



Strathmore
UNIVERSITY

Strathmore University
SU+ @ Strathmore
University Library

Electronic Theses and Dissertations

2017

Near field communication based-model for authentication in online banking

Esther Akinyi Omondi
Faculty of Information Technology (FIT)
Strathmore University

Follow this and additional works at <http://su-plus.strathmore.edu/handle/11071/5606>

Recommended Citation

Omondi, E. A. (2017). *Near field communication based-model for authentication in online banking*

(Thesis). Strathmore University. Retrieved from <http://su-plus.strathmore.edu/handle/11071/5606>

This Thesis - Open Access is brought to you for free and open access by DSpace @ Strathmore University. It has been accepted for inclusion in Electronic Theses and Dissertations by an authorized administrator of DSpace @ Strathmore University. For more information, please contact librarian@strathmore.edu

Near Field Communication Based-Model for Authentication in Online Banking

Omondi, Esther Akinyi

Master of Science in Computer-Based Information Systems

2017

Near Field Communication Based-Model for Authentication in Online Banking

Omondi, Esther Akinyi

**A dissertation submitted in partial fulfillment of the requirements for the degree of
Masters of Science in Computer Based Information Systems (MSc.IS) at Strathmore
University**

**Faculty of Information Technology
Strathmore University
Nairobi, Kenya**

June, 2017

**This dissertation is available for library use on the understanding that it is copyright
material and that no quotation from the dissertation may be published without proper
acknowledgement**

Declaration

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the dissertation contains no material previously published or written by another person except where due reference is made in the dissertation itself.

© No part of this dissertation may be reproduced without the permission of the author and Strathmore University

Omondi, Esther Akinyi

13th June, 2017

Approval

The dissertation of Omondi, Esther Akinyi was reviewed and approved by the following:

Prof. Ismail Ateya Lukandu, D. Sc.

Associate Professor, Faculty of Information Technology

Ag. Dean of Research,

Strathmore University

Dr. Joseph Orero,

Dean, Faculty of Information Technology,

Strathmore University

Professor Ruth Kiraka,

Dean, School of Graduate Studies,

Strathmore University

Abstract

Online banking has enabled bank customers to perform their banking activities at the comfort of their homes as opposed to physically visiting the bank branches. In the banking environment, authentication is very crucial because the bank should be able to give access to the only authorized customers. Currently, there are various authentication methods available to the banks for authenticating their customers. However, the empirical study has shown that there is an increasing number of identity theft leading to huge financial losses for both banks and bank customers. Additionally, the better authentication systems are complex for customers and more costly to the banks. This dissertation discusses the use of Near Field Communication (NFC), a short range based wireless communication technology currently improving the consumers' usability due to its ability to exchange digital material as well as connecting electronic devices remotely. It is an evolving technology employing the use of Radio frequency identification (RFID) that lets electronic devices like Smart phones interconnect over very close range. The NFC technology has been integrated into some available Smart phones, when employed together with other authentication mechanisms such as Master Card's Chip authentication program (CAP), its usability level is increased. The model employs the use of NFC enabled Smart phones and NFC enabled bank cards as third factor authentication. Agile methodology was used for the model development, and a java code that generates a QR code was developed. The NFC based model, when implemented is able to eliminate the need for a hard token which is an extra baggage to the customer and additional cost to the bank. Consequently, the NFC technology enhances security for online banking by protecting against online identity theft as well as form basis for future research in NFC application the banking industry.

Table of Contents

Declaration.....	iii
Abstract.....	iv
List of Tables	ix
List of Figures.....	x
Abbreviations/Acronyms.....	xi
Definition of terms	xii
Acknowledgements	xiii
Dedication	xiv
Chapter 1: Introduction	1
1.1 Background of the Study.....	1
1.2 Problem Statement.....	3
1.3 Research Objectives	3
1.4 Research Questions.....	3
1.5 Justification	3
1.6 Scope and Limitation	4
Chapter 2: Literature Review.....	5
2.1 Introduction.....	5
2.1.1 Authentication.....	5
2.2Online banking system overview.....	6
2.3 Authentication in online banking	7
2.4 Attacks on the online banking systems	7
2.4.1 Phishing.....	7
2.4.2 Data Breaches	8
2.4.3 Risks Driving the Need for Change in online banking authentication methods.....	9
2.5 Bank provided Anti-Phishing measures	9
2.5.1 Transaction Authorization Numbers (TANs)	10

2.5.2 Secure ID	10
2.5.3 Chip Authentication Protocol.....	12
2.5.4 Smartphone Solutions.....	13
2.6 NFC technology other Communication Devices	13
2.6.1 Operating modes of NFC Devices.....	14
2.6.2 NFC Protocol	15
2.6.3 NFC Security	16
2.6.4 Industry-wide application of NFC technology	17
2.6.5 How NFC compares with other communication modalities	17
2.6.6Incorporation of NFC in mobile phones.....	18
2.7 Debit Card Architecture	19
2.8Conceptual Framework.....	20
Chapter 3: Research Methodology.....	22
3.1 Introduction	22
3.2 Study Area	22
3.3Research Design.....	22
3.4 Population and Sample Size determination.....	23
3.5 Data sources and respondents	24
3.6 Data Collection methods	25
3.7 System Design, Development and Methodology	25
3.8 Data Analysis and Presentation	27
3.9 Validity and reliability of the research.....	27
3.10 Ethics in Research.....	27
Chapter 4: System Design and Architecture	29
4.1Introduction.....	29
4.2 Data Results, Presentation and Analysis	29
4.3 System Design and Architecture.....	42

4.3.1 Introduction	42
4.3.2 Analysis of the System	42
4.3.3 System Initiation and Planning.....	42
4.3.4 Analysis Phase	43
4.3.5 System Requirements	43
4.3.6 The Use Case analysis	44
4.4 System Design	47
4.4.1 Data flow modeling.....	47
4.4.4 Conceptual Design of the Model	50
4.5 Model Implementation	52
Chapter 5: System Implementation and Testing	53
5.1 Introduction	53
5.2 Implementation	53
5.2.1 System Requirement	53
5.3 Testing.....	57
Chapter 6: Discussions	59
6.1 Comparative analysis between research findings and existing literature.....	59
6.1.1 Bank employees	59
6.1.2 Bank Customers	60
6.2 Correlations of the functionalities of the model being developed with the java-based prototype.....	61
6.3 Why this research is unique	61
6.4 Constrains in NFC technology	62
Chapter 7: Conclusions and Recommendations	63
7.1 Conclusions	63
7.2 Recommendations	63
7.3 Suggestions for future research	64

REFERENCES.....	65
Appendices.....	69

List of Tables

Table 2.1 NFC Operating modes.....	15
Table 4.1 Enter the URL of the Bank Site Use Case.....	48
Table 4.2 QR Code Generation Use Case.....	59
Table 4.3 Scanning of QR Code Use Case.....	59

List of Figures

Figure 2.1 Phishing Activity Report 1st Quater 2016.....	8
Figure 2.2 Total NFC-Enabled Device and Chipset Shipment (2009-2015).....	18
Figure 2.3 NFC enabled mobile phone shipped.....	19
Figure 2.4 Challenge response authentication method	20
Figure 3.1 Software Development Process	26
Figure 3.2 Agile Development Methodology	27
Figure 4.1 Gender of Employees	29
Figure 4.2 Department in which the employees worked	30
Figure 4.3 Utilization of online banking services	31
Figure 4.4 Data about bank employees informing their customers about online banking	31
Figure 4.5 Likert scale on whether online banking is beneficial to customers	32
Figure 4.6 NFC Function on mobile phone	33
Figure 4.7 Importance of NFC in the banking industry	34
Figure 4.8 Gender distribution.....	34
Figure 4.9 Age Distribution among Customer Respondents	35
Figure 4.10 Access to Online Banking	36
Figure 4.11 Mode of access to online banking	36
Figure 4.12 Likert scale on benefits of online banking.....	37
Figure 4.13 Responses for those who don't have access to online banking service	38
Figure 4.14 Responses on whether the customer shared their password or PIN.....	38
Figure 4.15 Responses on whether Customers felt that the Bank shares their Login Credentials .	39
Figure 4.16 Responses on ownership of smartphones	40
Figure 4.17 Responses on NFC functionality on mobile phones.....	41
Figure 4.18 Use Case Diagram for the NFC-Based Online Banking Authentication.....	45
Figure 4.19 Context diagram of the system	47
Figure 4.20ER Diagram.....	48
Figure 4.21Sequence Diagram for customer authentication protocol.....	49
Figure 4.22 NFC Model System Architecture	51
Figure 4.23 Model Implementation.....	52

Abbreviations/Acronyms

AES	-	Advanced Encryption Standard
APWG	-	Anti Phishing Working Group
ATM	-	Automatic Teller Machine
BFID	-	Banking Fraud and Investigation Department
CAP	-	Chip Authentication Program
EMV	-	Euro MasterCard and Visa
HHD	-	Hand Held Device
ICT	-	Information Communication Technology
IP	-	Internet Protocol
MAC	-	Message Authentication Code
NFC	-	Near field communication
OTP	-	One time password
PC	-	Personal computer
POS	-	Point of sale
QR	-	Quick Response
RFID	-	Radio Frequency Identification
SSL	-	Secure Socket Layer
TAN	-	Transaction Authorization Number
TLS	-	Transport Layer Security
URL	-	Uniform Resource Locator

Definition of terms

Phishing- Refers to the attack intended to persuade online banking users to give away their online banking credentials to a third party, (Williamson, 2006).

Pharming- Refers to a phishing method where the Domain Name System is altered by an attacker with the resulting Uniform Resource Locator (URL) appearing as legitimate. (Gunter, 2005)

Acknowledgements

I thank the Almighty God for His love, wisdom and knowledge. It is through His guidance and Kindness that I am able to write this dissertation

I am grateful to my Supervisor Prof. Ateya for his guidance and patience throughout my dissertation writing. I am very grateful to the Masters students in both Computer Based Information Systems and Information Technology class of 2016 for their moral support and encouragement.

Dedication

I dedicate this to all who have assisted me to get to this point; particularly my spouse Lucas Onyango, my daughters-Hellen Bernice, MaryAnne and Margaret Fiona- for their understanding and perseverance. I also appreciate all my lecturers, friends, colleagues and fellow students who have been greatly supportive and instrumental in my endeavors.

Chapter 1: Introduction

1.1 Background of the Study

Authentication involves the matching of a provided credential to those stored on a bank database. According to (Zimmerman, 2002), the access is normally achieved by a person providing their identity by the use of some means of authentication. That is, a person must be able to confirm who they say they are before accessing information, and if the person is unable to do so, access will be denied

The Internet brought new alternatives to the financial markets and banks started to experience the possibilities of the Internet by around mid-1990s (Calisir & Gumussoy, 2008). The new technological advancements assisted banks to provide online banking services that enabled customers to get connected to the bank's computer systems via Internet connections (Claessens, et al., 2002).

Currently, the *modus operandi* is that the banks' clients are provided with accessibility to their accounts over the Internet. This functionality has enabled the banking system to introduce various financial Internet banking applications which comprises of money transfer services, investment services and currency exchange services. This has tremendously revolutionized financial transaction within the banking sector and as Amit & Zott (2001) points out, online banking functionalities bring effectiveness with regards to accessibility, cost reduction, speed and reliability while needing fewer bank employees and less bank branches than banking channels.

According to Anderson et al. (2012), the least validation needed to gain access to a bank's online site has been a problem because online attackers use their expertise to rob customers by tricking them to release confidential log in credentials for online banking accounts. Empirical evidence shows that there has been an increased case of personal information compromises that have taken place in the past years. This occurrence has made the customers wary about the safety of their information. In addition, customers do expect to enjoy some level of security while accessing their information online. This level of security should be same as the one enjoyed at the branch banking.

One of the central arguments that form the foundation of this research is the question of whether online banking is safe given that the banking security breaches are on the rise. As Anderson et al. (2012), puts it, the yearly worldwide monetary losses of monetary fraud undertakings can be estimated to be equivalent to the tune of a trillion Shillings.

Today's authentication methods identify an individual as an authorized user in three scopes including: what you know, what you have, or what you are. Usernames and passwords are nowadays not strong enough to prevent online attacks (Williamson, 2006). Out of the abovementioned authentication methods, the widely used authentication method is passwords which represents the "what you know" method. A more sophisticated method of authentication is what we have such as smart cards and tokens, where the devices are used to secure against content manipulation attacks with transaction signing solutions (Gunther & Borchert, 2013).

Modern technology has equipped Smart phones with mobile applications that are synchronized with the bank's server to offer authorization to customer's accounts. Additionally, customers are nowadays equipped with Smart phones and would not wish to have other additional devices like in the case of tokens. However, these applications are vulnerable to Smartphone Malware (Gunther & Borchert, 2013) hence the need for an alternative authentication method that incorporates the Smart phone application with bank card for secure transaction signing solutions. This solution will defeat online banking frauds such as man in the middle attack which can influence the communication shared between bank and the customer's Personal computer.

The use of bank card and a smart phone solution is not affected by the aforementioned attacks because the Personal Computer (PC) Trojan is not able to modify the operation since the display will be shown on the mobile phone's display. Additionally, mobile attack is not possible to modify the transaction because the genuine transaction has already been shown to the personal computer. The model described in this research will offer the much needed solution by integrating Smart phone technology with a bank card by applying the use of Near Field Communication (NFC) technology to allow for machine-to-machine communication. The general evaluation was considered and several aspects such as cost, security and performance taken into consideration.

1.2 Problem Statement

There are different authentication methods in use today which from to empirical studies have varied weaknesses, making their use challenging and difficult for some groups of users. The security of these applications must balance between a higher security level and practicality. The more security added to these systems, for example in the instance of pass phrases instead of passwords and many verification tokens, the lesser will be the approval rate of the customers and the usability will decline (Meyer, 2007).

The solution is to use an NFC-enabled technology which involves the use of a genuine bank card to approve transactions initiated via a personal computer in combination with an NFC enabled mobile phone. As a proof of concept there will be a development of a model that incorporates a Smart phone that reads the transaction via two dimensional (2D) Quick Response (QR) code from the Personal Computer, shows transaction on the display for verification by the bank provided card through the use of NFC.

1.3 Research Objectives

- i. To review the existing methods of authentication in online banking and their challenges
- ii. To review the architectures, models and prototypes in transaction authentication methods that support NFC-Based authentication methodology
- iii. To develop NFC-Based model transaction authentication in online banking
- iv. To test the model.

1.4 Research Questions

- i. What are the existing methods and challenges of authentication in online banking?
- ii. What are the architectures, models and prototypes in transaction authentication methods that support NFC-Based authentication methodology?
- iii. How will the NFC-Based model be developed?
- iv. How will the model be tested?

1.5 Justification

According to a report by Banking Fraud and Investigation Department (BFID), there is an increased use of Information Communication Technology (ICT) as a promoter of banking services with online banking taking the lead. Consequently, the report indicates that there have

been increased ICT related fraud cases in the recent period, with cases involving mobile, computer and Internet banking fraud being on the higher side. Other fraudulent cases such as card scam have also been linked to online attacks on customer's computers that lack proper firewall protection (Central Bank of Kenya, 2014).

The degree of authentication differs across banks and is governed by the bank's security structure as well as risk acceptance directed by the bank's risk policies. It is indeed true that the two factor authentication is most effective at avoiding masquerade; nevertheless tokens are not one hundred percent guaranteed and secret codes can easily be forgotten. Additionally, the tokens have a life cycle prompting the user to replace whenever it expires (Antonioni & Socha, 2016).

Therefore, there is a need for an alternative authentication system that will address the challenges facing the state of the art authentication methods. This research will fill this gap by proposing the development an NFC based authentication model that uses bank provided card to approve online banking transactions processed through personal computers in combination with a mobile phone (Gunther & Borchert, 2013). In addition, NFC is an emerging Technology that will transform the banking industry.

1.6 Scope and Limitation

The banking sector in Kenya comprises of over forty four banks and other stakeholders and players in the industry such as Central Bank of Kenya (Regulator) and Kenya Bankers' Sacco (Union). It would have taken more time and resources to conduct a research on all the Kenyan banks offering the online banking service. Findings of the study depended upon the obtainability of data with reference to time and convenience. The execution of the model was limited to the bank server accepting one instance of the same transaction. The development of the model covered the coding of the commands that was read by the NFC enabled Smart phone and confirmed by NFC enabled bank card.

1.7 Assumptions

The assumptions listed below were made regarding this research:

- a) That bank preferred a bank card over tokens because the card's security features are incorporated into the bank's database.
- b) Personal banking customers do not want a hard tokens (additional) and the bank application in form of a soft token loses synchronization hence not reliable
- c) Customers have Smart phones and have been issued with a bank card.

Chapter 2: Literature Review

2.1 Introduction

There are various online banking authentication methods in use today. However, these methods present varied challenges in regard to usability, reliability and cost effectiveness. In this chapter, these methods are discussed and their merits and demerits compared. The design and architectures of the studied authentication techniques formed the building blocks for the development of the model.

2.1.1 Authentication

According to Kilani and Jensen (2013), there are two divisions of authentication. These include; peer entity authentication and data origin authentication. Two peers are able to authenticate each other by providing a relationship between themselves in the peer entity authentication. On the other hand data origin authentication involves the proof of the source of a portion of data from a known entity. Furthermore, peer entity authentication, consists of the prover and the verifier as the participants. Here, the prover must be able to confirm the relationship while the verifier must be able to validate the accuracy the secret presented by the prover.

According to the authors, there are four essential issues that must be considered when operating with authentication systems. They include-(i) Effectiveness, (ii) usability, (iii) cost and (iv) impersonation attacks. Further, Kilani and Jensen (2013) alludes that it is difficult to achieve a perfect validation as a result of some factors that may be technical or non-technical. In the peer entity authentication, the prover provides information to the verifier inform of credentials or objects of value to prove the claim of who the prover is.

According to Kizza (2005), the objects of value or credentials are founded on numerous distinctive factors that reveal something you have, something you know, or something you are. The principal validation factor entails the use some mentally possessed secret by an individual. However, for the case of a device, some Personal Identification number is stored for comparison. The secret codes need to be difficult to predict so as to prevent predicting attacks like dictionary attacks. For this reason, online users are encouraged to always ensure to use passwords that are not easy to predict. Something a principal has forms the second factor including tokens (hardware or software code generators) and smartcards. Lastly, something you are is the third factor authentication that relates to what we are in the form of body parts like finger print.

