-authenticate to re-validate the user's identity (Crawford et al., 2013). As a result, there is an urgent need to verify the identity of the current user of a mobile device. A mobile phone is able to gather a user's behavioral data without requiring deliberate actions from the user and without requiring additional hardware.

Using behavioral profiling data on user behavior is gathered in the background without requiring any dedicated activity by the user, by regularly and periodically checking user behavior in order to continuously monitor the protection of the mobile device. Using behavioral profiling we refer to something the mobile phone user does such as typing, gait, application usage, voice or signature.

The use of Behavioral profiling is presented as a suitable method and is more commonly used for transparent and continuous authentication and providing usability (Clarke, 2011). Also adding on the security of information from the applications used on smart phones it is possible to ensure that they can only be accessed within specified areas set by the providers. Addition of location information in security mechanisms helps in making sure that only the authorized individual accesses secured information and guarantee that only devices positioned in specific zone can receive secured information (Shivhare et al., 2014). This means that if one wants to access his/her account then they

must be near a certain building or locality, through use of location based verification. Location verification can be used as a common authenticator for all systems the user accesses, that unlike most other types of authentication information, the location detail assures that the user conduct administrative functions only from authorized locations. These functions can be, transfer of funds, alter system files, controlling sub-user's access to resources, accessing files, transactions across the network, uploading the current location information, and downloading confidential files from secured web server, etc. Security remains a key factor especially now that Banks and other businesses are increasingly investing in mobility. Among the investment returns that banks expect to obtain are an increased customer fidelity, an increased user base, and additional revenue obtained from new services and from exploiting a better understanding of customer data (Fenu & Pau, 2015). It is due to the sensitivity of the user information that organizations aim at securing their systems.

This research focuses on the banking sector majorly on mobile banking and how using behavioral profiling and location verification can be used as an alternative to authentication banking transactions. Mobile banking refers to the use of a mobile device to deliver banking services to the customers. Mobile banking also abbreviated as (m-banking) and Internet banking are very similar, except you are using a smart phone instead of using computer to open bank website. Widespread usage of mobile devices in conjunction with malicious software attacks calls for the development of mobile-device-oriented mechanisms aiming to provide strong authentication and transaction security (Ortiz-Yepes et al., 2014). The success in increasing m-banking uptake amongst clients will ultimately rely upon how secure the financial data and transactions are. Jeong & Yoon (2013) found that because of the variety of mobile devices and platforms currently in the market, preparing the security on mobile banking is not easy at all.

A survey by (Islam, 2014) revealed that 31% of mobile banking customers are ready to pay for added security features, 63% are eager to switch accounts for better security features, the 71% of the rest are ready to switch accounts for guarantees losses According to Sarlak et al. (2012) in 2010 mobile banking was performed mostly via SMS or through the mobile web application. Banking services by means of mobile phones cause lower costs, plus ease of access and swiftness in providing services. So, banks are very eager to expand their market through mobile banking. Mobile banking has been seen as one of the most value-added application and vital mobile service available. In the study conducted by Singh (2013) the main business drivers that contributed towards the evolution of mobile banking were identified as: Customer experience, Customers are getting familiarity for having access to information at their convenience anytime and anywhere.

A mobile phone in most cases is always with the customer. As such it can be used over a greater geographical area. With the mobile device able to report your location, security can be improved by integrating location based intelligence with password authentication (Oluoch, 2014).

Through this research the objective will be to evaluate some of the existing authentication methods that have been proposed recently by researchers in their literature and to propose an alternative authentication method based on user behavioral profiling and location verification characteristics.

1.3 Problem statement

With rise of technology Cyber-attacks against individuals, businesses, and government are also on the rise increasing in frequency and sophistication, mobile devices are now

considered by threat actors to be one of the weakest links in the IT infrastructure of most enterprises. Security is a key issue when it comes to smart phone applications due to the sensitivity of the information being exchanged. According to Lin et al. (2015) they found that smartphone applications containing sensitive personal or company data are at risk when targeted by attackers. The need to secure private or sensitive information in mobile devices is one of the main problems in information security. Smartphones provide a central place of users' private information and are thus a primary target for cyber-attack, with the main goal of the attacker being try to access and exfiltrate the private information stored in the smartphone without detection (Mirsky et al., 2017).

Traditional authentication mechanisms like PINs, patterns and passwords being the most widely used authentication techniques suffer from well-known limitations and drawbacks in the security community such as shoulder surfing, key logging, brute force, guessing attack and phishing attacks Alzubaidi & Kalita (2016), Meng et al., (2018). As a response to such incidents security researchers have started to investigate other alternative authentication methods.

Location information obtained from mobile phones can be a potential solution for location-based authentication and authorization. Mobile phones can be used to detect and send the location of a particular user to back-end servers, which verifies the location as a factor for authorization and when you combine with a user's unique behavior profile creates an authentication alternative that is challenging to bypass. Through this research the objective will be to evaluate some of the existing authentication methods that have been proposed recently by researchers in their literature and to propose an alternative authentication method based on user behavioral profiling and location verification characteristics.

1.4 Research Objective

1.4.1 Main Research Objective

The objective of this study was to propose a method of securing mobile transactions using behavior profiling through use of keystrokes and location verification.

1.5 Specific objectives

1. Evaluate the existing mobile banking authentication methods and examine where these authentication technologies have been applied
2. Examine threats and vulnerabilities of mobile banking systems.
3. Propose use of behavior profiling through use of keystrokes and location verification as an alternative authentication method of securing mobile transactions and evaluate the proposed authentication technique.

1.6 Research Questions

- 1. What are the existing mobile banking authentication methods and Where have these authentication technologies been applied?**
- 2. Which are the threats and vulnerabilities of mobile banking systems?**
3. How does use of behavior profiling and location verification authentication offer an alternative method of securing mobile transactions and How to evaluate the proposed authentication technique?

1.7 Significance of the Study

According to a 2013 study, 5.6 million smartphone users experienced “undesirable behavior” on their smartphones (Catherine & Divya, 2013). Despite the number of people experiencing undesirable behavior, 64% of smartphone users choose not to protect their phones with passcodes for reasons ranging from the “cumbersome” task of entering a password every time a user wants to use the phone to not being “worried about the risk (Kayacik et al.,2014). Since the majority of smartphone users are unwilling to lock their phones and are thus susceptible to experiencing undesirable behavior, there is an obvious need to develop technologies to augment smartphone user security. One of the technologies to address user security on mobile phones is use of behavioral biometrics.

Use of behavioral biometrics involves uniquely identifying and measurable patterns in human activities unique biological characteristics of an individual to verify that he/she is who is says he/she is .Behavioral biometrics authentication makes it harder for someone with malicious intent to successfully capture a natural motion compared to a password or even a fingerprint. (Maghsoudi & Tappert, 2016).

Many people are using their mobile devices such as smart phones to access various online services on a daily basis. In particular, mobile banking applications are increasingly becoming popular. Many banks are offering mobile banking services which allow bank customers to check balance in their personal account, to transfer funds between accounts and make online payments anywhere and at any time by simply using mobile banking applications installed on their mobile devices (Elkhodr et al., 2012). Panja et al. (2013) found that mobile banking applications have attracted the attention of many cyber criminals and poses as a security concern.

The rest of the paper is organized as follows. Chapter 2 highlights the threats and vulnerabilities of mobile banking systems as well as existing techniques for authentication together with the proposed attention method and evaluation of existing authentication methods. Chapter 3 covers on the research methodologies and the data collection tools used for this research. Chapter 4 covers on the analysis of the results and discussion obtained from the survey findings. Chapter 5 covers the alternative authentication method for securing mobile transactions, composition of the proposed authentication method as well as its validation, discussion and analysis of both experiments carried out. Chapter 6 gives the summary, conclusion and recommendations for further research.

1.8 Conclusion

This chapter covered the background of information security and the various authentication methods that have been used. The problem statement of this research was also highlighted together with the research objectives both the main and specific objectives and the formulated research questions that this research aimed to answer. The implication and contribution of this paper seeks to build upon on the knowledge of mobile banking security as it proposes use of keystroke dynamic and location verification authentication as an alternative method of securing mobile transactions. This research will make a significant contribution to providing needed information to security professionals on improving security to information system factoring biometric authentication as an alternative and also to the researchers and students on the academic impact of the proposed research to adding knowledge on the current evaluation of security features and possible recommended future areas of research.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter starts by introducing the concept of information security and its importance to systems. It then proceeds to highlight the threats and vulnerabilities that are prone to systems once attackers get access to them and how the rise of mobile phones are emerging as the new target to these threats. To counter the threats this chapter also examines the various techniques for authenticating legitimate users aide from the traditional use of PIN and password to use of biometrics. Following the rise mobile phones and usage across various industries this chapter focuses on its impact and hindrances in mobile banking with attention to security based on the kind of information exchanged.

2.2 Information System Security

Information security is achieved by implementing a suitable set of controls. These controls can be embodied in various forms, ranging from policies, processes and procedures to organizational structures and software and hardware functions (ISO/IEC 27002:2013). ISO/IEC 27002 (2014) defines information security as a process involving the protection and preservation of the confidentiality, integrity and availability of information and ensuring that entities can be held accountable. Confidentiality is keeping information from those who do not have right to access information.

Integrity on the other hand ensures that aspects the information must not be altered without any permission from the owner of the information. Availability refers to in making the information readily available when it's needed by all authorized individuals, entities, or processes (Nancyia et., 2014).

Zhou & Huang (2012) in their study termed Security in computer systems to be concerned with protecting resources from unauthorized access while ensuring legitimate requests were satisfied all the time. With the development of information technology, especially with the wide popularity of mobile devices, more and more people are concerned about information security. Information security is a crucial component in the success of any organization, regardless of what environment the organization functions in. Information and Communication Technology (ICT) has become so pervasive in most organizations, that business functions are almost completely dependent on it. ICT is the platform that enables most of the organization's information processing and storage. Due to its high importance, the information and related ICT systems should be adequately protected by the process of information security management (De Lange et al., 2016). There are various established mechanisms to authenticate users, but by far the most widely deployed is the authentication by username and password. For example, short passwords can be easily broken using brute force techniques due to the increased computation power of today's personal computers or rented services in the Cloud.

Asif et al. (2017) defined authentication as the use of one or more mechanisms to confirm that you are the authenticated user claimed to be. Any given system faces challenges of threats and vulnerabilities. A threat may be defined in two ways:

techniques that attackers use to exploit the vulnerabilities in your system components or impact of threats to your assets (Jouini et al., 2014). While Cirnu et al.(2018) defined vulnerabilities as flaws or weaknesses in system security procedures, design, implementation, or internal controls. According to Abdellaoui et al. (2015) authentication can be distinguished into three types namely: simple, strong and single sign-on. In simple authentication the users must provide a single factor for authentication. Whereas in strong authentication the user uses at least two factors to access to resources. In Single Sign-on a user is allowed to access to multiple applications or services by means of only one authentication. Abdellaoui et al. (2015) later in their study generalized that authentication is based on something the user knows such as the (username and password), something the user has for example (smartphone, debit card), and something the user is biometric identifier capturing (fingerprint, iris, keystrokes, and walking pattern).

With the current rise of security attacks on mobile phones traditional methods to authenticate users are becoming ineffective due to their limitations such as being easily forgettable, discloser, lost or stolen. In the banking sector mobile Banking is becoming an important tool that allows users to access their information through their mobile device and it is with this comes the need of having a reliable user authentication to protect user's private information. Mobile banking is a revolution that is driven by the world's one of the fastest growing sectors mobile communication technology. The implications of the results provide practical recommendations to all concerned mobile banking security challenges (Nosrati & Bidgoli, 2016).

A reliable user authentication aims to verify legitimate users and prevent unauthorized access to an application. According to Visa Europe (2015) the new generation of banking customers would rather use biometric security devices than PINs and passwords

for authentication with 75 per cent of 18 to 24-year-olds having no problem using biometric security, and 69 per cent expecting it to be faster and easier than a password or a PIN. With the traditional authentication methods if an attacker knows a user's PIN or screen lock, the attacker can exploit the phone to steal sensitive data or conduct illegal activities using the phone. To prevent this You et al., (2015) had proposed the need to enhance the security of smartphones beyond use of PIN and passwords.

2.3 Threats and Vulnerabilities of mobile banking systems

Systems that require its users to authenticate themselves using the traditional authentication scheme where the user enters a password of their preference are weak to attacks such as shoulder surfing, key logging ,Brute-force attack ,dictionary attack and phishing.

2.3.1 Shoulder surfing

This is term that refers to a person using direct observation to gain information about, for example, another person's password. As the term suggests, this can be done by looking over the person's shoulder as they type in their password Wakabayashi et al., (2017). Someone can learn key presses by just looking at your fingers, even if the details are hidden by asterisks. Even users who are not actively out to exploit accounts may get tempted on learning the login details and passwords of people.

2.3.2 Key logging

A key logger is usually a hardware or software that is installed on a computer or mobile phone that tracks the keystrokes on a keyboard normally it is done in a secretive way. It is typically done without the knowledge of the person using the keyboard that their

actions are being monitored. A key logger recorder can record instant messages, e-mail, and any information a user types at any time using your keyboard (Bhave et al., 2016).

2.3.3 Brute-force attack

Yasin & AbuAlrub (2016) defined brute-force attack as an attack where software or tools are used to guess password and get access to sensitive data, in this attack, series of all possible passwords are sent in an attempt to guess the used password and obtain access. When the password is weak, it can be broken easily by hackers by using brute-force attack. Brute force attacks involve trying passwords or PINs combining with provided usernames until they gain access basically simple hit and trial method.

2.3.4 Dictionary attack

A pre-known list of passwords is gathered together to form a password dictionary file. Dictionary attacks leverage such password dictionaries and automate the attempt of breaking in to password-protected applications and systems by trying each word/password listed in the password dictionary. Attackers build comprehensive password dictionaries by compiling passwords from various dictionaries and password leaks (Madiraju, 2014).

2.3.5 Phishing

Carella et al. (2017) in their study defined phishing as a criminal activity where social engineering techniques and technology were used to obtain personal information without one's consent. Phishing attacks aid criminals in a wide range of illegal activities, including identity theft and fraud. They can also be used to install malware and attacker tools on a user's system. Although the majority of phishing attacks are widespread and

focus on financial gain, targeted phishing attacks also exist. These attacks are widely known as spear-phishing and have been used in a large number of sophisticated attacks against government, military and financial institutions. Shahriar et al. (2015) found out that phishing attacks target commonly popular financial organizations. A survey found that 71% of phishing attacks were related to spoofed financial organizations, compared with 67% in 2012.

2.3.6 Guessing attack

Bijeeta Pal et al. (2019) in their study found out that the primary application of password models was to educate brute-force guessing attacks. Such attacks fall into two main categories: offline and online. Offline attacks occur when an attacker obtains cryptographic hashes of some users' passwords and attempts to recover user passwords by guessing-and-checking billions (or even trillions) of passwords. A guessing attack is when an unauthorized user attempts to login to a system by guessing user names and/or passwords.

2.4 Existing Techniques for Authenticating Users

User authentication is the act of confirming a person using personal identities, which often involves verifying at least one form of identification. There are three major factors to authenticate users, based on something the user knows (password and challenge response), something the user has (ID, security token, device, and equipment), and something the user is (fingerprint, DNA, and other biometric identifiers). Each authentication factor covers a range of elements used to authenticate a person's identity, which can be used to grant the access authorization, approve a transaction request, and sign documents (Koong, et al., 2014).The authentication on mobile devices can currently

be classified into three major approaches. PIN (personal identification number) or passwords, SIM (subscriber identification module) and the third approach being biometric authentication. On the other hand, passwords seem alternatively more secure because of the more possible combinations by using all symbols and alphabets. Unfortunately, people always use the same password everywhere and rarely change it. Although the security level can be enhanced through forcing users to change password periodically, it may also add annoyances for users.

2.4.1 Personal Identification Number (PIN)

A mobile PIN code contains between four to eight digits. A user is required to enter the correct PIN code before accessing the mobile device and most of the time the user will not be required to re-enter the PIN until the next reboots. However, a PIN can be set to be requested again after a certain period of time for additional layers of authentication. Financial PINs are often four-digit numbers in the range 0000–9999, resulting in 10,000 possible numbers. However, some banks do not give out numbers where all digits are identical, consecutive, numbers that start with one or more zeroes, or the last four digits of your social security number. For preventing unauthorized persons accessing the SIM card, a PIN code is needed at “switch on” or when a SIM card is inserted into a mobile phone. The mobile device would not start and the SIM card would not authenticate with the cellular network without a correct PIN. In the case of entering SIM PIN code incorrectly for three times; the SIM card will be blocked; hence, a user cannot access the mobile network.

To be able to unblock the SIM the user has to ask for Personal Unblocking Key from the network operators (Nosrati & Bidgoli, 2016).

2.4.2 Password Authentication

Password authentication has protected mobile devices from unauthorized user access. A user has to enter the correct password before accessing the mobile device. Passwords can contain a string of letters, special characters and numbers, which can provide a large number of set of passwords in comparison to PIN. The length of a password is dependent on the security policy of the particular application. Nevertheless, it could be difficult to type long password on small keypads (Nosrati & Massoud, 2016).

2.4.3 Recognition-based passwords Authentication

The length of a pattern is approximately between four and nine. However, there is limitation in this method in which “a dot” cannot be used more than one time. As a result, this technique provides less number of password patterns than traditional PIN and password (George & Reshma, (2017). These make the PIN/password based authentication technique inadequate as a protection for mobile devices (Nosrati, Bidgoli - 2016). Furthermore, two other authentication techniques are available, which are token and biometrics.

2.4.4 Token based authentication

Token based authentication approach is considered where the user would need to carry them around with the mobile. Another issue is that if the authentication process requires the token to be placed into the device then it is highly probable that many users would leave it in mobile device. This can be illustrated by the use of a SIM card on current mobile devices. When the users do not want to use the mobile, users could remove it. However, removing the SIM card would be inconvenient. By utilizing contactless

technology it is possible to develop tokens that can be integrated within the item that users would always expect to have with them such as rings.

Although this technique can increase user convenience over the secret-knowledge authentication approach as no interaction is required. However, this approach requires the user to remember the token (Nosrati & Massoud, 2016).

2.4.5 Transparent authentication systems

Transparent authentication systems for mobile devices may be classified by use of physiological biometrics and behavioral biometrics. Physiological biometrics such as fingerprint scanning or face recognition, or of behavioral biometrics such as keystrokes or touch.

2.4.5.1 .Physiological biometric

Physiological biometric is commonly considered useful for one-off authentication (De Marsico et al., 2018) because they require considerable computing power and high quality images which are not easy to obtain. For instance, iris recognition needs the user to face the camera, takes more time for authentication and requires high-cost additional hardware. Meng et al., (2015) found that there are still challenges for iris recognition such as detection, segmentation, coding, and matching. On the other hand, fingerprint recognition suffers in the presence of poor conditions such as cuts and dirt (De Marsico et al.,2018) as a result, fingerprint scanning and iris scanning are considered intrusive.

2.4.5.2 Behavioral biometrics

Tanviruzzaman & Ahamed (2014) in their study found out that behavioral biometrics refers to something the user does such as typing rhythm also known as keystroke

dynamics, gait, application usage, voice or signature, which are considered to be less sensitive to darkness or noise. Behavioral biometrics is presented as a suitable method and is more commonly used for transparent and continuous authentication and providing usability. The term gait recognition describes a biometric method which allows an automatic verification of the identity of a person by the way he walks over a certain distance which can be used to identify persons (Lu et al., 2015). There are three different approaches in biometric gait recognition: Machine Vision Based, Floor Sensor Based and Wearable Sensor Based Gait Recognition. Banerjee & Woodard (2012) in their research found keystroke dynamics to be promising and attractive for defending the cyber space. Keystroke dynamics is considered of the most successful behavioral biometrics with the benefit of almost free as the only hardware required is the physical keyboard. Users' keystroke rhythms are measured to develop a unique biometric template for future authentication (Banerjee & Woodard, 2012). Monitoring keystroke dynamics is considered to be an effortless behavioral based method for authenticating users which employs the person's typing patterns for validating his/her identity (Alsultan & Warwick, 2013).

Behavioral biometrics relate to a specific behavior of a human being while performing some tasks, such as handwriting, speaking, walking and typing (Hoang & Choi, 2014). Usually handwriting recognition used signature as identity, which means it is not suitable for general purpose authentications (sea-Nogueras & Faundez-Zanuy, 2012). Voice biometric authentication uses the voice pattern to verify the identity of the individual. Gesture-based user identification uses human body gestures and gaits to recognize the user. This is usually tracking the patterns while human walking or performing poses in different ways. The benefits can be the easy operation while performing user authentication.

The challenges inherent in authentication make behavioral biometrics appealing for a number of reasons. For one, it will likely be harder for someone with malicious intent to successfully capture a natural motion compared to a password or even a fingerprint. Natural motions also provide the option of continuous authentication since motions such as holding the device, walking around with it, and holding it up to the user's ear are ongoing activities (Maghsoudi & Tappert, 2017).

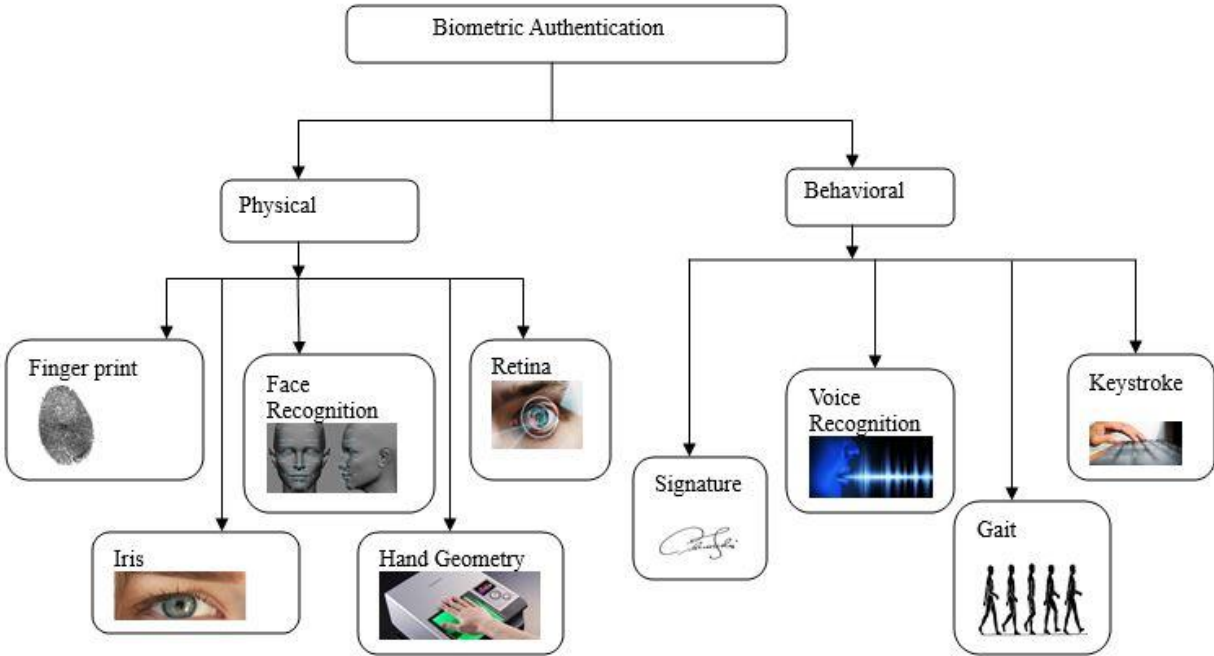


Figure 0.1 Biometric Authentication Types (Babaeizadeh , Bakhtiari , & Maarof, 2014)

)

Biometric authentication are unique enough to distinguish each person. The development of the biometric authentication technology has the trend of replacing the traditional verification method and can solve the traditional security problems. Biometrics authentication has thus become a primary focus of academic research and industry adoption/implementation to provide users enhanced security and authentications.

Biometric approaches are typically divided into two categories: physiological and behavioral biometrics. Physiologic biometrics refer to physical measurements of the human body, including face, fingerprint, hand geometry, retina, and iris. The recognition system based on physiological characteristics has a relatively high accuracy (Heydarzadegan et al.,2013).

When it comes to biometrics systems performance there set evaluation measures put in place:

The performance of a typical biometrics technique is measured by False Acceptance Rate (FAR), False Rejection Rate (FRR) and Equal Error Rate (EER). FAR refers to the percentage of access attempts by imposters that have been accepted by the system (incorrectly accepted) whereas FRR refers to the percentage of access attempts by legitimate users that have been rejected by the system (incorrectly rejected). In this context, low FAR indicates that the system is secure, and low FRR means the system is usable. The point at which FAR and FRR are equal is called EER, which means that a system is accurate. To be a more accurate and better performing system, the system needs a low EER (Alotaibi et al., 2015).

False Rejection Rate (FRR) calculated using the following expression

$$\text{FRR} = \frac{\text{Number of genuine rejections}}{\text{Number of genuine attempts}}$$

False Acceptance Rate (FAR) calculated using the following expression.

$$\text{FAR} = \frac{\text{Number of unauthorized accepts}}{\text{Number of unauthorized attempts}}$$

The main advantage of biometric technologies is that users don't have to remember or carry anything at the time of authentication. Another advantage of using biometric is that biometrics provide highest level of security and very hard to forge. Having two categories of biometric based authentication physiological and behavioral, physiological biometrics are considered to be more robust and secure, they are expensive to use because specialized hardware is needed to detect the features. On the other hand, behavioral characteristics are cheaper than physiological characteristics because additional hardware is not required. Thus behavioral characteristics are easy to reveal but hard to forge (Pahuja & Nagabhushan, 2015).

2.4.5.3 Keystroke Dynamics

Keystroke dynamics is the analysis of how users type from the monitoring of their keyboard input. Keystroke dynamics may be used either in the initial authentication of a system or as continuous authentication after the initial authentication. Keystroke dynamics can be characterized using timing (such as the key down time for each key, latency between consecutive keys, and users typing speed (Zhong & Deng, 2015).

Ivannikova et al. (2017) found Keystroke dynamics to be one of the authentication mechanisms which uses natural typing pattern of a user for identification. A study by (Ho & Kang, 2015) found out that Keystroke dynamics based authentication was one of the prevention mechanisms used to protect one's account from criminals' illegal access. In this authentication mechanism, keystroke dynamics are used to capture patterns in a user typing behavior. The use of keystroke dynamics for verification and identification purposes was first investigated back in the 1970's (Forsen et al., 1977) and (Spillane, 1975). Keystroke dynamics can be applied in two ways: static text or dynamic text. Static text only performs an analysis of fixed expressions as, for example, a password. While, in dynamic text, the analysis occurs for any text that is typed by the user. Keystroke dynamics in static text requires less effort to be implemented and it also reaches lower error rates in literature according to (Crawford & Ahmadzadeh, 2017). User Specific traits are a very strong method to strengthen the security of any system as it makes the system connected to a specific individual instead of being accessed through some token or key (Quraishi et al., 2018). Over the years, different pattern recognition methods have come into existence and have been applied to keystroke dynamics; neural networks, Fuzzy logic and support vector machines among others. They often used two features Dwell time and Flight time as biometrics features, Dwell time which refers to the amount of time between pressing and releasing a single key and Flight Time which refers to the amount of time between pressing and releasing two successive keys (Roy et al.,2014).

Chourasia (2014) introduced an additional layer of security for the authentication of the user using Keystroke Dynamics. The security can be implemented in android phones or any other smart phones through which internet is accessible as well as online transactions can be performed. Hemant et al., (2014) in their study found that Keystroke

Dynamics is a two factor biometric security. For a successful login into the system, firstly password should be known and secondly, typing pattern should match. Lee et al., (2018) reported that by combining PIN (or pattern) and keystroke dynamics as a multifactor authentication, keystroke dynamics strengthens user authentication.

Keystroke Dynamics is a two factor biometric security. For a successful login into the system, firstly password should be known and secondly, typing pattern should match Vinayak & Arora (2015). When it comes to location verification a study by Hang et al., (2015) found out that users were good in recalling the location-answers to their questions while strangers failed most of the time when attacking these questions. Currently there is a growing body of research to improve user authentication based on physiological and behavioral biometrics (Habib & Alqatawna, 2017). Keystroke dynamics falls under behavioral biometrics and IBIA (2017) described keystroke dynamics as the future of user authentication.

2.5 User Profiling

User Profiling is the process of collecting information about a user so as to know him very well and recommend him with more accurate and relevant information. In order to profile a user a set of personal information relating to the specific user must be collected. The information contained in user profiles such as keystrokes dynamics, geographical location, professional background, interests and preferences (Hasan et al., 2013). In order to verify the proof, the system needs to have a prior user's knowledge, for example, the user profile. Generally, there exist two stages in a user authentication system: enrollment and verification stages. The purpose of enrollment stage is to register the users' data in the system by acquiring, extracting and storing biometric templates corresponding to the user (Ortiz-Yepes et al., 2014). Mahfouz et al. (2017) in their

research showed the possibility of using smartphones' sensors and accessories to extract some behavioral attributes such as touch dynamics, keystroke dynamics and gait recognition. Based on mobile devices, behavior profiling aims to identify patterns of usage based upon characteristics of a user's behavior such as how they talk, walk or type on their phones (keystrokes).

Profiling information can be exploited by a system taking into account the person's characteristics and preference to learn user behavior that personalize the individual user's pattern (Alnajjar, 2013). The current smartphones and tablets sold in the market are equipped a number of sensors such as accelerometer, ambient light sensor, digital compass, gyroscope, GPS, proximity sensor, touchscreen or WiFi. Such sources can be adopted for user behavioral profiling verification through mechanisms such as keystroke dynamics, gait recognition and touch dynamics (Khan et al., 2013).

These sensors are capable of providing raw data with high precision and accuracy and are useful to monitor three-dimensional device movement or positioning. For example, sensors are used to get gestures and motions, such as tilt, shake, rotation or swing. We can use accelerometers to identify and authenticate smartphone users based on a person's movements since a person's movements form a unique signature. It is also feasible to observe the users' own behavior to see if they are acting in their 'usual' way, reporting on any sufficiently-aberrant behavior. Doing this requires a user profile, a feature found more often in marketing and education, but increasingly in security contexts (Peng et al., 2016).

Research in mobile behavioral-based can be divided into two categories: network and host based mechanisms. The former will focus upon profiling user's calling and migration behavior over the service provider network based upon the hypothesis that

people have a predictable travelling pattern (Naboulsi et al., 2016). A host-based mechanism is founded upon the hypothesis that mobile users utilize their applications differently in different time periods and at different locations. This approach would for example monitors user's calling features (e.g. the day of calling, start time of call, duration of call, dialed telephone number and the location), mobile phone device usage and Bluetooth scanning, thereby providing a richer set of potential user profiling features than network-based approaches (Clarke et al., 2013). The identity of the user is given to the system along with a proof of the biometric information through users keystroke profile which is used for user authentication.

Correctness of the identity is then evaluated by the system based on user's stored profile. After that, either accepting or rejecting the user is given based on the evaluation result.

2.6 Location Authentication

Geo Location authenticates the user based on the location of the user at the current time. Geo location is a term used to refer to the geographical location of the user, based on available information. Geo Location can authenticate users based on cookies, IP address or MAC address. Geo location authentication is gaining importance as it is found most suitable for mobile devices. It ensures security of mobile transactions based on the user location (Akoramurthy & Arthi, 2017). Given the widespread use of mobile devices, geographical location is a particularly interesting modality for behavior driven authentication. We can determine which places the user typically visits and then compare them to the reported location for the current authentication attempt. There are numerous applications which might harness geographical location for low-friction authentication such as online banking and retail, insurance companies or media companies (Callsign, 2019). Smart phones and hand held devices are increasingly being

used for mobile transactions. These devices are mostly GPS-enabled and can provide location information. The geographical location of clients as an authentication factor is integrated with applications to enhance security (Ahmadian et al., 2017). Geo location based authentication provides a secured transverse authorized environment with the help of location signature which includes longitude, latitude and altitude. The location details guarantees that the user performs administrative functions only from authorized locations. Location authentication is in fact two practically separate methods, the verification and validation of a system or user specification and authorization of an entity's access acquire based on their location with respect to their physical location. Identity of user location is typically acclaimed through a combination of knowledgeable and location information through which geo metric device received its signal. The GPS receiver that is inbuilt in GPS device captures the real location with its attribute like latitude, longitude and altitude of the user location gives the location information to the server that gets stored in the server's database along with the time stamp those changes readily time to time. Tracking mobile device location data provide a great opportunity for tapping into the power of user behavior analytics.

As mobiles have become important for our existence its important have them secured and have them authenticated. Location-based technique is one of the new technologies used to check authentication through smart phones (Nisar, 2019).

2.7 User Profiling and Location Authentication

Having described both user profiling and location authentication separately now we combine both of them as an alternative user authentication. User location cannot be used for authentication on its own, but combining it with any of the other authentication factors can boost security and create Multi-Factor Authentication (MFA). Dasgupta et al.

(2017) found out that Multi-Factor Authentication was a secure process of authentication which required more than one authentication technique chosen from independent categories of credentials. The aim of this approach is to improve the reliability of the authentication by providing an alternative authentication method. The presented approach in this research uses the typing behavior also known as keystroke of a user to create a profile for the user and location authentication. The typing behavior of the valid user is observed and is compared with the typing behavior of unauthorized user based on which the user is authenticated. Authentication based on user's behavior such as typing pattern was analyzed by Gurary et al. (2017) which served as a means of securing a mobile device in cases of mobile theft. Capturing user's location is usually done through Global Positioning System (GPS) system for a position determination. GPS is a space-based satellite navigation system that provides location and time information in an all-weather conditions, anywhere on or near to the Earth where there is unobstructed line of sight to four or more GPS satellites, Gurary et al. (2017) found that there were two key characteristics of the GPS location data. That one, it was relatively unique for each individual even for people living in the same area of a city. Two, outside of occasional travel, it does not vary significantly from day to day and with this captured with the help of Google maps. When a user accesses the mobile banking application from a different location then the application will have to ascertain the authorized user through a security question prior entered during initial registration and when answered correctly then the user is allowed to transact. The similarity between user profiling and location authentication is that they uniquely identify an authorized user based on the existing data stored and being able to distinguish from the unauthorized user at the time of authentication which makes it ideal for this research.

2.8 Mobile Banking

Mobile banking also abbreviated as m-banking is considered to be one of the most value-added and important mobile commerce applications currently available (Lee et al., 2012). Akoramurthy & Arthi (2017) defined Mobile banking as the use of a smartphone or a tablet to carry out banking activities such as receiving account alerts, checking balances or making payment from anywhere, at any time. A survey by Federal Reserve Board (2015) found mobile banking to be a low cost transaction between two parties and over the years, the trend towards transactions made through mobile phone would be growing. Khan (2014) found out that the appeal of mobile phone banking was not one-dimensional; rather consumers readily appreciate a number of advantages. Convenience, speed and control emerge as the key benefits for a group who value their time and the ability to regularly monitor their finances to avoid bank charges and stay in the black. Mobile banking is moving up on the adoption curve, which is evident in the number of implementations known in the world and the level of interest and discussion around the technology and its implementation. It is also evident in the number of technology providers emerging in the mobile banking space. There are several choices when considering how to implement mobile banking. These choices include whether or not to develop the technology within the bank, use a shared infrastructure, or purchase the enabling technology from one of many vendors. Miranda et al. (2014) found out that according to Rogers (1962) model of the diffusion of innovations, knowledge was produced when an individual is exposed to an existing innovation and acquires some understanding about its mechanisms and functions. To reach the Persuasion stage, the individual must form a view toward the innovation based on its perceived attributes such as relative advantage or complexity. For Decision to occur, the individual must be involved in an activity that would ultimately require him or her to make a choice

between using or to dismiss the innovation. For Adoption to occur, the individual must arrive at the decision that the innovation is the best available option for moving forward. Several researchers have incorporated pieces of Rogers's model in empirical work that examined technological innovations.

2.9 Hindrances in the uptake of mobile banking

Rogers (2003) in his study found that the adoption of any innovation depended on the relative advantage, compatibility, complexity, triability and observability of the innovation. New technology and innovation is believed to present risk for many customers, hence they react differently based on their innate characteristics, the wants and the needs of their companies and the behavior of other buyers.

2.9.1 Use of a Trial Application

1. The extent to which various financial institutions offer "introductory" M-banking to their customers impacts the trial ability and accessibility of the innovation. Empirical studies on the acceptance of technologies have found consistently positive relationships between usefulness and to a lesser extent, ease of use, and the adoption of a variety of specific technologies, ranging from computer software to e-mail (Rogers, 2003).

2.9.2 Relative advantage

Relative advantage is the degree to which consumers perceive a new product or service as different from better as its substitutes (Rogers, 2003). In the case of M-banking, savings of time, money and convenience have been cited as relative advantages. At the same time, financial management conducted online raises concerns of privacy, a relative disadvantage for some.

2.9.3 Simplicity/complexity

This is the extent to which consumers perceive a new innovation as easy to understand or use. For consumers without previous computer experience, or for those who believe that m-banking is difficult to use, adoption of these innovations may be thwarted.

2.9.4 Compatibility

This refers to the extent to which a new product or service is consistent and compatible with consumers' needs, beliefs, values, experiences, and habits. In the case of M-banking, we must consider the degree to which a given technology fits in with the banking behavior of a consumer, and the way in which they have historically managed their finances. Technological service innovations differ from other commodities in so far as their adoption may require behavior different from consumers' typical routines. This includes "bricks and mortar" issues such as not having a branch bank to visit, as well as "paper" issues including receiving statements electronically and not in the mail. Elkhodr et al. (2012) attributed that the success in increasing m-banking uptake amongst clients will ultimately rely upon how secure the financial data and transactions are. That is, the end user must be confident in the financial institution carrying out the transaction, the transmission of financial data and the technology itself.

In Kenya, the first bank to adopt mobile banking was the Cooperative Bank of Kenya then later other banks also started adopting mobile banking. Mobile money was first created to respond to the demand for affordable and accessible financial services. It was quickly proclaimed the solution for financial exclusion in the global south, largely because of its tremendously successful implementation in East-Africa. In March 2007 it

is realized that over 1.1 million Kenyans were recorded to have used mobile banking, which is called M-Pesa. M-Pesa refers to mobile money i.e M-pesa meaning money.

This service was introduced in Kenya by a telecommunication company called Safaricom and Vodacom. Its main aim was to deliver banking services to different people in the country with the use of a phone (Hove & Dubus, 2019). According to the research done by (Thinking, 2014) shows that there are 352.1 million mobile banking customers at the top four Chinese banks, according to their 2013 annual reports. China is king of m-banking. The two largest banks, China Construction Bank (CCB) and Industrial and Commercial Bank of China (ICBC), have more than 100 million mobile banking customers each. That means each one has more than all US mobile banking customers put together.

In quarter four of 2013 Analysis International (2014) found that Chinese mobile users made transactions worth 4.7851 trillion Yuan (US \$768.8 billion). Also Forrester Research (2014) estimated that there were 51 million mobile banking customers in Europe in 2013, 42 million mobile phone banking and 19 million tablet banking users. This is predicted to grow to 214 million in 2018 – 99 million mobile phone banking and 115million tablet banking users. In the US, Chase and U.S. Bank tie for the top spot for their mobile offerings, followed by Wells Fargo, Bank of America, and Citi. “Before banks can serve customers through mobile touch points, they have to ensure that customer can interact with them via mobile.

Today, banks have to develop mobile banking services for many different smartphone and tablet platforms, not to mention mobile browsers. That’s driving many firms to explore approaches like responsive design.” Peter Wannemacher, (Forrester Data ,

2016). Another research done by Javelin Strategy & Research (2017) estimated that there were 95 million mobile bankers in the US in 2013 up by 40 percent from 2012.

It forecasts that there will be 108 million in 2014; 119 million in 2015 and 130 million in 2016. Increasingly the world's top banks are including the numbers of m-banking customers in their annual reports. Some still do not perhaps out of embarrassment.

The top Chinese banks lag behind the rest of the world in m-banking subscribers but some US banks are starting to show good progress in m-banking, while the European banks are miles behind (Thinking, 2014). New research from Juniper Research (2016) found that over 2 billion mobile users will have used their devices for banking purposes by the end of 2021, compared to 1.2 billion as at 2016 globally. Growth in mobile banking is being driven by consumer adoption of banking applications changing way consumers manage their finances. International remittances via mobile phones exceeded US \$10 billion for the first time in 2013.

In another research by Gartner (2013) found out that money transfers were at 71 percent of total mobile payments in 2013. Total m-payment users worldwide in 2013 was 245 million making collective payments of \$235 billion. This means mobile transfer users equate to 174 million, with total transactions worth \$167 billion. According to Gartner (2013) forecasts that Asia Pacific will overtake Africa as the largest region for mobile payments by 2016 worth \$165 billion against Africa's \$160 billion. While there are 5 billion mobile users globally, the mobile banking users are only about 200 million (Jeong & Yoon, 2013). There is less use of mobile phone and mobile banking services in the advanced economies such as USA, Sweden and United Kingdom. While consumers continue to express concern over using their mobile phone to conduct banking and financial services transactions, it is a fear born more of perception than reality. There are

threats, but the security controls available to mitigate risk at this level are substantial and effective. However, security practices will need to continue to evolve as more and more smart phones enter the market running more and more applications, creating an ever growing opportunity for security threats (Islam, 2014).

The rest of the research is organized as follows: The research methodology that will be used in this research to conduct the experiments, the sampling technique together with the data collection method to be used. In the final section of this research will present the results and draw conclusion highlighting possible future research work.

2.9.5 2.10 Evaluation of existing authentication methods

From the above covered authentication methods that are used in mobile banking systems were evaluated of these methods using the criteria of authentication feature, the improvement made and their limitation.

2.9.6 2.10.1 Personal Identification Number (PIN)

A mobile PIN code contains between four to eight digits. Financial PINs are often four-digit numbers in the range 0000–9999, resulting in 10,000 possible numbers. However, some banks do not give out numbers where all digits are identical, consecutive, numbers that start with one or more zeroes, or the last four digits of your social security number. For preventing unauthorized persons accessing the SIM card, a PIN code is needed at “switch on” or when a SIM card is inserted into a mobile phone. In the case of entering SIM PIN code incorrectly for three times; the SIM card will be blocked; hence, a user cannot access the mobile network. For unblocking key to unlock from network

operators, the user has to ask for Personal Unblocking Key the limitation with this method is that it makes it easy to guess PINS according to (Nosrati & Bidgoli, 2016).

2.9.7 Password Authentication

Passwords can contain a string of letters, special characters and numbers, which can provide a large number of set of passwords in comparison to PIN. The length of a password is dependent on the security policy of the particular application. This disadvantage with this method is that it's difficult to type long password on small keypads.

2.9.8 Recognition-based passwords Authentication

This type of authentication use a pattern approximate 4-9 in length and where "a dot" cannot be used more than one time. This technique provides less number of password patterns than traditional PIN and password (George & Reshma, 2017).

2.9.9 Token based authentication

Authentication token or simply a token may be a physical device that an authorized user of computer is given to aid in authentication. Such a token may be physically connected or plugged into the client system. The term may refer to software token as well. Zahid et al. (2009) in their study found the limitation with this approach was that it required the user to remember the token and that the tokens cannot be replaced as easily as passwords incase the user failed to remember. Additionally Belk et al. (2014) mentioned that token-based authentication mechanism incurred more cost to users and that they are comparatively slower.

2.9.10 Transparent authentication systems

They are classified into two physiological biometrics and behavioral biometrics. Physiological biometrics involve use of iris, Face, finger and palm prints, Keystroke dynamics, gait (walking sensors), Signature and Mouse. They are useful for one-off authentication. Identity uniqueness of each user and there is no need to cram or remember authentication is based on what the user has. They require considerable computing power and where the device is not capable to handle the feature a high-cost additional hardware is used. In behavioral biometrics this include capturing user typing rhythm also known as keystroke dynamics, gait (how user walks), application usage, voice or signature.

Keystroke dynamics is considered of the most successful behavioral biometrics since as the only hardware required is the physical keyboard that comes with every mobile phone. The advantage with behavioral authentication is that it's unique in that it's harder for someone with malicious intent to successfully capture a natural motion compared to a password or even a fingerprint. The other advantage is that compared with other methods it's easier for one to remember because it is something the user has all the time whenever or wherever he or she is. This method also is prone to limitations, with the use of transparent authentication systems comes with additional computing power that becomes costly. This system also takes more time for authentication Crawford & Renaud (2014).

Table 0.1: Authentication Evaluation Table

Authentication Method	Features	Improvement	Limitation
<ul style="list-style-type: none"> Personal Identification Number <p>(Meng et al., 2018)</p>	<ul style="list-style-type: none"> 4-8 digits 	<ul style="list-style-type: none"> Preventing unauthorized person accessing a mobile phone. It's limited to number of trials e.g 3 times 	<ul style="list-style-type: none"> Easy to guess PINS
<ul style="list-style-type: none"> Password Authentication <p>(Nosrati & Bidgoli, 2016)</p>	<ul style="list-style-type: none"> Can contain a string of letters, special characters and numbers. 	<ul style="list-style-type: none"> Provides a large number of set of passwords in comparison to PIN length of a password is dependent on the security policy of the particular application. 	<ul style="list-style-type: none"> Difficult to type long password on small keypads. Use of default passwords that make it easy to login.

<ul style="list-style-type: none"> • Recognition-based passwords Authentication <p>(George & Reshma, 2017)</p>	<ul style="list-style-type: none"> • Pattern length 4-9 		<ul style="list-style-type: none"> • This technique provides less number of password patterns than traditional PIN and password.
<ul style="list-style-type: none"> • Token based authentication <p>(Nosrati & Bidgoli, 2016)</p>	<ul style="list-style-type: none"> • fast authentication 	<ul style="list-style-type: none"> • Requiring minimal user interaction compared to other authentication techniques. • Increase user convenience over the secret-knowledge approach. 	<ul style="list-style-type: none"> • Tokens cannot be replaced as easily as passwords.

<ul style="list-style-type: none"> • Transparent authentication <p>(De Marsico et al., 2015)</p> <p>(Tanviruzzaman & TSheikh, 2015)</p> <p>(Maghsoudi & Tappert, 2017)</p>	<p>use of</p> <ul style="list-style-type: none"> • Keystroke dynamics • Gait (walking sensors) • Signature • Mouse • Iris • Face • Finger print • Palm print 	<ul style="list-style-type: none"> • Identity uniqueness of each user • No need to cram or remember authentication is based on what the user has 	<ul style="list-style-type: none"> • Some require considerable computing power. • Takes more time for authentication and requires high-cost additional hardware.
---	--	--	--

2.10 Key Research Gaps based on the Authentication Evaluation.

2. From the evaluation table above the use of single factor authentication using PINs or Password authentication is both weak and vulnerable according to (Handson, 2016). When it comes to recognition based graphical passwords systems lie in a variety of

images used since the technique provides less number of password patterns than the PINs and passwords (George & Reshma, 2017& Togookhuu et al., 2017).When it comes to often used one-time password based systems they provide additional transaction security, but are still incapable of differentiating between a genuine user trying to authenticate or an adversary with stolen credentials (Kulkarni & Namboodiri ,2014). Belk et al. (2014) in their research found out that token-based authentication mechanism incurred more cost to users and were comparatively slower. Crawford & Renaud, (2014) found transparent authentication as an alternative authentication mechanism with minimal or no noticeable involvement of users. Transparent authentication implicitly authenticates the users on the basis of their unique interactions with the device and creates a logic for authentication decisions. IBIA (2017) described behavioral biometrics as the future of user authentication and that the focus of the research has been shifted to develop newer behavioral biometric-based solutions. For example, applications like e-wallet, m-commerce, and mobile banking are some of the sensitive domains, where behavioral biometric-based solutions have shown to be handy in authenticating the customers on their smartphones.

Keystroke dynamics being an example of behavioral authentication does not require any additional dedicated hardware and data can be collected, unobtrusively however according to a study by of Singh et al., (2017) they reported that keystroke dynamics was not enough by itself which is why this study addresses the research gap by improving the authentication method with the addition of location verification which ensures security of mobile transactions based on the user's transaction location captured by smartphones GPS sensor and it' application to mobile banking. Forward-looking security programs are able to use the location tracker on smartphones as a data point in user behavior analytics. Through tracking mobile devices, security teams are able to flag

any situation where an authentication is coming from a different physical location than the location of the smartphone (Saurav et al., 2019).

2.11 Conceptual Framework of the study

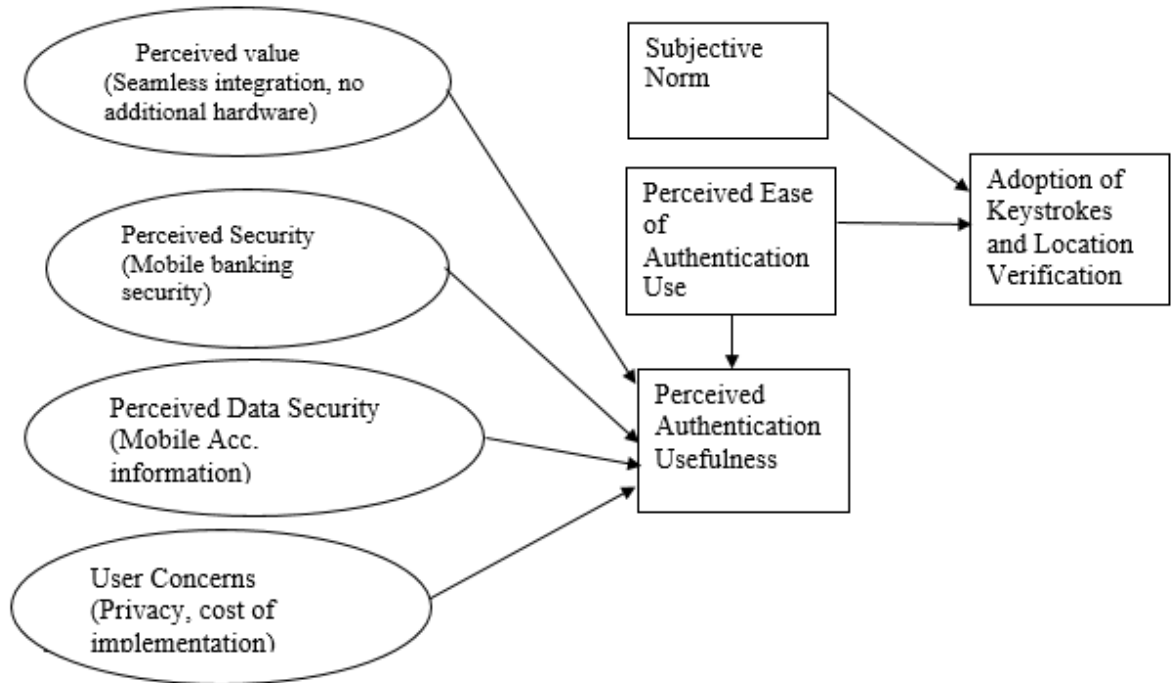


Figure 0.2 Conceptual Framework

The proposed authentication method will have a mobile banking application prototype that will capture users typing behavior through in built touch screen keyboard sensors available on smartphones as user's type in their 4 digit PINs during registration of new users and authentication of registered users. The obtained data will be used to distinguish the user's unique typing behavior. In the background as the user types their PIN, their location is captured via a GPS module or cellular data which determines the device's location under any weather condition at any time from a smartphone. Based on the user's transaction location and typing behavior will be stored in the database. To be able to verify a legitimate user their typing behavior as per their keystroke profile and transaction location stored in the database should be accurate within the given range.

2.12 Conclusion

This chapter highlighted the threats and vulnerabilities that are targeted to systems explaining how the rise of mobile phones are emerging as the new target to these threats. To counter the threats this chapter also examined the various techniques for authenticating legitimate users to systems ranging from the traditional PIN and password to biometrics. An evaluation of existing authentication methods was done and summarized in a table, mobile security remained to be a key factor from the evaluation. According to Alotaibi et al. (2015) they noted that there was lack of investigation and study of behavioral profiling, and in particular, application usage for transparent authentication systems on mobile devices. It is for this reason that this research aims to

contribute to knowledge by proposing use of behavior profiling and location verification authentication as an alternative method of securing mobile banking transactions since behavioral biometric authentication methods are cheaper than physiological ones.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

Rajasekar et al., (2015) defined research methodology as a systematic way to solve a problem. It is a science of studying how research is to be carried out. Essentially, the procedures by which researchers go about their work of describing, explaining and predicting phenomena are called research methodology. It is also defined as the study of methods by which knowledge is gained. Its aim is to give the work plan of research. This chapter covers the design and methodology of this research including the sampling size, sampling technique, the research design to be used together with the research experiments and data collection tools to be used to address the research questions.

3.2 Research Methodology

This research used quantitative research method where surveys were used to gather information from users and none users of mobile banking and their knowledge to security of their applications. Also there will be an experiment to demonstrate use of

behavioral profiling and location verification as an alternative authentication method that increases security when it comes to mobile banking.

3.3 Target Population

In this research the target population comprised of staffs from Kenya Commercial Bank (KCB) head office branch at Kencom in Nairobi, Kenya. The bank has a total population size of 247 staffs according to a report by (Kenya Commercial Bank, 2014). This study targeted 153 respondents which included junior and senior level employees as well as departmental heads. To calculate the sample size Yamane (1967) formula was used. These population had experience in mobile banking hence exhibited typical characteristic of a mobile banking user. Thinking Business Awards (2017) recognized KCB mobile banking service as the best in Kenya winning an award and this was the reason for choosing KCB bank for this research's target population.

3.4 Sampling Technique

The sampling technique used was simple random sampling. It is considered the purest and the most straightforward probability sampling strategy. It is also the most popular method for choosing a sample among population for a wide range of purposes. In random sampling each member of population is equally likely to be chosen as part of the sample. It has been stated that the logic behind simple random sampling is that it removes bias from the selection procedure and should result in representative samples. It is important to note that application of random sampling method requires a list of all

potential respondents (sampling frame) to be available beforehand and this can be costly and time-consuming for large studies (Gravetter & Forzano, 2012).

In this research a total of 153 out of 247 respondents were sampled who comprised of Kenya Commercial Bank (KCB) head office branch at Kencom. From the sampled population 138 completed the survey giving a 90% response rate which comprised of junior and senior level employees as well as departmental heads. In any research the participants are purposively selected according to the typical case sampling strategy according to (Patton , 2002). The selection in this strategy involves selecting participants who exhibit typical, or average, characteristics for the group being studied hence the sampled population of respondents constituted a knowledgeable component with regards to the subject matter of the current study being mobile banking. According to Adler et al.(2006) they found that in order to have confidence that your survey results are representative, it is critically important that you have a number of randomly-selected participants in each group you survey.

The respondents were sampled based on their skills on interacting with mobile applications whether installed on phone by default or user's downloading them for their use and their experience with these applications be it financial, health or entertainment and also their security considerations if any. This was done within a period of 30 days. To capture this users were required to rate themselves on a likert 5 point scale of 1-5, 5 being the highest on their skills and experience with smart phone application usage and 1 being the lowest. This kind of rating scale is the easiest indicator of user highs and lows. The responses provide terrific data for the creation of charts and graphs. According to Joshi et al., (2016) this method provides independence to a participant to choose any response in a balanced and symmetric way in either directions.

3.5 Research Design

The research design refers to the overall strategy that you choose to integrate the different components of the study in a coherent and logical way, thereby, ensuring you will effectively address the research problem; it constitutes the blueprint for the collection, measurement, and analysis of data. De Vaus (2006) indicated that a research problem determines the type of design to be used and not the other way around. Parahoo (1997) described research design as a plan that described how, when and where data is to be collected and analyzed. This research focuses on user behavioral profiling and location verification for authentication. The research approach will be experimental.

3.6 Experimental Design

Experimental research approach is a quantitative approach that is put in place to discover the effects of presumed causes. The main feature of this approach is that one thing is deliberately varied to see what happens to something else, or to discover the effects of presumed stated causes. There will be two groups of mobile phone users, those who use traditional authentication methods (PINS and Passwords) to access their mobile banking application and the second group comprising of users who use behavioral profiling and location verification in authenticating their mobile banking application.

3.6.1 Scenario 1

Here a developed prototype of a mobile banking application that required use of account and PIN number for authentication will be used among the selected participants. In this experiment the objective will be to subject users on use of traditional authentication methods such as PINs and Passwords and what their preferences are when it comes to

creating them and whether the default settings issued by the bank are changed and also examining their considerations for authentication. Through use of an android mobile banking application prototype that will be developed for the basis of this research the selected participants will be required to download and install on their phones. Through a period of 30 days they will be required to interact with it from initial registration to performing transactions. The authentication preferences will be captured and later on used to determine how easy it was accessing the sampled participant's accounts by subjecting them to randomly selected imposters.

3.6.2 Data collection procedures

In the first experiment the objective will be to engage users for a period of 30 days on use of traditional authentication methods such as PINs and Passwords through use of a developed prototype of a mobile application that uses PINs and Account numbers for authentication, the experiment also seeks to find out what their preferences are when it comes to creating them and whether the default settings issued by the bank were changed and examine their considerations for authentication.

3.6.3 Scenario 2

In the second experiment a mobile banking application that used PIN incorporated with use of Keystrokes and location verification will be used as part of user authentication. Users will be required to type their PINs 10 times as the system trains on identifying user's unique typing behavior each time it is typed. Location data will be also captured through the phone's GPS, Wi-Fi or Cellular data as the users interact with the application in making transactions such as payments for their bills, cash deposits and withdrawals among others. The obtained data was used to create user's profile. Later on

determination on the uniqueness of each user in terms of profiling and the location of the transaction will be carried out. Later on a comparison shall be drawn between users who use traditional authentication methods using PINS/Passwords and if they change their default authentication details. If they change how easy or difficult is it to guess and by pass authentication, compared with users who use behavioral profiling and location verification method when the authentication is shared to random selected imposters compared to the first experiment. Later on get user's concern compared to the traditional method and how easy or difficult is it to access and bypass authentication.

When the user accesses the mobile banking application the phone's GPS will be used to get location data of where the application is being accessed from. Over a period of 30 days a user's location data will be analyzed together with the location of at least 10 transactions done identified and stored as the users preferred transaction location and when it changes then a location question is sent to the user of his/her recent location visited. To get user's profile the phone's in built accelerometer will be used to capture user typing rhythm as he/she enters their username and PIN over the same period of 30 days where a user typing pattern will be analyzed and similarities identified forming a combination of user's typing patter profile with the user's transaction location .When for example someone gets hold of a user's phone even when they know their PIN number the application will compare their typing pattern with what is in the database together with location verification based on comparison of location in regards to the previous transaction upon match with respect to the allowed variation they will be allowed access otherwise they are not allowed to transact and the bank gets notified if it exceed three attempts.