In order to achieve data origin authentication, the calculation of Message Authentication Code and usage of some symmetric key is employed. For the case of key calculation, some symmetric key is generated and shared between the two entities validating each other. The other available technique involves the usage of the digital signatures whereby data is signed using a private key PK of the person establishing its validity. Since a Message Authentication Code is based on symmetric keys, it is considerably faster to estimate. However, the two parties must have a shared key.

The message authentication code has a distribution challenge which is countered by the use of the key generation methodology. Asymmetric keys are generally realized by the use of an open key cryptography, permitting an entity to compute a challenge so that the challenge can be interpreted by the other entity who is aware of the challenge (Kizza, 2005). The model discussed in this dissertation used the abovementioned authentication technique to demonstrate NFC-based authentication model for online banking.

2.2 Online banking system overview

An online banking set up encompasses a customer who accesses the online banking portal over the Internet using a web browser. The bank is signified by the bank server which hosts the online banking portal and replies to the demands sent by the browser acting on behalf of the customer. Banks and customers want to have access to financial services over the web, at the same time, they want to do so in a secure and cost effective way. According to Ortiz-Yepes (2009), the main goal of online banking system is to strike the balance between security, usability and cost efficiency.

Both the customer and the bank server must authenticate each other before any of them can release sensitive information like authentication credentials. The customer must certify that he or she is communicating to the bank server and not to a third party posing as the bank. On the other hand, the customer requires authentication from the bank. To ensure that only permitted customers use the online system, stop impostors from pretending to be genuine users, anyone trying to get connected to the online banking portal need to be positively validated by the bank. An invader should not be able to make a transaction if he or she is not a genuine customer. This indicates that the bank needs to authenticate both the customer and the transaction that he or she requests (Ortiz-Yepes, 2009).

According to Ortiz-Yepes (2009), the information exchanged between the customer and the bank during the online banking session need not to be made available to the unauthorized person except when the transaction includes another bank account where the other bank will require the details to facilitate the transaction. The security system for the bank should be usable

2.3 Authentication in online banking

Online banking users must first be authenticated by the systems before any access is granted to specific services. More specifically, the banking system need to determine whether a user is, who he or she claims to be by requesting for direct or indirect evidence of awareness about some sort of secret information or credentials. With the notion that only genuine user can provide such responses, positive validation ultimately allows online bank consumers or customers to have access to their information (Kramp & Weigold, 2005). The warranty of integrity and confidentiality in bank server validation is achieved by the Secure Socket Layer (SSL) and Transport Layer Security (TLS) mechanism.

2.4 Attacks on the online banking systems

All online banking authentication methods can be classified according to their resistance to common attacks such as offline credential stealing attacks and online channel-breaking attacks respectively. Offline credential stealing attacks aim to fraudulently gather a user's credentials either by invading an insufficiently protected client Personal Computer via malicious software such as a virus or Trojan horse or by tricking a user into voluntarily revealing his or her credentials via phishing. Online channel-breaking attacks occurs when the intruder unnoticeably intercepts messages between the client PC and the banking server by masquerading as the server to the client and vice versa (Kramp & Weigold, 2005).

2.4.1 Phishing

Phishing is a fraudulent attempt, usually made through email, to steal one's personal information like usernames, passwords, PINs, credit card numbers, bank account numbers and many others. The purpose of obtaining the information is usually to commit identity theft or identity fraud. There several different types of phishing attacks including misleading e-mails, man in the middle, URL obfuscation, page content overriding, malware phishing, key loggers and screen grabbers, session hijackers, web Trojans, IP address manipulation, and system reconfiguration attacks (Williamson, 2006). Phishing has become a big concern of those

involved in Internet security, as it impacts almost all organizations that do business online. Phishing is largely responsible for the disbelief many customers have of online banking.

2.4.2 Data Breaches

Data security is on everyone's mind, from concerned consumers, to privacy groups. Data breaches occurring in large organizations often are highly publicized. The publication of these breaches adds to the uncertainty of many customers in using the Internet. For example a report by ID Analytics, a leader in fraud prevention shows that fifty seven percent of breached identities occurred in the financial services industry (Williamson, 2006). The research also reported that sixty eight percent of breaches are intentional breaches (Williamson, 2006). These kinds of attacks often result in many customers either cancelling their online banking services or new users declining to sign up for the service.

Figure 2.1 below shows findings by the Anti Phishing Group's data presentation on the trends in phishing attacks in the first quarter of 2016.

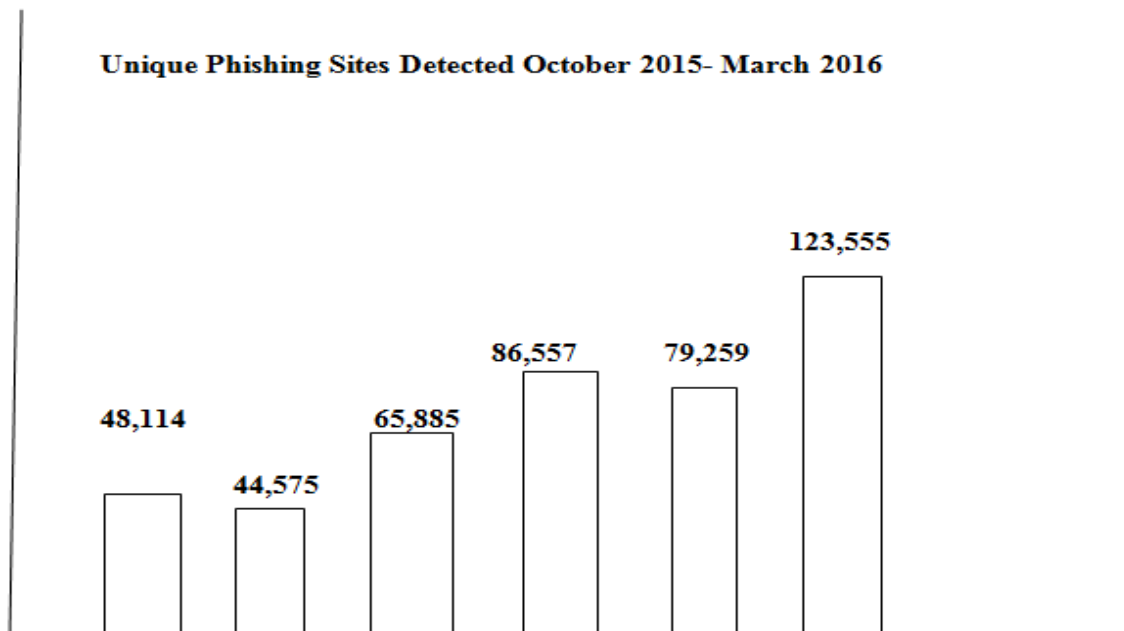


Figure 2.1 Phishing Activity Report 1st Quater 2016(Adapted from APWG Report, 2016)

2.4.3 Risks Driving the Need for Change in online banking authentication methods

The different types of attacks described above have a huge impact on the customer, as well as the Bank. The increased reputation risks and cost pressures on banks, exploit the need for stronger methods of authenticating customers as a way to fight against the attacks. The main risks that banks face are:

- i. **Loss of Consumer Confidence** - the banks' persistent toward online banking can be attributed to the competitive advantage, low cost of the channel, the convenience for the customer, and customer service (Ponemon Institute, 2005). One example of how online banking helps to reduce costs is allowing customers to view statements online, which results in a reduction of postal and paper costs. Therefore, every time an institution becomes a victim of an attack; customers lose confidence in the institutions ability to protect them on the Internet. Customers feel very vulnerable when they receive phishing emails or hear of new breaches. The Bank then suffers a loss of integrity when it becomes victim of an attack; customers wonder if the bank can truly protect their identity, when the bank cannot protect itself.
- ii. **Reputation impact** - once the bank becomes victim to an attack its image is damaged, it begins to lose face among competitors, and its integrity is questioned by both customers and competitors. According to David Jevans, Chairman of the Anti-Phishing Working Group (APWG), brand is everything and there is a lot of brand risk. Fraud is easier to sweep under the rug. It is however, very different when people are getting emails from you. The bank's whole thing is about security. Some banks for example introduced the One Time Password (OTP) to help contain this risk.
- iii. **Financial Impact** - It is estimated that phishing attack can cost a bank huge amounts of money (Williamson, 2006). According to Williamson (2006), some of the costs that are absorbed by banks during and after an attack include response, identification, and clean up. Responding to an attack consists of identifying the course of the email and website and immediately shutting it down. Communications need to be sent immediately to all customers to warn them of the threat and to give instructions on what to do if they have already fallen victim.

2.5 Bank provided Anti-Phishing measures

The risks discussed in section 2.4.3 have put the banks on the spotlight. They have become very active in preventing phishing attacks. The authentication methods presented in the

following sub-sections are among the measures banks have adopted in preventing online banking security attacks, their merits and demerits.

2.5.1 Transaction Authorization Numbers (TANs)

Transaction Authorization Numbers (TANs) are application of one time passwords used by some banks. The customer is issued with a list of multiple passwords, usually this is done via some out of band mechanism like at the bank branch. For every transaction a new TAN is generated sequentially as per the request in order to complete the transaction (Johnson, 2008). Just like other one time password authentication systems, TANs guard against snooping of the credentials on authentic transaction in order to use them later.

2.5.1.1 Demerits of TANs

TANs do not protect against a middle person attack in which the victim is convinced to connect to the attacker instead of the real bank and the transaction challenges and responses are forwarded between the real bank and the user, but transaction details are altered to transfer funds to the attacker instead. Phishing websites also have been able to harvest several codes for later use, without the complexity of a middle person attack (Johnson, 2008).

2.5.2 Secure ID

These are two factor authentication tokens based on the principle of a time-synchronized code encrypted under a key shared between the token and the authenticating server. They come in the following specification;

- i. **Secure ID 200 or 600 or 700** – The Secure ID 200 has a credit card form factor and Secure ID 600 or 700 are key fob designs. The three are otherwise functionally equivalent. They provide an eight digit digital display which recharges every minute. In the current implementation each code is the AES hash of the current time and the device specific key (Bram & Ben, 2001). To log into a server the user must present their password and the current hash value. The authenticating server has the matching key for the token and a synchronized clock so that it can calculate the same hash.

The time dependent part of the credentials is created to prevent copying of the credentials and replay attacks, the physical token prevents the user from giving away their password. The protection is limited to a window of sixty seconds. If the attackers can get a

log in session before the code expires by eavesdropping the log in process then they can use that session.

- ii. **Secure ID 520** – The Secure ID 520 is similar to the Secure ID 200 except that it also includes a PIN pad. The user must enter their PIN before a code is displayed. The resulting code is then a function of the PIN the code and the time. This is additional protection against theft of the token, since stealing the PIN is significantly more difficult than stealing the token or the password. It does not however improve any of the security features like protection against the middle person attack.
- iii. **Secure ID 800** – The Secure ID 800 is a modification to the Secure ID 700 key fob token. It also includes universal serial bus (USB) interface which allows applications to programmatically request authentication codes from the device without the user having to transfer numbers. This is good for convenience, but actually bad for security. The account cannot be accessed without the presence of the token, but if the terminal to which it is connected has been compromised, a malicious program can request any number of authentication codes without the user being aware.
- iv. **Secure ID 990** – The secure ID 990 is another credit card form factor device which in addition to the authentication code in the Secure ID 200 also provides challenge and response functionality via a ten digit PIN pad. The normal Secure ID code is used to log in, but when specific transactions are requested a challenge is presented in the form of a confirmation number which they must enter into the token. The token signs this and displays a response which the user types back into the site to authorize the transaction.

This reduces the available window of attack; a middle person attack cannot make arbitrary numbers of transactions once they have access to a session. However, it does not stop a middle person attack entirely. The attacker can only perform the same number of transactions as the user is trying to make, but any of those transactions can be rewritten by the attacker. The challenge code presented to the user gives no indication as to the nature of the transaction and therefore could be authorizing any transaction, not necessarily the one the user intended to authorize.

2.5.2.1 Demerits of Secure ID solutions

As indicated on section 2.5.2, the use of these time dependent codes have the same middle person vulnerability as TANs. If an attacker can convince the user to connect to their web site

instead of the real one, either through phishing, pharming or Trojans, the user will enter the credentials and the session can be used to carry out other transactions without the knowledge of the user. Additionally, the use of tokens implies that the user carry an additional gadget. The applications also lose synchronization with the bank server hence making their use less effective.

2.5.3 Chip Authentication Protocol

This is one form of multi-factor authentication which derives from the EMV (Chip and PIN) specification and is called chip authentication protocol (Johnson, 2008). The CAP reader is a hand held device very similar to a calculator. It has a slot in the top for inserting a credit card or bank card, a PIN pad and a small display on the front. It uses the feature of the EMV protocol whereby the card will produce the message authentication code (MAC) of data with which it is supplied using the secret key it shares with the bank. There are two primary modes of operation with CAP, generating random OTP and challenge/response.

- i. **Random OTP generation** – This involves the use of the card to generate a random OTP. When performing a transaction the web site will ask the user to generate a code with the reader which they do by inserting their bank card and pressing the new code button. The CAP reader displays the code on the screen and the user transcribes this into the web site and the server checks the validity of the MAC (Johnson, 2008).

- ii. **Challenge Response**

The second mode is a challenge response mode. In this case the user is asked to enter some details from the transaction as part of the challenge. These are then sent to the card which produces the MAC under the key shared with the bank. The user copies the number into the system as before (Johnson, 2008). This type of authentication is important for this paper since the methodology will be based on a challenge response mechanism.

2.5.3.1 Demerits of Chip Authentication Protocol

Random One Time Password (OTP) generation is a weaker form of Secure ID. It is vulnerable to real time and offline middle person attacks because the user cannot know what they are authorizing. In addition, the code is not time dependent, so easily be cached by the attacker for later use. Challenge response on the other hand is an improvement over many of the schemes discussed in this section, but unless the user enters all the details of the transaction, there is still

scope for middle person attack. Additionally, there are many types of transactions which are still vulnerable since the scheme is suitable for setting up mandates (Anderson, 2006).

2.5.4 Smartphone Solutions

Authentication techniques that use smartphone instead of secure signature creation devices are appropriate to customers because they do not have to carry additional device but instead use their smartphone as a second display in order to check the transaction details before confirming them. The smartphone solutions also provide communication channels for the transfer of transaction data to the Smartphone and for the transfer of the signature to the PC or server (Gunther & Borchert, 2013). They include;

- i. **Photo Transaction Authentication Number**-This class of solutions uses 2D codes to conveniently transfer the transaction data to the Smartphone via camera. A Smartphone app then displays the transaction data and computes a signature using a key stored on the Smartphone. The signature is then either sent to the server via mobile Internet or entered manually on the PC browser (Dodson et al. 2010). In some banks where it has been implemented, the server encrypts the transaction and a TAN and the Smartphone decrypts the message and displays both components.
- ii. **Mobile Transaction Authentication Number**- Another well-known solution is mTAN. The customer enters the transaction details in the PC browser and sends them to the server. The server sends the transaction and a TAN to the customer's mobile phone via text/SMS. In order to confirm the transaction, the customer enters the TAN in the PC browser (The H security, 2012)

2.5.4.1 Demerits of Smartphone Solutions

Given the rise of mobile malware, Photo TAN has severe vulnerabilities because none of the basic requirements for secure signature creation is fulfilled. Smartphone malware is possibly able to steal the customers' signature key and send it to any recipient. Moreover it may be able to manipulate the display and the communication with the crypto-module and send signatures to any recipient.

2.6 NFC technology other Communication Devices

Communication between electronic devices can be achieved by the use of Near-field communication (NFC) a new short-range wireless technology developed by Phillips in 2002. It operates as a combination of Radio-Frequency Identification (RFID) and interconnection

technologies that allows devices communicate when in close proximity and a reach of 10cm (Mulevu, 2012).

According to Mulevu (2012), NFC is based on RFID technology and uses the same working principles. It is an interface technology for short range data communication working in the frequency band of 13.56 MHz, standardized in ISO/IEC 18092 and is compatible to ISO/IEC standards 14443 (proximity cards) and 15693 (vicinity cards) and to Sony's Felica contactless smartcard system. Consequently, NFC is able to be used in existing infrastructures based on the aforementioned standards, eliminating the need for separate NFC infrastructure (Onyancha, 2016)

Smart Card Alliance White Paper (2015) states that NFC technology is found in a variety of devices running a number of operating systems (OS) which includes Android, iOS for Apple products, Blackberry and Windows. It is also important to note that NFC is also supported in over 330 phone models, tablets, and other mobile devices, with one billion in market now and over two billion estimated to be in the market by 2017.

Mobile phones have been classified by Mulevu (2012) as regular phones and NFC-enabled Smartphone, whereby regular phones refers to phones that do not have inherent NFC capability but have the basic cellular communication channels(CDMA or GSM) for messaging. NFC – enabled Smartphone on the other hand have in-built readers that are able to capture data from or store data onto external tags. The paper further states that some models of the NFC-enabled phones also have in-built tags that can be used to store user's data, such as phone number. These phones are programmable to support regular cellular communication.

2.6.1 Operating modes of NFC Devices

There are three operating modes of devices as illustrated by Figure 2.3. The first is Reader/Write mode where the NFC –enabled device reads NFC forum mandated tag types. The other is peer-to-peer mode where two NFC-enabled devices are able to exchange information. Lastly, there is the Card Emulation mode where the NFC-enabled device appears to an external reader same as a traditional contactless smart card. This allows contactless transfer and manipulation of data by NFC devices without changing the existing infrastructure. The NFC specifications do not dictate a security approach for any of the three modes. How security is implemented depends on the mode and the app's requirement (Smart card Alliance, 2015).

Table 2.1 NFC Operating modes (Adapted from Smart Card Alliance, 2015)

Operating mode	ISO	Strengths	Future Perspective
Card Emulator Mode	14443	Contactless Payments Data Storing Access Control	Integration of Personal ID cards Storage of sensible data
Reader/Writer Mode	14443 15693	Applicability in many scenarios Marketing opportunity for brands	Allow an higher customization Increase the number of possible scenarios
Peer-to-Peer Mode	18092 21481	Devices connection through physical proximity Quick sharing of data between devices	Secure share of confidential/private information

2.6.2 NFC Protocol

NFC has published technical specifications concerning the data exchange format, data types, data exchange protocol, link protocol and NFC tag operations. The following is a description of the most important specifications provided by NFC Forum;

a) NFC Data Exchange Format (NDEF)

NFC Data Exchange Format (NDEF) is a specification of the format in which data is exchanged by NFC Forum devices. This format is built upon messages which encapsulate one or more records that contain a payload described by a type, length and optionally an identifier. Supported forms for the record type field are NFC Forum well-known types, NFC Forum external types, absolute URIs and MIME media type constructs. NDEF also specifies a mechanism to build unique NDEF record type names (Kilani & Jensen, 2013).

b) Simple Data Exchange Format Protocol (SNEP)

Simple NDEF Exchange Protocol (SNEP) is an application level communication protocol which specifies how two NFC devices should send and receive NDEF messages. SNEP is a

request/response protocol, the client sends request messages and the server answers with response messages. In the NFC Forum architecture, SNEP is located on top of the Logical Link Control Protocol (LLCP) in the protocol stack (Kilani & Jensen, 2013).

c) Logical link control protocol (LLCP)

Logical link control protocol (LLCP) is responsible for the upper half of the Data Link layer in the well-known Open System Interconnection (OSI) model. The Media Access Control (MAC) is responsible for the lower half of the Data Link layer accessed by the LLCP by a set of mapping specifying the binding requirements. One of the main features of LLCP is Link Activation, Management and Deactivation which specifies how two NFC Forum devices recognize compatible LLCP implementations, establish a link, manage and deactivates it. LLCP also provides the Asynchronous Balanced Communication which offers a communication protocol separate from Normal Response Mode. Asynchronous Balanced Mode (ABM) liberates peers from being bound to a master/slave relation where the initiator only is allowed to send data as a response to a request from the Target. In ABM both peers may send information at any time. LLCP facilitates both connectionless and connection-oriented transport (Kilani & Jensen, 2013).

2.6.3 NFC Security

NFC benefits highly from its low range when it comes to security against attacks such as eavesdropping. The mode in which the peers communicate is also a vital factor in the likelihood of an eavesdropping attack. Two peers communicating in Active mode are vulnerable to eavesdrop at a larger range than if Passive mode was used. In the article by Kilani and Jensen (2013), the rough estimate given regarding the possible range in which a eavesdrop attack can occur is up to ten meters when transmitting in active mode and one meter when in passive mode.

A Man in the Middle (MITM) attack against NFC is not practically feasible because one cannot send data to the attacked parties individually without the other party also hearing the received data. When the attacker has intercepted and blocked a message from A to B and then starts sending a new packet to B, A will receive the message and recognize the problem protocol. The blocking of the first message from A to B could also be detected by A which, if A is listening while sending, it would make A to stop the protocol (Haselsteiner & Breitfub, 2006).

2.6.4 Industry-wide application of NFC technology

Studies have shown that NFC technology permeates various sectors of society and its industry-wide reach is wide. This technology is used for a number of purposes which includes storage of tickets that open transportation gates, sharing of business cards, and storage of loyalty program information. Additionally, NFC has been used to transfer pictures to a printer which is NFC-enabled monitor or printer. Others applications includes making payments through tapping of phone on a contactless card reader. (Smart card Alliance, 2015)

2.6.5 How NFC compares with other communication modalities

a) NFC compared to Barcode

Whereas barcode application need consistent power, NFC do not necessary require power to operate. Another differentiating factor between NFC and barcode is that NFC incorporates RFID technology and in this case data moves from a passive tag to an NFC-enabled device via radio waves. It has been pointed out that one of the major advantage of the RFID tag reader can be able to operate at a relatively large distance from the tag and this can even occur when the reader cannot be seen(Onyancha, 2016)

b) NFC compared to QR Code

Onyancha (2016) argues that much as QR codes provide an efficient information storage and retrieval, they cannot be relied upon because they have a propensity to being damaged which leads to their inoperability. On the other hand, NFC optimizes ease of use as information is transferred when the NFC tag is brought closer to the NFC-enabled phone. Further, there are two things that are essential for data transfer to occur and the first is pre-processing. The second is an active application. It is imperative to note that once QR codes are printed, they cannot be modified. This sharply differs with NFC tags whereby the information that is written on it can be changed.

c) Bluetooth

The Bluetooth technology is a short range wireless communication technology which is designed to replace cable between electronic devices. The difference with the NFC is that for two devices to communicate through Bluetooth, they must first be paired. This procedure is cumbersome and the connections are vulnerable to eavesdropping and Man-In-The-Middle attacks (Onyancha, 2016).

2.6.6 Incorporation of NFC in mobile phones

Onyancha (2016) asserts that numerous mobile phones are being produced by phone manufacturing companies and there is a general increase in this production. The banking sector can leverage on this direction NFC is taking by incorporating NFC technology in its operations. Online banking is a key area where when NFC technology is applied, as will be seen in subsequent chapters, there's a benefit.

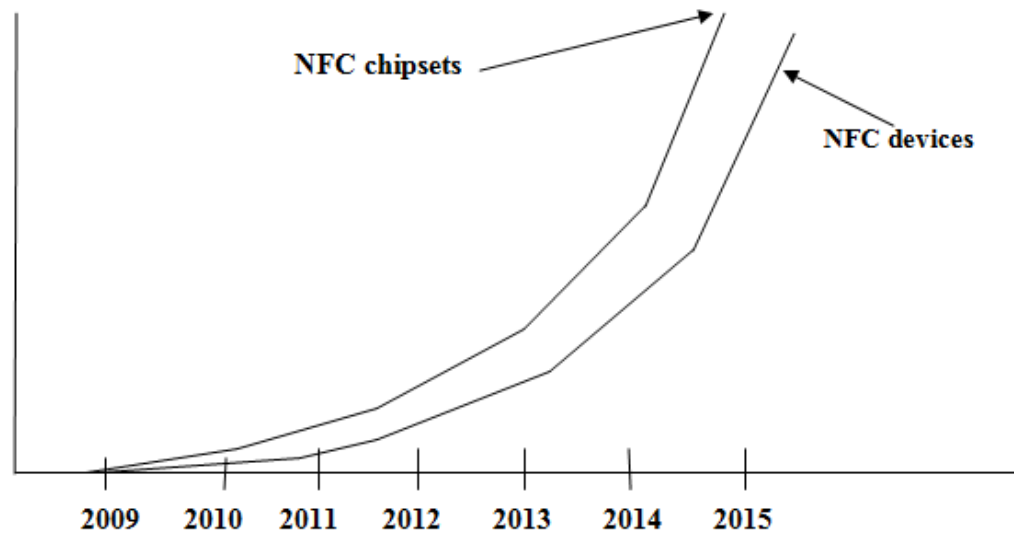


Figure 2.2 Total NFC-Enabled Device and Chipset Shipment (2009-2015) (Adapted from Onyancha, 2016)

Figure 2.2 illustrates the total number of NFC-based devices and chip shipment and the projections from 200-2015. This illustration shows an exponential increase in NFC shipment and hence adoption.

Clark (2014), as illustrated on Figure 2.3 shows an increase in mobile phone shipment. This confirms the findings of Onyancha (2016)

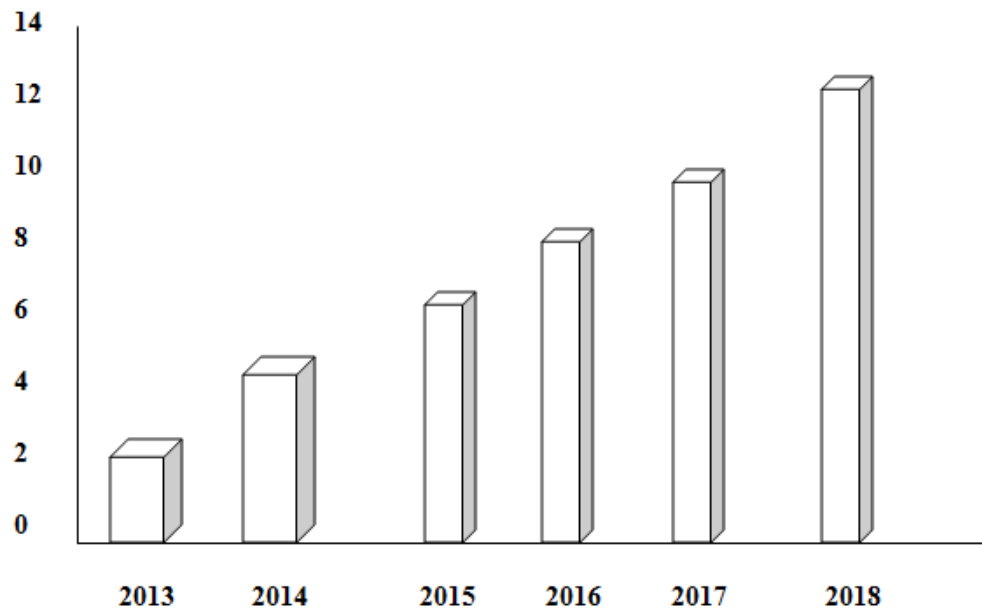


Figure 2.3 NFC enabled mobile phone shipped (Adapted from Clark, 2014)

2.7 Debit Card Architecture

Debit cards or general bank cards, are bank issued smartcards that host an array of different applications. NFC model described in this paper will utilize the bank cards ability to compute a signature as a function of a given challenge and a secret stored on the card. The inter-operation of terminal and card for this functionality is specified by Euro pay MasterCard and Visa (EMV), a generic industry standard based on ISO7816 contact and ISO14443-contactless (Gunther & Borchert, 2013).

On the basis of EMV, card issuers developed standards for applications like Automated Teller Machine (ATM), Point of Sale (POS), and online banking with MasterCard CAP being a noticeable example. The German banking industry committee *Central Credit Committee* developed the standard HHD (hand held device) which is used for online banking transactions (Zentraler, 2010). As the EMV protocol has no notion of transaction details like beneficiary's account number and amount, HHD specifies how reader devices aggregate those details into a challenge for the smartcard. The abovementioned chipTAN solution is one implementation of HHD, where the transaction is transmitted to the TAN Generator, which aggregates the transaction and hands it over to the plugged in bank card.

The implementation of the NFC model will be based on the HHD specification. Consequently, the Smartphone app of NFC model will contain a software implementation of the TAN Generator. NFC model will therefore be compatible with the chipTAN solution but adaptable to many solutions using EMV based or other specifications since the only strong requirement towards the smartcard is the ability to compute a response for challenge using a stored secret.

2.8 Conceptual Framework

The model described in this paper will adopt the methodology of challenge response as illustrated in Figure 2.4.

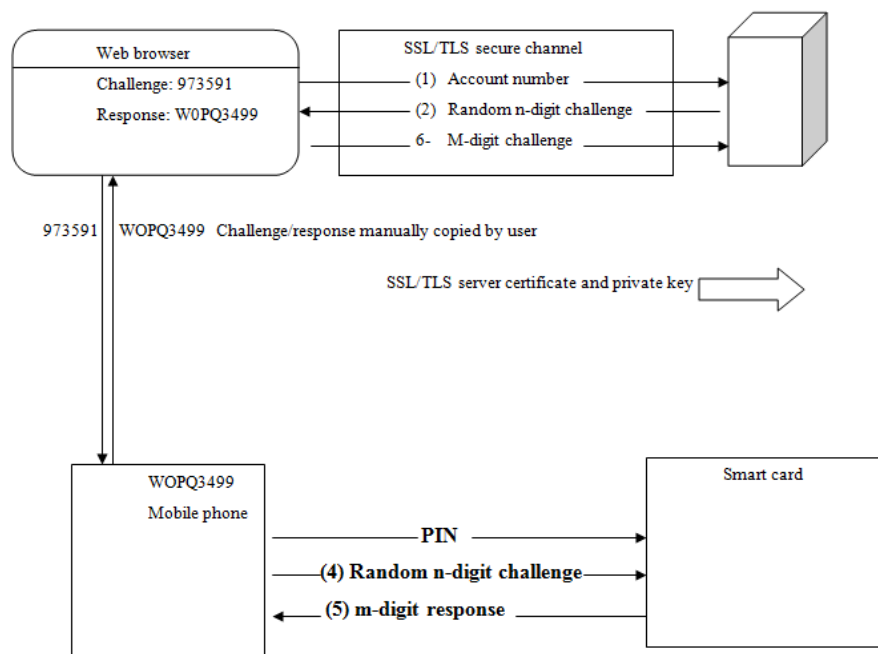


Figure 2.4 Challenge response authentication method (Adapted from Kramp & Weigold, 2006)

- i. The consumer links to the online banking server via Secure Socket Layer or Transport Layer Security with server side authentication. The user is guaranteed connection with the real banking server by clearly authenticating the server credential.
- ii. The consumer claims his or her self by entering a user name in the bank's login form. The banking server presents a k-digit challenge and asks for a corresponding l-digit reply.
- iii. The consumer opens his or her smart card by inputting the equivalent code in the reader before inputting the displayed challenge. The matching response is calculated by the

smartcard by translating the challenge and the given on card login counter with its symmetric cryptographic key, lastly it encrypts the outcome as a suitably presentable reply string.

- iv. The consumer manually replicates the given response to the bank's login form to be checked by the bank's verification server, which repeats the same calculation independently. Because the login counters on the smart card and the server can diverge (if a user playfully calculates a response, for example), the server tries to securely synchronize its local counter within a small range of counter values.

Chapter 3: Research Methodology

3.1 Introduction

This Research Methodology chapter explores the area of study, data collection tools, research design and population sampling. Additionally, this chapter covers the methodology and how the model was designed and developed and the eligibility criteria of the participants for this research. It also covers the methods of data presentation and analysis, validity and reliability and ethical considerations for the research.

3.2 Study Area

Most Kenyan Banks have embraced the use of alternative channels of banking. However, NIC Bank Limited has been selected by the researcher as the representation of all the banks. The Bank has a broad network of Branches spread out across the country ranging from Nairobi, Mombasa, Kisumu, Nakuru, Eldoret, Meru and Thika. The researcher believes that with this, a good representation of Kenyans who seek banking services was catered for.

The development of the system is tailor- made to suit the technological advancement in the bank's online system. The bank account data such as usernames and bank cards to be input into the database will be collected from the selected staff members and bank customers using the data collection instruments outlined in section 3.6.

3.3 Research Design

This was an applied research because it is aimed at finding a solution to alternative transaction authorization method for online banking. A model was then created and as an applied concept which addresses issues of online identity theft and reputational risk for the bank.

The application of this research is in the banking sector which involves customers authenticating themselves and approving transactions before the bank can process the requested transaction. The researcher collected both qualitative and quantitative data and presented the quantitative data in bar graphs and pie charts. Onyancha (2016) asserts that qualitative methods of research is related to the study of things in their natural setting and interpret the phenomenon in terms of what meaning people brings to them. Qualitative was achieved by carrying out interviews on the bank employees who interact with the system as well as select customers who are currently enrolled for online banking.

3.4 Population and Sample Size determination

The population that was requested to offer data relevant for the study was the NIC bank's staff and customers who visited the Prestige branch and those stationed at IT department. The relevance of the population was the system and the model developed depended on the interaction of the three sets of the population, that is, branch staff, customers and IT staff. Onyancha (2016) described an NFC model for Health Information Portability and argued that during the development of the model, the study of population was important because the model depended on the interaction between doctors and patients. In the same breath, the population in the context of online banking was studied and the model developed was based on how the bank customers, the branch staff and the IT staff interacted.

Purposive sampling for both bank customers and bank employees was done because of the heterogeneous nature of the population. In other words, the population consisted of people from different socio-economic backgrounds, tribes, gender, technological knowhow and knowledge and perceptions of NFC technology and online banking. It was noted that the customers who visited the Prestige branch also visited other bank branches and are not always at the branch, hence distributing questionnaires could cause a challenge hence the rationale for purposive sample. The bank customers and employees of Prestige Bank branch were provided with questionnaires and their views were captured as shown in the Appendices section.

3.4.1 Sample Size Calculation and eligibility criteria

Equation 3.1 shows the equation that the researcher used for the calculation of the sample size for the online banking users.

$$n = z^2 pq / c^2$$

Equation 3.1 Sample size calculation for Online banking users (Onyancha, 2016)

Where:

n=sample size

z=the standard normal deviation (1.96 for a 95% confidence level)

c=level of accuracy desired, or sampling error

p=proportion of the population having the characteristic being measured

q =proportion of the population that does not have the characteristics $(1-p)$

Thirty (30) online banking customers selected through convenient sampling and also a total of twenty (20) bank employees were selected. A sample has been described as a subset of population selected to participate in a research study and it further defines the selected groups of elements, that is, individuals, groups or organizations. The sample is chosen from the study population that is commonly referred to as the 'target population or accessible population' (Burns & Grove 2003). In this study, the sample consisted of NIC bank customers and employees who interact with the system.

The participants that were chosen met the eligibility criteria set for the study. Burns and Grove (2003) points out that the eligibility criteria are the reason or criteria for including the sample in the study and this criteria of the study require that:

- i. The Bank customer who is registered for online banking
- ii. The bank employee who deal with customer issues in regard to online banking
- iii. The bank employee who is responsible for the security of the online system
- iv. The bank employee who is directly involved with the online banking system design and implementation

3.5 Data sources and respondents

Data sources can be classified into primary and secondary data sources. The primary data sources include questionnaires and observations while the secondary sources of data include review of journals, scientific papers, books and magazines (Onyango, 2014). Respondents who are the data sources included bank customers and bank employees based at the Prestige branch and IT department.

The relevant data that included names of users, authorization problems with the transaction authorization, data on NFC and other mobile applications in use for online banking, and recommendations on the NFC-enabled methods.

3.6 Data Collection methods

Burns and Grove (2003) mentions that gathering of data is a precise, systematic collection of information that is relevant to the research sub-populations using methods such as narratives, interviews and focus group discussion. The main techniques that were employed in this research study included semi-structured interviews, questionnaires, and participant observation. The researcher was the main research tool or primary instrument and the data collection was reflective because the aim was to give the participants the opportunity to reflectively express their experience.

The tools used for data collection were questionnaires and interviews for the primary data. For online banking customers, structured questionnaire was used and the purpose for this was to study the user's interaction with the system, level of confidence in regards to online security, user friendliness and views on the various gaps and strengths of the existing authentication technique.