3.6.4 Data collection procedures

In the second experiment in order to be able to capture user's keystroke behavior this study will use a touch screen keyboard sensor available on android operating systems which is an open source software that most smartphones operate on, through a prototype of a mobile banking application that stores the typing data as users key in their PINs. The location data will be obtained through the phone's cellular data, Wireless networks or GPS. Training and testing of the system will be done to learn user's typing patterns through classification which is used to differentiate legitimate user's profile from an imposter as user's key in their PINs by recognition and reference based on stored data in the database.

3.7 Sample Size

A sample size is a smaller set of the larger population that is selected cautiously as a representative of the population that guarantees the subdivisions used in the study are provided for accurately (Cooper & Schindler, 2014). A good sample size should provide information that is detailed and comprehensive. The sample size in this research was made of 153 participants comprising of mobile banking users between the ages of 18 and 55 years. According to a world bank report in 2019 Kenya was found to be the highest user of mobile phones for money transactions in the Sub Saharan Africa region. Sixty-eight percent of Kenyan adults use mobile phones to transact money, making them the biggest users of mobile banking in sub-Saharan Africa. Mobile money services and mobile banking have grown significantly in sub-Saharan Africa with the World Bank saying mobile banking has expanded to 16% of the market (World Bank, 2019). According to Google (2017) 76% of Kenyans aged between 16-24 years are online

everyday 72% are aged between 25-34 years while 70% are aged between 35-44 years. 69% aged between 45-55 years who use the internet are also on the internet daily.

The largest number of online traffic is usually through smartphones which represents 71% with 21% using computers and less than 2% using tablets to access the internet.

To calculate the sample size of this survey Yamane (1967) formula was used.

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

Where n is the sample size, N is the population size, and e is the level of precision (margin of error).

$$152.70 = \frac{247}{1 + 247 (0.05)^2}$$

Using a sample size of 153 in our research would give a 95% confidence level which means that there is only a 5% margin of error chance of the sample results differing from the true population average according to Yamane (1967) which is a common choice in determination of sample sizes.

3.7.1 3.8 Data Collection Tool

There are several data collection tools that can be used namely use of observation, surveys, interviews, written questionnaires and focus group discussions. In this research surveys and questionnaires were used as the data collection tools. The choice to surveys is because they are used to collect, analyze and interpret the views of a group of people from a target population which is what this research used in finding out from the sample size while the use of questionnaires feedback is generally anonymous, which encourages

openness and honesty from respondents. The data obtained from the study was coded, tabulated. Through use of Microsoft Excel 2013 and survey monkey online data analysis tools such as cross tabulation, combined filters and sentiment analysis. Use of descriptive statistics was used to describe the features of the data collected in the study to provide simple summaries in regards to the sample and the measures which were later presented in the form of graphs and tables.

3.7.2 Survey

Surveys are non-experimental and involves investigating a community or a group of people. Surveys are ideal in collecting data from a targeted group of people about their opinions, behavior or knowledge. In this research the data collected from the survey was the information from users and none users of mobile banking and their knowledge to security when authenticating to mobile applications. The data collected was used to gather information from users and none users of mobile banking and their knowledge to security of their applications. The common types of surveys are written questionnaires, face-to-face or telephone interviews, focus groups and electronic (e-mail or Web site) surveys (Tague, 2004).

In this research an online survey platform survey monkey was used enabling the 153 sampled participants share their opinions on their knowledge of mobile banking security. The benefit of using the online platform is that one can design the survey and generate a link that can be shared on email and on social media enabling easy reach to the selected sample group. Through use of the proposed survey and analysis of the responses on user's knowledge of mobile security within 30 days and those that don't have any knowledge in relation to user's consideration in their mobile banking applications. The respondent's profile was of between the ages of 18-55 years comprising of both males

and females. According to a research done by GSMA (2018) found that users between the age brackets of 18-55 are the majority of smartphone users in the country with varying usage.

For this research a prototype of a mobile banking application will be developed that would authenticate users based on their behavioral profiling and location verification functionalities when users change their common location of transacting. To track user's location use of GPS data will be used which is the most straightforward way to track a smartphone and for behavioral profiling there will be use of sensors built into mobile phones such as accelerometers, gyroscopes and force sensors to capture the data. The chosen platform for simulating and developing the mobile application will be Android. Since Android is an open development platform providing access to the device hardware, ports, background services, notifications and others are open and free to use.

3.7.3 Questionnaires

This research used written questionnaires as one of the data collection tool since they are cheaper than personal interviewing and quicker if the sample is large and widely dispersed. The other reason would be that they are very familiar with people almost everyone. Questionnaires provide a relatively cheap, quick and efficient way of obtaining large amounts of information from a large sample of people. Data can be collected relatively quickly because the researcher would not need to be present when the questionnaires are completed. This is useful for large populations when interviews would be impractical (McLeod, 2013). The questionnaire was administered to 153 respondents who were believed to be active on their smart phones with the questions focusing on experience with mobile banking services. The questionnaire consisted of both closed and open ended questions. For closed ended questions respondents were

given a list of predetermined responses from which to choose their answer while in open ended questions respondents are asked to answer each question in their own words.

3.8 Conclusion

This chapter covered the research methodology to be used for this research, a justification of the sample size used was also given together with the sampling technique used and the research design to be used as well as the data collection instruments and description of the research experiments going to be used for this research were shared.

CHAPTER FOUR

RESULTS AND DISCUSSION

4.1 Introduction

This chapter presents the analysis, discussions and findings of the respondent's knowledge of mobile banking security and the use of Keystroke dynamics and location verification as an alternative method for authentication in mobile banking. The survey data was collected and analyzed to be able to come up with results.

4.2 General survey respondents' information.

A total of 138 respondents participated in the survey out of the sampled 153 giving a 90% response rate. Most of the respondents were male comprising of 84 (62%) while females were 52(38%) of the total respondents sampled through the online survey.

Table 0.2: Survey Participation

Name	Number
Completed Surveys	138
Did not participate in the survey	15
Total	153
Response Rate	90%

Table 0.3: Gender Distribution

Gender	Responses	Response in %
Male	86	62
Female	52	38
Total	138	100

Age bracket of the respondents

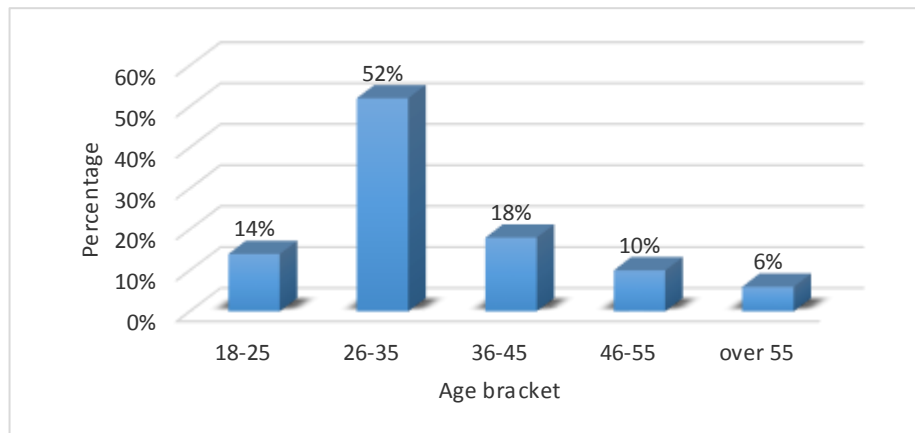


Figure 0.3 Age distribution

From the figure 4.1 above showed that the most of the respondents were in the age bracket of 26 years old to less than 35 years old comprising of 52%. This was followed by respondents who were in the age bracket of 18 years old and less than 25 years old comprising of 14%. Those between 36 years old to less than 45 years old were 18% of the respondents another 10% of the respondents were of the age bracket of 46 years old and less than 55 years old. While those that were of the age bracket of 55 years and above were 6%.

Education level of the respondents.

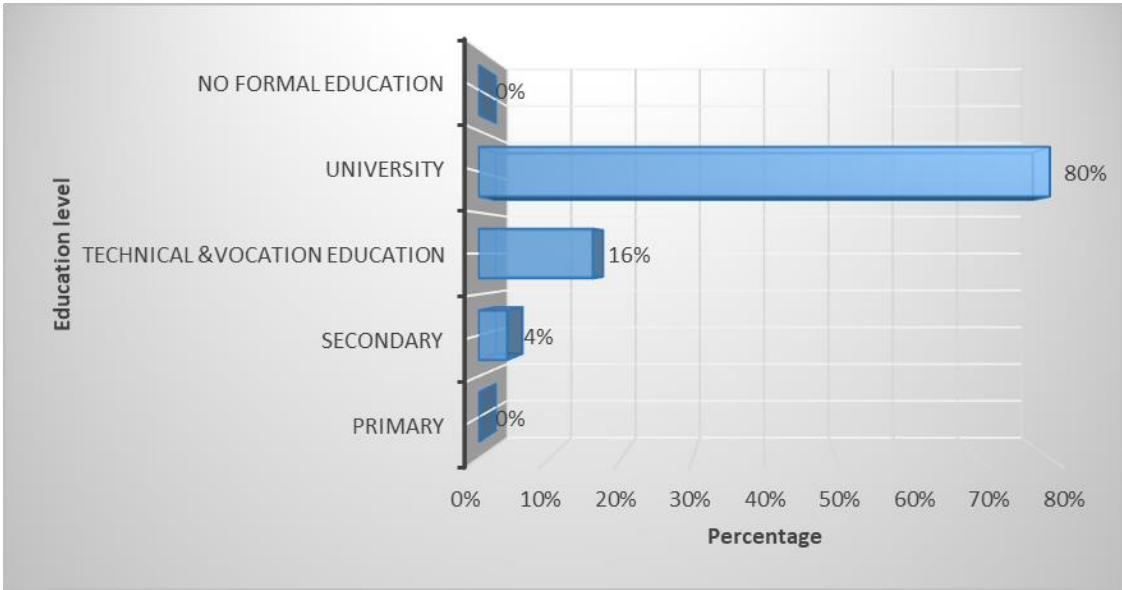


Figure 0.4 Education level distribution

Most of the respondents from the survey had attained university level of education as the highest education level as they comprised of 80% of the total respondents, those with technical and vocation level of education were 16% whereas those with secondary level of education were 4%. Primary education level and no formal education had no respondents with each comprising of 0%.

Smartphone Ownership

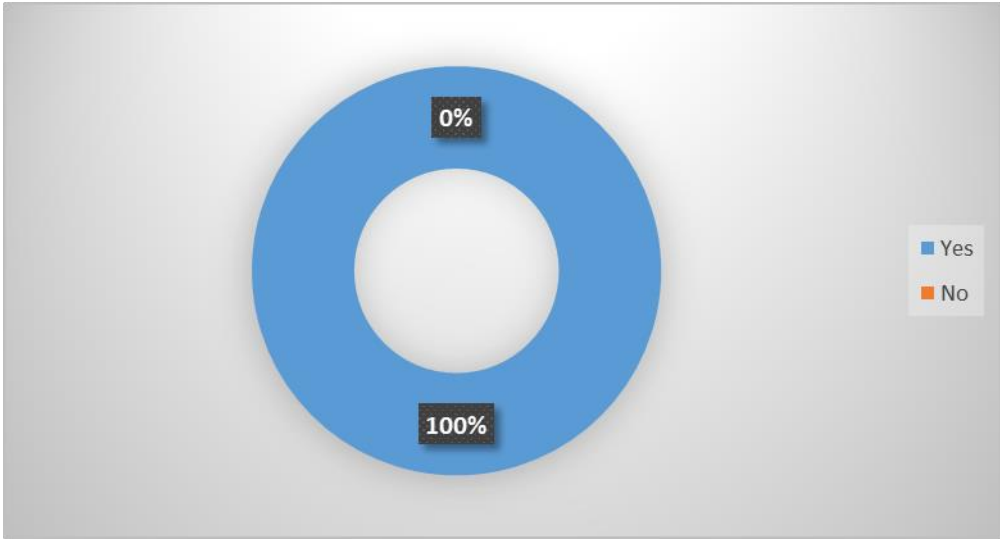


Figure 0.5 Smartphone ownership

From the survey all of the respondents comprising of 100% reported that they owned a smartphone. This rise in the uptake of smartphones is similar to the findings of a report by GSMA (2018) where they found out that more than 60% of Kenyans owned a smartphone, while the mobile subscription was at 82%. This can be attributed to a drop in average price of smartphones leading to the growth of smartphone users. Comparing the survey findings with another report by Poushter (2016) where they reported that since 2013 smartphone ownership rates in emerging and developing nations are rising at an extraordinary rate.

Bank Account Ownership

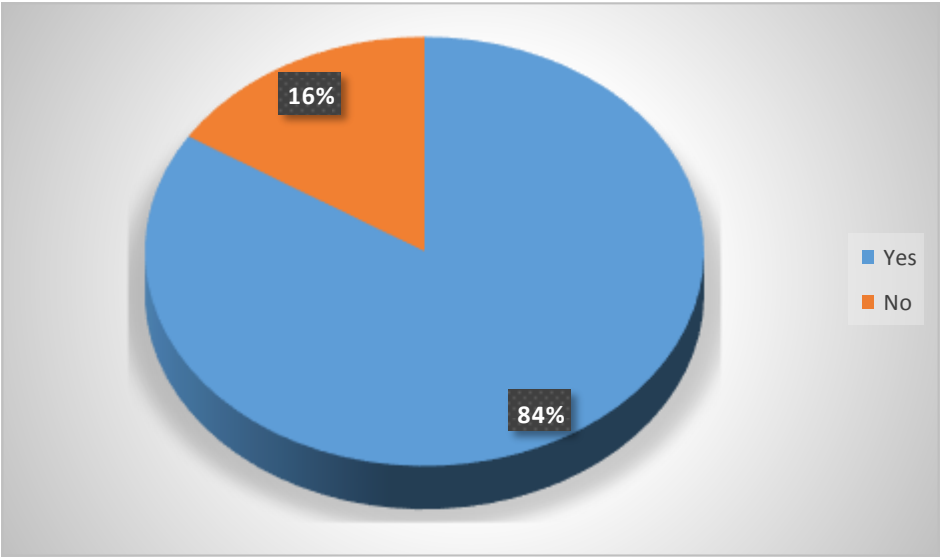


Figure 0.6 Bank account ownership

A majority comprising of 84% of the total respondents being 138 had a bank account while 22 comprising of (16%) did not have a bank account. This shows that a larger population in Kenya has a bank account. Comparing the findings of this survey to a report by the Demirgüç-Kunt et al. (2017) where they reported that 75%, or eight out of every 10 Kenyan adults, is banked through bank and mobile money accounts rising top among countries such as South Africa, which has 70% of its population banked, Nigeria, with 44%, and Ghana with 40%. Leading in terms of banking population is Kenya where the banked population is above the global average of 62% ,coming in second is Uganda in East Africa with 44% of its citizens having access to banking services, followed thirdly by Rwanda at 42%, Tanzania comes in fourth at 40% and lastly Burundi at 7%.

Mobile banking subscription

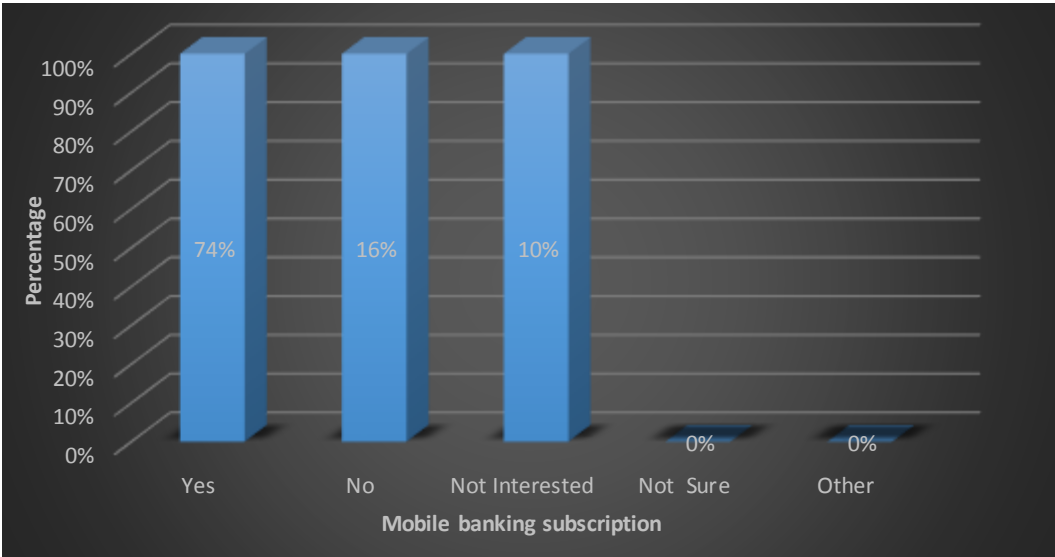


Figure 0.7 Mobile banking subscription

From the survey 74% of the respondents reported to have subscribed to mobile banking services while 16% of the respondents said they did not subscribe to mobile banking services, another 10% of the sampled respondents were not interested in subscribing to mobile banking, out of the sampled respondents who participated comprising of 138 none were not sure of subscribing to mobile banking. Referring to figure 4.3 with the rise of smartphone ownership comes with the rise in mobile banking adoption. According to a survey by Federal Reserve Board (2015) they found out that mobile banking among smartphone users with a bank account was substantially higher at 52% compared to earlier surveys. They found that as smartphone adoption continues to increase, mobile banking usage may also increase.

Mobile banking usage

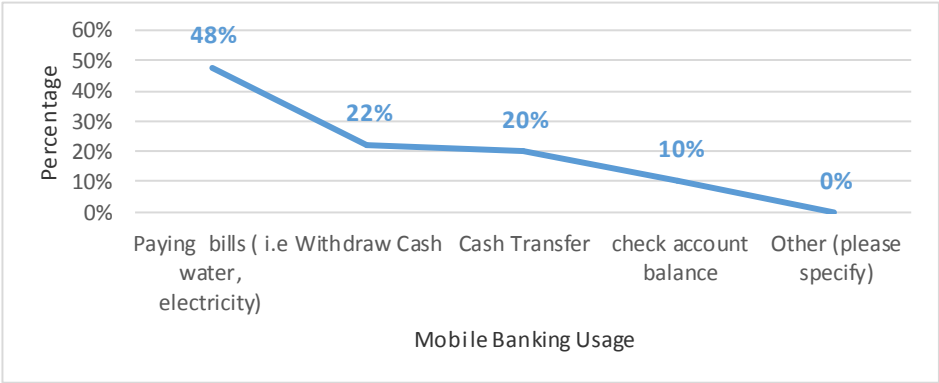


Figure 0.8 Mobile banking usage

Mobile banking is used to provide several services among them include the capability of withdrawing cash, paying bills, cash transfers from the bank to phone or from bank to

bank, checking of user account balance. From the sampled respondents majority at 48% reported to be using mobile banking for paying bills such as electricity bills, water bills among others while 22% of the respondents they reported to be using mobile banking to withdraw cash another 20% reported to use mobile banking for transferring cash either from bank to phone or from bank to bank lastly 10% of the respondents used mobile banking to check their account balance. The results of this survey were on the contrary to the study of Luvanda et al., (2014) where they found that most respondents reported to be using mobile banking services mostly to check their bank balances, following closely was the action of withdrawing money at third place was use of cash transfer.

Interval of mobile banking usage

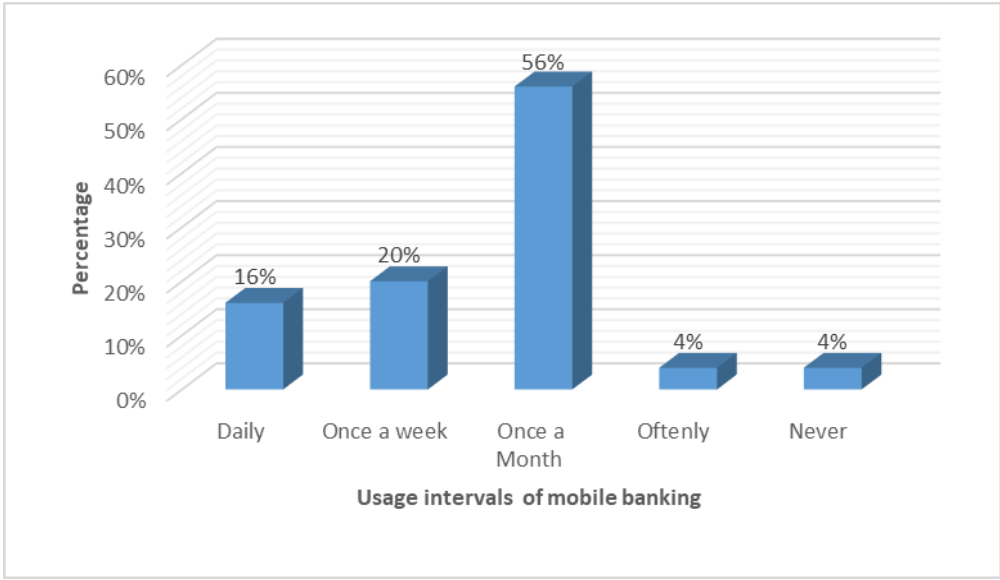


Figure 0.9 Interval of mobile banking usage

From the survey 56% of the respondents reported to be using mobile banking service once a month, following second was 20% who reported to be using mobile banking once

a week .The results from the survey showed that 16% of the respondents used the mobile banking service on a daily basis whereas those that used the service often share 4% with those that never used mobile banking service.

Reasons that hinder mobile banking adoption

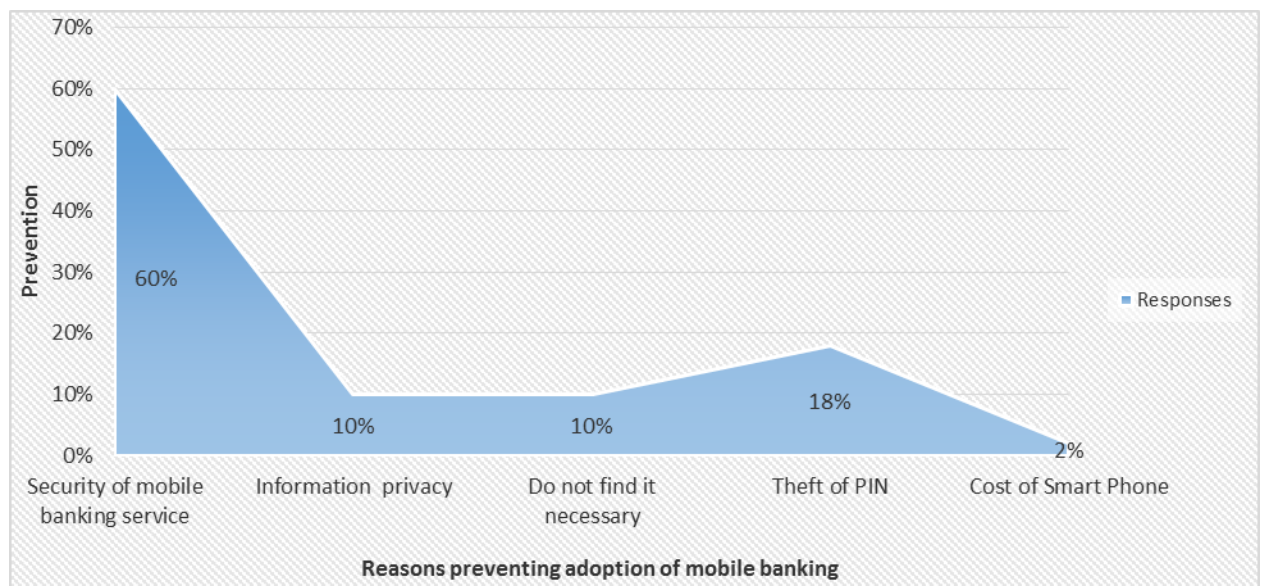


Figure 0.10 Reasons that hinder adoption

Security of the mobile banking service is a major concern that would prevent majority of the respondents comprising of 60% from adopting any mobile banking service. This shows that users of mobile banking need to gain the trust of the bank that their mobile banking service is secure, another 18% of the respondents reported that theft of PIN was one of the reasons that would prevent them from adopting mobile banking while 10% of

the respondents reported that information privacy would be a reason that would prevent their adoption of the mobile banking service. Cost of smart phone and not finding the service necessary would cause 2% and 10% respectively of respondents not to adopt mobile banking. The findings of this survey can be compared to the study by Pegueros (2012) where he found that in order to gain user adoption of mobile banking and payments, confidence in the security of the mobile banking services need to be addressed.

Concerns in mobile banking adoption

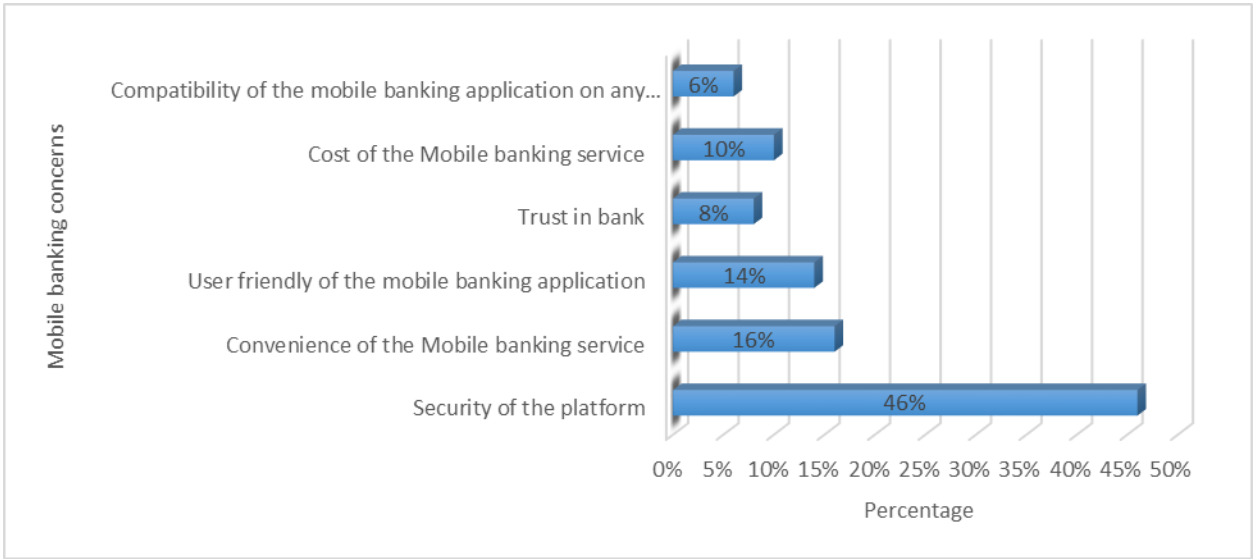


Figure 0.11 Concerns in mobile banking adoption

According to the findings 46% of the respondents reported that security of the mobile banking platform was a major concern in mobile banking adoption, 16% reported to be concerned about the convenience of the mobile banking service. Mobile banking application user friendliness was a concern in among 14% of the respondents reporting that it would be a concern in adopting the service while 10% of respondents reported that the cost of the mobile banking service would be a concern in mobile banking adoption. Trust in the bank providing the service and compatibility of the mobile banking application on any smartphone was a concern among 8% and 6% of the respondents respectively. These findings are similar to the study by Monitise & Cognizant (2013) where they found that 70% of respondents believed that security was a major concern, 32% of non-mobile banking users cited security as the most important concern when considering mobile banking adoption. Another survey that also showed similarity to the survey findings was Crowe et al. (2016) survey on mobile shopping, banking and payment, where security concerns was top on the list of mobile banking barriers among the respondents, followed by a preference for physical locations and those that did not need the service came in last. However a study by Luvanda et al., (2014) on Kenyan mobile phone users, had contradicting results compared with the survey findings in that from their study they reported that majority of mobile banking users were more interested with the ease of performing financial transactions rather than with the related security issues in mobile banking.

Smartphone Skills and experience

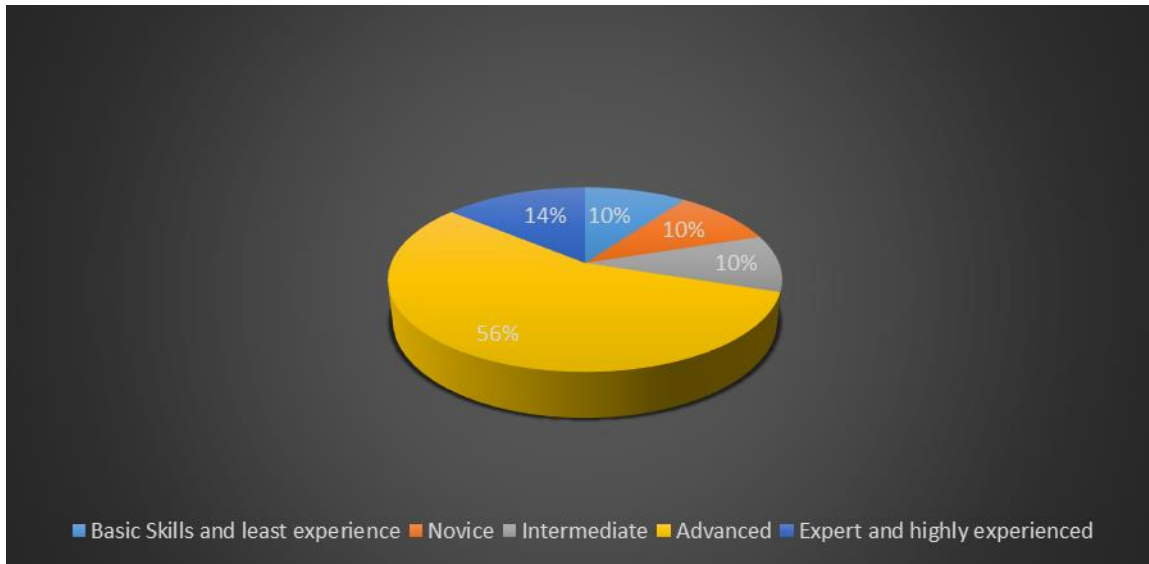


Figure 0.12 Smartphone skills and expertise

This question wanted the respondents to rate themselves in terms of smartphone skills and experience using likert scale of 1 to 5, where 1 being the lowest and 5 being the highest. From the findings 56% of the respondents reported to have advanced skills and experience with smartphone application usage while 7% reported to be experts and highly experienced when it comes to using smartphones. Respondents with intermediate skills, novice, basic skills and least experience each shared 10%.