3.7 System Design, Development and Methodology

Systems Development Life Cycle (SDLC) Phases follows the sequence of Planning, analysis, design and implementation. The steps involved are as follows: the planning phase involving the analysis of feasibility of the system and development of a work plan, analysis phase involves development of the analysis strategy and creation of use cases and model processes. The design phase involves designing of the physical system which includes designing the interface, architecture and databases. Lastly, implementation involves construction, installation and maintenance of the system and post implementation. (Dennis, Wixom & Roth, 2012). The development of this model followed the steps as outlined earlier.

The model development followed the software development process as illustrated in Figure 3.1. The process involved the analysis of system requirements through use cases, the design structure through class diagrams and Entity relations and implementation through programming. Lastly, validation and verification performed through unit testing (Onyancha, 2016).

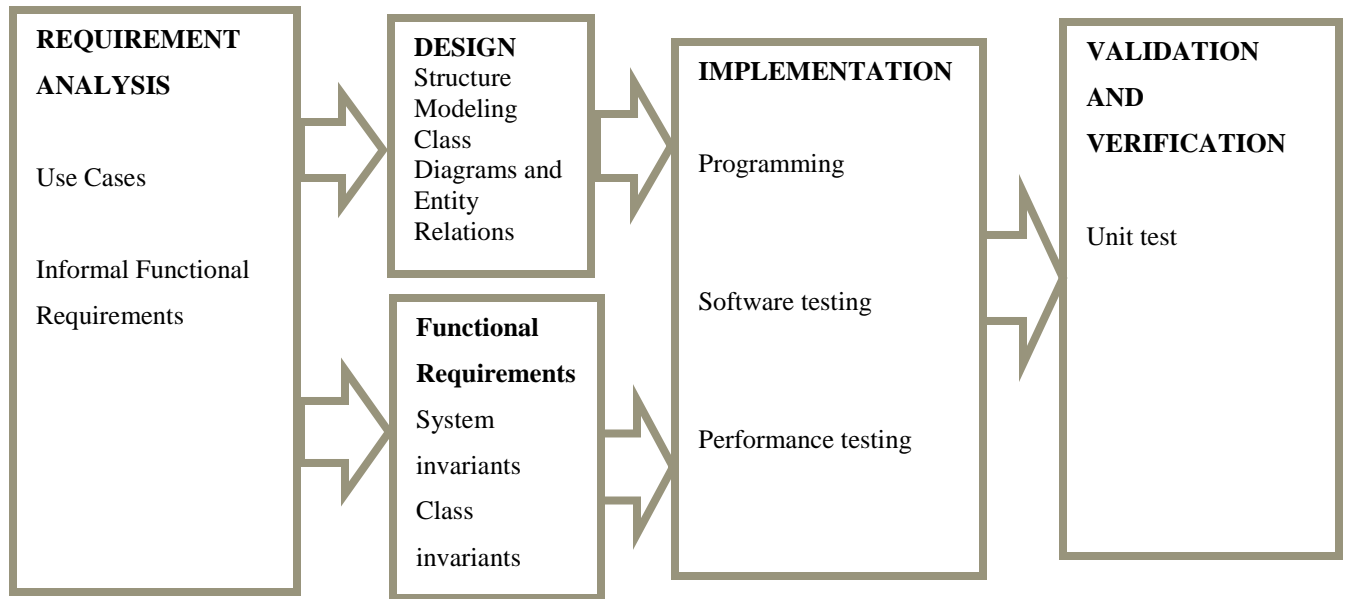


Figure 3.1 Software Development Process (Adapted from Onyancha, 2016)

According to Onyancha (2016) and Dennis et al. (2012), the various methods of project methodology include agile development, parallel development, V- model, Rapid development and iterative development. The agile development is further classified into scrum, extreme programming and dynamic systems. This research employed agile development as illustrated on Figure 3.1. Onyancha (2016) argues that agile development, defined as a collection of programming-centric methodologies that geared towards streamlining Systems Development Life Cycle, puts more emphasis on simple, iterative application development whereby every iteration as a fully fledged software project. This process moves from planning, requirements analysis, design, coding, testing to documentation.

The other rationale for usage of agile development is that it is applied when user requirements are unclear, developing systems that are reliable and systems that have a short time schedule. The disadvantage of this methodology, according to Dennis et al. (2012) is that it is poor in developing systems with unfamiliar technology and the ones that are complex.

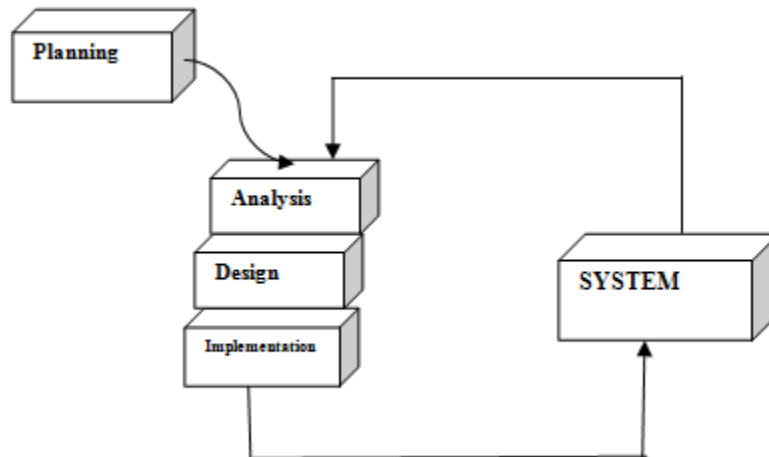


Figure 3.2 Agile Development Methodology (Adapted from Dennis et al., 2012)

3.8 Data Analysis and Presentation

According to Onyancha (2016), data analysis is processing and analyzing using both descriptive and inferential statistical data by employing SPSS and MS Excel. Data can be presented in graphs, tabular form and percentage and the key reason why this analysis is done is that one can draw conclusions from the data analyzed. The data collected in this research was presented in graphs, column charts, pie charts using Microsoft Excel software.

3.9 Validity and reliability of the research

The reliability was done using re-tests to measure the consistency of the results of data input, data output and modification of the customer's transactions from the bank server and on the other hand the validity of the research was achieved using content validity method whereby the online banking users were asked to identify the content of the prototype developed and verify its authenticity. Validation was also done by the bank's System administrator who had vast experience in information systems design and implementation. Further, validation included validation of the technology used and its suitability and relevance and as Onyancha (2016) argues, it is important to carry out this validation as it meant to ensure that the model developed met the requirements needed technically and financially.

3.10 Ethics in Research

According to Silverman (2000), researchers should always remember that while doing the research, they are entering the private spaces of their participants. Creswell in (Silverman, 2000)

states that the researcher has an obligation to respect the rights, needs values and desires of the informants. The relationship between the researcher and the subject during an interview needs to be considered in terms of the values of the researcher and cultural aspects Silverman (2000).

Therefore, appropriate steps were taken to adhere to strict ethical guidelines in order to uphold participant's privacy, confidentiality, dignity, rights, and anonymity. The following section describes how ethical issues in the conduct of research were addressed:

- a) **Informed consent** -The researcher informed the participants- the bank, bank employees and customers- of the purpose, nature, data collection methods, and extent of the research prior to commencement.
- b) **Harm and risk** - In this research study, participants were guaranteed of their safety. In other words, the researcher did not put them in a situation that they were subject to danger as a result of their participation, physical or psychological.
- c) **Honesty and trust** - Adhering strictly to all the ethical guidelines serves as standards about the honesty and trustworthiness of the data collected and the accompanying data analysis.
- d) **Voluntary participation** - The participants were reassured that this study is only for academic purpose and their participation in it was absolutely voluntary. No one was forced to participate.

Chapter 4: System Design and Architecture

4.1 Introduction

This chapter will highlight the research findings and use pie charts and bar graphs to present the data that was collected. A brief explanation on each result is provided but a comprehensive discussion follows immediately after. The data collected was aimed at studying authentication and NFC with respect to online banking. The presentation and analysis of the data was divided into bank employee's data and bank customer's related data, and also data that is specific to authentication and the one specific to NFC usage in smartphones. The total number of respondents included thirty bank customers and twenty bank employees.

4.2 Data Results, Presentation and Analysis

i. Bank employees personal profile

a) Gender

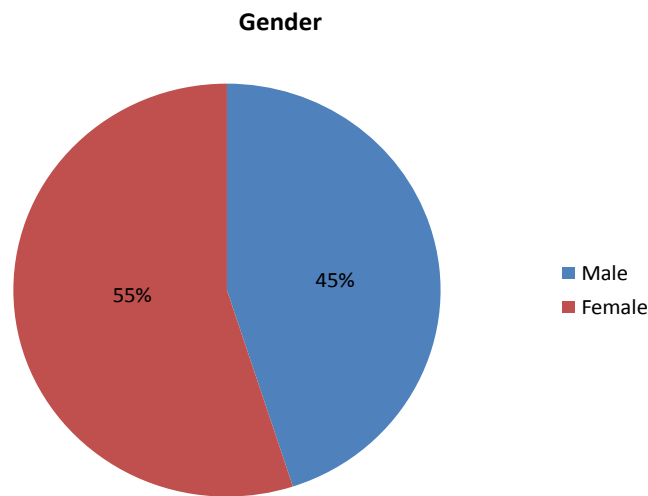


Figure 4.1 Gender of Employees

Figure 4.1 showed that there were more females (55%) than male bank employees (45%). Even though it is not the premise of this research to study gender differences in relation to online banking, it can be concluded that there is no statistical significance between male and female respondents.

b) Which department of the bank do you work?

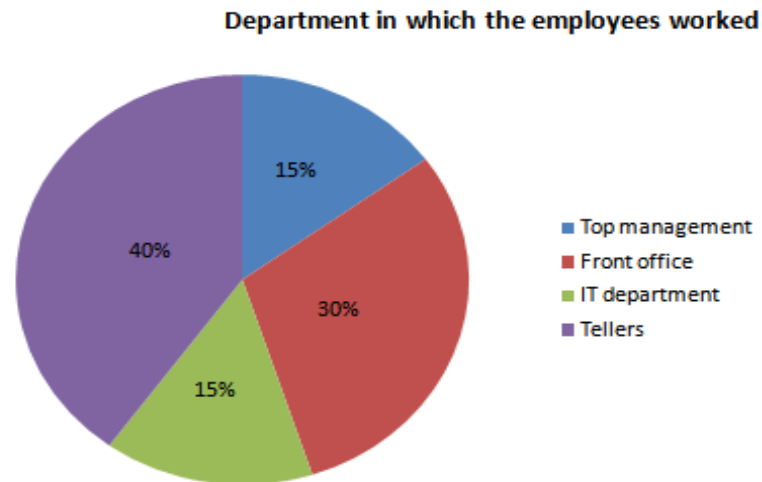


Figure 4.2 Department in which the employees worked

Both top level management and IT department recorded 15% of the representation and tellers who were the bulk of the respondents recorded 40%. Lastly, front office employees had a 30% representation. The relevance of this question was to find out which department in the bank had more influence on the customers in terms of sensitization of online banking. Since tellers (40%) and front office employees (30%) recorded the highest percentage of bank representation, the conclusion is that they are better placed to encourage customers to adopt this technology.

ii. Online banking

a) Utilization of online banking services

Figure 4.3 showed that the majority of bank employees (88%) were subscribers of online banking services which was an indication of their willingness to embrace this technology partly because of awareness. It should be noted that online banking in this regard also touches on those customers who didn't have smartphones but were able to access

banking services through their mobile phones through SMS and functionalities that doesn't require internet connection.

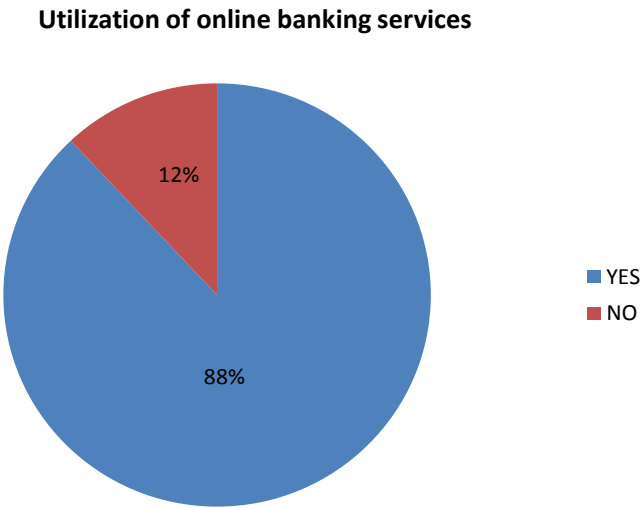


Figure 4.3 Utilization of online banking services

b) Do you inform your customers about online banking when they visit the bank?

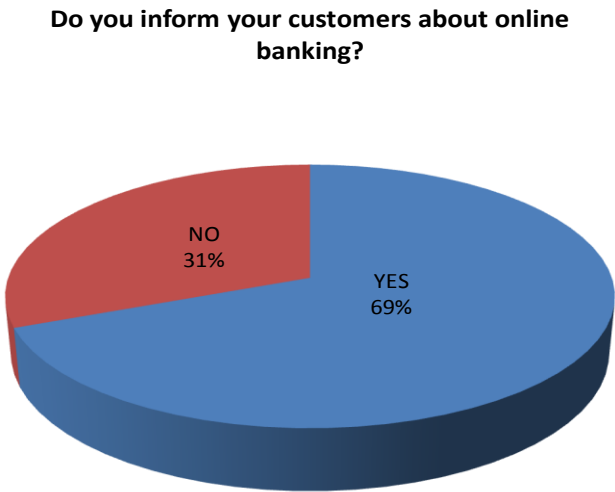


Figure 4.4 Data about bank employees informing their customers about online banking

Sixty nine percent (69%) of the bank employees said that they give information on online banking to their customers which is illustrated on Figure 4.4. This question sought to study the bank employees' attitude and willingness to inform their customers about online banking because this is crucial in ensuring that the customers are well informed about this technology. This research acknowledges that since there exists a digital divide among customers and the customers may vary in their attitudes towards online banking, there will be easily and late adopters of this technology.

c) Online banking is beneficial to bank customers

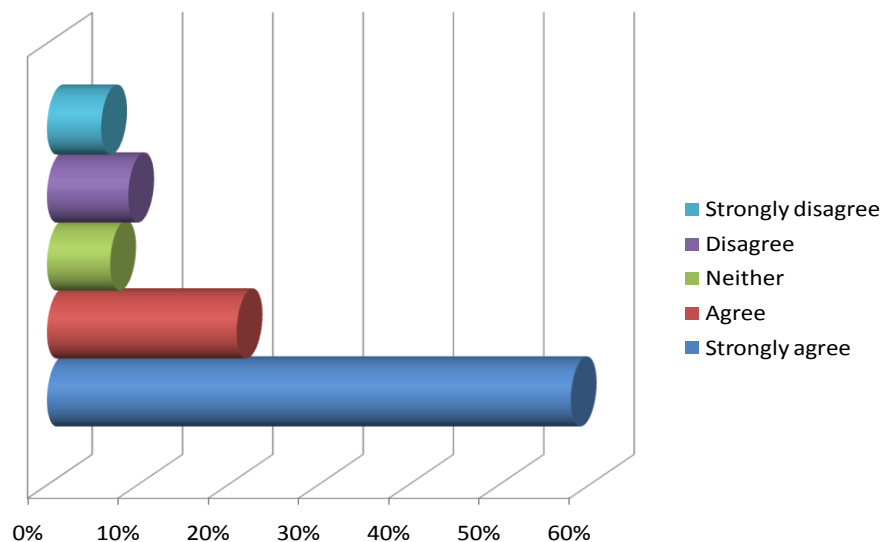


Figure 4.5 Likert scale on whether online banking is beneficial to customers

As shown in Figure 4.5, majority of the bank employees strongly agreed that online banking was beneficial to their customers. This section sought to study the effects of the information that the bank employees gave to their employees and since the majority of the employees responded that they strongly agreed that online banking has benefits to the employees, it can be projected that more customers will adopt this technology in the future and therefore need for a robust authentication mechanism.

iii. NFC function on Mobile Phone

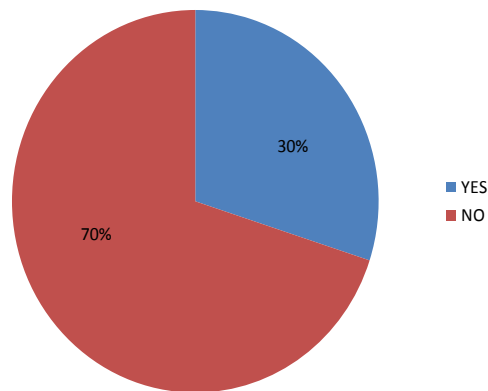


Figure 4.6 NFC Function on Mobile Phone

Only thirty percent (30%) of the bank employees were aware of the NFC functionality on their mobile phones compared the majority (seventy percent) who were not aware as represented on Figure 4.6. this question was aimed at studying the awareness of NFC technology in mobile phones and as illustrated, majority of the bank employees did not know of the existence of NFC functionality on their mobile phones. As such, it posed a challenge to this research because banking employees are an important part of the adoption of this model since they are required to give information to customers on the NFC usage.

iv. Importance of NFC in the banking industry

A question was posed to the respondents “Do you agree (or disagree) that this technology is revolutionizing banking industry and how customers and banks interact?” and as Figure 4.7 shows, sixty percent (60%) of the respondents strongly agreed, twenty eight percent (28%) agreed, two percent (2%) chose neither, and the respondents who disagreed and strongly disagreed both had five percent (5%). This question targeted the bank employees and it sought to study the general view of the employee’s understanding of how wide or narrow the NFC technology has permeated the banking industry

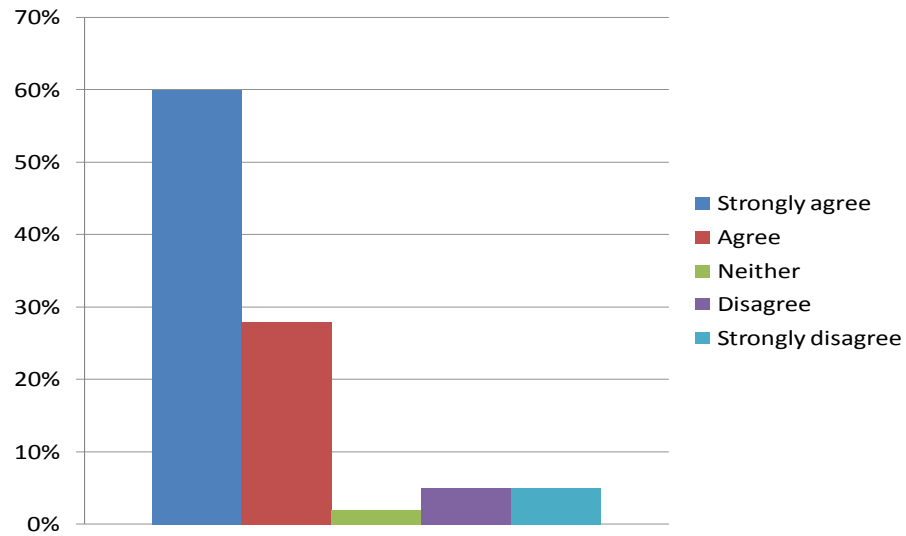


Figure 4.7 Importance of NFC in the banking industry

a) Bank customers

i. Gender

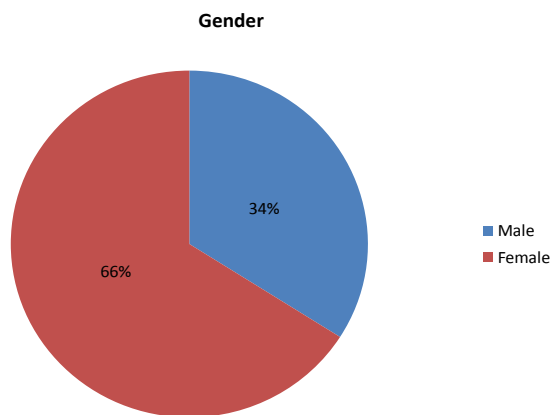


Figure 4.8 Gender distribution

Figure 4.8 shows that there were more females respondents at sixty six percent (66%) than male respondents at thirty four percent (34%) in the gender distribution

ii. Age distribution

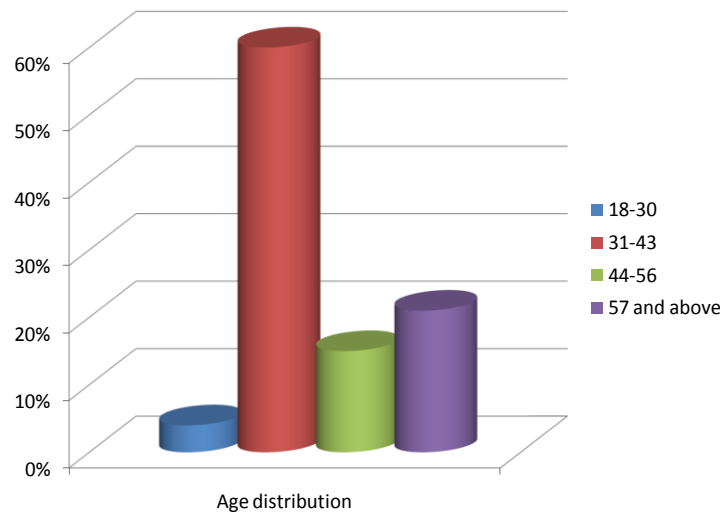


Figure 4.9 Age Distribution among Customer Respondents

As illustrated on Figure 4.9, majority of the customers fifty eight percent (58%) belonged to the 31-43 age group. The age bracket that had least representation was 18-30. Stratifying the ages of the customers was crucial because it gave an insight into how different age groups respond to NFC and online banking technology. This is crucial in how the bank can strategize on how to market this technology to its customers.

iii. Access to online banking services

Fifty five percent (55%) of the customers, as shown on Figure 4.10, said they had access to online banking as compared to 45% who had no access to this banking service. Even though the disparity between these two groups was not very large, the number of those who had access to online banking was significant because it shows that customers must be given proper information on authentication mechanisms.

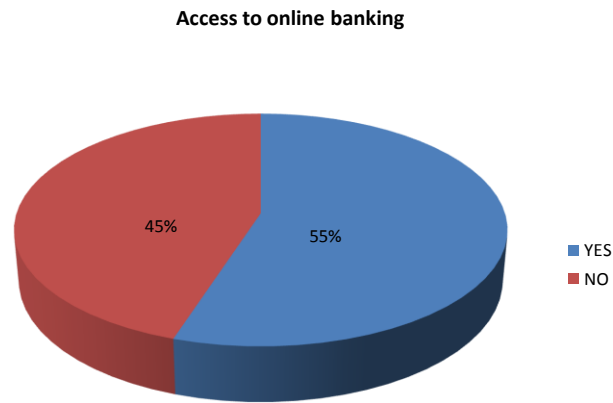


Figure 4.10 Access to Online Banking

iv. Mode of accessing online banking services

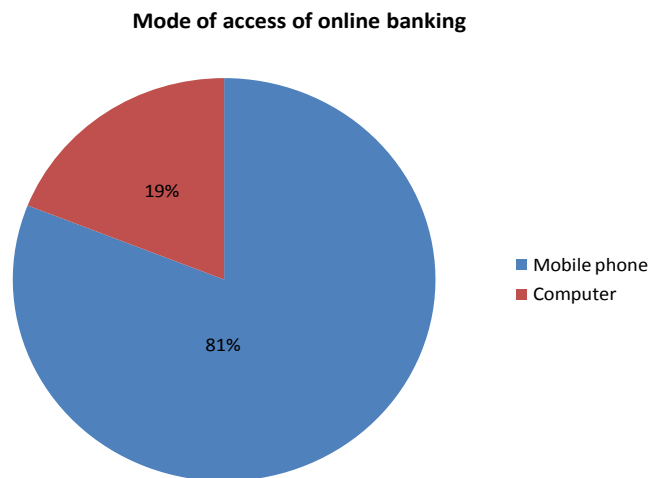


Figure 4.11 Mode of access to online banking

As illustrated on Figure 4.11, 81% of the respondents said they access their bank information and transact via their mobile phones. Only 19% have access to online banking via the PC. This brings a major focus on security on mobile devices as far as online banking is concerned.

v. Is online banking service beneficial to customer?

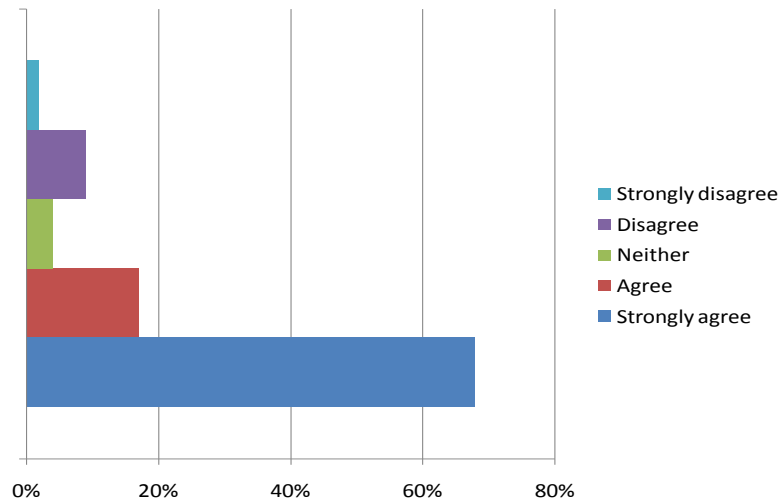


Figure 4.12 Likert scale on benefits of online banking

One of the pertinent question asked on the questionnaire was “If your answer on (ii) above is YES, is the service beneficial to you?” this question sought to investigate if online banking was beneficial to the customer. A majority of the respondents at sixty eight percent (68%) strongly agreed as shown on Figure 4.12. The conclusion is since a large number of the respondents said they strongly agreed that online banking is beneficial to them, it will be prudent to address the issue of how well to protect themselves from intrusion attacks and impersonation.

vi. Responses for those who do not have access to online banking services

Figure 4.13 illustrates the responses by the customers who didn’t subscribe to online banking services and as shown, the majority of the respondents indicated that online banking was too complex (65%), Fifteen percent (15%) said they preferred to personally go to the bank while five percent (5%) had no access to the internet. In this section, the researcher sought to study the various reasons why the respondents didn’t utilize online banking because this question had a direct impact on the adoption of this technology. Since the majority of the respondents reported that they found online banking too complex, there was a need for a simpler technology that not only ensures that users are able to access banking services but a technology that had security features to protect customer’s identity and banking information.

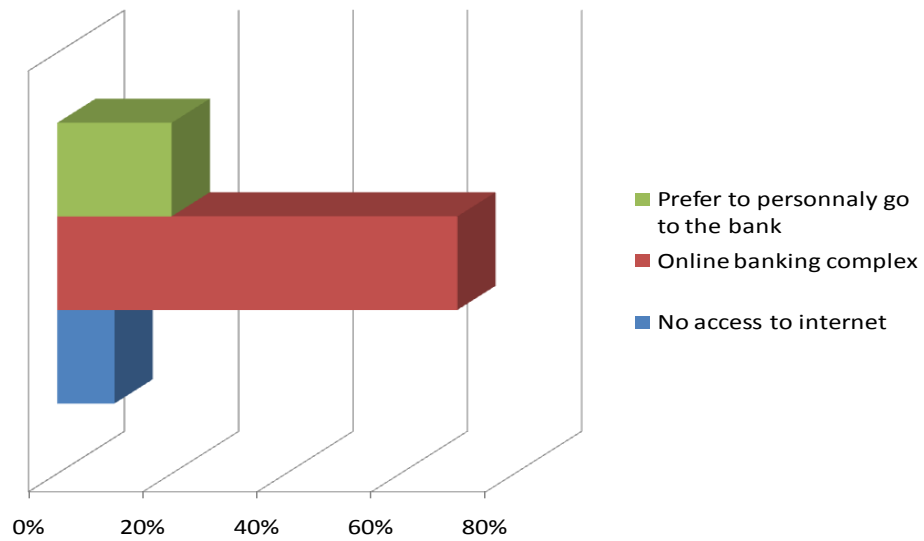


Figure 4.13 Responses for those who do not have access to online banking service

a. Authentication issues

i. Sharing of password or PIN

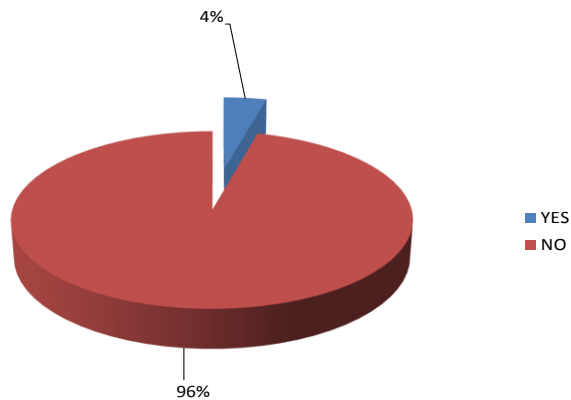


Figure 4.14 responses on whether the customer shared their password or PIN

A majority of respondents (96%) reported that they do not share their password or PIN to anyone as compared to only four percent 4% who reported that they shared their password. This

question was an important question with respect to this research because it sought to study the issue how wide or narrow the issue of sharing password is and how it affected online banking. This is statistically significant because this research is focused on authentication as login credentials is a crucial factor in online banking.

ii. Do you feel that the bank shares your login credentials with a third party?

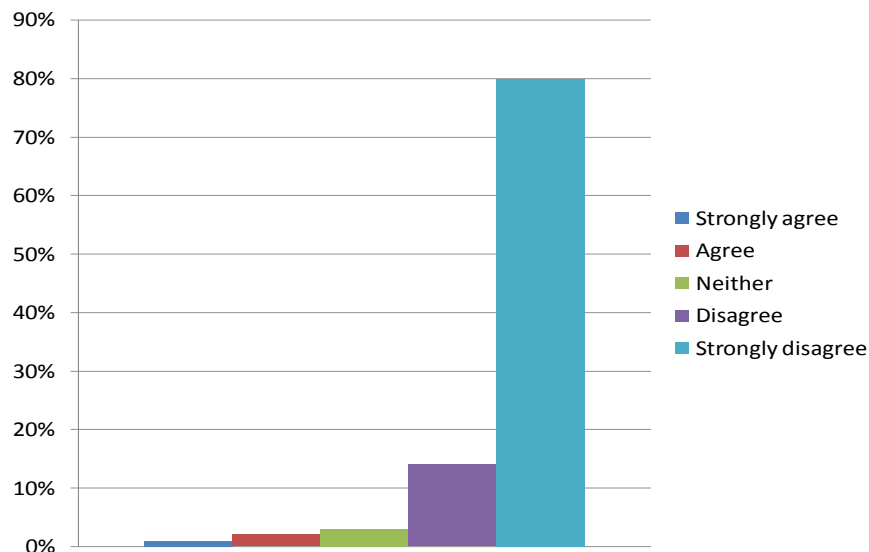


Figure 4.15 Responses on whether Customers felt that the Bank shares their Login Credentials

As illustrated on Figure 4.15, majority of the bank customers strongly disagreed that bank shared their login credentials when asked the question “Do you feel that the bank shares your login credentials with a third party?” Respondents had full confidence in the bank’s ability not to share their personal bank details. For online banking to succeed, customer must be assured that their bank information is secure.

b. NFC functionality

i. Do you have a smart phone?

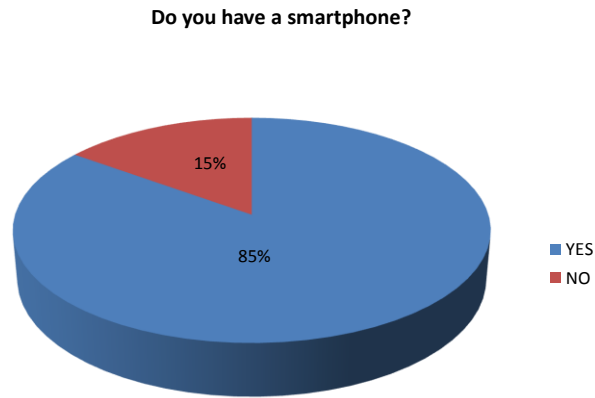


Figure 4.16 responses on ownership of smartphones

This question was aimed at studying the level of permeation of smartphones and 85% of the respondents reported that they had smartphones as compared to 15 % who said they didn't own a smartphone as shown in Figure 4.16. This is significant because only smartphone have NFC capability.

ii. Responses on whether the customers were aware of NFC functionality on their smartphone

For the respondents who reported that they had smartphones, another question was posed and it dwelled on whether these bank customers were aware of the NFC functionality. The illustration on Figure 4.17 shows that an overwhelming majority (78%) were not aware of the NFC functionality on their phone.

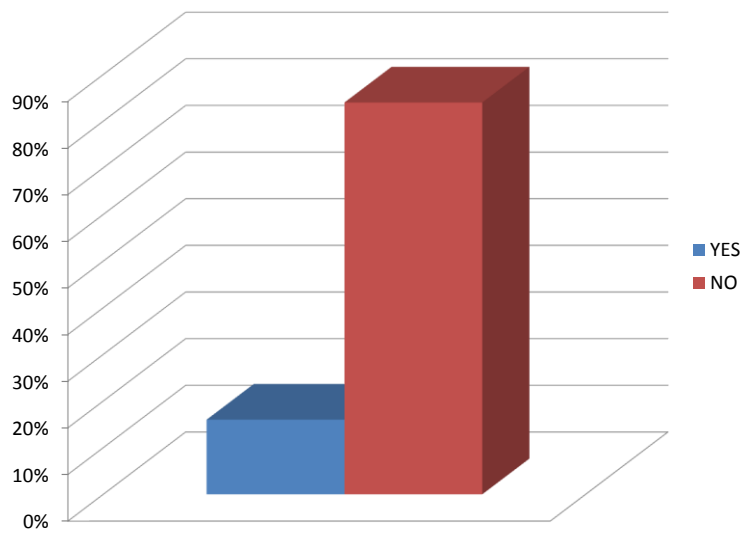


Figure 4.17 Responses on NFC functionality on mobile phones

4.3 System Design and Architecture

4.3.1 Introduction

As explained in the research methodology section of this research, the applied research method, problem on the real world is identified and then a proposal of the solution made (Mwenda, 2016). The literature review section of this research clearly outlines the major problems of user authentication in online banking. This section explores the various steps in the development of the model.

4.3.2 Analysis of the System

As illustrated in Research Methodology Chapter in this paper, Systems Development Life Cycle (SDLC) phases according to Dennis, Wixom and Roth (2012) follows the sequence of Planning, analysis, design and implementation. This is the standard process used by an organization to conduct all the stages required to analyze, design and maintain information systems, also referred to as system development methodology. The methodology used in this paper to execute the five stages is the agile development methodology as shown in Chapter 3.

4.3.3 System Initiation and Planning

Roth et al. (2013) points out that system initiation and planning, the factors that are considered are identification and documentation of the purpose, cost, scope and economic value of the perceived system.

Mwenda (2016) argues that in this stage, the purpose, scope, cost and the economic value of the perceived system are identified and documented. In the Literature review section in this research, it has been demonstrated that NFC Technology is a very secure authentication method because of its peer-to-peer operation mode. Further as outlined, the numerous online banking obstacles that exist have been discussed. Consequently, the model developed was based on the proposed application for addressing these obstacles alongside the risks driving the need for change as outline in the Literature review section of this research.

4.3.4 Analysis Phase

A study by Mwenda (2016) posts that the analysis phase is one of the most critical stages of SDLC. In this second stage, functional and non-functional requirements of the new system are determined and documented. Mwenda (2016) further outlines the main steps that an actual systems analysis entails three key steps- (a) understanding the existing system, (b) identification of improvements and (c) defining the requirements for the new system.