Mobile Banking experience

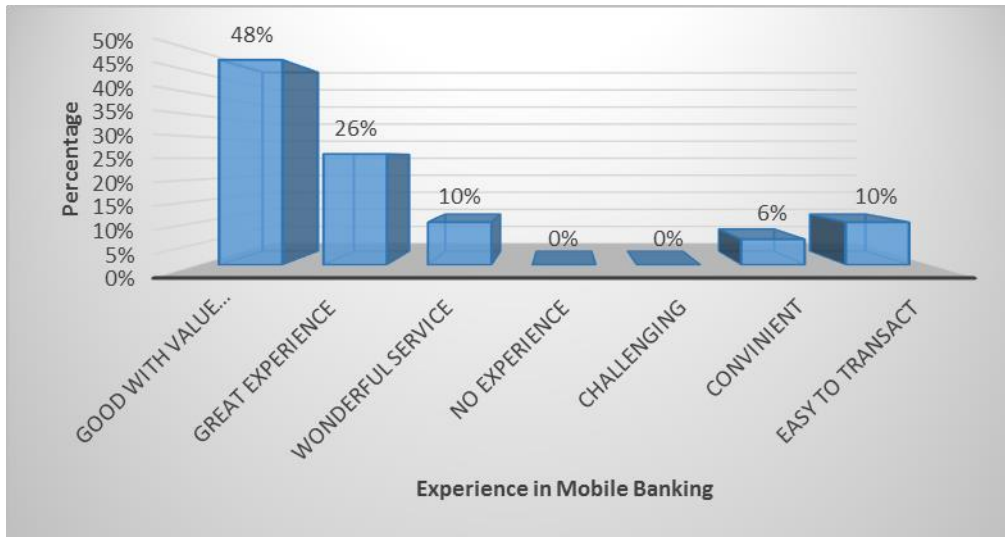


Figure 0.13 Mobile banking experience

There was a question from the survey that sought to get an understanding of the experience the respondent has had while carrying out financial transactions through their smart phones where a majority of the respondents at 48% reported to have found conducting financial transaction through smartphones good with value addition while 26% reported to have had a great experience with conducting financial transaction through their smartphones finding the transactions efficient and convenient another 10% of the respondents found it being of wonderful service and this was shared also shared with 10% who found it easy to transact. None of the respondents reported of having challenges with conducting financial transactions or of having no experience. Sharing similar findings to this survey were the study by Ndumbi & Muturi (2014) where they found that 77% of KCB Nakuru branch customers found mobile banking easy to use due to its accessibility, time saving and comfort.

Security in mobile banking service

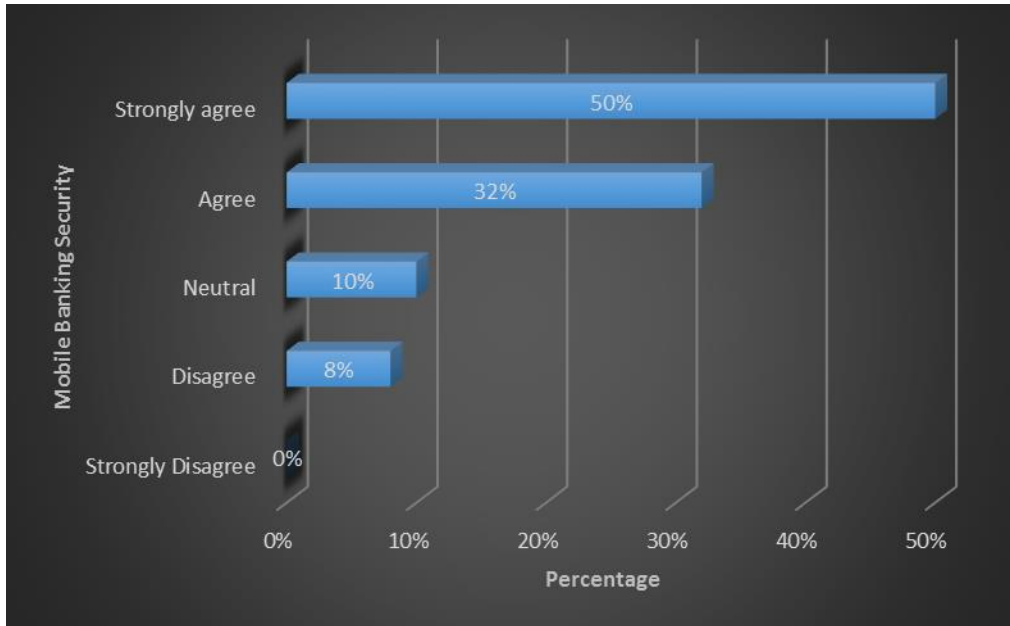


Figure 0.14 Security in mobile banking service

From the findings 50% of the respondents strongly agreed that their preferred banks were secure in service provision through mobile banking while 32% of the respondents reported to agree that their mobile banking service was secure from their preferred banks. There were 10% of the respondents who were neutral when it came to whether their preferred banks had a secure mobile banking service another 8% reported to that they disagreed with how secure the mobile banking service was from their preferred banks.

There were no respondents who reported to have strongly disagreed with how secure their mobile banking service was from their preferred banks. Worth noting is that the respondents had trust in their banks that their mobile banking service was secure which is contrary to what to the study by TESPOK (2014) that focused on thirty three local banks where from their findings they reported that only two local banks had adequate safety measures geared towards securing their customers. This shows as much as users have trust in their banks when it comes to mobile banking service ,majority of the local banks need to invest more on security measure to prevent possible attacks that are targeted to their customers. Africa Cyber Security Report (2018) reported that Kenyan Commercial banks remain attractive to cyber criminals since they still hold the biggest cash reserves. Banks are getting hit through their web applications, Internet and Mobile banking platforms. Cyber criminals gain access to bank systems through sharing of authentication details opening a backdoor to systems. In order to address this security concerns this research proposed use of Keystrokes dynamics and location verification in authentication in that even if the authentication details are shared it would be a challenge to type exactly as the account owner and carryout transactions at their known location.

Security features on mobile banking transaction

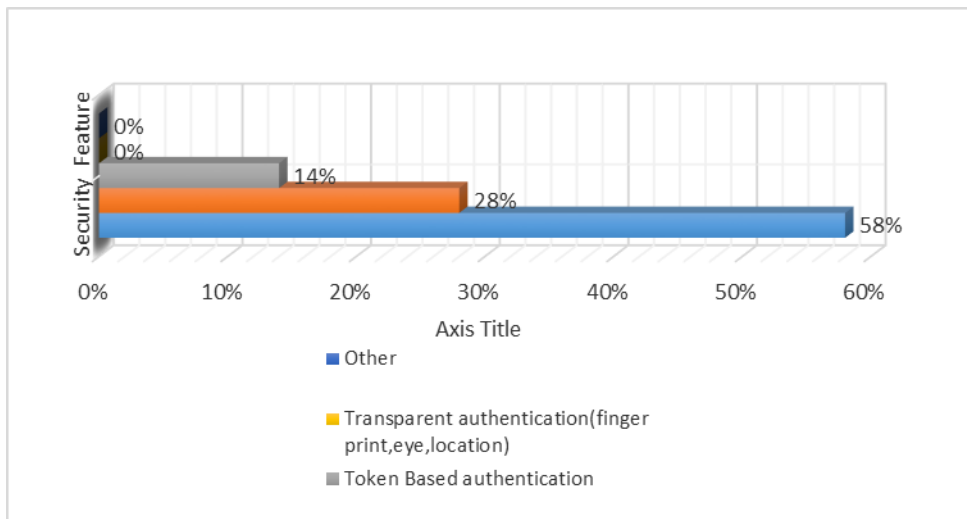


Figure 0.15 Security features on mobile banking

This question was meant to find out and answer one of the research questions about the existing mobile banking authentication methods deployed by local banks. From the findings, most of the banks are using PIN as an authentication feature in mobile banking transactions according to 58% of the respondents. In this research, 28% was the use of password as an authentication security feature on mobile banking transactions, where 14% of the respondents reported that their preferred banks used token-based authentication as a security feature for their transactions. There were no respondents who reported the use of transparent authentication as a security feature for their mobile banking.

transactions. Aloul et al., (2009) shared similar findings with this survey, in that most mobile banking systems relied on single non dynamic PIN/passwords to verify the user's identity.

Mobile banking service updates

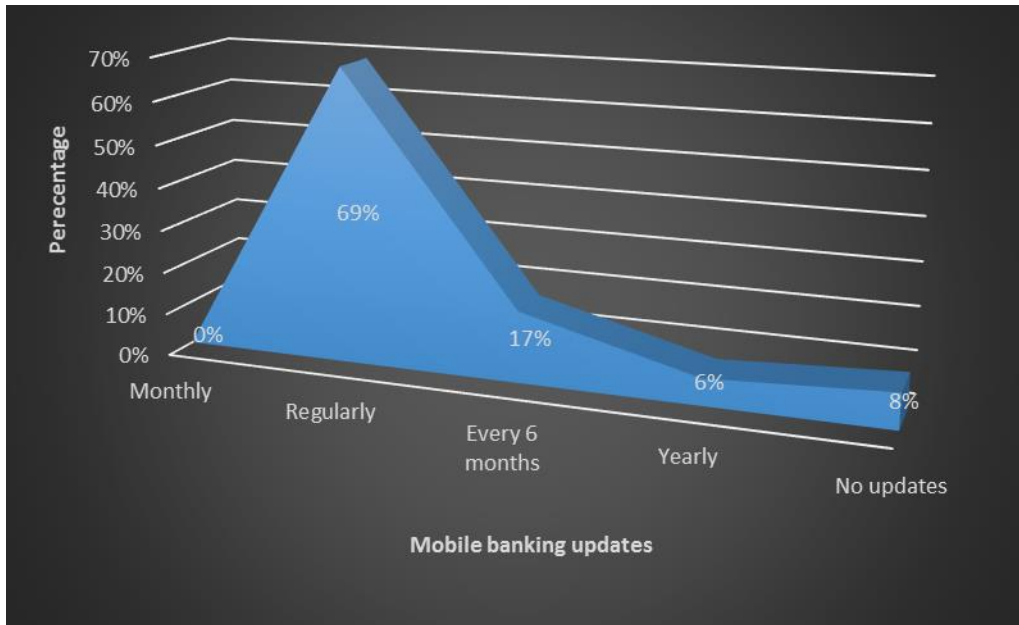


Figure 0.16 Mobile banking service update

With the advancement of technology new threats and vulnerabilities are on the rise hence it is essential for any financial institution to ensure that their systems are updated to prevent unauthorized access. Results from the survey showed that 69% of the respondents reported that their preferred banks did mobile banking service updates on a quarterly basis. There are other banks that did updates after every 6 months based on

findings from 17% of the respondents while 6% of the respondents revealed that their banks did updates on the mobile banking service on a yearly basis.

There are 8% of the respondents who claimed that they did not receive any updates on their mobile banking service. None of the respondents claimed that they received updates on a monthly basis.

Change of authentication details

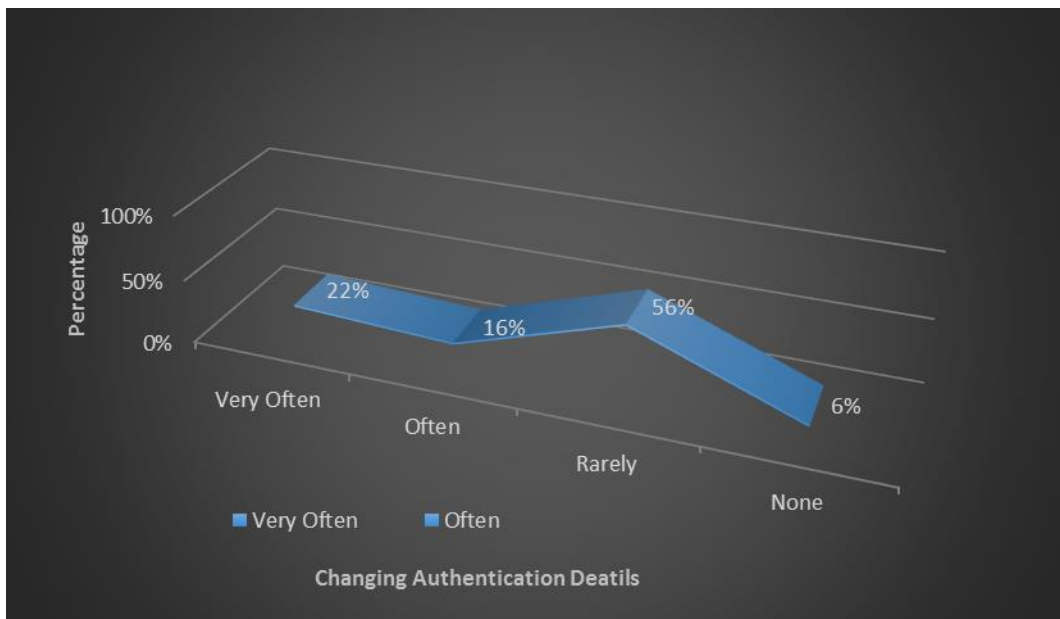


Figure 0.17 Change of authentication details

Majority comprising of 56% of the respondents reported that rarely did they change their authentication details while 22% reported that they did change their authentication details very often another 16% reported to be changing their authentication details often.

There were 6% of the respondents that responded they did not change their authentication details by answering none from the choices provided in the question. This meant that they continued to use the default authentication details issued to them by the bank when they subscribed to mobile banking. The findings of this survey can be compared to a survey by CSID (2012) where he found that 61% of the consumers reused their passwords while 54% had less than five passwords another 44% reported to be changing their passwords less than once a year. Another study that shared similarities with the survey findings was a study by Koong et al., (2014) where they found that people always use the same password everywhere and rarely change it.

Suspicious activity on mobile banking account

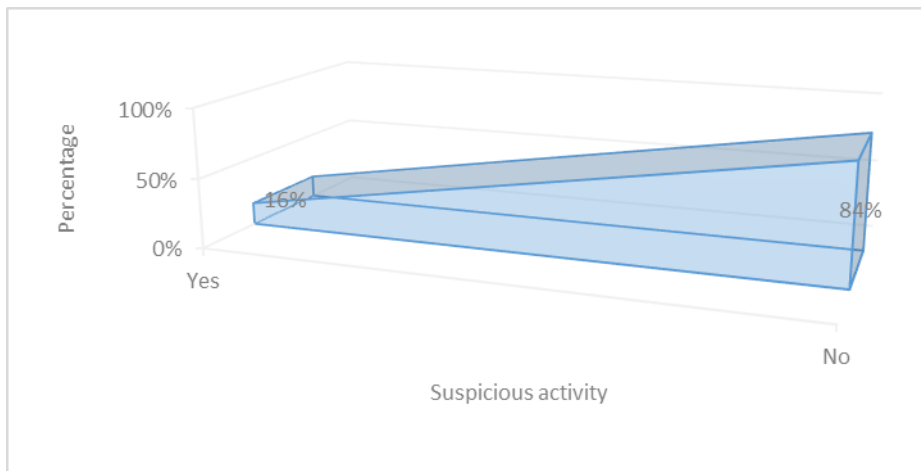


Figure 0.18 Suspicious activity on mobile banking account detected.

Financial systems are prone to attacks hence why banks invest in ensuring that their systems are secure to gain trust of their customers. Criminals know this and they have

moved to targeting individual users trying to get unauthorized access to their accounts resulting into suspicious activity on the mobile banking accounts. Most of the respondents comprising of 84% who claimed to not having any suspicious activity on their accounts while 16% reported to have experienced suspicious activity on their mobile banking accounts. Cases of mobile application breaches have been low a report by Identity Theft Research Center (2016) showed that Mobile application breaches represented less than 3% of all computer records hacked in 2016.

Capturing user behavior through Keystrokes dynamics and location verification to secure mobile banking transactions

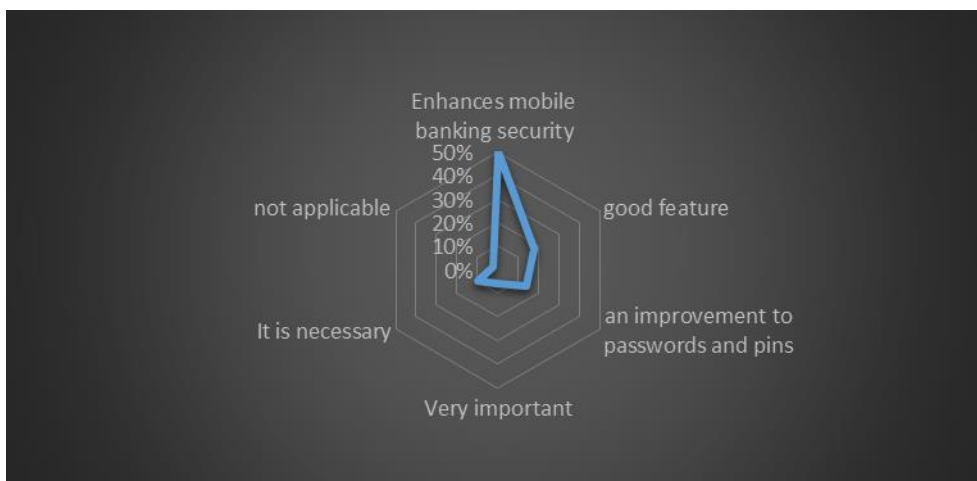


Figure 0.19 Capturing user behavior and location verification to secure mobile banking transactions

Respondents were asked about their take on capturing user behavior through Keystroke dynamic and location verification to improving mobile banking security from the survey

50% of the respondents reported that they saw this method as a way of enhancing mobile banking security while 18% saw it as a good feature to have on their mobile banking application another 14% claimed that it was an improvement to the commonly used pins and passwords, thirdly 10% found it necessary to have this feature while 6% reported to have seen this as an important feature when it came to security of mobile banking transactions, comprising of 2% of the respondents found that this method wasn't applicable to security of mobile banking transactions. Capturing user behavior and location verification has been found to enhance mobile user verification leveraging on either the geographic data or the smartphone sensory data Montoya et al., (2013) and Gambs et al., (2013). Another study by Krishna (2017) found use of Location Awareness and an intelligent multi-modal Authentication could provide higher security.

Using user typing behavior and location verification to secure mobile banking transactions

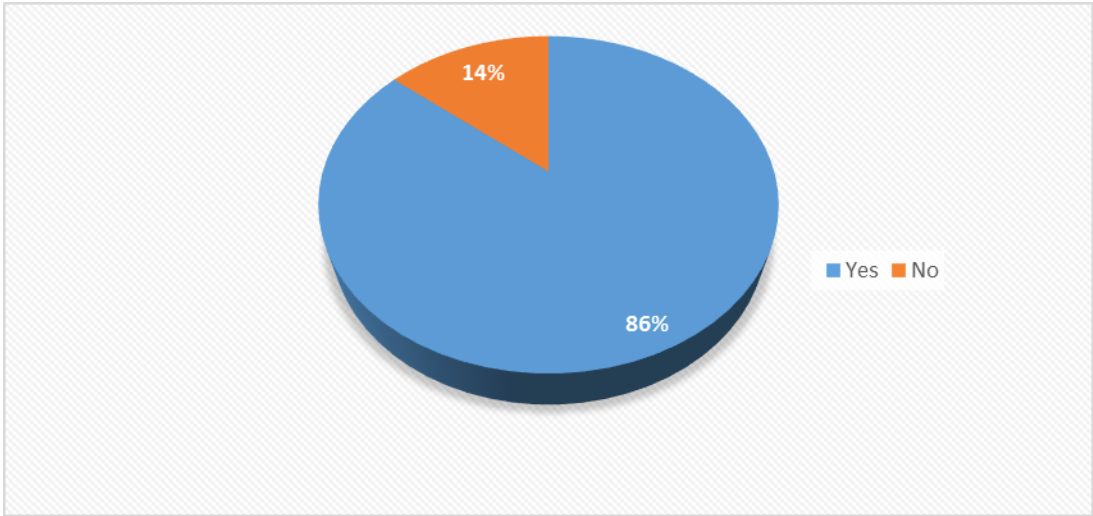


Figure 0.20 Using behavior and location verification to secure mobile banking transactions

Following the findings in the figure 4.17 where a majority of the respondents reported that using typing behavior and location verification to secure mobile banking transactions was a way of enhancing mobile banking security hence 86% of the respondents from the figure 4.18 above reported that banks could adopt this method for their mobile banking application while 14% reported that they didn't find it needful for banks to adopt this method.

Similar to the survey findings a research by Lin et al., (2015) found out that the main objective of mobile user profiling and identification was to discover the discriminative pattern that can be consistently rediscovered for the same person not for another different person. Another survey by Prasad et al., (2015) that can be compared to this survey found that banks could make some innovation and customization in mobile banking services with the use of Location authentication and other advanced technology,

Enhancing mobile banking security

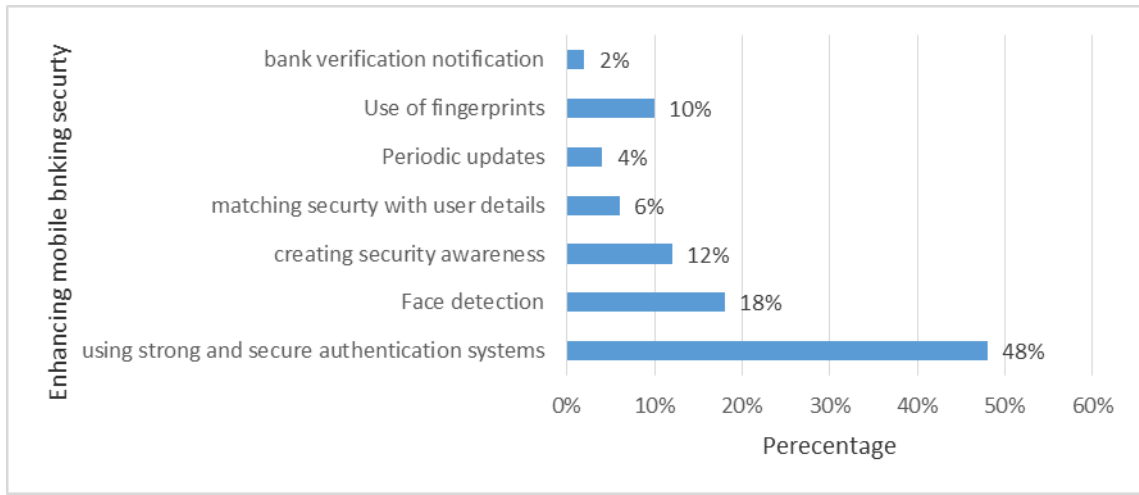


Figure 0.21 Using behavior and location verification to secure mobile banking transactions

From the findings majority of the respondents at 48% reported that using strong and secure authentication systems could make mobile banking more secure. The need to have use of biometric authentication to secure mobile banking transactions was considered among 18% of the respondents who suggested use of face detection while 10% suggested use of fingerprints. Creating security awareness was a consideration among 12% of the respondents as another 6% of the respondents felt that matching security with finer user details an example of this could be use of security questions tied to user's details, comprising of 4% of the respondents reported that periodic updates could enhance security of mobile banking authentication ,lastly 2% of the respondents suggested use of bank's verification of the user before proceeding with mobile banking could enhance its security. Worth noting is that the use of biometrics and multi factor authentication has been proposed as a secure method in user authentication and

verification this is from a study by Aithal (2015) where he found that this method assessed its relevance for mobile banking.

Another survey by EyeVerify (2017) found that 79% of respondents wanted the use of biometrics such as use of eye, face, and fingerprint and voice authentication to log into their mobile banking or payment apps.

4.3 Discussion and Analysis of survey questionnaire responses.

An online survey questionnaire was prepared of which a total of 138 respondents participated in the survey from a sampled population of 153 out of 247 respondents who comprised of Kenya Commercial Bank (KCB) head office branch at Kencom according to KCB Integrated report and Financial Statements (2014) giving a 90% response rate. KCB mobile banking platform was declared the best in Kenya (Thinking Business Awards, 2017). Most of the respondents from the survey were male comprising of 31 (62%) while females were 19(38%) of the total respondents sampled.

4.3.1 The Use of Smartphones in Mobile Banking

All of the respondents who participated in this survey reported to have smartphones and most them at 57% reported to be advanced in skills and expertise with use of smartphones. According to a report by GSMA (2018) where their findings showed that more than 60% of Kenyans owned a smartphone, while mobile subscription was at 82%. The report attributed this to the growth of smartphone penetration in Kenya owing it to the availability of affordable smartphones over the last 5 years.

With the rise of smartphone usage comes with the rise of mobile banking according to the respondents who participated in this survey most reported to have subscribed to

mobile banking service. According survey by Federal Reserve Board (2015) mobile banking among smartphone users with a bank account was substantially higher at 52% compared to earlier surveys. The higher incidence of mobile banking adoption among smartphone users suggests that as smartphone adoption continues to increase, mobile banking usage increases. Similar to the findings of this survey, a research by Juniper Research (2016) showed that an increase to consumer adoption of banking applications was a major contributor to mobile banking the research also found that over two billion mobile users will have used their devices for banking purposes by the end of 2021, compared to 1.2bn in 2016 globally. Mobile banking offers several services among them include paying bills, cash transfers, cash withdraw services, loan services, checking account balance.

From the respondents who had subscribed to mobile banking most of them reported to be using the service mainly for checking account balance and withdrawing cash. Other uses reported were cash transfer and paying of bills was the least used mobile banking service among the respondents. The findings of this survey compared to the study of Luvanda et al., (2014) where they found that most respondents indicated that they accessed their banking services via mobile phones to check their bank balances, closely followed by the action of withdrawing money and cash transfer being the third most accessed banking service from his study.

4.3.2 Mobile Banking Security

From the survey majority of the respondents reported that security of the mobile banking service would prevent them from using mobile banking. This showed that security was key in respondent's adoption for any mobile banking service. Pegueros (2012) found that in order to gain user adoption of mobile banking and payments, confidence in the

security of the mobile banking services should be addressed from within the mobile banking solutions. Security of the mobile banking platform was the most considered among respondents as an important consideration of mobile banking followed by Convenience of the Mobile banking service, user friendliness of the mobile banking application and trust in the bank.

According to a report by Cognizant (2013) among mobile banking consumers, 70% of respondents believe security is a major concern 32% of non-mobile banking users cite security as the most important concern when considering mobile banking adoption. Similar to the findings of this survey was a recent report on Consumers and Financial Service in 2016 conducted by Federeal Reserve System (2016) showed that concern about the security of the technology was a common reason given for not using mobile banking or mobile payments with 73 percent and 67 percent, respectively of non-users. Crowe et al. (2015) survey on mobile shopping, banking and payment found security concerns was top on the list of mobile banking barriers among 53% of the respondents , followed by a preference for physical locations 31% and not needing the service 28%. Contrary to this survey findings was a study conducted by Luvanda et al., (2014) on Kenyan mobile phone users reported that the majority were more interested with the ease of performing financial transactions rather than with the related security issues in mobile banking. Despite his findings he considered mobile banking security issues are still a major concern within the mobile computing circles.

From the findings majority of the respondents reported that they found transacting on mobile banking easy. Davis et al., (1989) defined perceived ease of use as the degree to which a person believes that using a particular system would be free of effort within an organizational context.

4.3.3 Mobile Banking Acceptance

The findings of this survey shared similarities with the study of Luvanda et al., (2014) where he found that users experienced mobile banking in terms of speed and ease of use. Another study conducted by Ndumba & Muturi (2014) found that 77% of KCB customers in Nakuru found mobile banking easy to use due to its accessibility, time savings and comfort. Majority of respondents report that their banks were secure when its came to providing mobile banking service. Those who were neutral about the security of their mobile banking service came in third while those who disagreed with how secure their mobile banking service was came in fourth. The respondents felt that their banks were secure when it came to mobile banking hence why they expressed confidence when performing transactions.

The findings from the survey were different from how banks were secure when it came to mobile banking according to Kigen et al. (2015) study that focused on thirty three banks where he found that only two banks had adequate safety measures geared towards securing their customers. According to the Vedapradha and Ravi (2018)

report, 83% of respondents reported that they used mobile banking and that banks were investing in mobile banking capabilities at rare levels to attract and keep customers. The study ranked the largest 15 banks and credit unions in the US by whether they offer the mobile features that customers say they care most about. Wells Fargo Chase, Citibank and Bank of America lead the way relative to mobile banking functionality being the banks that offered in-demand mobile transfer capabilities, along with competitive features related to security and mobile wallets.