It should be noted that Chapter 3 addressed issues regarding understanding the existing system and ways of improving the system. The premise for this section is to explore the various system requirements. For user requirements to be elicited, the techniques available includes interviews, document analysis and observations, questionnaire and Joint Application Development (JAD) (Mwenda, 2016)

To capture the system requirements, this research used observations and document analysis and as will be outline in subsequent sections of this research, there are data flow diagram (DFD), use cases, entity relations (ER) diagram were employed to document the system requirements

4.3.5 System Requirements

a) Functional Requirements

- i. **Bank server challenge-response** - the bank server should produce an unpredictable challenges and cannot be compromised.
- ii. **Customer Authentication** – the bank customer should be able to login to their PC browser using the bank provided user name and PIN. The customer is to exercise due care with his or her PIN in order to keep it secret.
- iii. **Bank application installed on the NFC Mobile phone**—it is assumed that an attacker is not able to compromise the application once installed on the phone
- iv. **Wireless communication between card and phone** – this channel should carry information reliably over a few centimeters, after which the signal's power should decrease making the information meaningless.
- v. **Customer and Phone Interaction** – the customer should be able to interact with the phone via the phone's screen and keypad.
- vi. **Interaction between the customer and the PC or Browser** – the customer should be able to interact with the Browser's via the PC's screen, keyboard and mouse
- vii. **Internet connectivity** – the customer's PC or Browser should be able to interact with the bank server via the Internet.

b) Non-functional requirements

- i. **Availability** – both the customer's phone and bank card should be available when needed
- ii. **Performance** – the smartphone should be able to scan 2D- code within a second and smartcards should be able to compute the response within less than a second.
- iii. **Server session** – the server should have only one open session and only one open transaction at a time for one account to ensure that software attacks like credential stealing attacks are prevented.
- iv. **Familiarity** – the method is similar to Chip TAN method hence familiar to the customers.
- v. **Data Encryption** – this security feature is geared towards protecting the customer's credentials.
- vi. **User friendly** – the application on the mobile phone should be easy to use by the customers.

After receiving the transaction, the bank server generates a 2-D code containing the transaction details and OTP. This 2D code is included in the server response. The smartphone app builds a challenge from the transaction details and the OTP and sends it to the bank card. The bank card calculates the response as a function of the challenge and a secret key and returns it to the Smartphone app. The Smartphone app selects the TAN from this response. The server can compute the correct TAN since it knows the transaction details, OTP, and secret key and therefore is able to check the TAN received.

4.3.6 The Use Case analysis

A use case describes the behavior of a system under various conditions as the system responds to requests from the principal actors (Hoffer et al., 2014). According to Roth et al. (2013), each use case describes how an external user triggers an event to which the system must respond. More specifically the use case represents an identified complete system function. The use case model diagrammatically represents the system showing all the use cases and then actors of the use cases. Hoffer et al. (2014) defines an actor in this case as an external entity that interacts with the system. It can be a person or another system. An actor represents a role that can be played by a user when he or she interacts with the system. In the use case model, the actor's name indicates the role played in the system.

According to Hoffer et al. (2014), use cases focus on system functionality and business processes but provide minimal information about the data flow through the system and that is why they are combined with the data flow diagrams (DFDs) to give the analysts a more complete picture of the whole system. Figure 4.18 shows the use case diagram for the NFC based authentication model for online banking.

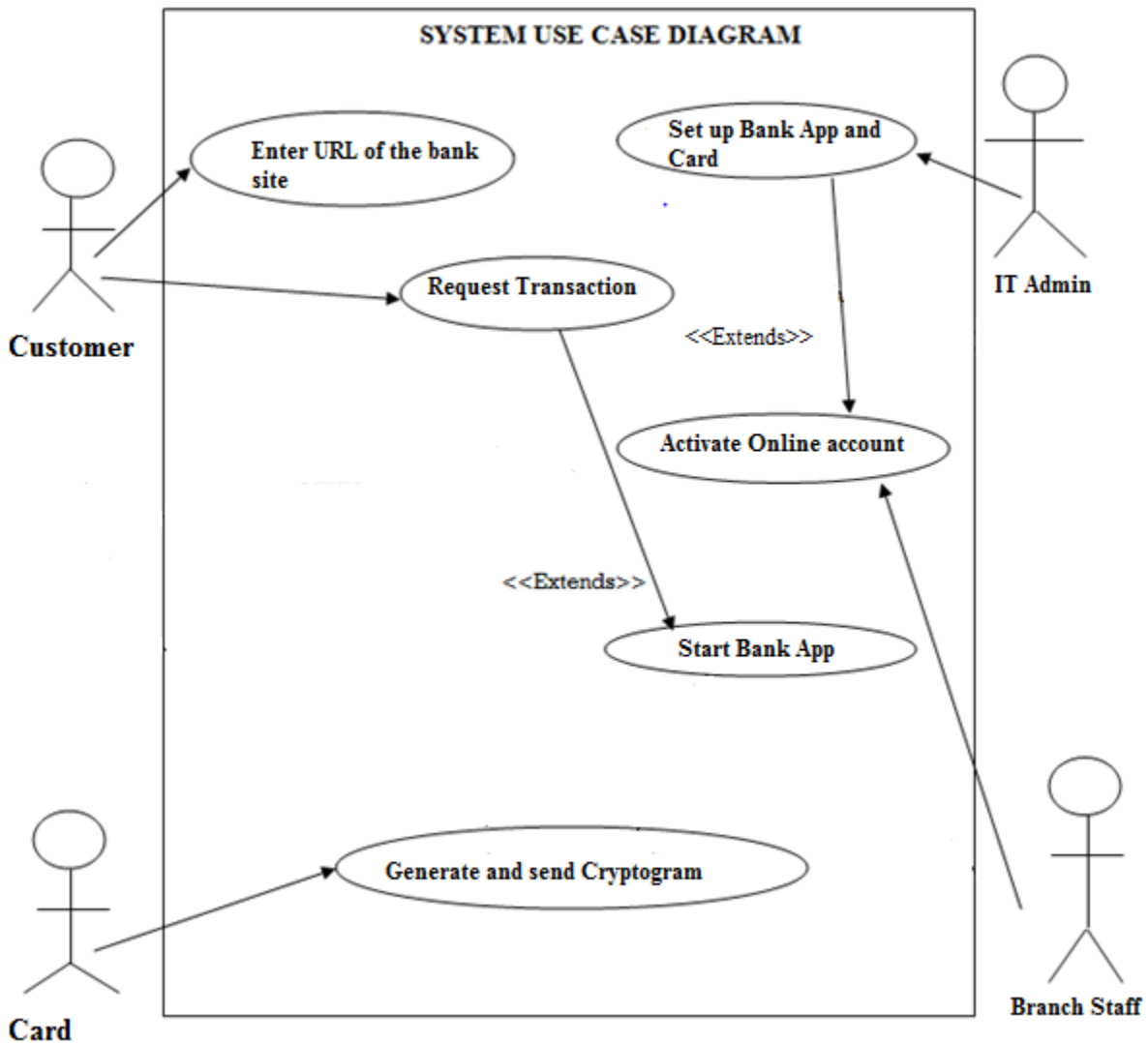


Figure 4.18 Use Case Diagram for the NFC-Based Online Banking Authentication

Table 4.1 Enter the URL of the Bank Site Use Case

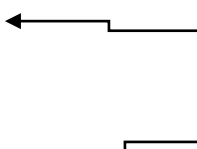
Use Case Name: Enter the URL of the bank site		ID Number : 1	
Short Description: This describes how the customer types the address of the bank site in order to access the website.			
Trigger: Customer enters the URL on their PC or browser Type: External			
Major Inputs		Major outputs	
Description	Source	Description	Destination
a. Typing the URL of the bank site on the PC	Customer	Bank Website and login page displayed	Bank server
b. Bank server sends a form to the browser with Customer login field	Bank server	Customer types in the user name on the form	Bank server
<u>Major Steps Performed</u> 5 The customer power's on the PC 6 The customer logs in to their PC 7 The customer gets the URL of the bank site 8 The customer enters the URL on their browser			Information for steps  Browser Customer Coordinates

Table 4.1 shows a description of the enter URL into bank site use case. The description of the rest of the use cases are illustrated on appendix B of this paper.

4.4 System Design

In the system design stage, various techniques are used to represent the system requirements gathered in the previous stages in a format easily understood by both the system analysts and the users. The techniques used in this research include data flow modeling and the Entity Relationship models.

4.4.1 Data flow modeling

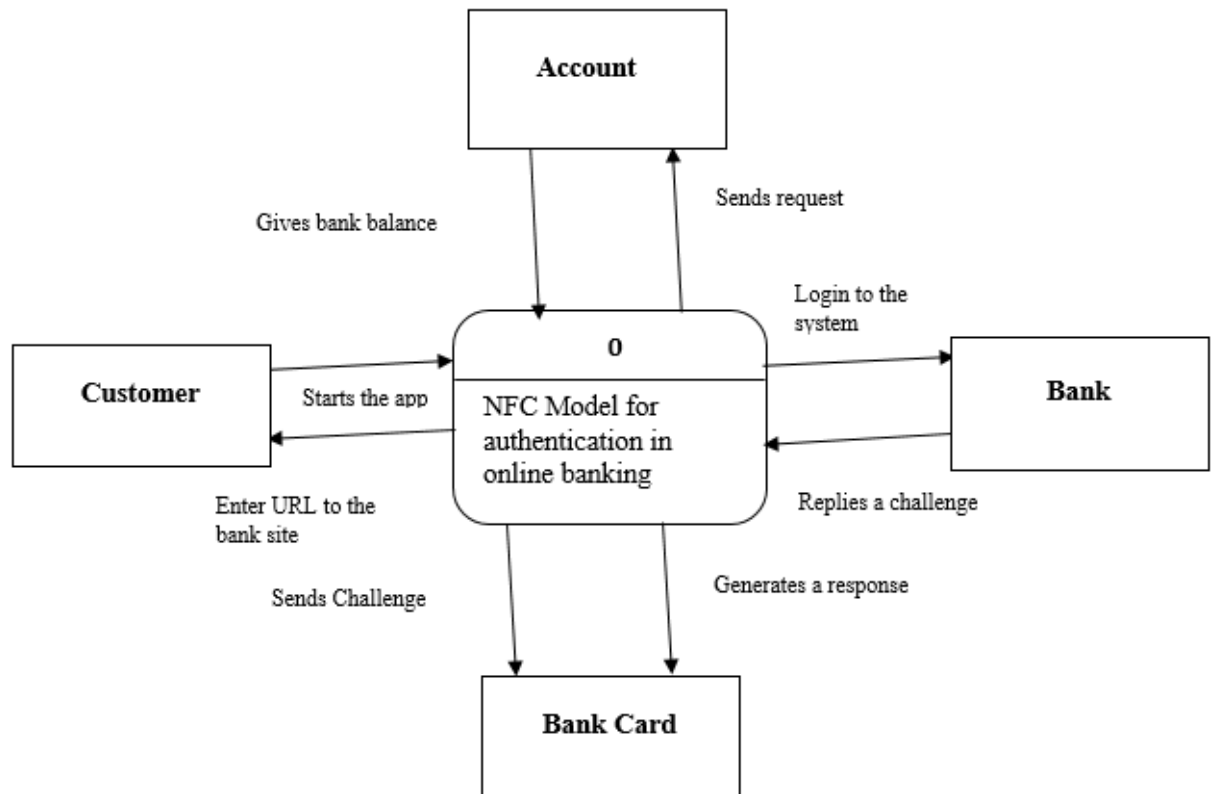


Figure 4.19 Context diagram of the System

Data flow diagrams enable the modeling of how data flows through an information system, the relationship among the data flows, how data come to be stored at specific locations and the processes that transform the data (Hoffer et al., 2014). Since data flow diagrams represent movement of data between the various processes of the system, these diagrams are

called process models. One of the popular process model used by many analysts is the data flow diagram (DFD).

It graphically represents the processes that capture, manipulate, store, and distribute data between a system and its environment and between components within a system in varying levels of granularity (Hoffer et al., 2014). The highest level view of the system is depicted by a DFD called the context diagram which shows the entire system as a single process and the data sources that interact with the system from the environment. Figure 4.19 shows the context diagram of the NFC based authentication model.

4.4.2 The Entity- Relationship (E-R) data model

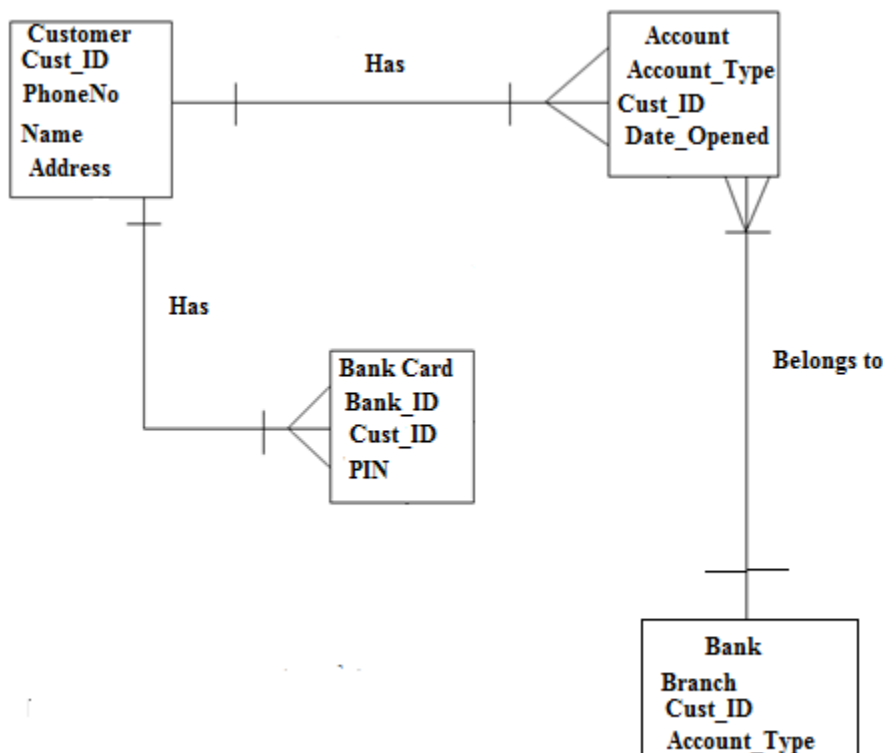


Figure 4.20 ER diagram

According to Hoffer et al. (2014), Data modeling develops the definition, structure and relationship within the different data being used by the system. The authors goes ahead to state that data is not only the most complex aspect of many modern information systems but also the pillar in many of such systems. Therefore the data aspect must be taken into consideration during the system design. Further, the authors points out that the characteristics of data captured and

agreed upon during the system analysis phase, determine not only the design but also the actual system functionality. The entity relationship diagramming is used for data modeling and in the design of the conceptual application. Figure 4.20 shows the ER of the model entities and their attributes.

4.4.3 Sequence Diagram

According to Roth et al. (2013), a sequence diagram illustrates the objects that participate in a use case and the messages that pass between them over time for one use case. A sequence diagram is a dynamic model that supports a dynamic view of the evolving systems. It shows the explicit sequence of messages that are passed between objects in a defined interaction. Sequence diagrams are helpful for understanding real time specifications and complex use cases because they emphasize the time-based ordering of the activity that takes place among a set of objects. Figure 4.21 shows the sequence diagram for the NFC model.

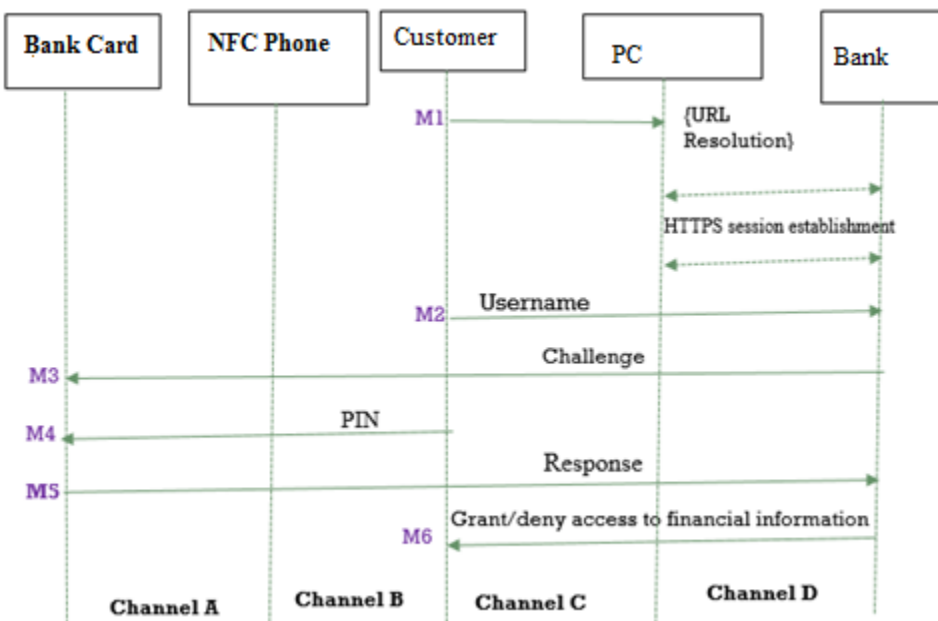


Figure 4.21 Sequence Diagram for customer authentication protocol

Following is a short description of the sequence diagram;

- The customer enters the URL of the online banking site in the PC (M1).
- The PC resolves the URL and opens up the bank's site. An https session is established between the bank and the browser over channel D.

- iii. The server sends a form to the browser with the customer user name field.
- iv. The user types in her user name and password in the PC (M2).
- v. The server replies a challenge, which is a random number between 4 and 6 digits associated with the SSL connection and the user name and password provided in the previous step (M3).
- vi. The user starts the mobile application in the phone
- vii. The user selects the Login mode and types the challenge in the phone (M3)
- viii. The customer types her PIN into the phone (M4).
- ix. The phone sends the challenge and the PIN to the card obtaining a cryptogram in return. Using that cryptogram, the phone generates a code (response) that it displays to the user in its display.
- x. The user sends the response to the server by typing it in the appropriate field of the web form in the PC (M5).
- xi. The server checks that the received response corresponds to the issued challenge. If the response is valid, the bank presents the customer with the account information as well as transaction options (M6).
- xii. The user can perform a transaction by selecting the appropriate option and filling the necessary fields.

Data exchanged between card and phone is protected against eavesdropping by the intrinsic characteristics of the radio signal used to carry the information across this channel. The low power of the electromagnetic field generated by the phone makes it very hard to recover any information from distances greater than a few centimeters.

4.4.4 Conceptual Design of the Model

Figure 4.22 shows the conceptual design for the NFC Model method derived from Java Modeling Language. The system architecture comprises of; the customer who login to the bank server via a Personal Computer. The Smartphone, which reads the transaction via 2D code from the PC, and shows the transaction data for confirmation on its display, the bank card is contacted by the Smartphone via NFC and sends the confirmation to the Smartphone. The customer also transfers the code to the PC. The model allows for online banking transaction authorization with the customers bank card as credential and Smartphone as communication device. The workflow of the model requires the customer to:

- i. Log in on the PC browser, enter transaction and submit it to the bank server.
- ii. Scan the 2D code shown on the PC screen with the Smartphone.

- iii. Double-check the transaction on the Smartphone display and confirm with the bank card.
- iv. Transfer the TAN to the PC browser and submit it to the bank server.

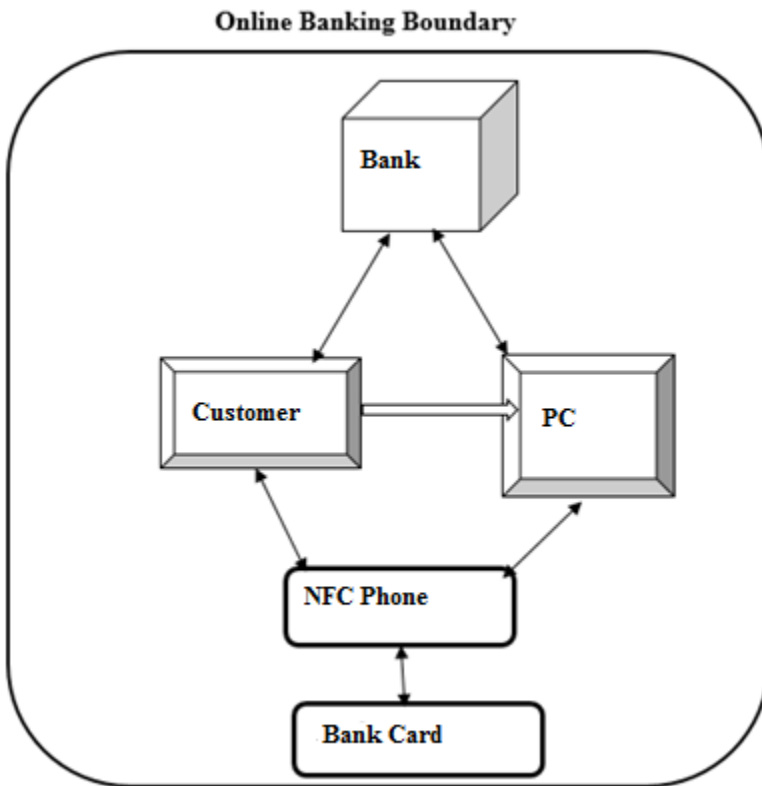


Figure 4.22 NFC Model System Architecture

Under the hood, the following interaction and computation is done:

- a) After receiving the transaction, the bank server generates a 2D code containing the transaction details and OTP. This 2D code is included in the server response.
- b) The Smartphone app builds a challenge from the transaction details and the OTP and sends it to the bank card. The bank card calculates the response as a function of the challenge and a secret key and returns it to the Smartphone app. The Smartphone app selects the TAN from this response
- c) The server can compute the correct TAN since it knows the transaction details, OTP, and secret key and therefore is able to check the TAN received.

4.5 Model Implementation

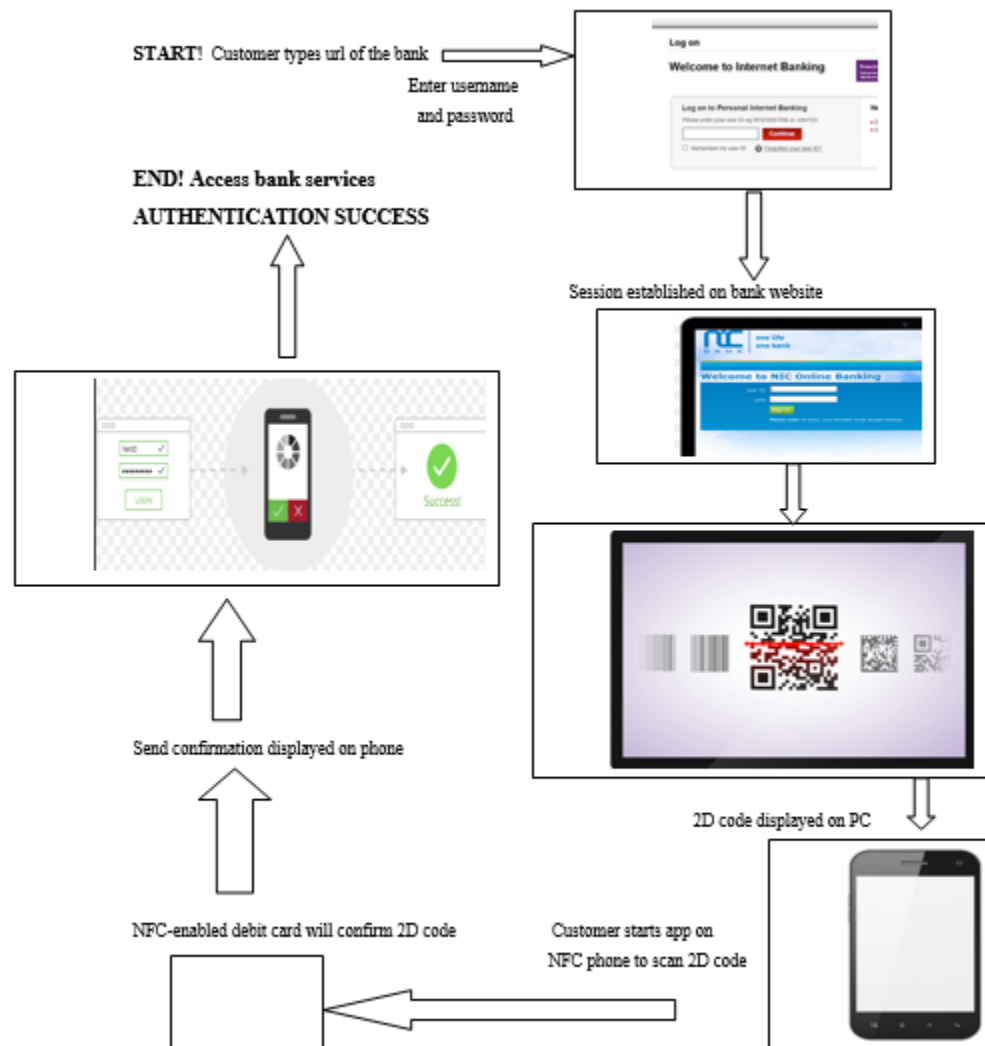


Figure 4.23 Model implementation

Figure 4.23 shows the implementation of the system and it begins by the customer typing the URL of the bank and then the bank's website prompts the customer to enter username and password. A session is established on the bank website which is followed by the website displaying the 2D code on the PC. The customer will then start the app on phone in order to scan the 2D code. The NFC-enabled debit card will then confirm the 2D code. A unique number will then be displayed on the phone and this will result into successful authentication.

Chapter 5: System Implementation and Testing

5.1 Introduction

This chapter discusses implementation and testing of the model developed. The model development encountered some difficulties like unavailability of the hardware card and NFC enabled smartphone, instead a quick response code was generated to represent the challenge response while the QR code reader represented the mobile app. QR code generator and reader was used to evaluate whether the model meets the objectives of the system as outlined in Chapter

5.2 Implementation

The system that this model attempts to prove involves a wireless connectivity whereby the machine to machine communication is achieved by the use of NFC technology between the phone, bank card and the PC. The researcher will show with the model the creation of a Quick Response code (QR code), establishing a connection, reading and interpreting the code with the QR code reader.

Java programming language was used for the creation of the QR code. This language was chosen because of its user friendly built-in libraries. A bar code reader was downloaded on an android based phone to facilitate the reading of the code generated.

5.2.1 System Requirement

The following system requirements were considered for the development of the model;

i. Personal Computer (host)

The host is the Personal computer that accesses the bank server and which stores the QR code that the QR code reader communicates with when accessing customer details. The laptop used is running on Windows 2010 Operating System.

ii. Smartphone (client)

Mobile phone connection with Samsung Galaxy Grand Prime+ (running on Android OS version 6.0.1). The smartphone has the ability to read the QR codes.

a. QR Code Generation

A new java application was created using NetBeans version 8.0.2. Java Libraries added to the java project to facilitate image creation included qrgen-1.0, zxing-core-1.7 and zxing-j2se-1.7 as illustrated in figure 5.1. The application created QR code on the PC/browser. The resulting code is presented in Figure 5.2 of this chapter.

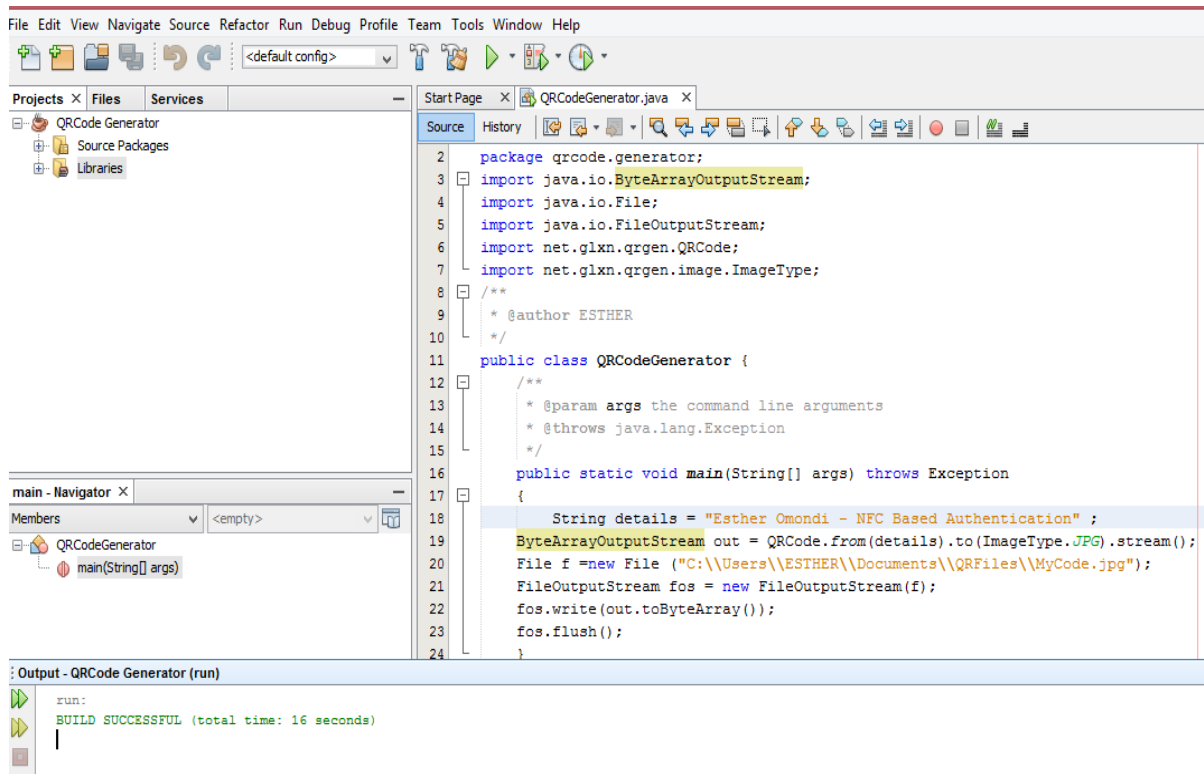


Figure 5.1 QR code generator Java application

b. QR Code

Figure 5.3 shows the resulting image after the Java code in Figure 5.1 is executed. The code was saved as a file in the folder of the researcher's laptop as shown in Figure 5.2. This is the code that, when scanned with the QR code reader, showed a text on the mobile phone.

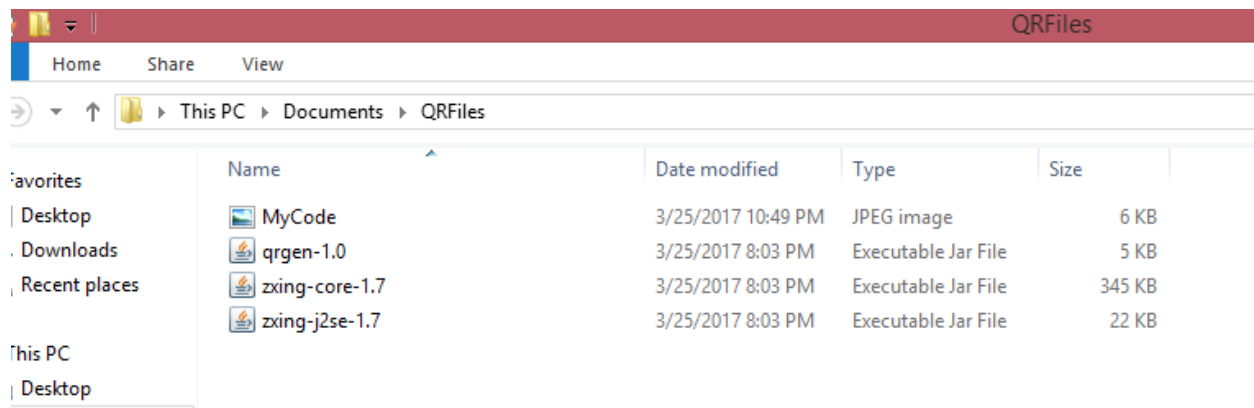


Figure 5.2 QR Code file folder

Figure 5.2 shows a screen shot of the folder of the QR code generated. The following Figure 5.3 shows what happens when the file is opened.

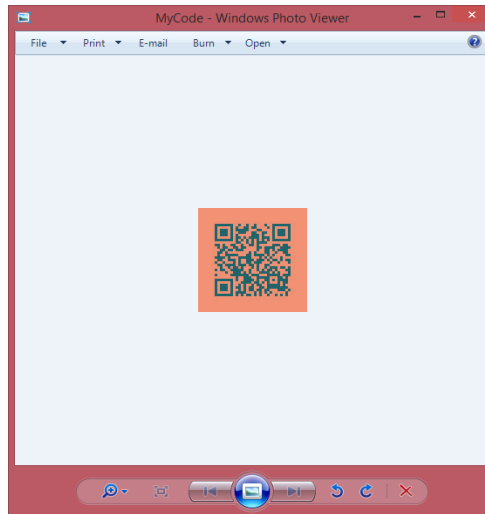


Figure 5.3 QR code

Figure 5.3 shows the QR code generated and stored in a folder. When the code is scanned, the resulting text represents a unique response as shown in Table 4.6.

c. QR code Reader

The QR code reader was downloaded from the Google Play store using Samsung Galaxy running on Android Operating System. This was used to scan the QR code created on the laptop.



Figure 5.4 QR Code reader App.

d. Generation and scanning of the Code

Figure 5.5 represents the flow diagram of the process from when the code is generated on the Personal Computer, the downloading of the QR code reader and the scanning of the code.

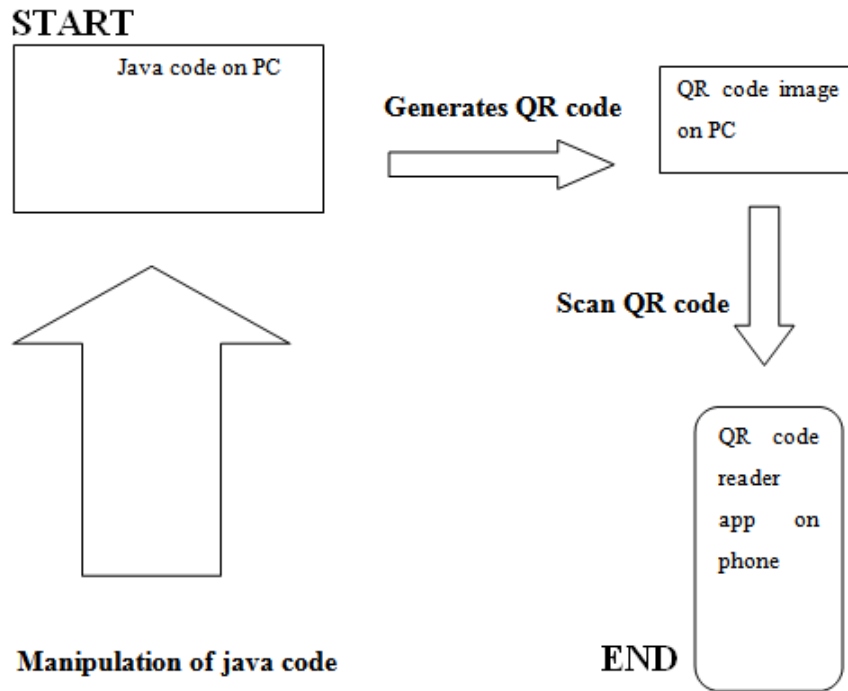


Figure 5.5 Start of Java code generating QR code and scanning of code

5.3 Testing

The testing was done on the use cases by establishing connectivity between the phone and the laptop. The challenge response functionality which is the backbone of this research was tested by changing letters on the java code. Every time a text was changed on the code, it was interpreted differently by the code reader. This showed that the challenge response sent by the server to the phone and confirmed by the bank card is unique for each customer.

5.3.1 QR Code Generation Use Case

Table 4.2 QR Code Generation Use Case

Java code manipulated	QR code generated	Result
String details = “Esther Omondi –NFC Based Authentication” ;	QR code 1	Pass
String details = “John Dodd –NFC Based Authentication” ;	QR code 2	Pass
String details = “Grace Jane” –NFC Based Authentication” ;	QR code 2	Pass

5.3.2 Scanning of QR Code Use Case

Table 4.3 Scanning of QR Code Use Case

Scanning of QR code	Data displayed	Result
QR code 1	“Esther Omondi –NFC Based Authentication	Pass, Authentication established
QR code 2	John Dodd –NFC Based Authentication	Pass, Authentication established
QR code 3	Grace Jane” –NFC Based Authentication	Pass, Authentication established

The java code was manipulated by changing the code as shown on Table 4.2 and the resultant QR code generated as an image on the PC is also shown. The other use case that was tested was the scanning of the QR code by the QR code reader and the corresponding data displayed is shown on Table 4.3. This aimed at showing that there was:

- i. Authentication by having a unique QR code generated by manipulation of java code
- ii. There was wireless communication between the app on the phone (QR) code reader and the PC which had the QR code image.
- iii. There was the generation of a unique code that could be confirmed through a communication device

Chapter 6: Discussions

6.1 Comparative analysis between research findings and existing literature

6.1.1 Bank employees

The data from the findings indicated that the majority of the bank employees who were the respondents were from the front office departments (30%) and tellers (40%) and the least were from the top level management (15%). This is a crucial finding because the majority of the bank customers that would request for online banking set up, are most likely to meet the front office bank employees and these employees thereby become a key source of information on online banking security and matters that pertain authentication. These group of employees therefore need good training on cyber security and online banking security so that they can be able to transfer this information to the bank customers.