4.3.4 Existing mobile banking authentication methods

When it came to securing mobile banking transactions the most common security feature among the majority of respondents was use of Personal Identification Numbers (PINs) followed by Passwords and use of Tokens came at a distant third. None of the respondents reported the use of transparent authentication feature which involves use of physiological biometrics or behavioral biometrics.

Physiological biometrics such as fingerprint scanning or face recognition or behavioral biometrics such as keystrokes, location or touch. A study by Aloul et al., (2009) shared similar findings with this survey, in that most mobile banking systems relied on single non dynamic PIN/passwords to verify the user's identity.

4.3.5 Threats and vulnerabilities of mobile banking systems

Aloul et al., (2009) found that passwords faced major challenges in management and security. Where users may use easy passwords that can be guessed, or similar passwords for different accounts, or store their passwords on devices or write them on a piece of paper. Management and security challenges may be a weak point for hackers to steal passwords through shoulder surfing, snooping, sniffing, and guessing. Passwords and PINS are not secure for mobile and the internet originating transactions. Passwords that are based on first or last names, account holders age, or date of birth, can easily be predicted using dictionary attack applications that are freely available to hackers. Another research by Leigh (2013) showed that PINs are weak and vulnerable to simple hacking. Armed with only four possibilities, hackers can crack 20% of all PINs. According to Kigen et al. (2015) the most common attacks to local banks recently include insider threats, spear phishing and ransom ware attacks. To be able to counter these threats the Central Bank of Kenya

(2017) issued a guidance note on cyber security to all local banks meant to help banks deal with cybercrimes and prepare for emerging threats which were on the rise with advancement of technology.

4.3.6 Mobile Banking Application Updates

Regarding the how banks carried out security updates to their mobile banking service most of the respondents reported that they received updates on a regular basis, followed by those who received updates after every 6 months and thirdly those who received updates on an yearly basis. Lastly there were also those who reported that they did not receive any updates. According to Thinking Business Awards (2017) Kenya Commercial Bank (KCB) was recognized as the best bank in mobile banking. KCB's mobile application was launched in 2016 and the bank has been doing regular updates on their application with the recent one being on September 2018 (KCB, 2018). Despite the banks issuing regular updates the Kigen et al. (2015) findings revealed that individuals who have subscribed to mobile banking services risk exposure to cyber related criminal activities. They also found that the number of institutions using mobile money and have adequately implemented security controls were minimal within the country.

Following this report this study aims to provide an alternative authentication method that banks can use to address the issue of security.

4.3.7 Change of Authentication Details

There was a question seeking to find out how often the respondents changed their authentication details on their mobile banking applications. A majority of the

respondents reported that they rarely changed their PINs, this was followed by those who reported they changed their PINs very often, thirdly were those who reported that changed their passwords often. A small percentage of the respondents reported that they did not change their PINs at all. Comparing the findings of this survey to a survey by CSID (2012) about password habits of American consumers, 61% of the consumers reused their passwords, 54% had less than five passwords, 44% reported to be changing their passwords less than once a year .Another study by Zaidi et al. (2016) found that almost all the smartphone OS provide mechanisms for users to enhance the security of their devices by certain login mechanisms. However, more than 30%, Mobile phone users do not use the PIN on their Phones. Similar to the findings of this survey a study by Koong et al. (2014) found that people always use the same PINs/Password everywhere and rarely change it.

4.3.8 Suspicious activity on their mobile banking

Respondents were asked if they had experienced any suspicious activity on their mobile banking account a larger percentage of the respondents reported that had not experienced anything suspicious with few reporting that they had experienced suspicious activity on their mobile banking account. A report by Identity Velasquez et al. (2017) showed that Mobile application breaches represented less than 3% of all computer records hacked in 2016.

4.3.9 Behavior profiling and location verification authentication

Respondents were asked what their take was on capturing user typing behavior also known as keystrokes dynamics and location verification to improving mobile banking security, from the findings majority of the respondents reported that they thought of it as

an enhancement of mobile banking security. Those that considered it as a good feature came in second, followed closely at third place were those who considered it as an improvement to passwords and pins. There were respondents who found it necessary and important while the least percentage of the respondents found it not being applicable to mobile banking.

According to Lin et al. (2015) entering a short personal identification number (PIN), drawing a one-stroke pattern require users' active cooperation to set up and to memorize a numeric or graphic draw pattern such methods have been widely adopted the imposition on users to memorize and manage their secret credential, and enter it all the times is a significant burden. To ease the burden they proposed passively modelling and monitoring the subtle behavioral patterns of the users on the ubiquitous location-analyzed data. Several studies Montoya et al. (2015) and Gambs et al. (2012) have also leveraged on either the geographic data or the smartphone sensory data in enhancing mobile user verification. Parkavi et al. (2017) found that through an intelligent multi-modal Authentication with Location Awareness could provide higher security for new mobile banking services such as Digital deposit apps, advanced bill payment apps, and Electronic meeting for mini loan services and Mobile payment apps.

The location, where the mobile banking transaction has been executed is captured giving the additional option for a Bank to verify if the transaction has been executed normally or if the parameters are at variance with normal practice. Previously, relevant research works have been carried out in the areas of mobile user profiling and user identification.

A research by Bayir et al., (2009) on mobile user profiling, profiled individuals' mobility patterns using spatial-temporal data. This research proposed use of user profiling as a compliment to existing smartphone protection method providing a more secure user verification mechanism similar to the findings of the survey where majority of the users reported enhancement of mobile banking security through capturing user behavior and location verification to improving mobile banking security.

The use of behavior profiling through keystrokes dynamics and location verification to be adopted by banks for their mobile banking service was recommended from most of the respondents with a few denying its adoption. Several researchers have gone ahead and proposed use of user profiling and location verification an alternative to the existing authentication methods. Krishna Prasad & Karani (2017) from their research shared that with the aid of Location authentication and other advanced technology, banks can make some innovation and customization in mobile banking services. Lin et al. (2015) in their study found that the main objective of mobile user profiling and identification was to discover the discriminative pattern that can be consistently rediscovered for the same person not for a different person.

4.3.10 Enhancing security of mobile banking

From the survey there was a question on what could make mobile banking authorization more secure. This question aimed at getting the respondent's view on the security features that could enhance security of mobile banking. Using strong and secure authentication systems was on top of the list from the survey findings that respondents thought could make mobile banking authorization more secure. Aloul et.al. (2009)

explained that two-factor authorization gave more security for mobile based financial transactions other than usual username and password, by utilization biometric identification mechanism. In order for an authentication to be both strong and secure, Agoyi & Seral (2011) through their study suggested that a number of factors have to be considered that is ease of breaking the authenticating and its usability.

According to the European Central Bank (2016) strong authentication combines at least two mutually-independent factors so that the compromise of one method should not lead to the compromise of the second. Use of biometric authentication came in second with respondents recommending usage of features such as face detection and use of finger prints. A study by Aithal (2015) found that there had been a lot of work on biometric identity systems in recent years and that the biometric identity system also work and assesses its relevance for mobile banking. When a customer initiated a mobile banking transaction, the handset would request that the user to register his or her fingerprint on the sensor, and the handset would compare the fingerprint to the one already stored in the phone and also to the one stored on the bank mobile transaction server.

Aithal (2016) in his research found that biometrics is a measurable physical characteristics or personal behavioral trait used to recognize the identity or verify the claimed identity of an enrollee. Examples of physiological characteristics that are used in biometric device include fingerprints, the geometry of the face or hand and patterns within the iris or retina or in the layout of veins. Behavioral characteristics include voice pattern, gait and the dynamics of handwriting or keystrokes. For the authentication process the chosen characteristics must be unique to each individual. Also it is possible to measure the characteristics with the reasonable degree of accuracy. Once the measurement has been taken the data is converted into a biometric template. A template

is a representation of the measurement that retains all the relevant information but takes up far less space than the original.

It is this template that is compared to a template generated in the same manner during the initial enrolment procedure and based on the similarity of the two, a decision is made whether the user should be granted access. The suggestion to have use of biometrics in mobile banking can be compared to a survey by Eyeverify (2017) where they found that 79% of respondents want the opportunity to use eyes, facial, voice and fingerprint authentication methods to log into their mobile banking or payment apps. Most people (78%) perceive biometrically enabled mobile applications as more secure, according to the study, and 80% said they believe apps that can access bank accounts should use biometric authentication.

Other suggestions from the respondents in regards to making mobile banking more secure included:

- Creating security awareness
- Matching security with user details
- Periodic updates
- Bank verification notification

4.4 Conclusion

This chapter presented the survey findings as well as its analysis that aimed in answering the research questions. In general the use of smartphones is high owing it to the low

costs of acquiring them provided by competitor brands. From the survey the use of PINS and passwords is still high among local banks, however some banks are starting to embrace the use of additional features in the applications. There is need for additional security controls when it comes to mobile banking to fill in the current existing gap especially in the security controls put in place for mobile money services as the current authentication methods could easily be overridden when the authentication details are shared to cyber criminals. The number of institutions using mobile money and have adequately implemented security controls were minimal within the country. This research aims to contribute to mobile banking security by proposing use of behavioral profiling through keystrokes dynamics and location verification in securing mobile banking transactions. The expected outcome is to demonstrate a method that incorporates behavior profiling and location verification as an alternative authentication of mobile banking transactions.

CHAPTER FIVE

ALTERNATIVE METHOD FOR SECURING MOBILE TRANSACTIONS

5.1 Introduction

Mobile banking is becoming an attractive target for criminals due to the increase in number of users and the limited fraud detection and prevention capabilities. From the analysis of the survey there is need for additional security controls from users when it comes to mobile banking.

5.2 Behavior profiling and location verification authentication

From the evaluation of the current existing authentication methods behavioral authentication is unique in that it's harder for someone with malicious intent to successfully capture a natural motion improving on PIN/password only authentication. The addition of location verification to behavioral profiling not only authenticates a user based on how they type but also provides a procedure to grant access to the application by verifying that the user actually did the transaction at the submitted location which is compared with the information stored in the database.

This method of authentication combines a user's typing sequence behavior together with the transaction location over a period of 30 days creating a user's profile with an average of ten transactions based on the location visited. The use of behavior profiling systems can provide continuous and transparent identification while users interact with mobile applications for various services. The aim here is to be able to study the user's typing sequence behavior and the location visited and being able to create an authentication method that uniquely identifies the user moving away from PIN/password only authentication. With the current technological advancement of smartphones it is possible to capture user's behavior through special inbuilt sensors and features. In this authentication method the user's typing behavior profile is captured using an android touch screen keyboard sensor as it's able to note down each user's typing sequence and speed every time they log into their mobile banking application. The location of where the transaction was done is captured via a GPS (Global Positioning System) module which is a set of satellites, that provide an opportunity for anyone with a GPS receiver to determine the device's location under any weather condition at any time from a

smartphone, Location information can also be obtained through a cell tower triangulation and through Wi-Fi networks.

The application is location aware as it keeps track of the user location in real time. The mobile banking application works on smartphones that operate on android operating system which is available on most smartphones that are in the market and from the survey conducted all of the 138 respondents had smartphones that operated on android. The transactions done on the mobile banking application include depositing money, withdrawing money, paying bills such water, electricity, internet, checking banking statements and account balance. As the user logs into their account the smartphone's touch screen sensor captures their typing sequence and their location that gets stored in the database. This happens for a period of 30 days as the application studies the user and creates their profile. The location verification is meant to get current user's transaction location and do a verification based on the last transaction location and if there's difference a security question will be asked which when entered wrongly over three attempts the user cannot be able to access their mobile banking application. The capturing of the user's typing behavior and location is done in the background as they interact with the application.

Once the user's profile has been created in the database every time they log into their mobile banking application as they type their PIN and account number the application compares the current typing sequence with an existing template in the database, once there is a match the application proceeds to verify user's transaction location upon which there is a match gives access to carry out a transaction. This method demonstrates that each user has a different typing behavior and a preferred location transaction which can

be obtained based on an average of ten transactions of which a transaction should take place within a given range.

This authentication method is unique to a person and rarely can a user can have the same typing sequence as the other user even if they share their PIN/passwords and carry out a transaction at the same place. It is for this reason that this research proposes use of behavior profiling and location verification authentication as an alternative method of securing mobile banking transactions since behavioral biometric authentication methods are cheaper than physiological ones as they do not add costs to smartphones.

5.3 Composition of the proposed authentication method

The proposed alternative method for securing mobile transactions is based on behavioral profiling which is an improvement from the study of Singh et al., (2017) on behavioral profiling users as they type their passwords having features such as keyboard monitoring, features extraction, classifier algorithm and a database. In their study they reported that keystroke dynamics was not enough by itself which is why this study seeks to improve their authentication method with the addition of location verification which ensures security of mobile transactions based on the user's transaction location captured by smartphones GPS sensor and it' application to mobile banking.

5.3.1 User Behavioral profiling

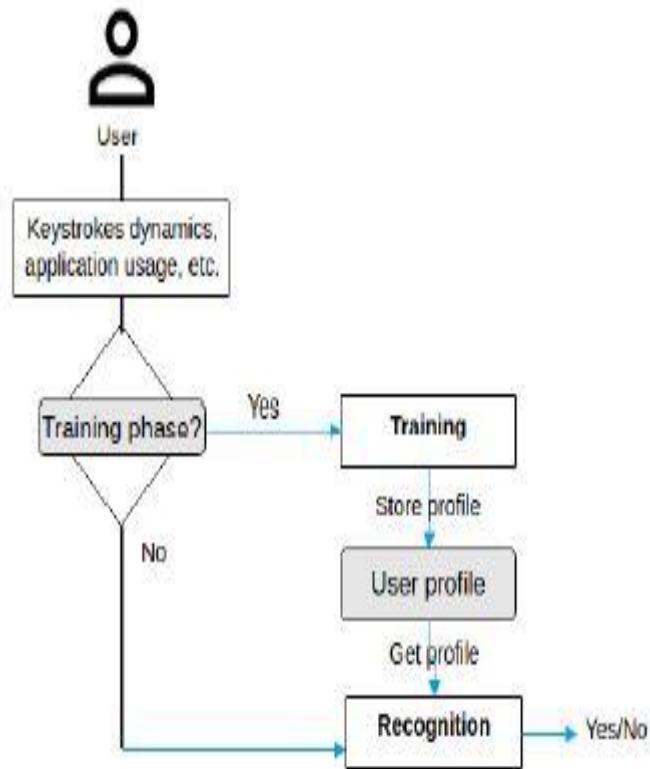


Figure 0.22 User Profiling Singh et al., (2017)

5.3.2 Users Location Verification

Based upon the hypothesis that people have a predictable travelling pattern, a user's location can be detected through use of mobile cellular network or through Global Positioning System (GPS) link (i.e. longitude, latitude). Geo location authentication is gaining importance as it is found most suitable for mobile devices. It ensures security of mobile transactions based on the user location (Akoramurthy & Arthi, 2017). By

recording the users' location information over a time period and combining the location information pattern with the user's behavioral profile creates a distinctive verification to a user which is unique to each individual in line with Aithal (2016) research that for an authentication process the chosen characteristics must be unique to each individual.

This method can provide sufficient discriminatory information to identify mobile users. Callsign (2019) in their research found out that geographical location for low-friction authentication could be used in online banking and retail, insurance companies or media companies. Given the widespread use of mobile devices, geographical location is a particularly interesting modality for behavior driven authentication. Providing the user has consented to collecting location information, we can determine which places the user typically visits and then compare them to the reported location for the current authentication attempt. In this way, we are able to determine whether the reported location matches the user's typical behavior.

5.3.3 Keystroke Capture

Through use of in built touch screen keyboard sensors available on smartphones user's typing behavior is captured which later on used to characterize the user's unique typing behavior. This takes place as users' type in their 4 digit PINs during registration of new users and authentication of registered users. Keystroke capture stores the timing information in relation to the pressed key buttons. Behavioral profiling takes place based on user's PIN typing behavior that will be used to uniquely distinguish him/her after training and getting to differentiate from an imposter having to compare with an existing typing template stored in the database. Cherkashina & Gerget (2016) in their study found out that keystroke dynamics may be compared using different kinds of methods, especially bio-inspired or neural networks-based algorithms and probabilistic-statistical

methods of decision making. Kochegurova et al. (2017) found that neural network based methods, provide high precision and they require high computation performance as well and cannot be used in real-time computations. Statistical approach is the common choice, both at the infancy stage of keystroke dynamics research and in present work. Its popularity is mainly due to its simplicity, low overhead and ease of implementation. The static keystroke is used to monitor the typing behavior of users at a specific time. Patil & Amar (2016) utilized mean and average time for pressing time, dwell time and total password.

5.3.4 Location Capture

In the background as the user types their PIN, their location is captured via a GPS module which determines the device's location under any weather condition at any time from a smartphone, Location information can also be obtained through a smartphone's cellular data and through access of Wireless networks.

Location Based Authentication Algorithm Mathematical Module (Ramatsakane et al., 2015)

1. User (U) this is actor that handles system functionality.

SET OF U= {1.....N}

2. Capture GPS Co-ordinates of User Device Latitude and Longitude factor.

2.1 Get Stored Location Co-ordinates Latitude and Longitude factor.

2.2 Calculate Distance between capture Co-ordinates and Stored Co-ordinates to define the periphery i.e. certain range within which user can get access to the data.

Formula-

Var phi1=lat1 to radian ()

```

    Var phi2= lat2 to radian ( )
    Δlambda= (long2-long1) to radian ( )
    Doubledist=Math.sin(phi1)*Math.sin(phi2)+Math.cos(phi2)
    Math.cos(Δlambda);
    Output = Find Nearest Location.

```

5.3.5 Training Phase

When the users will be typing their PIN for the first time the system will prompt them to type their preferred PIN 10 times. If a user works with the system for the first time, characteristics of their keystroke dynamics are saved with a specified account name. Otherwise, the current keystroke dynamics are added to a list for this user. When there is many records for one person the oldest one is deleted by the system. Such approach takes into account the fact that the keystroke dynamics of one person may vary in different psycho-emotional states or at different times of the day. As a background process this trains the system for recognizing user's typing behavior which will be used to recognize the user the next time they access the system. It is in this phase that the user's unique profile is generated based on their uniqueness in typing following successful training. The algorithm was created based on the probabilistic-statistical method. It enables the mobile banking application to save users typing behavior and later compare them for the authentication purpose. The system was tested with the help of sampled users. The analysis of the results aimed to show that users typing behavior combined with location verification can be an efficient authentication tool. The keystroke dynamics recognition algorithm in the training phase can be divided into 2 stages. Stage one being that the program collects a set of statistics from keystroke dynamics characteristics of a user. The second stage involves comparing the obtained

user's keystroke characteristics with standard values stored for this user. The comparison may be made with the help of any proximity measure recognition and reference. Following the stored user's profile in the database each time the user types in their PIN, a comparison based on the stored profile is done. Upon successful recognition in obtaining a user's behavioral profile the user will be prompted to verify their transaction location this is done verify in reference to the captured location that this is the actual user trying to gain access to the application.

Keystroke Capture Algorithm for in the training phase.

/* CONDITIONS

=> Initial authentication must be at least 10 logins.

=> For time, time taken to type must be average + or - 10 seconds

=> For pattern, get average of last logins. If < 90% deny else allow=>

=>For location, based on your frequent transaction locations if current login distance is greater than 200M from past transaction locations deny.

//checks if typing sequence is within the user sequence

Function getAverageTypingTime (\$userId)

{Include 'connectconfig.php';

\$typingSequence = 0;

\$arraySeconds = array();

\$arrayCount = array();

if(!\$getTyping = mysqli_query(\$link,"SELECT * FROM typingsequence WHERE
userId = \$userId AND successflag = 1"))

{

echo "Error login ".mysqli_error(\$link);

}

else

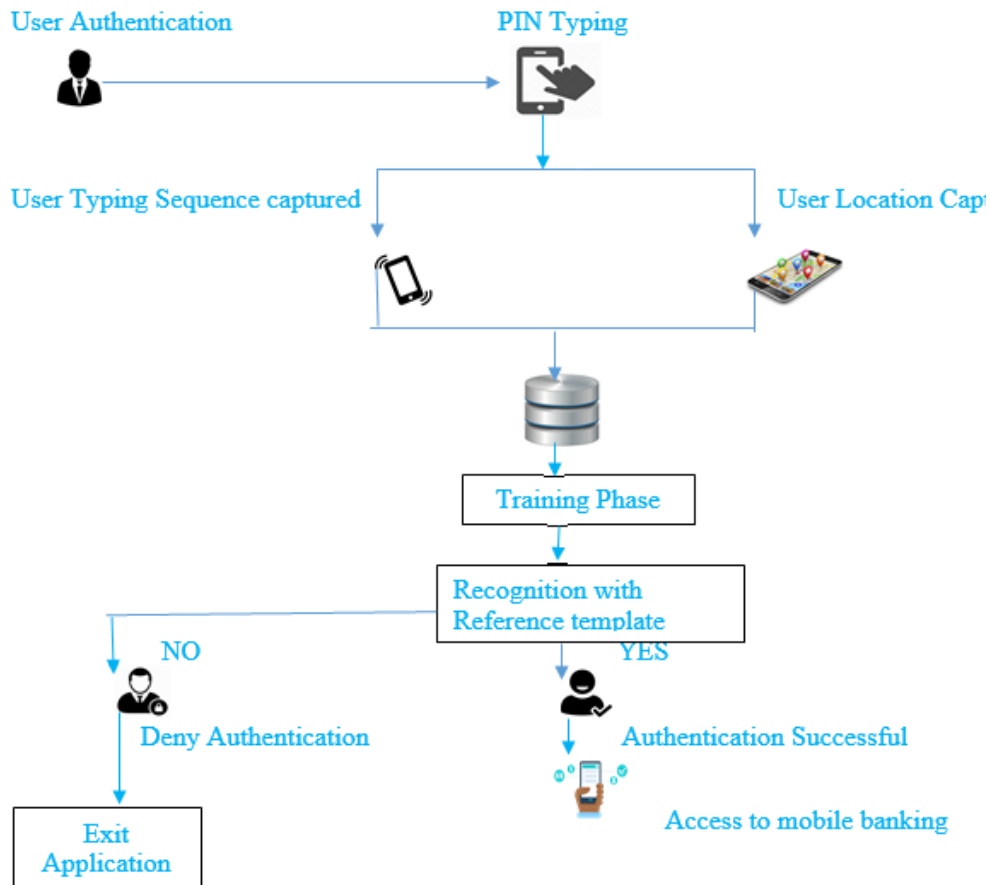
{ if(mysqli_num_rows(\$getTyping) >= 10)

```

{ while($getTypingRow = mysqli_fetch_array($getTyping ,MYSQL_ASSOC))
{
$timetaken = $getTypingRow['timetaken'];
if(in_array($timetaken, $arraySeconds)//exists - get it and increment
{ $pos = array_search($timetaken, $arraySeconds);
$arrayCount[$pos]++;}
else{ array_push($arraySeconds, $timetaken);
$pos = array_search($timetaken, $arraySeconds);
array_push($arrayCount, 0);
$arrayCount[$pos]++;}}
}
//get highest
$num = 0;
$largestNo = 0;
$largestTime = 0;
foreach($arraySeconds as $theTime)
{ if($arrayCount[$num] > $largestNo)
{ $largestTime = $theTime;
$largestNo = $arrayCount[$num]; }
$num++;
}
return $largestTime; }

```

Proposed Authentication Method



Figure

0.23 Proposed alternative authentication method

From the survey findings most of the respondents at 50 % reported that the method of capturing user behavior and location verification would be an enhancement to mobile banking security. With the rise in usage of smartphones in everyday life, comes also

with the increase in usage of mobile phones in performing banking services where a key area of concern for consumers and financial service providers is security. When it comes to behavioral biometrics such as signatures the typing pattern behavior of a user is unique to a person and is also the same for him.

5.4 Validation of the proposed method through an Experiment

5.4.1 Participant Profile

A total of 60 respondents comprising of 86% out of the sampled population from Kenya Commercial Bank (KCB) head office branch participated in the two experiments. The respondents had advanced level of skill when it came to smartphone use and experience with mobile banking based on the survey findings and their participation in this experiment was ideal for evaluating the proposed alternative authentication method.

5.4.2 Experiment 1

In this experiment the objective was to engage users for a period of 30 days on use of traditional authentication methods such as PINs and Passwords and what their preferences were when it came to creating them and whether the default settings issued by the bank were changed and examine their considerations for authentication.

5.4.3 Results

From the experiment the findings in use of traditional authentication methods showed that a majority at 56% of the respondents used easy PINs that could easily be guessed which pose as a security challenge for their mobile banking accounts in the event that they are the only authentication used for a user to gain access to their accounts.

3. Default Authentication details on mobile banking application are changed with complex passwords.

Majority of the respondents at 75% who interacted with their banking application changed their default authentication details to their preference. The findings showed that most respondents at 56% had weak PINs in terms of the complexity where they formulated their PINs around their, birthday years, sequence of numbers among others.

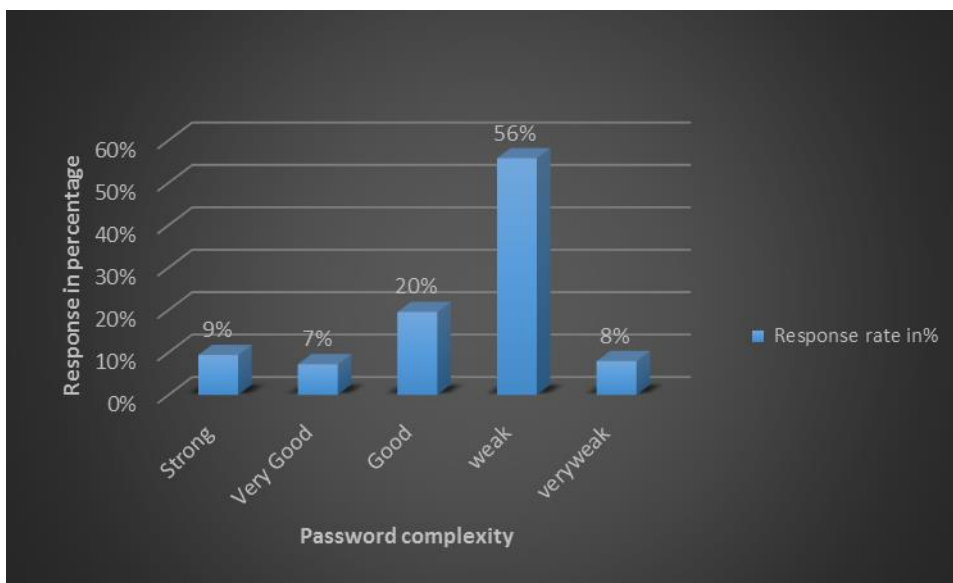


Figure 0.24 Respondents' Authentication complexity

4. Does the use of password only authentication form a strong authentication method

Majority of the respondents at 51% reported that they strongly disagreed that PIN/Password only authentication was a strong method of authentication this is due to the use of easy passwords and wanted an additional feature.

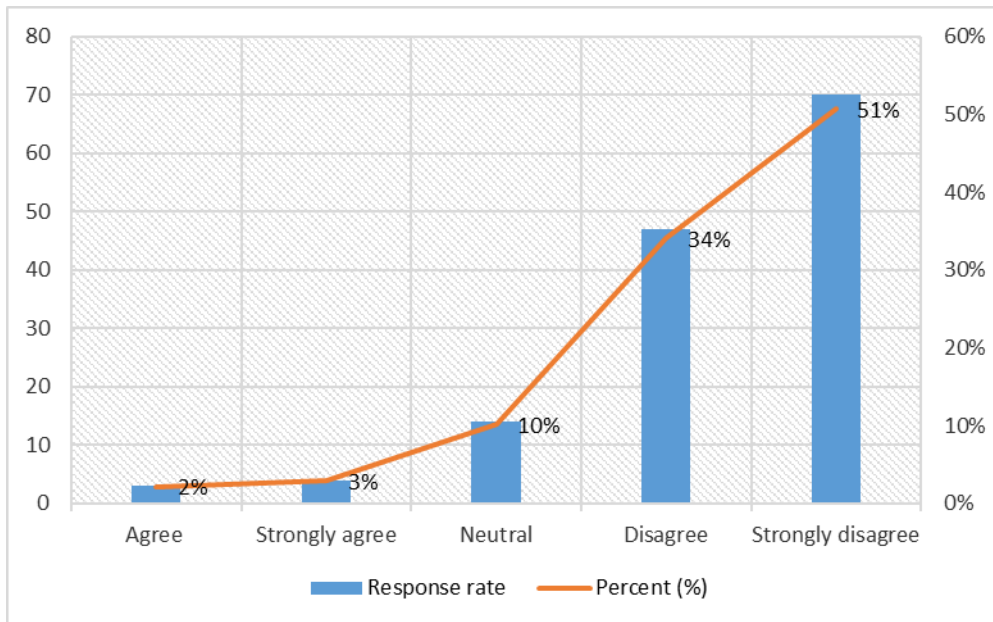


Figure 0.25 PIN/Password as a strong authentication method

5. What do you suggest could make mobile banking authentication stronger and secure?

This experiment wanted to find out the respondents consideration on authentication where from the responses majority of the respondents at 92% considered that use of PIN/Password only authentication was not strong and suggested the use of security

features that matched with the finer specific details of the client such as use of biometrics such as finger prints, face detection, typing sequence.

6. Frequency of change of passwords on mobile banking application

From the experiment 75% of the respondents within the experiment period did not change their PINs regularly even with the option to do so was made available on the application. This results are similar to the survey findings when the respondents reported to rarely change their passwords.

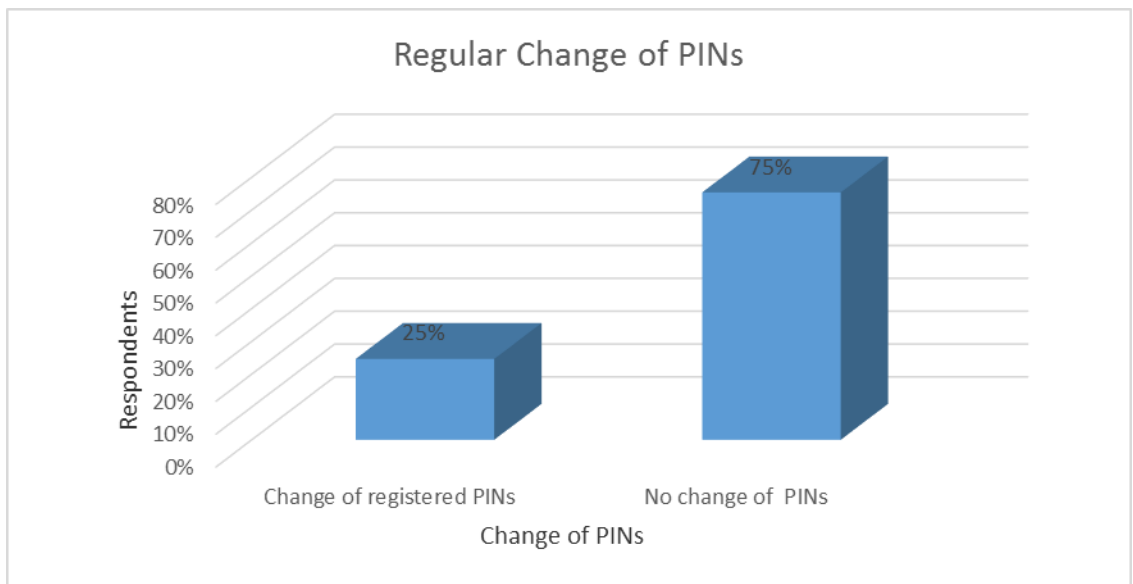


Figure 0.26 Respondents regular change of PINs

7. Do you carry out most of your mobile banking transactions at different locations?

This statement had different views across the respondents with most respondents at 49% who strongly disagreed with it and those who agreed at 9% shared similar numbers with those that were neutral. There were also those that strongly agreed at 21% and those who disagreed at 12%.

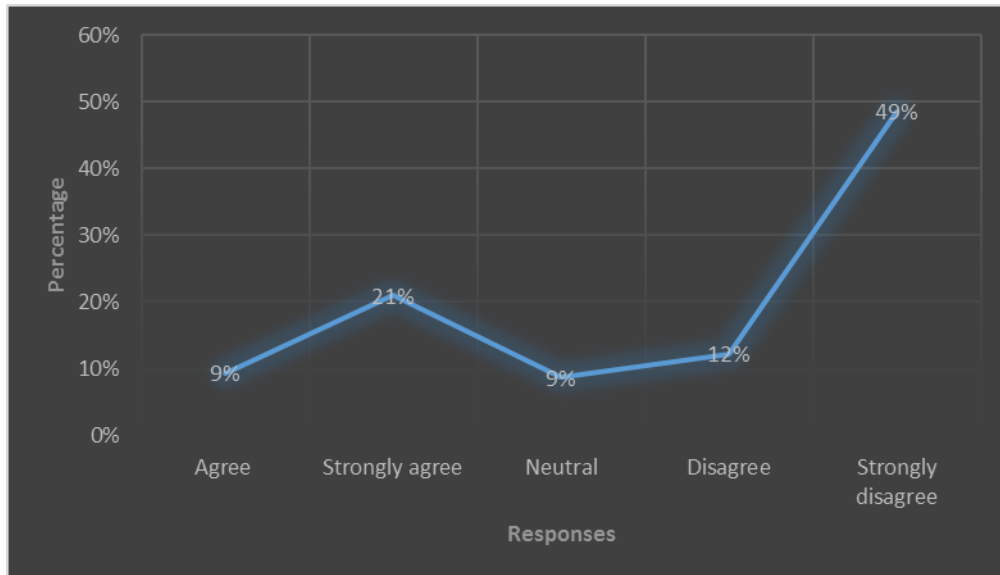


Figure 0.27 Respondents view on location of the transaction

5.5 Discussion and Analysis

From the first experiment carried out users usually tend to use easy PINs that could easily be bypassed when they were the only form of authentication as the user's account can be accessed by an intruder. Users formulated their PINs around current year, their date of birth and similar sequence of digits that they found easier to remember. Similar to the findings of this paper a study by the Data Genetics (2012) found the second most popular PIN was 1111, followed by 0000, 1212 and 7777. They reported that many

people also used the year of their birth to create their PIN, with every single combination of the digits in the years 1901 to 1999. When compared with the second experiment with incorporation of keystroke dynamics and location verification where the respondents still used the same PINs, it was challenging from the randomly selected people who acted as imposters to intrude the application even when the users PIN were shared to them.

As much as the intruder had the user's PIN they could not match the stored user's profile which was unique to each user. A study by Singh et al. (2017) shared similar findings where they found that in that Keystrokes dynamics are a part of behavioral biometrics and are unique to a person. Another study by Mahfouza et al. (2017) on behavioral biometric authentication on smartphones found that due to the weaknesses of the traditional authentication mechanisms such as PIN, Pattern and Password, the research community proposed the development of authentication mechanisms based on behavioral biometric traits such as gesture, keystroke and gait. These mechanisms are known as active or continuous authentication mechanisms. Even though the respondents considered themselves savvy reported to be using such PINs for it was easy for them to remember. The findings of this experiment can be compared to the findings of a study by Meng et al. (2015) which pointed out that PINs/Passwords suffered from security and usability problems in that users tend to use short passwords that are easy to remember. The use of short and easy-to-remember passwords presents a security risks from attacks such as the dictionary attack and brute force attack.

The use of PINs/Passwords as the only authentication method does not provide strong authentication as reported by majority of the respondents and they recommended use of an additional authentication feature. The findings of this experiment can be compared to a study by Asif et al. (2017) following the limitation of passwords being that they can

be written down, forgotten and stolen, easily guessed, deliberately being told to other people, they proposed use of two factor authentication that guaranteed a higher protection level compared to password only authentication.

From the survey findings most of the respondents reported that the use of biometrics such as face detection ,finger prints among others was as an alternative to PIN/password only authentication. These findings are similar to the experiment findings where majority of the respondents at 92% suggested the use of security features that matched with the finer specific details of the client such as use of biometric features such as finger prints, face detection, typing sequence, gait and location. Lin et al., (2014) found out that over 30% of mobile devices were currently using biometrics and reported that banks needed to see it as an opportunity rather than a barrier to adoption.

Over a period of 30days as respondents interacted with the application majority of the respondents did not change their PINs regularly as some of them only changed in the initial phase. These results are similar to the survey findings where 56% of the respondents reported to rarely change their PINs. This can be a security challenge in the event a user shares their login details with someone at a particular point in time and fails to change their PINs.

A survey done by (Digital Guardian, 2017) on internet users to gain some insight into current authentication habits, had similar findings to this experiment where they found out that 29.4% of respondents changed their passwords rarely or never, 10.9% of respondents reported that they never changed their passwords and 18.5% reported to changing their passwords only when they had been notified of a security issue.The location of the transactions across majority of the respondents within the experiment period was done averagely at the same place being either at work, home or at a shopping

mall. This predictability of respondents location pattern can be compared to a study by (Ponieman et al., 2013) where they found out that human being had predictable mobility patterns especially during weekdays than during the weekend.

Experiment 1 Sample User Training Results

Table 0.4: Sample user Training Results

Registered User	PIN Used	PIN Typing attempts
1	0004	10
2	4321	10
12	7777	10
20	2015	10
33	8124	10
37	0938	10
40	2018	10
47	3533	10
55	1234	10
60	4433	10

Experiment 1 Sample User Testing Results

Registered users	PIN		Expectation	Actual Result
1	0004		Authenticate	Authenticated
2	4321		Authenticate	Authenticated
12	7777		Authenticate	Authenticated
20	2015		Authenticate	Authenticated
27	2471		Authenticate	Authenticated
21	1988		Authenticate	Authenticated
24	1992		Authenticate	Authenticated
33	8124		Authenticate	Authenticated
42	2018		Authenticate	Authenticated
47	3533		Authenticate	Authenticated
Non Registered User No.	Name	PIN Used	Expectation	Actual Result
3	Patrick	8124	Denied	Authenticated
4	Timothy	3533	Denied	Authenticated
7	Mary	0004	Denied	Authenticated
9	Jane	2018	Denied	Authenticated
10	Timmy	4321	Denied	Authenticated

Table 0.5: Sample user Testing Results

From the first experiment both training and testing results showed that when use of PIN authentication was used access to the mobile banking application was easy both to

registered users and non-registered users who acted as imposters as the it required only the user to remember their PINs and when shared one could be able to 100% login despite an expectation of failed login. When both legit users and imposters typed the PIN the only distinguishing factor was if the account and the PIN number matched otherwise when shared anyone could gain access the mobile banking application. According to (Africa Cyber Security Report, 2018) they found out that Kenyan Banks got most of their attacks through their web applications, Internet and Mobile banking platforms. Where cyber criminals gained access to bank systems through sharing of PINs authentication details. With this in mind we aim improve this authentication method by adding behavioral profiling through keystrokes dynamics and location verification features as an alternative authentication method.

5.5.1 Experimental 2

To able to capture user's keystroke behavior this study used a touch screen keyboard sensors available on android operating systems which is an open source software that most smartphones operate on, through a prototype of a mobile banking application that stores the typing data as users keyed in their PINs. The location data was obtained through the phone's cellular data, Wireless networks or GPS. Training and testing of the system was done to learn user's typing patterns through classification which is used to differentiate legitimate user's profile from an imposter as user's key in their PINs by recognition and reference based on stored data in the database.

5.5.2

5.5.3 Results.

1) The use of Behavioral profiling and location verification as an authentication method.

Majority of the respondents at 62% found and strongly agreed that the use of user profiling based on typing sequence and location verification to be secure compared to PIN/Password only authentication application and that it was difficult for someone to have the same typing sequence and know your transaction location.

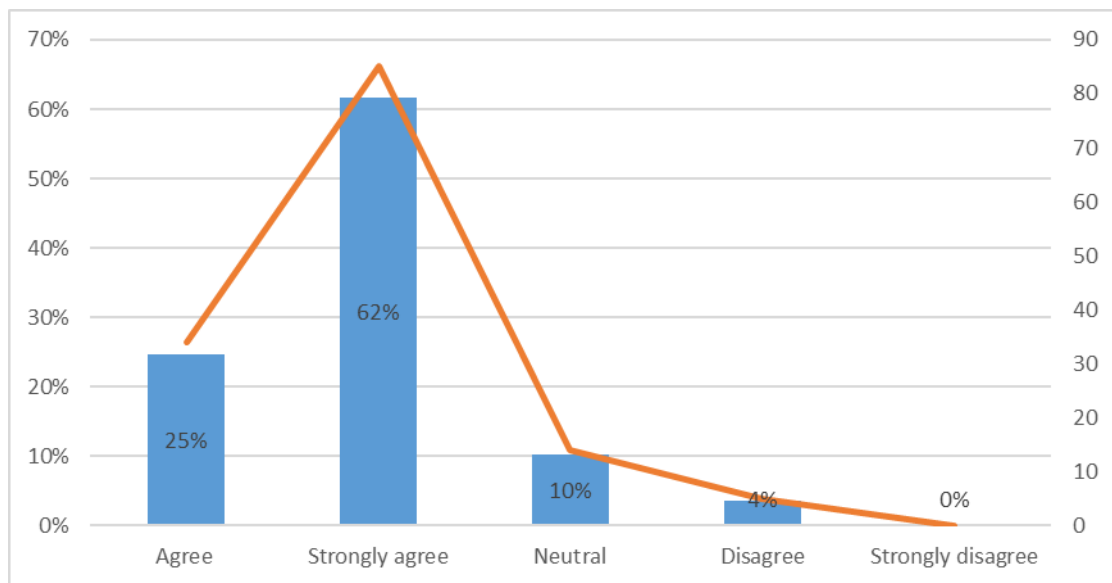


Figure 0.28 Use of user profiling and location verification

2) The authentication method can be applicable to mobile banking applications

From the carried experiment majority of the respondents reported at 47% strongly agreed on its use as it provided security as the authentication details were unique to a particular user. However there were those respondents who were neutral at 20% about this authentication method as 3% and 8% of the respondents reported to strongly disagree and agree respectively.

Table 0.6: The use of proposed authentication method on mobile banking

Strongly agree	28	47%
Agree	13	22%
Neutral	12	20%
Strongly disagree	2	3%
Disagree	5	8%
Total	60	100%

3) The authentication method uniquely identifies a user based on typing sequence and location.

The results obtained from the experiment showed that most of the respondents did their transactions at predictable locations based on an average of 10 transactions categorized as work, home, entertainment spot and shopping locations.

When it comes to typing sequence as they entered their password each respondent had a different typing sequence hence it was uniquely to a respondent.

Table 0.7: Sample Data from the experiment

User ID	Typing Sequence Speed (mili seconds)	Category of Most Transaction Location
1	2000	Home
2	4000	Work
12	7000	Work
20	13000	Home
33	5000	work
37	15000	Entertainment spot
40	6000	shopping
47	19000	work
55	12000	work
60	10000	home

When registering users were trained to key in their PINs ten times in order for the system to generate their typing sequence profile which would later on be stored in the database. Upon logging in users typing sequence and location would have to be compared with the stored profile. Based on the user's typing behavior the application expected to allow access to the application upon match in typing sequence and location verification. Experiments were done using both registered and non-registered who acted as imposters.

Table 0.8: Sample user Training Results

Registered User	PIN Used	PIN Typing attempts
1	0004	10
2	4321	10
12	7777	10
20	2015	10
33	8124	10
37	0938	10
40	2018	10
47	3533	10
55	1234	10
60	4433	10

Registered user	PIN	Expectation	Actual Result
1	0004	Authenticate	Authenticated
2	4321	Authenticate	Authenticated
12	7777	Authenticate	Authenticated
20	2015	Authenticate	Authenticated
27	2471	Authenticate	Authenticated
21	1988	Authenticate	Authenticated
24	1992	Authenticate	Denied
33	8124	Authenticate	Authenticated
42	2018	Authenticate	Authenticated
47	3533	Authenticate	Denied

55	1234		Authenticate	Authenticated
Non Registered User No.	Name	PIN Used	Denied	Denied
3	Patrick	8124	Denied	Denied
4	Timothy	3533	Denied	Denied
7	Mary	0004	Denied	Authenticated
9	Jane	2018	Denied	Denied
10	Timmy	4321	Denied	Denied

Table 0.9: Sample user Testing Results

Table 0.10: User typing and anomaly detection

Registered User	Mean (ms)	Threshold ($\geq 90\%$)Acceptance	T(ms)
1	2000	1800	
2	4000	3600	
12	7000	6300	
20	13000	11700	
33	5000	4500	
37	15000	13500	
40	6000	5400	
47	19000	17100	
55	12000	10800	
60	10000	9000	

From the second experiment once the user's typing behavior was captured inform of total time taken to type their PIN numbers 10 times. This enables the creation of the corresponding behavioral typing profiles. These profiles were used to train the keystroke

algorithm to be able to create their profile the threshold for anomaly detection was 90% meaning when typing the PIN any value within the threshold (T) would allow access to the mobile application anything else would be denied .The threshold is usually based on the assumption that the user's typing behavior changes from time to time and will not be always accurate following several factors such as being tired, lack of concentration among others hence why having a threshold is important. From the second experiment there were instances that legitimate users were not able access their accounts which is the False Rejection Rate access attempts by legitimate users that have been rejected by the system and a False Acceptance Rate (FAR) access attempts by imposters that have been accepted by the system incorrectly. It is due to this that the study of Singh et al., (2017) on behavioral profiling users as they type their passwords/PINs reported that keystroke dynamics was not enough by itself which is why this study seeks to improve the authentication method with the addition of location verification which ensures security of mobile transactions based on the user's transaction location captured by smartphones GPS sensor and it' application to mobile banking.

In the second experiment adding the location capture feature one can determine the location the user typically does most of his transactions from and then compare them to the reported location for the current authentication attempt. Through this we are able to determine whether the reported location matches the user's typical transaction location or not. Thus, we have a means of helping identify users with low associated friction. Based on users keystroke and transaction location profile match they are given access. For location, based on your frequent transaction locations if current login distance is greater than 200M from past transaction locations then users are denied access an alert raised if it's a genuine user then they answer a security question failure to answer a

security alert email is sent out to account holder with request to report to their nearest bank branch.

4) Behavioral profiling and location verification authentication provides an alternative security on mobile banking.

This authentication method on mobile banking applications was strongly agreed and recommended by majority of the respondents comprising of 59% followed closely who agreed at 30%. There were those who were neutral about this authentication method at 5% while those who strongly disagreed with this authentication method comprised of 3%. The respondents attributed their confidence due to the fact that it would be unlikely for someone to type like them and be at the same location while carry out a mobile transaction.

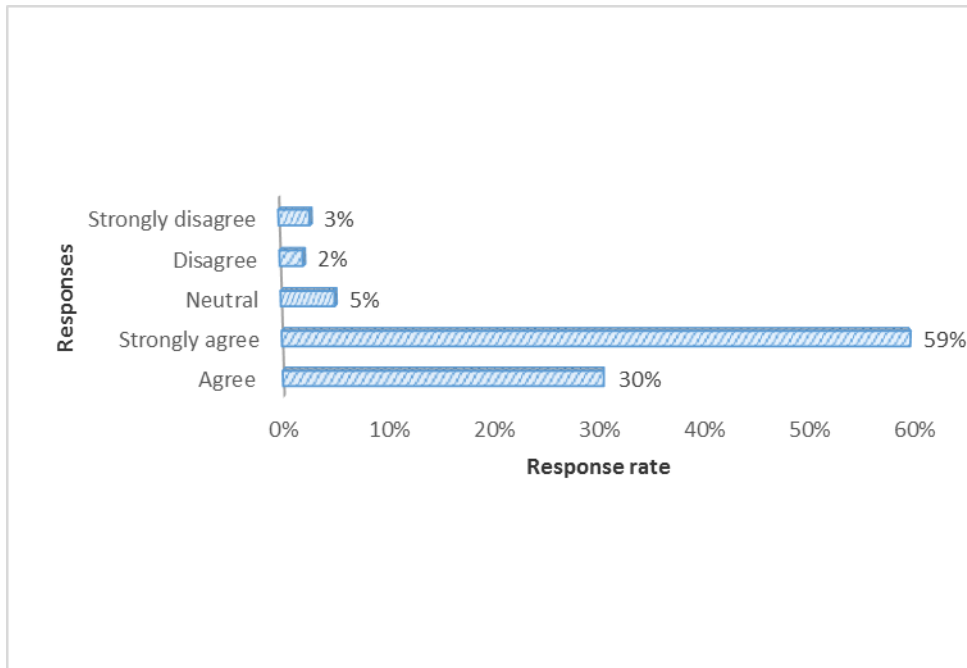


Figure 0.29 Mobile Banking Authentication Using Behavioral Profiling and Location Verification

5) What is your concern when it comes to this authentication method?

From the experiment most of the respondent's at 57% major concern was the assurance that even if they used the most common known PINs someone could not easily access into their mobile banking application account. The respondents gave their concerns as they tend to make their passwords easily to remember hence with the proposed authentication method they still needed to feel safe. Another 33% of the respondents reported the ease of use as a concern of the proposed authentication method and thirdly

at 11% reported to be concerned about the cost implications of the proposed authentication method.

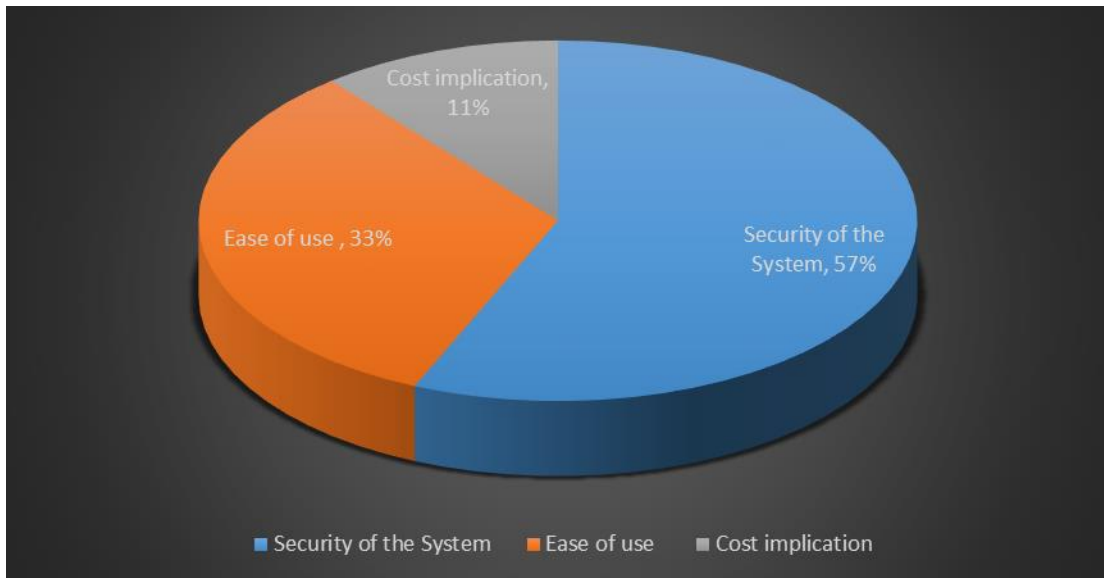


Figure 0.30 Respondents Concern in using the proposed authentication method

5.5.4 Discussion and Analysis

From the first experiment users tend to use easy passwords that are often weak and can easily be bypassed when passwords are the only form of authentication then the user's account can be accessed by an intruder. This is unlikely as showed in the second experiment as additional behavioral profiling and location verification was used the respondents still used their weak passwords but it was challenging from the randomly selected people who acted as imposters to intrude the application even when the users PIN numbers were shared to them. As much as the intruder had the user's PIN number they could not match the stored user's profile which was unique to each user. A study by

Singh et al., (2017) shared similar findings where they found that in that Keystrokes dynamics are a part of behavioral biometrics and are unique to a person to a large extent.

According to a survey by Mahfouz et al., (2017) on behavioral biometric authentication on smartphones found that due to the weaknesses of the traditional authentication mechanisms such as PIN, Pattern and Password, the research community proposed the development of authentication mechanisms based on behavioral biometric traits such as gesture, keystroke and gait. These mechanisms are known as active or continuous authentication mechanisms. Majority of the respondents strongly agreed on the application of the use of behavioral profiling and location verification in mobile banking applications.

This was similar to the survey findings where 86% of the respondents reported to recommend its use in mobile banking. The respondents were willing to use this authentication method provided it added a level of security to their application. Similar to this findings was a study by Ciampa et al. (2013) where they found that users were willing to deal with more than the usual user name/password authentication if it meant stronger security. Another comparison that shared with these findings was a study by Butler & Butler (2015) where they reported that users had a high degree of acceptance of 'risk-based' authentication, in which a positive inclination was towards the user's identity based on such things as log-on location, IP address, and transaction behavior.

From the experiments carried out the use of behavioral profiling through respondents typing sequence and location verification as an alternative authentication provided a distinctive method. 60 legitimate users' samples were collected over a trial period of 30 days with 10 attempts of logging into the system and 10 random people who were

randomly selected to be imposters with each having 5 attempts over the 30days period. Different from the first experiment is that although the account numbers and authentication details were shared with imposters it was challenging to gain access this is because in the second experiment the imposters needed to type as the legitimate users and also be at a recent location similar to where a legitimate has done a transaction before hence provided additional security as compared to the first experiment where imposters were able to gain access once the PINs and account numbers were shared with them. The results gave a False Rejection Rate (FRR) of 5.33% which is the percentage of access attempts by legitimate users that have been rejected by the system and a False Acceptance Rate (FAR) of 3.33% which is the percentage of access attempts by imposters that have been accepted by the system incorrectly, giving an Equal Error Rate (EER) of 4.3%. Kambourakis et al. (2014) found the Equal Error Rate (EER) to be generally employed to examine the performance of biometric systems similar to ours. Specifically, EER is a kind of percentage rate which both accepts and rejects errors as equals ($EER = (FAR + FRR) / 2$).

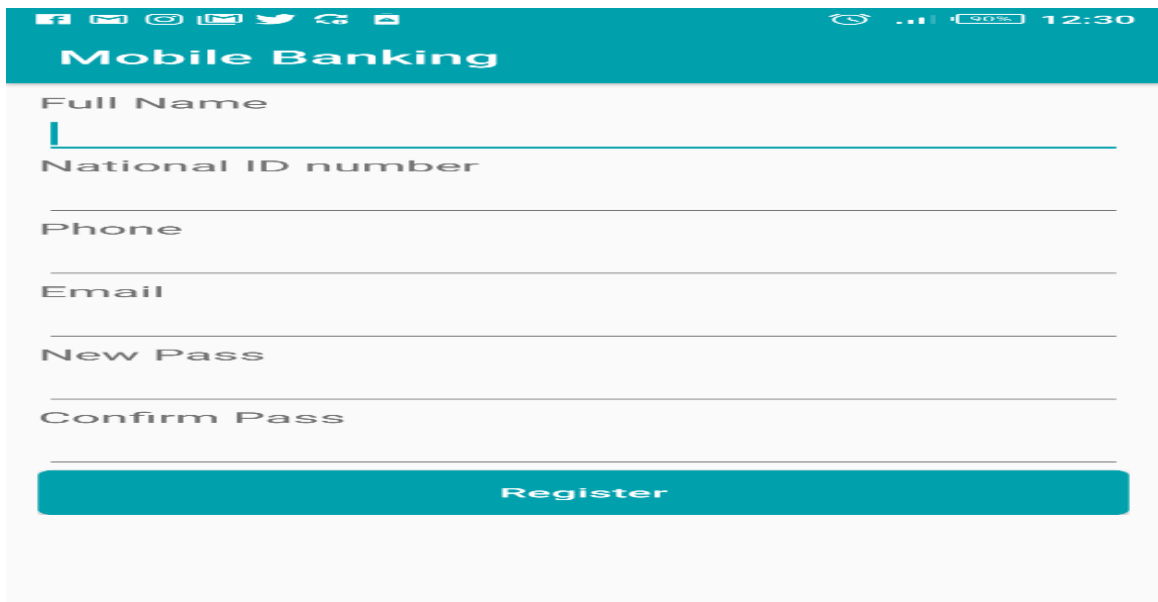
A study by Li et al. (2011) found that on the application level profiling of a user activity experiment gave an EER of 13.5% which compared to the results of this study is an improvement having an EER of 9.06% combined with the feature of location verification. Elsewhere a study by Kambourakis et al.(2014) on Keystroke Authentication System for smartphones concluded that Keystroke authentication which is an authentication based on how a user types had significant potential in designing enhanced authentication systems destined to future smartphones after they obtained a minimum EER value of 12.5%.

The proposed authentication method does not increase any costs to the current smartphones that operate on android system and works in the background causing no

interruptions as one uses the application offering an alternative security method which were concerns raised by the respondents. These findings are similar to the study by Ciampa et al. (2013) where they found that consumers were willing to take extra steps to protect their identities, but they do not necessarily want to pay extra for these services.

1. Interfaces of the proposed behavioral profiling and location verification authentication

When a user installs the mobile banking application the user is required first to register on the application providing details such as their name, ID and phone numbers and their email address. Once their details are captured the user receives details to their account sent to their phones via a text message.



The image shows a mobile banking registration interface. At the top, there is a teal header with the text "Mobile Banking". Below the header, the form contains several input fields: "Full Name", "National ID number", "Phone", "Email", "New Pass", and "Confirm Pass". Each field is represented by a horizontal line with a small vertical bar on the left side. At the bottom of the form, there is a teal button with the text "Register". The background of the form is white, and the overall layout is clean and modern.

Figure 0.31 User Registration

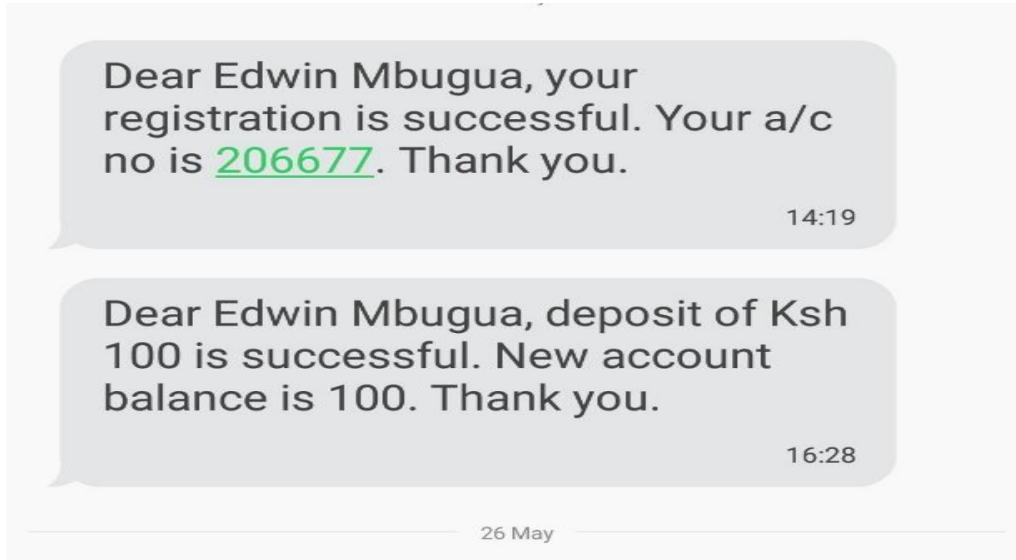


Figure 0.32 User Account Confirmation

The user's typing sequence is captured as they type in their account and PIN number. For the purpose of this experiment a training period of 30days was used in order to create a user's behavioral profile. After the training period the user's profile is crated and stored in the database. This information is used as the user authenticates while in the background a comparison based on the profile is done.

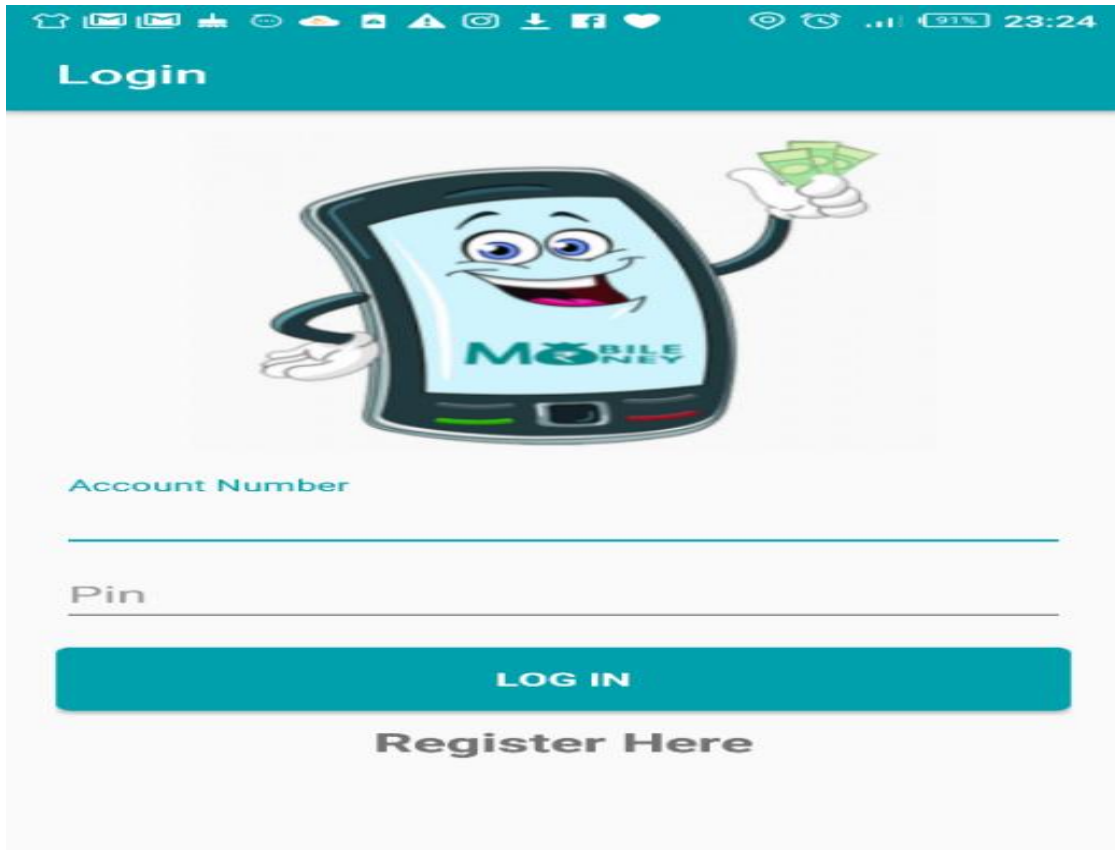


Figure 0.33 User Authentication

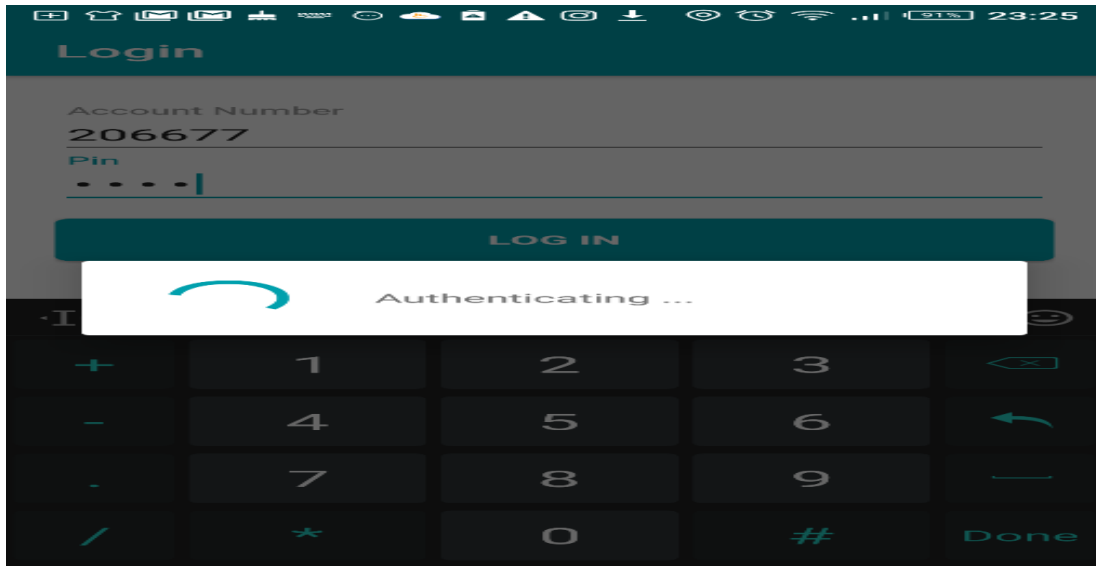


Figure 0.34 User Profiling Authentication

Upon successful match in obtaining a user's behavioral profile the user will be prompted to verify their transaction location this is done to verify that this is the actual user trying to gain access to the application. The location of the user is already captured in the database and the application will be verifying that the current user transaction location matches with the stored location.

When the application returns a successful match the user proceeds in accessing their account else the user is denied access into the mobile banking application account.

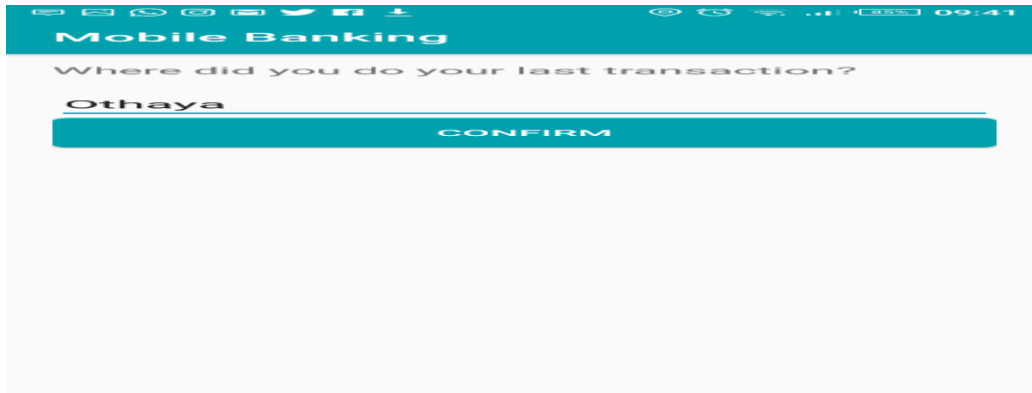


Figure 0.35 User Location Verification

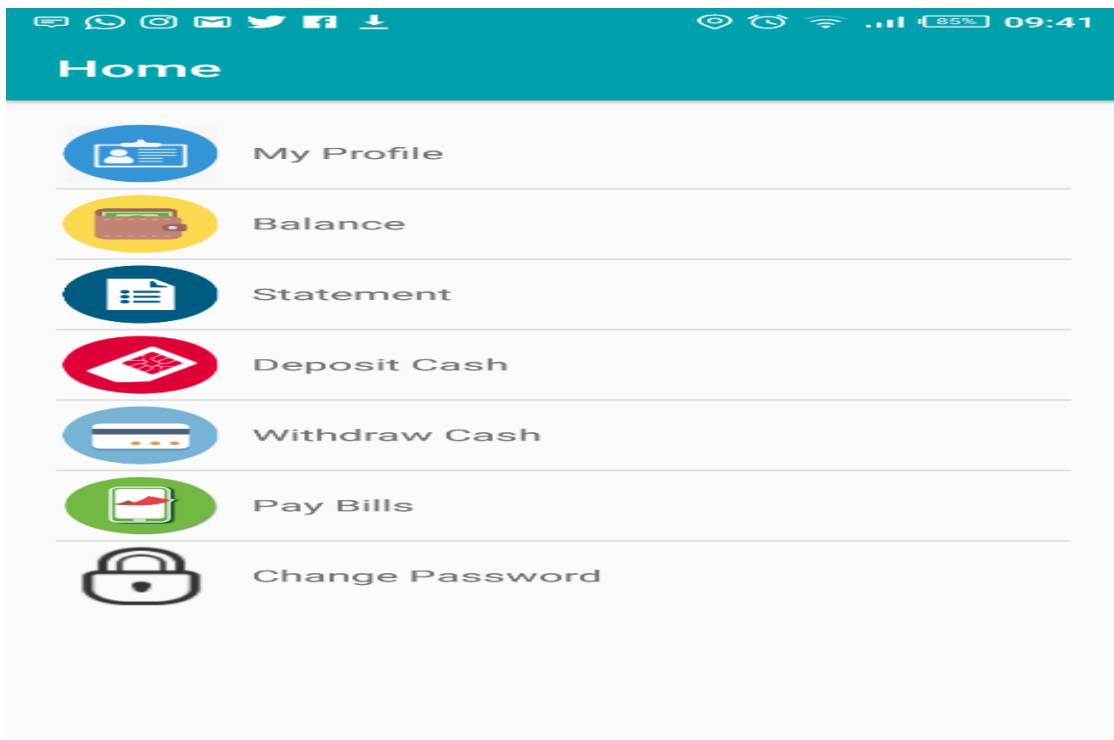


Figure 0.36 Successful Login

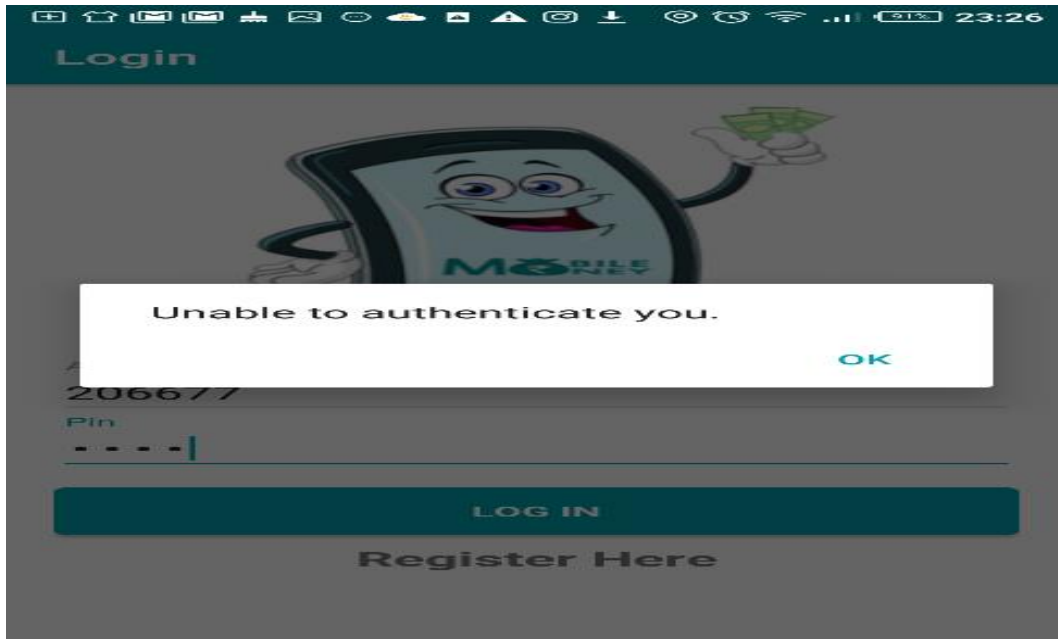


Figure 0.37 Unsuccessful Login

5.6 Conclusion

One of the objectives of this research was to evaluate the proposed authentication method that uses behavioral profiling and location verification. This chapter proposes the use of an alternative method for securing mobile transactions. The experiment carried out shows that mobile banking users use easy PINs which can be costly to the bank customers and banks in general. As banks try to compete with each other in terms of innovative products and services on mobile banking security remains a concern and needs to be a priority since the individuals who have subscribed to mobile banking services risk exposure to cyber related criminal activities affecting user accounts where they exploit the gaps in security controls put in place for mobile money services. It is for this reason that this research aims to address this gap by proposing an alternative

authentication method which involves use of behavioral profiling and location verification. From the results of the experiment the evaluation of the proposed authentication method showed it was offering an alternative method of securing mobile transactions as it provided better results compared to previous studies.

CHAPTER SIX

SUMMARY, CONCLUSION AND RECOMMENDATIONS

6.1 Summary

This research proposes an authentication method of security mobile banking transactions through use of behavioral profiling and location verification. This research addresses the weaknesses of traditional authentication mechanisms such as use of Passwords and PINs by proposing a method that uniquely identifies a user's typing behavior and the location of the transaction to be able to access their accounts. Evaluation of existing authentication methods are given in this research highlighting the features, improvements and their respective limitations. This study also contributes to knowledge through proposing of user behavior profiling and location verification authentication as an alternative method of securing mobile banking transactions since behavioral biometric authentication methods have been found to be cheaper than physiological ones with no additional costs to smartphones.

The proposed authentication method was evaluated through conducting online surveys and carrying out two experiments which later on an analysis and discussion of the data collected was done with the objective of establishing the weaknesses of PINs in terms of how easy one can access the application when they are easily guessed or if shared and how the proposed authentication method improves on security to accessing such systems by addressing these limitations. In the proposed method among the major user's concern was the security of their mobile banking application where others suggested an alternative to PIN/password authentication such as the use of biometrics, the ease of its

use and the cost to have it implemented. From the experiments carried out 60% of the respondents strongly agreed on the use of behavioral profiling and location verification in authentication where they attributed their confidence due to the fact that it would be unlikely for someone to type like them and be at the same location while carry out a transaction. Most respondents at 92% considered that use of PIN/password only authentication was not strong and suggested the use of security features that matched with the finer specific details. The outcome of this study can be used to address the gap in security control for mobile banking services when it comes to authentication through use of behavioral profiling and location verification.

6.2 Conclusion

Most of the respondents strongly agreed and recommended the use of an alternative authentication method other than the widely used pins and passwords. Majority of the respondents suggested the use of security features that matched with the finer specific details of the user such as use of biometrics such as finger prints, face detection, typing sequence. The respondents preferred use of biometric authentication as they perceived it to be more secure and unique to each user. Based on the survey findings all of the respondents had smartphones and preferred to do most of their work on phone such as accessing information, socializing with their peers, accessing their bank accounts and paying of bills due to the convenience and ease of use. Among the major concern among most respondents in performing financial transactions on their phone was security of the mobile banking as currently there have been a rise in fraud related incidents and threats such as phishing and ransom ware attacks affecting both local and international banks.

This research showed how users tend to use easy PINs/passwords that if shared, closely observed or guessed could cost them heavily as their use could not differentiate an

authorized user from an imposter. The current use of PINs and passwords lack user uniqueness differentiating factor as the system only checks if what the user has entered is what exists in the database. With the current wide spread of affordable smartphones the respondents wanted an alternative authentication method that they could use and would not result in raising the cost of the smartphone or purchase of addition hardware. The respondents indicated that the use of behavioral profiling and location verification as an authentication method provided additional security unlike PIN/password only authentication. Most respondents attributed their confidence to the proposed alternative authentication method due to the fact that it would be unlikely for someone to type like them and be at the same location while carry out a mobile transaction. From this research users used weak passwords and rarely changed them which was a security loophole, with the current proposed authentication method as much as users are advised to change their passwords regularly random selected imposters had a challenge in bypassing the authentication page.

Using behavioral profiling and location verification in authentication, the system can be able to differentiate a legit user from an imposter based on how they type compared to the stored profile in regards to a particular user account. The main objective in this method is to be able to consistently rediscover a user's unique typing behavior. This type of biometric authentication falls under behavioral type of biometrics and could also be referred to as keystroke dynamics.

The findings of the experiments done in this research showed an improvement from previous studies and could be adopted for use. The research findings showed that the implementation of the proposed authentication method addressed most of the respondents concerns such as cost of implementation, ease of use and security of the system.

As commercial banks compete with each other in service delivery and innovative products, security of the service will remain to be a key factor among majority of the users in their adoption, as well as its convenience, user friendliness and perceived user trust in the bank. It is with this that banks will need to invest more in securing customer transactions with updated methods to be able to counter security breach by hackers.

With the advancement of technology superior and affordable smartphones will be introduced to the market and as the increase of mobile uptake rises banks that will be able to prove to their customers of their improved innovative security features on financial services that are compatible with their clients phones will end up gaining more customers as focus shifts to security.

6.3 Recommendations

The implementation of behavioral profiling and location verification on mobile phones is cost effective and is compatible as the integration of additional hardware is not required. When it comes to financial services the ability to secure user accounts plays a key role.

6.3.1 User Unique Identity

Mobile banking systems need to be able to identify users differently aside from using just PINs/passwords. Biometric use in authentication uniquely differentiates authorized users from imposters it is usually based on what the user has in our case user's typing behavior an improvement to PINs/passwords only authentication.

Each user types differently and no matter how easy or difficult a PIN/password is ,how it's typed will be different across many users and it is with this that the system should be able to differentiate login attempts.

6.3.2 User location Verification

Adding location verification feature will allow banks be able to map the various transaction locations per user and be able to verify them based on existing data in their database hence preventing transactions to be carried out in non-defined locations. The location details provided guarantees that the user performs administrative functions only from defined locations. This means the application will be location dependent hence the phone's GPS or cellular data will be required to be active.

6.3.3 Cost of Implication

The implementation of this authentication method does not involve any software or hardware additional costs to the phone and commercial banks can able to integrate this feature onto their current mobile banking applications as an improvement to user authentication. The use of behavioral biometric authentication is cheaper in implementation compared to physical biometric where additional hardware costs have to be factored in.

6.4 Area of further research

This research has shown that security concerns remain a key priority in the adoption of mobile banking among users. To be able to counter cyber related activities banks will be required to stay up to date by addressing security control gaps emerging with the technological advancements in the mobile banking services. In this research the use of

behavioral profiling and location verification was proposed as an alternative authentication to mobile banking, future work would focus on its implementation in the ATMs lobby. Further research would be on how to integrate user typing behavior and location verification to bank ATMs.

REFERENCES

- Abdellaoui,, A., Khamlichi, Y. I., & Chaoui, H. (2015). An Efficient Framework for Enhancing User Authentication in Cloud Storage Using Digital Watermark.*International Review on Computers and Software (IRECOS)*, 10(2) 130-136.
- Agoyi, M., & Seral, D. (2011). The use of SMS encrypted message to secure automatic teller machine. *Procedia Computer Science*, 3, 1310-1314.
- Ahmadian, M., Khodabandehloo, J., & Marinescu, D. (2015). A security scheme for geographic information databases in location based systems. *IEEE SoutheastCon*, (pp. 1-7). IEEE
- Aithal, L. (2015). Biometric Authenticated Security Solution to Online Financial Transactions. *International Journal of Management, IT and Engineering (IJMIE)*, 455-464.
- Aithal, P. S. (2016). A Review on Advanced Security Solutions in Online Banking Models. *International Journal of Scientific Research and Modern Education (IJSRME)*, 421-429.
- Akoramurthy, B. &. (2017). GeoMoB — A geo location based browser for secured mobile banking. *Eighth International Conference on Advanced Computing IEEE* (pp. 83-88.). IEEE

- Akoramurthy, B., & Arthi, J. (2017). GeoMoB : A geo location based browser for secured mobile banking. *Eighth International Conference on Advanced Computing IEEE*.
- Alariki, A. A., & Manaf, A. A. (2014). Biometrics Authentication Using Touch-Based Gesture Features for Intelligent Mobile Devices. *1st Int'l Conf. of Recent Trends in Information and Communications Technologies*, (pp. 528-538).
- Aldhaban, F., Daim, T. U., & Harmon, R. (2015). Exploring the adoption and use of the smartphone technology in emerging regions: A literature review and hypotheses development". *Management of Engineering and Technology (PICMET) 2015 Portland International Conference*, (pp. 2355-2370).
- Alotaibi, S., Furnell, S., & Clarke, N. (2015, December). Transparent authentication systems for mobile device security: A review. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 406-413). IEEE.
- Aloul, F., Zahidi, S., & El-Hajj, W. (2009). Multi factor authentication using mobile phones. *international journal of mathematics and computer science*, 4(2) 65–80.
- Aloul, F., Zahidi, S., & El-Hajj, W. (2009). Multi factor authentication using mobile phones. *International Journal of Mathematics and Computer Science*, 4(2), 65-80.
- Alsultan, A., & Warwick, K. (2013, October). User-friendly free-text keystroke dynamics authentication for practical applications. In *2013 IEEE International Conference on Systems, Man, and Cybernetics* (pp. 4658-4663). IEEE.

- Alzubaidi, A., & Kalita, J. (2016). Authentication of smartphone users using behavioral biometrics. *IEEE Communications Surveys & Tutorials*, 18(3), 1998-2026.
- Amor, D. J., Bentley, K., Ryan, J., Perry, J., Wong, L., Slater, H., & Choo, K. A. (2004). Human centromere repositioning “in progress”. *Proceedings of the National Academy of Sciences*, 101(17), 6542-6547.
- Asif, A. Israr, uH & Monisa, N., 2017. Two factor authentication. *International Journal of Computer Science and Mobile Computing*, 6(7), 5-8.
- Babaeizadeh, M., Bakhtiari, M., & Maarof, M. A. Keystroke Dynamic Authentication in Mobile Cloud Computing. *International Journal of Computer Applications*, 9(91), 29-36
- Banerjee, S. P., & Woodard, D. L. (2012). Biometric authentication and identification using keystroke dynamics: A survey. *Journal of Pattern Recognition Research*, 7(1), 116-139.
- Bayir , M. A., Demirbas, M., & Eagle, N. (2009). Discovering spatiotemporal mobility profiles of cellphone users. *In: World of Wireless, Mobile and Multimedia Networks and Workshop*. Kos, Greece : IEEE.
- Belk, M., Germanakos, P., Fidas, C., & Samaras, G. (2014, July). A personalization method based on human factors for improving usability of user authentication tasks. *In International Conference on User Modeling, Adaptation, and Personalization* (pp. 13-24). Springer, Cham.
- Bhave, D., Bhavsar , P., Chavan , S., & Gore, K. (2016). “Keylogging-resistant visual authentication protocol”. *International Journal of Advanced Research in Computer and communication Engineering*, 5(2), 520-524.

- Butler, M., & Butler, R. (2015). Investigating the possibility to use differentiated authentication based on risk profiling to secure online banking. *Information and Computer Security* 23 (1), 421-434. <https://doi.org/10.1108/ICS-11-2014-0074>.
- Carella, A., Kotsoev, M., & Truta, T. M. (2017). "Impact of Security Awareness Training on Phishing Click-Through Rates. *ieee international conference on big data* (pp. 4458-4466).
- Catherine, S., & Divya, M. (2013). Smartphone applications as software engineering projects. *J.Comput. Sci. Coll*, 27-34.
- Central Bank of Kenya. (2017). *Bank Supervision Annual Report*. Nairobi, Kenya: Central Bank of Kenya.
- Cho , S. Z., & Han,, D. H. (2000). *Patent No. 6151593*. U.S. Patent.
- Chourasia, N. (2014). "Authentication of the User by Keystroke Dynamics for BankingTransaction System". *Proceedings of International Conference on Advances in Engineering & Technology*
- Ciampa , M., Enamait, J., & Mark, R. (2013). A Comparison of User Preferences for Browser Password Managers. *Journal of Applied Security Research Vol. 8, No. 4,*, 455-466.
- Cirnu, C. E., Rotună, C. I., Vevera, A. V., & Boncea, R. (2018). Measures to mitigate cybersecurity risks and vulnerabilities in service-oriented architecture. *Studies in Informatics and Control*, 27(3), 359-368.

- Clarke, N., AL, A., Funnel, S., & Stengel, I. (2013). A conceptual model for federated authentication in the Cloud. *the 11th Australian Information Security Management Conference Edith Cowan University*.
- Clayton, R. (October, 2001). "Brute force attack on cryptographic keys". Retrieved from -file:///H:/brute force attack / brute.html, Oct 2001.
- Cognizant . (June, 2013). *Segment-Based Strategies for Mobile Banking*. Retrieved from cognizant.com: : [http://www.cognizant.com/insights Whitepapers/Segment-Based-Strategies-for-mobilebanking](http://www.cognizant.com/insights/Whitepapers/Segment-Based-Strategies-for-mobilebanking).
- Cooper , D., & Schindler, S. (2014). *Business Research Methods*. Graw-Hill Irwin. New York.
- Crawford, H., & Ahmadzadeh, E. (2017). Authentication on the go: Assessing the effect of movement on mobile device keystroke dynamics. *Proc. 13th Symp. Usable Privacy Secur. (SOUPS)*, , (pp. 73-163).
- Crawford, H., & Renaud, K. (2014). Understanding user perceptions of transparent authentication on a mobile device. *Journal of Trust Management*, 1(1), 1-28.
- Crawford, H., Renaud, K., & Storer, T. (2013). "A framework for continuous, transparent mobile device authentication". *Elsevier Computers & Security*, 39(2), 2013.
- Crowe, M., Tavilla, E., & McGuire, B. (2015). Mobile banking and mobile payment practices of US Financial institutions: Results from 2014 survey of FIs in five federal reserve districts. *Federal Reserve Boston*, 1-66.

- CSID. (1 August, 2012). *Comsumer survey: Password*. Retrieved from csid.com: www.csid.com/wp-content/uploads/2012/09/CS_PasswordSurve
- Dandass, Y. S. (2008). Using FPGAs to Parallelize Dictionary Attacks for Password Cracking. *Hawaii International Conference on System Sciences*, (pp. 486- 493).
- Dasgupta, S., Paul, R., & Fuloria, S. (2009). Factors affecting beha vioral intentions towards mobile banking usage: Empirical evidence from India. *Romanian Journal of Marketing* , 3 (1),, 6-28.
- Data Genetics. (3 September, 2012). *PIN analysis*. Retrieved from datagenetics.com: <http://www.datagenetics.com/blog/september32012/>
- Davis , F. D., Bagozzi , P. R., & Warshaw , P. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, 982-1003.
- De Lange , J., Solms , R. V., & Gerber , M. (2016). De Lange J, Von Solms R, Gerber Information security management in local government. *In:Cunningham P, Cunningham M, editors. 2016 IST-Africa Week Conference, 11-13 May 2016* (pp. 1-11). Durban, South Africa IIMC International Information Management Corporation.
- De Marsico, M., & Nappi, M. (2018). Face recognition in adverse conditions: A look at achieved advancements. In *Computer Vision: Concepts, Methodologies, Tools, and Applications* (pp. 2184-2210). IGI Global.

- De Marsico, M., Nappi, M., Riccio, D., & Wechsler, H. (2015). Mobile iris challenge evaluation (MICHE)-I, biometric iris dataset and protocols. *Pattern Recognition Letters*, 57, 17-23.
- De Marsico, M., Nappi, M., Riccio, D., & Wechsler, H. (2015). Mobile iris challenge evaluation (MICHE)-I, biometric iris dataset and protocols. *Pattern Recognition Letters*, 57, 17-23.
- De Oliveira Paula, M. V., Kinto, E. A., Hernandez, E. D., & Carvalho, T. C. M. D. B. (2005). User Authentication based on Human Typing Pattern with Artificial Neural Networks and Support Vector Machine.
- De Ru, W. G., & Eloff, J. H. (1997). Enhanced password authentication through fuzzy logic. *IEEE Expert*, 12(6), 38-45.
- De Vaus, D. (2006). Editor's Introduction. Research Design—A Review. *Research design*, 1, 1-11.
- Demirguc-Kunt, A., Klapper, L., Singer, D., Ansar, S., & Hess, J. (2018). *The Global Findex Database 2017: Measuring financial inclusion and the fintech revolution*. The World Bank.
- Deng, Y., & Zhong, Y. (2015). Keystroke dynamics user authentication using advanced machine learning methods. *Recent Advances in User Authentication Using Keystroke Dynamics Biometrics, GCSR*, 2, 23-40.
- Digital Guardian. (2017). *Digital Guard Rule Implementation Guide*. Digital Guardian.

- Eldefrawy, M. H., Khan, M. K., Alghathbar, K., Kim, T. H., & Elkamchouchi, H. (2012). Mobile one-time passwords: two-factor authentication using mobile phones. *Security and Communication Networks*, 5(5), 508-516.
- Elkhodr, M., Shahrestani, S. A., & Kourouche, K. (2012). A proposal to improve the security of mobile banking applications. *Proceedings of 2012 Tenth International Conference on ICT and Knowledge Engineering*, (pp. 260-265). Bangkok, Thailand.
- European Central Bank. (2016). *Revised oversight framework for retail payment* . Governing Council and Executive Board of the ECB.
- Eyeverify. (2017). *Creator of Eyeprint ID*. Retrieved from www.tswg.com.au/wp-content/uploads/EyeVerify.pdf
- Fabbri, R., Costa, L. D. F., Torelli, J. C., & Bruno, O. M. (2008). 2D Euclidean distance transform algorithms: A comparative survey. *ACM Computing Surveys (CSUR)*, 40(1), 1-44.
- Federal Reserve Board. (2015). *102nd Annual Report*. Board of Governors of the Federal Reserve System.
- Federal Reserve Board. (2015). *Consumers and Mobile Financial Services*. Washington, DC: Board of Governors of the Federal Reserve System.
- Federal Reserve System. (2016). *Consumers and Mobile Financial Services 2016*. Washington, DC : Board of Governors of the Federal Reserve System.

- Fischer, N., & Smolnik, S. (2013, January). The impact of mobile computing on individuals, organizations, and society-synthesis of existing literature and directions for future research. In *2013 46th Hawaii International Conference on System Sciences* (pp. 1082-1091). IEEE.).
- Forsen, G. E., Nelson, M. R., & Staron Jr, R. J. (1977). *Personal Attributes Authentication Techniques*. Pattern Analysis and Recognition Corp Rome Ny.
- Fridman, L., Weber, S., Greenstadt, R., & Kam, M. (2016). Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location. *IEEE Systems Journal*, *11*(2), 513-521.
- Fridman, L., Weber, S., Greenstadt, R., & Kam, M. (2016). Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location. *IEEE Systems Journal*, *11*(2), 513-521.
- Gambs, S., Killijian, M. O., & del Prado Cortez, M. N. (2012, April). Next place prediction using mobility markov chains. In *Proceedings of the first workshop on measurement, privacy, and mobility* (pp. 1-6).
- Gartner. (10 November, 2013). *Gartner Technology*. Retrieved from Gartner.com: <http://www.gartner.com/newsroom/id/2636073>
- George, S., & Reshma, M. (2017). Literature Survey on Mobile Banking Security. *International Journal of Innovative Research in Computer and Communication Engineering*, ISSN, 2320-9801

- Ghogare, S. D., Jadhav , S. P., Chadha, A. R., & Pa. (2012). Location based authentication: A new approach towards providing security. *International Journal of Scientific and Research Publications*.2(4), 2250-3153.
- Gravetter, F. J., & Forzano, L. B. (2012). *Research Methods for the Behavioral Sciences*. (4th.ed) Belmont, CA: Wadsworth: CENGAGE.
- Gundecha, S. S., & Naidu, M. (2016, December). Multilevel biometric authentication by using different techniques. In *2016 IEEE International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT)* (pp. 50-54). IEEE.
- Gurary, J., Zhu, Y., & Fu, H. (2017). Leveraging 3d benefits for authentication. *International Journal of Communications, Network and System Sciences*, 10(8), 324-338.
- Habib, M., & Alqatawna, J. F. (2017, October). A Proposed Password-Free Authentication Scheme Based on a Hybrid Vein-Keystroke Approach. In *2017 International Conference on New Trends in Computing Sciences (ICTCS)* (pp. 173-178). IEEE.
- Hang, A., De Luca, A., Smith, M., Richter, M., & Hussmann, H. (2015). Where have you been? using location-based security questions for fallback authentication. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)* (pp. 169-183).
- Harbach, M., Von Zezschwitz, E., Fichtner, A., De Luca, A., & Smith, M. (2014). It's a hard lock life: A field study of smartphone (un) locking behavior and risk

- perception. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)* (pp. 213-230).
- Hasan, J., Crawford, R. J., & Ivanova, E. P. (2013). Antibacterial surfaces: the quest for a new generation of biomaterials. *Trends in biotechnology*, *31*(5), 295-304.
- He, D., Chan, S., & Guizani, M. (2015). Mobile application security: malware threats and defenses. *IEEE Wireless Communications*, *22*(1), 138-144.
- Hemant , N., Waikar, V., & Khande, A. (2014). Online banking system using template based & keystroke dynamics password. *International Journal of Engineering Research & Technology*, *3*(3), 1071 - 1075.
- Heydarzadegan, A., Moradi, M., & Toorani, A. (2013). Biometric recognition systems: a survey. *International Research Journal of Applied and Basic Science*, *6*(11), 1609-1618.
- Ho, J., & Kang, D. K. Sequence Alignment with Dynamic Divisor Generation for Keystroke Dynamics Based User Authentication. *Journal of Sensors*, 2015. Retrieved from <https://www.hindawi.com/journals/js/2015/935986/#references>
- Hoang, T., & Choi, D. (2014). Secure and privacy enhanced gait authentication on smart phone. *TheScientificWorldJournal*, 2014, 438254-438254.
- Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74-81.
- Van Hove, L., & Dubus, A. (2019). M-PESA and Financial Inclusion in Kenya: Of Paying Comes Saving?. *Sustainability*, *11*(3), 568.

- Hussien, B., McLaren, R., & Bleha, S. (1989). An application of fuzzy algorithms in a computer access security system. *Pattern Recognition Letters*, 9(1), 39-43.
- IBIA. (2017). *Behavioral Biometrics*. Retrieved from [ibia.org: https://www.ibia.org/biometrics-and-identity/biometric-technologies/behavioral-biometrics](https://www.ibia.org/biometrics-and-identity/biometric-technologies/behavioral-biometrics).
- Islam, S. (2014). Systematic literature review: Security challenges of mobile banking and payments system. *International Journal of u-and e-Service, Science and Technology*, 7(6), 107-116.
- ISO/IEC 27033-4 (2014). Information technology - Security techniques - Network security - Part 4: Securing communications between networks using security gateways. Switzerland; ISO/IEC Retrieved from http://www.iso.org/iso/catalogue_detail?csnumber=54533
- Ivannikova, E., David, G., & Hämäläinen, T. (2017, July). Anomaly detection approach to keystroke dynamics based user authentication. In *2017 IEEE Symposium on Computers and Communications (ISCC)* (pp. 885-889). IEEE.
- Javelin strategy(February, 2017). . Identity Fraud: Securing the Connected Life,. *Technical Report* Retrieved from <https://www.javelinstrategy.com/sites/default/files/17-1001J-2017-LL-Identity-Fraud-Hits-Record-Highs-Javelin.pdf>
- Jeong, B. K., & Yoon, T. E. (2013). An empirical investigation on consumer acceptance of mobile banking services. *Business and Management Research*, 2(1), 31-40.

- Joshi, R., Venkatesan, S., & Myles, P. R. (2016). A UK general practice population cohort study investigating the association between lipid lowering drugs and 30-day mortality following medically attended acute respiratory illness. *PeerJ*, 4, e1902-e1902.
- Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, 32, 489-496.
- Joy, J. P., & Jyothis, T. S. (2016, November). Secure authentication. In *2016 Online International Conference on Green Engineering and Technologies (IC-GET)* (pp. 1-3). IEEE.
- Kambourakis, G., Damopoulos, D., Papamartzivanos, D., & Pavlidakis, E. (2016). Introducing touchstroke: keystroke-based authentication system for smartphones. *Security and Communication Networks*, 9(6), 542-554.
- Kayacik, H. G., Just, M., Baillie, L., Aspinall, D., & Micallef, N. (2014). Data driven authentication: On the effectiveness of user behaviour modelling with mobile device sensors. *arXiv preprint arXiv:1410.7743*.
- Kenya Commercial Bank. (2014). *Intergrated Report and Financial Statement*. Nairobi: KCB.
- Kenya Commercial Bank. (2017). *Consumer Barometer Study 2017 - The year of the mobile majority*. United Kingdom: Google/TNS, Consumer Barometer Study.
- Khan, W. Z., Xiang, Y., Aalsalem, M. Y., & Arshad, Q. (2012). Mobile phone sensing systems: A survey. *IEEE Communications Surveys & Tutorials*, 15(1), 402-427.

- Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: a literature survey. *IEEE Communications Surveys & Tutorials*, 15(4), 2091-2121.
- Kigen , P. M., Kimani, C., Mwangi, M., Shiyayo, B., Ndegwa, D., Kaimba, B., et al. (2015). *Kenya Cyber Security Report 2015*. Nairobi: Serianu Limited.
- Koong, C. S., Yang, T. I., & Tseng, C. C. (2014). A user authentication scheme using physiological and behavioral biometrics for multitouch devices. *The Scientific World Journal*, 2014, 1-14 .
- Krishna Prasad, K., & Aithal, P. S. (2017). A Study on Enhancing Mobile Banking Services using Location based Authentication. *International Journal of Management, Technology, and Social Sciences (IJMTS)*,(ISSN 24XX-XXXX), 1(1), 48-60.
- Kuseler, T., & Lami, I. A. (2012). Using geographical location as an authentication factor to enhance mCommerce applications on smartphones. *International Journal of Computer Science and Security (IJCSS)*, 6(4), 277-287.
- Kwapisz, J. R., Weiss, G. M., & Moore, S. A. (2011). Activity recognition using cell phone accelerometers. *ACM SigKDD Explorations Newsletter*, 12(2), 74-82.
- Lee, H., Hwang, J. Y., Kim, D. I., Lee, S., Lee, S. H., & Shin, J. S. (2018). Understanding keystroke dynamics for smartphone users authentication and keystroke dynamics on smartphones built-in motion sensors. *Security and Communication Networks*, 2018.

- Lee, Y. K., Park, J. H., Chung, N., & Blakeney, A. (2012). A unified perspective on the factors influencing usage intention toward mobile financial services. *Journal of Business Research*, 65(11), 1590-1599.
- Leigh, L. (04 August, 2013). *Personal identification number*. Retrieved from <https://www.revolv.com/page/Personal-identification-number>
- Li, F., Clarke, N., Papadaki, M., & Dowland, P. (2011, July). Behaviour Profiling for Transparent Authentication for Mobile Devices. In *European Conference on Cyber Warfare and Security* (p. 307). Academic Conferences International Limited.
- Lin, Y. D., Huang, C. Y., Wright, M., & Kambourakis, G. (2014). Mobile application security. *Computer*, 47(6), 21-23.
- Liu, F., Zhang, D., & Guo, Z. (2013). Distal-interphalangeal-crease-based user authentication system. *IEEE transactions on information forensics and security*, 8(9), 1446-1455.
- Lu, Y., Li, L., Yang, X., & Yang, Y. (2015). Robust biometrics based authentication and key agreement scheme for multi-server environments using smart cards. *PLoS One*, 10(5), e0126323.
- Luvanda, A., Kimani, S., & Kimwele, M. (2014). Identifying threats associated with man-in-the middle attacks during communications between a mobile device and the back end server in mobile banking applications. *IOSR Journal of Computer Engineering (IOSR-JCI)*, 12(2), 35-42.

- Mabel, J. J., & Balakrishnan, M. C. RESISTING PASSWORD BASED SYSTEMS FROM ONLINE GUESSING ATTACKS. In *International Conference on Information Systems and Computing . (ICISC-2013), INDIA*. pp 291-296
- Madiraju, T. (2014). *Dictionary Attacks and Password Selection* (Doctoral dissertation, Rochester Institute of Technology).
- Maghsoudi, J., & Tappert, C. C. (2016, August). A behavioral biometrics user authentication study using motion data from android smartphones. In *2016 European Intelligence and Security Informatics Conference (EISIC)* (pp. 184-187). IEEE.
- Maghsoudi, J., & Tappert, C. C. (2017, May). Increasing Accuracy Rate of Behavioural Biometrics for User Authentication on Android-Based Smartphones. In *2017 Proceedings of Student-Faculty Research Day* (pp.1-8)CSIS.
- Mahfouz, A., Mahmoud, T. M., & Eldin, A. S. (2017). A survey on behavioral biometric authentication on smartphones. *Journal of information security and applications*, 37, 28-37.
- Mallat, N., Rossi, M., & Tuunainen, V. K. (2004). Mobile banking services. *Communications of the ACM*, 47(5), 42-46.
- McLeod, J., & McLeod, J. (2003). *An introduction to counselling* (pp. 191-204). Buckingham: Open University Press.
- Meena, S & O'Grady M. (2016). Forrester Data Mobile, Smartphone, and tablet Forecast 2016 to 2021 (global) and Forrester's Consumer technographics. *North*

american online Benchmark Survey (Part 1). Retrieved from <https://www.forrester.com/report/Forrester+Data+Mobile+Smartphone+And+Tablet+Forecast+2016+To+2021+Global/-/E-RES135775>

- Meng, W., Wang, Y., Wong, D. S., Wen, S., & Xiang, Y. (2018). TouchWB: Touch behavioral user authentication based on web browsing on smartphones. *Journal of Network and Computer Applications*, *117*, 1-9.
- Meng, W., Wong, D. S., Furnell, S., & Zhou, J. (2014). Surveying the development of biometric user authentication on mobile phones. *IEEE Communications Surveys & Tutorials*, *17*(3), 1268-1293.
- Miranda, M. Q., Farias, J. S., de Araújo Schwartz, C., & de Almeida, J. P. L. (2016). Technology adoption in diffusion of innovations perspective: introduction of an ERP system in a non-profit organization. *RAI Revista de Administração e Inovação*, *13*(1), 48-57.
- Mirsky You, W., Qian, K., Lo, D. C. T., Bhattacharya, P., Chen, W., Rogers, T., ... & Yao, J. (2015, March). Promoting mobile computing and security learning using mobile devices. In *2015 IEEE Integrated STEM Education Conference* (pp. 205-209). IEEE.
- Montoya, D., Abiteboul, S., & Senellart, P. (2015, November). Hup-me: inferring and reconciling a timeline of user activity from rich smartphone data. In *Proceedings of the 23rd SIGSPATIAL International Conference on Advances in Geographic Information Systems* (pp. 1-4).

- Nancyliya, M., Mudjtabar, E. K., Sutikno, S., & Rosmansyah, Y. (2014, October). The measurement design of information security management system. In *2014 8th International Conference on Telecommunication Systems Services and Applications (TSSA)* (pp. 1-5). IEEE.
- Ndumba, H. W., & Muturi, W. (2014). Factors affecting adoption of mobile banking in Kenya; Case study of Kenya Commercial Bank Limuru. *International Journal of Social Sciences Management and Entrepreneurship*, *1*(3), 92-112.
- Nosrati, L., & Bidgoli, A. M. (2016, October). A review of authentication assessment of Mobile-Banking. In *2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)* (pp. 1-5). IEEE.
- Oluoch, S. O. (2014). Improving Password Security Using Location-Based Intelligence. *International Journal of Scientific and Research Publications*, *4*(2), 1-4.
- Ortiz-Yepes, D. A., Hermann, R. J., Steinauer, H., & Buhler, P. (2014). Bringing strong authentication and transaction security to the realm of mobile devices. *IBM Journal of Research and Development*, *58*(1), 4-1.
- Owens, J., & Matthews, J. (2008, March). A study of passwords and methods used in brute-force SSH attacks. In *USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*.
- Pahuja, G., & Nagabhushan, T. N. (2015, March). Biometric authentication & identification through behavioral biometrics: A survey. In *2015 International Conference on Cognitive Computing and Information Processing (CCIP)* (pp. 1-7). IEEE.

- Pal, B., Daniel, T., Chatterjee, R., & Ristenpart, T. (2019, May). Beyond credential stuffing: Password similarity models using neural networks. In *2019 IEEE Symposium on Security and Privacy (SP)* (pp. 417-434). IEEE.
- Panja, B., Fattaleh, D., Mercado, M., Robinson, A., & Meharia, P. (2013, May). Cybersecurity in banking and financial sector: Security analysis of a mobile banking application. In *2013 international conference on collaboration technologies and systems (CTS)* (pp. 397-403). IEEE.
- Parahoo, K. (2014). *Nursing research: principles, process and issues*. Macmillan International Higher Education.
- Parkavi, R., Babu, K. C., & Kumar, J. A. (2017, January). Multimodal biometrics for user authentication. In *2017 11th International Conference on Intelligent Systems and Control (ISCO)* (pp. 501-505). IEEE.
- Patil, R. A., & Renke, A. L. (2016). Keystroke dynamics for user authentication and identification by using typing rhythm. *International Journal of Computer Applications*, *144*(9), 27-33.
- Patton, M. Q. (2014). *Qualitative research & evaluation methods: Integrating theory and practice*. Sage publications.
- Pegueros, V. (2012). Security of mobile banking and payments. *SANS Institute InfoSec Reading Room*, *1*.
- Peng, J., Choo, K. K. R., & Ashman, H. (2016). User profiling in intrusion detection: A review. *Journal of Network and Computer Applications*, *72*, 14-27.

- Pisani, P. H., & Lorena, A. C. (2013). A systematic review on keystroke dynamics. *Journal of the Brazilian Computer Society*, 19(4), 573-587.
- Ponieman, N. B., Salles, A., & Sarraute, C. (2013, August). Human mobility and predictability enriched by social phenomena information. In *Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining* (pp. 1331-1336).
- Poushter, J. (2016). Smartphone ownership and internet usage continues to climb in emerging economies. *Pew research center*, 22(1), 1-44.
- Quraishi, S. J., & Bedi, S. S. (2018, November). Keystroke Dynamics Biometrics, A tool for User Authentication—Review. In *2018 International Conference on System Modeling & Advancement in Research Trends (SMART)* (pp. 248-254). IEEE.
- Rajasekar, S., Philominaathan, P., & Chinnathambi, V. (2013). Research Methodology. Retrieved April 8, 2015. Saifan, R., Salem, A., Zaidan, D., & Swidan, A. (2016). A Survey of behavioral authentication using keystroke dynamics: Touch screens and mobile devices. *Journal of Social Sciences (COES&RJ-JSS)*, 5(1), 29-41.
- Ramatsakane, K. I., & Leung, W. S. (2017, May). Pick location security: Seamless integrated multi-factor authentication. In *2017 IST-Africa Week Conference (IST-Africa)* (pp. 1-10). IEEE. Naboulsi, D., Fiore, M., Ribot, S., & Stanica, R. (2015). Large-scale mobile traffic analysis: a survey. *IEEE Communications Surveys & Tutorials*, 18(1), 124-161.
- Reid, R., & Van Niekerk, J. (2014, August). From information security to cyber security cultures. In *2014 Information Security for South Africa* (pp. 1-7). IEEE.

- Revett, K., Gorunescu, F., Gorunescu, M., Ene, M., Magalhaes, S., & Santos, H. (2007). A machine learning approach to keystroke dynamics based user authentication. *International Journal of Electronic Security and Digital Forensics*, 1(1), 55-70.
- Rogers, E. M. (1962). Library of Congress Cataloging in Publication Data. *Innovation*, 11(2).
- Rogers, E. M. (2003). Diffusion of innovations, 5th edn Tampa. *FL: Free Press.[Google Scholar]*.
- Sang, Y., Shen, H., & Fan, P. (2004). Keystroke characteristics identity authentication based on levenberg-marquardt algorithm. *Computer Applications*, 24(7), 1-3.
- Sarlak, M. A., Roustaei, M., & Moqadasan, M. H. (2012). Factors affecting the mobile banking adoption in Iran. In *Fourth International Conference Marketing of banking services*. Kigen, P. M., Muchai, C., Kimani, K., Mwangi, M., Shiyayo, B., Ndegwa, D., ... & Shitanda, S. (2015). *Kenya Cyber Security Report 2015*. Serianu Limited.
- Sesa-Nogueras, E., & Faundez-Zanuy, M. (2012). Biometric recognition using online uppercase handwritten text. *Pattern Recognition*, 45(1), 128-144.
- Shahriar, H., Klintic, T., & Clincy, V. (2015). Mobile phishing attacks and mitigation techniques. *Journal of Information Security*, 6(03), 206.

- Shih, D. H., Lu, C. M., & Shih, M. H. (2015, August). A flick biometric authentication mechanism on mobile devices. In *2015 International Conference on Informative and Cybernetics for Computational Social Systems (ICCSS)* (pp. 31-33). IEEE.
- Shivhare, B., Sharma, G., & Kushwah, S. P. S. (2014, November). A study on Geo-Location Authentication techniques. In *2014 International Conference on Computational Intelligence and Communication Networks* (pp. 744-748). IEEE.
- Singh, D., Jaggi, B., Nayyar, H., & Kumar, A. (2017). Presskey-A Keystrokes Dynamics Based Authentication System. *International Journal of Advanced Research in Computer Science*, 8(5).
- Singh, S. (2014). The impact and adoption of mobile banking in Delhi. *International Research Journal of Business and Management*, 1(7), 19-31.
- Spillane, R. (1975). Keyboard apparatus for personal identification. *IBM Technical Disclosure Bulletin*, 17, 3346. Adler, T., Niles, F., & Spitz, G. (2007). *Web-Based Survey Techniques. A Synthesis of Transit Practice* pp 69.
- Spolaor, R., Li, Q., Monaro, M., Conti, M., Gamberini, L., & Sartori, G. (2016). Biometric Authentication Methods on Smartphones: A Survey. *PsychNology Journal*, 14(2).
- Sung, K. S., & Cho, S. (2006, January). GA SVM wrapper ensemble for keystroke dynamics authentication. In *International conference on Biometrics* (pp. 654-660). Springer, Berlin, Heidelberg.

- Tague, N. R. (2005). *The Quality Toolbox*. Milwaukee, WI: American Society for Quality.
- Tanviruzzaman, M., & Ahamed, S. I. (2014, July). Your phone knows you: Almost transparent authentication for smartphones. In *2014 IEEE 38th Annual Computer Software and Applications Conference* (pp. 374-383). IEEE.
- Tapiador, M., Sigüenza, J. A., & de Neurocomputación Biológica, G. (1999). Fuzzy keystroke biometrics on web security. In *IEEE Workshop on Automatic Identification Advanced Technologies* (pp. 133-136).
- Thinking Business Awards. (2017). ThinkingBusinessAwards. Retrieved from *Businessdailyafrica.com*:<https://www.businessdailyafrica.com/corporate/companies/KCB-named-Bank-of-Year-at-global-fete/4003102-4216150-10s4bj8z/index.html>.
- Thinking, M. (2014). Global mobile statistics 2014 Part A: Mobile subscribers; handset market share; mobile operators. *Consulté le September, 5, 2015*.
- 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).
- Vedapradha, R., & Ravi, H. (2018). Application of artificial intelligence in investment banks. *Review of Economic and Business Studies*, *11*(2), 131-136.

- Velasquez, E., Ferguson, J., Cullina, M., Beck, T., Bond, P., Donahue, M., ... & Terry, M. (2017). Identity Theft: The Aftermath 2017.
- Vinayak, R., & Arora, K. (2015). A survey of user authentication using keystroke dynamics. *International Journal of Scientific Research Engineering & Technology (IJSRET)*, 4(4), 378-384.
- Virvilis, N., Gritzalis, D., & Apostolopoulos, T. (2013, December). Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game?. In *2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing* (pp. 396-403). IEEE.:
- Visa Europe (2015). Annual Report.UK: Visa Europe from https://s1.q4cdn.com/050606653/files/doc_financials/annual/VISA-2015-Annual-Report.pdf
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, 38, 97-102.
- Wakabayashi, N., Kuriyama, M., & Kanai, A. (2017, January). Personal authentication method against shoulder-surfing attacks for smartphone. In *2017 IEEE International Conference on Consumer Electronics (ICCE)* (pp. 153-155). IEEE.
- Wewege, L., Lee, J., & Thomsett, M. C. (2020). Disruptions and Digital Banking Trends. *Journal of Applied Finance & Banking*, 10(6), 15-56.
- Yamane, T. (1967). *An Introductory Analysis* (2nd Ed) . London: Harper and Row, .

- Yasin, A., & AbuAlrub, F. (2016). Enhance RFID Security Against Brute Force Attack Based on Password Strength and Markov Model. *Int. J. Netw. Secur. Its Appl*, 8(5), 19-38.
- Zahid, S., Shahzad, M., Khayam, S. A., & Farooq, M. (2009, September). Keystroke-based user identification on smart phones. In *International Workshop on Recent advances in intrusion detection* (pp. 224-243). Springer, Berlin, Heidelberg.
- Zaidi, S. F. A., Shah, M. A., Kamran, M., Javaid, Q., & Zhang, S. (2016). A survey on security for smartphone device. *International journal of advanced computer science and applications*, 7(4), 206-219.
- Zhou, Z., & Huang, D. (2012, October). Efficient and secure data storage operations for mobile cloud computing. In *2012 8th international conference on network and service management (cnsm) and 2012 workshop on systems virtualization management (svm)* (pp. 37-45). IEEE.

APPENDICES

Appendix A Survey Questionnaire

INSTRUCTIONS:

I am a post graduate student pursuing a degree of master of Computer Systems at Jomo Kenyatta University of agriculture and technology (Nairobi CBD Campus). I am conducting a research survey for my MSc. Final Project and your input would be highly appreciated. The information you will provide will be treated with great confidentiality and will not be used for any other purpose other than for the purpose of this academic research. This online survey has been divided into two parts. Please, indicate the correct option from the provided choices. For the questions that require your own opinion use the provided spaces. Kindly complete the Survey to the best of your knowledge.

Survey questions

This is a survey regarding research on using behavioral profiling and location verification authentication as a method of securing mobile banking transactions.

Please select the appropriate answer(s)

Section A: User Demographics

1) What is your gender?

Male

Female

2) What is your age bracket?

18-25

26-35

36-45

46-55

Over 55

3) What's your highest level of education completed?

Primary

Secondary

Technical and vocational education

University

No formal education

4) Do you own a smart phone?

Yes

No

5) Do you have a bank account?

Yes

No

6) Have you subscribed to any mobile banking service?

Yes

- No
- Not Interested
- Not Sure
- Other (Please Specify)

7) If you answered Yes on question 6 above , what do you use mobile banking for?(Check all that apply)

- Paying bills (i.e. water, electricity)
- Withdraw Cash
- Cash Transfer
- Check account balance
- Other (please specify)

8) How often do you use mobile banking (M-banking)?

- Daily
- Once a week
- Once a Month

9) What are some of the reasons that would prevent you from using mobile banking?(Click all that apply)

Security of mobile banking service.

Information privacy

Do not find it necessary

Theft of PIN

Cost of Smart Phone

10) What do you consider important to you in considering mobile banking? (Click all that apply)

Security of the platform

Convenience of the Mobile banking service

User friendly of the mobile banking application

Trust in bank

Cost of the Mobile banking service

Compatibility of the mobile banking application on any smart phone

2.

Please select the appropriate answer(s)

Section B: Mobile Banking

11) Using the scale of 1 to 5, 1 being the lowest and 5 being the highest. How do you rate yourself on skills and experience with smart phone application usage.

- 1 = Basic skills and Least Experienced
- 2 = Novice
- 3 =Intermediate
- 4 =Advanced
-

3. **5= Expert and highly experienced**

4.

12) How is your experience when conducting financial transaction through smart mobile phone?

-

13) On a scale of 1 to 5: where 5= Strongly Agree, 4= Agree, 3= Neutral, 2=Disagree, 1= Strongly Disagree Is your preferred bank secure in terms of service provision through mobile technology. (*Tick where necessary*)

- 1 (Strongly Disagree)
- 2 (Disagree)

- 3 (Neutral)
- 4 (Agree)
- 5 (Strongly Agree)

14) What are authentication features that your bank has placed to secure mobile banking transactions?*(Click all that apply)*

- Personal Identification Number (PIN)
- Password Authentication
- Token based authentication
- Transparent authentication (i.e Finger print, Eye, location, Face recognition)
- Other (please specify)

15) Are there security updates that the bank does to their mobile banking service? If yes ,how often are they done

- Monthly
- Regularly
- Every 6 months

Yearly

No Updates

16) How often do you change your authentication details on your mobile banking application?

Very Often

Often

Rarely

None

17) Have you ever experienced suspicious activity on your mobile banking account?

Yes

No

18) What is your take on capturing user behavior and location verification to improving mobile banking security?

19) Do you think banks can adopt this method for their mobile banking application?

Yes

No

20) In your own opinion what could make mobile banking authorization more secure?

Thank you for your cooperation

Appendix B: Letter of introduction

EDWIN MBUGUA MIIRI,
P.O.BOX 3629-20100.
NAKURU.
MOBILE NO: +254 710506667.
EMAIL: mbugua.edwin@gmail.com.
5TH JANUARY 2018.

THE BRANCH MANAGER,
KCB HEAD OFFICE,
KENCOM HSE NAIROBI,
P. O. Box 48400-00100.
NAIROBI.

KENYA.

Dear Sir/Madam

RE: REQUEST TO CONDUCT ACADEMIC SURVEY

I am a post graduate student (SCT312-C004-5880/2015) pursuing a degree of master of Computer Systems at Jomo Kenyatta University of agriculture and technology (Nairobi CBD Campus).Currently I am at the research stage where my thesis is based on Active authentication for mobile devices utilizing behavior profiling and location verification.

I do request you to assist me in according me the permission to administer the online survey at your branch. The survey is entirely for academic purposes and the bank's confidentiality will be maintained.

Thanks in advance.

Edwin Mbugua