The banking employees, as indicated in Chapter 4 recorded a statistically significant percentage of usage of online banking services. By embracing this technology, the employees are better placed to transfer this knowledge to their customers and it is worth noting that the areas that should be addressed by the bank include:

- i. Care taken not to open attachments or installation of free online software whose source is unknown.
- ii. Avoid giving PIN and password information to people you don't know
- iii. Do not follow a link sent via email or provide personal banking details if the link is not from the bank.
- iv. Avoid saving your passwords on mobile phones.
- v. Always remember to log out from the online site after every completing the transaction.
- vi. Do not access your online account through unprotected WiFi connections.

The results that show that only 30% of the bank employees were aware of the NFC functionality on their mobile phones compared the majority (70%) who were not, brings to focus the need for awareness of this technology. It is imperative to note that since smartphones have wireless functionality such as WiFi and Bluetooth, users of these smartphones can also transfer their knowledge of usage of these smartphone to NFC.

This research findings runs counter to the assertion by Mulevu (2012) that mobile phone manufacturers have produced smart phones with NFC capabilities and the trend seems to rise and hence projection that NFC adoption will rise.

It is interesting to note that even though a higher number of smartphone users did not know about NFC functionality, a majority (60%) strongly agreed that NFC incorporation in the banking industry was important. This finding is important because it shows that there exists an intra-organizational digital divide that needs to be addressed and adoption of NFC can be widespread when proper measures are taken to ensure that NFC adoption is realized.

6.1.2 Bank Customers

The findings on the age distribution among the customer respondents were eye opening. The majority of the respondents were from the age bracket of 31-43 which shows the demographic that is likely to adopt online banking technology.

Fifty five percent (55%) of the customer respondents indicated that they access their banking details online as compared to 45% who do not. As it has been alluded to earlier, this difference is not statistically significant but it does show that the majority of the bank customers are responding well to the idea of online banking and the minority needs to be adequately informed. This research projects that NFC adoption will largely depend on the customer's willingness to embrace online banking, in other words there will be a direct correlation between customer's willingness to adopt NFC technology and online banking.

Research findings indicate that eighty one percent (81%) of the respondents said they access their bank information and transact via their mobile phones compared to nineteen percent (19%) who have access to online banking via the PC. This is significant because when this data is compared with data provided by Clark (2014), which shows that NFC will be included in sixty four percent (64%) of the mobile phones shipped in 2018 up from 18.2% in 2013, there is a general trend towards an increase in mobile phone ownership and usage and this can be leveraged by the banks. Further, since the majority of customer respondents indicated that they strongly agreed (68%) that they found online banking beneficial to them, it goes a long way to show the relevance of online banking study.

Sixty five percent (65%) of those who did not subscribe to online banking indicated that this technology was too complex. So this begs the question- is there need for a simpler, user-friendly technology to address the complexities that involves online banking? The answer is that this research provides a simpler solution. The NFC-based model for Authentication in Online

Banking removes the need for additional gadgets such as no need to carry hard token. The token can also be lost and is an additional cost to the bank. The customers are already in possession of the bank card and a smartphone.

It was encouraging to see that the majority of the respondents (96%) reported that they did not share their passwords or PIN. This finding supports this research premise in ensuring that bank customer's information remains secure because the customer's unwillingness to share their personal bank information will ensure the success of this NFC based model for online authentication when it is adopted in the banking industry. Additionally, the confidence that the bank customers have in the bank's ability to keep their personal information confidential as shown by data that shows that 80% of the respondents who strongly disagree that the bank shares their login credentials.

The findings on whether bank customers have smartphones or not was similar to the findings which resulted from the research seeking to find out if bank employees had smartphones. Eighty five percent (85%) of the customers reported that they had smartphones and this also supports the research idea on the need for NFC adoption since this technology is projected to increase in years to come.

6.2 Correlations of the functionalities of the model being developed with the java-based prototype

The Java code that creates a QR code image to be read by a QR code reader is a mirror image of the model proposed.

- i. The reading of the QR code wirelessly corresponds with NFC functionality of the model. This also shows machine-to-machine communication.
- ii. The manipulation of code to generate a unique QR code corresponds with authentication because each code generated when the code is slightly altered creates a unique QR image

6.3 Why this research is unique

The mechanism of authentication shown in this research is novel because the NFC phone takes the active role in the authentication process. By using NFC technology, the banking sector will join a growing number of sectors in the society that have already embraced this technology in their operations. This will not only ensure that the banking sector stays ahead of the curve, but also restore confidence in customers when they know that they can conduct their business in a safe and secure environment.

Additionally, rolling out of this idea in the banking sector will be cost effective as it will eliminate the usage of tokens. Having a simple, yet effective approach to customer authentication will always be studied by scholars in years to come and this research offers a firm foundation in this regard.

6.4 Constrains in NFC technology

For this research idea to materialize, the researcher acknowledges that there has to be firm grip of the banking industry as far as NFC adoption is concerned. Market penetration of NFC is critical and so there has to be healthy interplay between the business aspect of this technology (market adoption) and the technical advancement in NFC technology. The aforementioned factors notwithstanding, NFC will be a disruptive technology in the banking sector upon which authentication modalities can be built.

Chapter 7: Conclusions and Recommendations

7.1 Conclusions

Authentication and NFC technology which are the mainstay of this research are important security areas in online banking research. This research presented a detailed approach on how to address the complexities of online banking research, based on the empirical data on both NFC technology and authentication and came up with a Near Field Communication Based-Model for Authentication in Online Banking.

The model developed in this research forms the foundation on which future research in authentication as far as online banking will be based. The addition to new knowledge that this research brings is elimination of need for additional device for authentication. Additionally, the bank card used in this model referred to the bank provided debit card. This is not an additional device but rather something that the customer is already accustomed to and the bank has already incorporated in its security details in the system. Data collected showed mixed information on knowledge and awareness of NFC technology and both the bank customers and employees.

7.2 Recommendations

We are operating in an increasingly complex, interconnected online world and since this reach model developed will operate online, it is important to bear in mind that online security is prioritized. A number of countermeasures to security threats with reference to mobile technology include:

- i. Installation of antivirus, firewall or anti-spyware software on the mobile phone. These will ensure that spyware doesn't infiltrate the system and steal customer's valuable bank data.
- ii. Keeping the phone's operating system with the up-to-date software
- iii. Enabling screen lock functionality on the mobile phone
- iv. Avoiding the temptation to install free games and other free software online on the mobile phone because these software may contain malicious software that may steal the customer's bank details.

7.3 Suggestions for future research

A number of future research areas to be explored include:

- a. Improvements in the model are required in terms of having a simple user interface on the Mobile Phone to enable users to view different Applications on the screen and is secure.
- b. It would be much better if the bank card could be done away with all together and instead, an app like the java cardlet to be downloaded on phone together with the QR Code reader for transaction authentication.

REFERENCES

- Alpa'r, G., Batina, L., & Verdult, R. (2012). *Using NFC phones for proving credentials*. In: Proceedings of the 16th international GI/ITG conference on Measurement, Modelling, and Evaluation of Computing Systems and Dependability and Fault Tolerance.
- Amit, R., & Zott, C. (2001). *Value Creation in E-Business*. Strategic Management Journal 22 (6-7)
- Anderson, R. (2006). *Yet another insecure banking system*. Light Blue Touch paper.
- Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M. J. G. & Levi, M., et al. (2012). Measuring the cost of cybercrime. Retrieved from http://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012
- Antoniou, D., & Socha, K. (2016). *Authentication Methods*. (Retrieved from CERT-EU Security White Paper 16-003).
- Bram, C. & Ben, L. (2001). *AES hash*. Proposal, National Institute of Standards and Technology.
- Burns, N. & Grove, S.K. (2003). *Nursing Research*. 3rded Pennsylvania: Saunders.
- Calisir, F., & Gumussoy, C.A. (2008). *Internet banking versus other banking channels: Young consumer's view*. International Journal of Information Management. 28(3)
- Central Bank of Kenya (2014). *Bank Supervision Annual Report*. (Retrieved from a report by Banking Fraud and Investigation Department) Nairobi, Kenya.
- Clark, S. (2014). *Two in three phones to come with NFC in 2018* Forecast for world shipments of NFC handsets, in millions. Retrieved from www.nfcworld.com on 5/4/2017
- Claessens, J., Dem, V., Cock, D. D., Preneel, B., & Vandenalle, J. (2002). *On the Security of Today's Online Electronic Banking Systems*. Elsevier Science Ltd. Retrieved from [https://doi.org/10.1016/S0167-4048\(02\)00312-7](https://doi.org/10.1016/S0167-4048(02)00312-7)
- Dennis, A., Roth, R.M., A. & Wixom, H.B. (2012). *Systems Analysis and Design*. 5th Edition. John Wiley & Sons, Inc.
- Dodson, B., Sengupta, D., Boneh, D., Lam, M. (2010). *Secure, consumer-friendly web authentication and payments with a phone*. In: Conference on Mobile Computing, Applications, and Services (MobiCASE 10)
- Drimer, S., Murdoch, S., Anderson, R. (2009). *Optimized to Fail: Card Readers for Online Banking*. In: Dingledine, R., Golle, P. (eds.) Financial Cryptography and Data Security, vol. 5628, pp. 184–200.
- Gomez, M. (2015, March 20). *Are Biometrics the future of Online Banking?* [Blog post]

- Gunter, O. (2005). The Pharming Guide: *Understanding & preventing DNS-related attacks by phishers*. <http://www.ngssoftware.com/papers/ThePharmingGuide.pdf>.
- Gunther, M. & Borchert, B. (2013). *Online Banking with NFC-enabled Bank Card and NFC-enabled Smartphone*. Department of Computer Science. Germany.
- Haselsteiner, E., & Breitfub, K. (2006). Security in near field communication (NFC)
- Hoffer, J.A., George, J. F., & Valacich, J.S. (2014). Modern Analysis and Design. Pearson Education Ltd. Edinburgh Gate, Harlow England.
- Ishani, S, et al. (2010). *Palm Vein Authentication System: A Review*. International Journal of Control and Automation, 3(1).
- Janardan C. & Bhaskar C. (2013). *Secure User Authentication in Internet Banking: A Qualitative Survey*; International Journal of Innovation, Management and Technology, 4(2)
- Joao, R.N. (2013). *Hand Veins Recognition System: A Thesis Paper for Masters in Electrical and Computing Engineering*. Tecnico Lisboa.
- John, V., S. (1998). *Qualitative Data Analysis: Qualis Research*. quails@qualis
- Johnson, J. M. (2008). *A new approach to Internet banking* (Doctoral dissertation). Retrieved from a technical report by university of Cambridge (UCAM-CL-TR-731)
- Kilani, R., & Jensen, K., (2013). *Mobile Authentication with NFC Enabled Smartphones*. Department of Engineering, Aarhus University. Denmark. Pg32- Technical report ECE-TR-14
- Kizza, J. M. (2005). *Computer network security*. New York: Springer.
- Kramp, T., Weigold, T., & Hiltgen, A. (2006). Secure Internet banking authentication. IEEE Security and Privacy, 4(2)
- Kunyu, P., Jiande, Z., & Jing, Y. (2009). An identity authentication system based on mobile phone token. Network Infrastructure and Digital Content, 2009. IC-NIDC 2009. IEEE International Conference.
- Liu, Z., & Song, S. (2012). *An Embedded Real Time Finger-Vein Recognition System for Mobile Devices*, IEEE Transactions on Consumer Electronics 58 (2)
- Madlmayr, G., Langer, J., & Scharinger, J., (2008). Managing an NFC ecosystem. Mobile Business, 2008.
- Mallikarjuna, A, & Madhuri, S. (2013). Palm Vein Technology Security. International Journal of Advanced Research in Computer Science and Software Engineering, 3(7).
- Meyer, R. (2007). Secure Authentication on the Internet. SANS Institute InfoSec Reading Room

- Mrunali J. & Priya M. (2015). *A Biometric System for Person Authentication Based on Finger Vein Patterns on FPGA*, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering 4(6)
- Mulevu, C. (2012). *Investigating Applicability of Near Field Communication Technology in Kenya: A Model for Adopting NCF-Based Mobile Phone Payment Systems*. Submitted in partial fulfillment of the Requirements for the degree of Masters of Science in Information Technology (MSc.IT) at Strathmore University 2012
- Mwenda, P., K. (2016). A prototype for locating and choosing office space as a service: a case of Nairobi city. Submitted in partial fulfillment of the Requirements for the degree of Masters of Science in Information Technology (MSc.IT) at Strathmore University. Nairobi, Kenya.
- Mwikali, F. (2013). *Framework for Medical Collaborative Systems in Public Hospitals Case Study: Mbagathi District Hospital & Health Centres*. Faculty of Information Technology Strathmore University, Nairobi, Kenya.
- NFC Forum (2006). NFC Data Exchange Format (NDEF). Technical Specification.
- Onyancha, P. M. (2016). Near-Field Communication Based-Model for Health Information Portability. Master dissertation of Science in Computer Based Information Systems submitted at Strathmore University. Nairobi, Kenya.
- Onyango, J. O. (2014). *A model for Adoption of Unified Communication and Collaboration in Organizations*. Master of Science in Computer Based Information Systems.
- Ortiz-Yepes, D.A. (2009). *Enhancing Authentication in eBanking with NFC-Enabled Mobile Phones*. In: ERCIM News. No. 76, European Research Consortium for Informatics and Mathematics
- Ponemon Institute. (2005). Privacy Trust Survey for Online Banking. Retrieved from <http://www.watchfire.com/news/whitepapers>.
- Rana, T, & Mumtaz A. K. (2012). *Evaluating biometrics for online banking: The case for usability*. International Journal of Information Management, 32(5). Retrieved on 28th September, 2015.
- Roth, R.M., Dennis, A. & Wixom, B.H. (2013). Systems Analysis and Design. 5th Edition. John Wiley & Sons Singapore
- Silverman, D. (2000). *Doing Qualitative Research: A practical Handbook*. London: Sage.

- Smart Card Alliance, (2015). *A Smart Card Alliance Mobile and NFC Council White Paper NFC Non-Payments Use Cases*. Card Alliance 191 Clarksville Rd. Princeton Junction, NJ 08550
www.smartcardalliance.org
- The H. Security (2012) Millions stolen with mTAN fraud. Retrieved from
<http://www.honline.com/security/news/item/Millions-stolen-with-mTAN-fraud-1763923.html>
- Wang, D., Li, J., & Memik, G. (2010). *User Identification based on Finger-vein patterns for Consumer Electronics Devices*, IEEE Transactions on Consumer Electronics, 56 (2)
- Weigold, T., Hiltgen, A. (2011). Secure confirmation of sensitive transaction data in modern Internet banking services. In: World Congress on Internet Security (WorldCIS). pp. 125–132
- Williamson, G. (2006). *Enhanced Authentication in Online Banking*. Journal of economic crime management, 4(2).Retrieved <http://www.jecm.org>
- Zentraler K. (2010) Hand Held Device (HHD) Retrieved from
- Zimmerman, M. (2002). Biometrics and User Authentication. Retrieved from SANS Institute InfoSec Reading Room. <https://www.sans.org/readingroom/whitepapers/>

Appendices

Appendix A: Questionnaire

Appendix A: 1 Questionnaire for Bank Employees

Researcher's Name: Esther Akinyi Omondi

Research Topic: Near Field Communication Based-Model for Transaction Authentication in Online Banking

Purpose: Questionnaire for the above research topic towards a degree of Master of Science in Information Systems at Strathmore University.

The following is a structured questionnaire that seeks to gather information about the technological applications available for the online banking service for academic purposes only. The researcher and the University undertake to protect the privacy of individuals and entities mentioned herein. No data pertaining to such institution will be revealed or published apart from that which is already in the public domain.

For the purpose of this research, Online banking also known as E-banking is defined as the use of the Internet by the bank to deliver traditional banking services such as transferring funds, electronic bill payment and secure communication between the bank and the Customers.

A- Personal Profile

- i. What is your name? (Optional).....
- ii. What is your gender? (Tick the appropriate box)
M ☐ F ☐
- iii. Which department of the bank do you work? (Tick the appropriate box)
Top level management ☐
Front office ☐
IT department ☐
Tellers ☐

B- Online Banking

i. Do you utilize online banking services?

YES ☐

NO ☐

ii. Do you inform your customers about online banking when they visit the bank?

YES ☐

NO ☐

iii. Online banking is beneficial to bank customers? Rate as shown

Strongly agree ☐ Agree ☐ Neither ☐ Disagree ☐ Strongly Disagree ☒

C- Authentication Issues

Comment on some of the problems you encounter with authentication within the bank.....

.....
.....
.....

D- Near-field communication (NFC)

i. Does your phone have NFC functionality?

YES ☐

NO ☐

ii. Do you agree (or disagree) that this technology is revolutionizing banking industry and how customers and banks interact?

Strongly agree ☐ Agree ☐ Neither ☐ Disagree ☐ Strongly Disagree ☒

Appendix A: 2 Questionnaire for Bank Customers

Researcher's Name: Esther Akinyi Omondi

Research Topic: Near Field Communication Based-Model for Transaction Authentication in Online Banking

Purpose: Questionnaire for the above research topic towards a degree of Master of Science in Information Systems at Strathmore University.

The following is a structured questionnaire that seeks to gather information about the technological applications available for the online banking service for academic purposes only. The researcher and the University undertake to protect the privacy of individuals and entities mentioned herein. No data pertaining to such institution will be revealed or published apart from that which is already in the public domain.

For the purpose of this research, Online banking also known as E-banking is defined as the use of the Internet by the bank to deliver traditional banking services such as transferring funds, electronic bill payment and secure communication between the bank and the Customers.

i. What is your Gender? (Tick on the appropriate box)

M ☐

F ☐

ii. What is your age? (Tick on the appropriate box)

18-30 ☐ 31-43 ☐ 44-56 ☐ 57 and above ☐

iii. Do you have access to online banking services?

YES ☐

NO ☐

iv. If your answer on (ii) above is YES, how do you access the service?

Via a mobile phone ☐

Via a computer ☐

v. If your answer on (ii) above is YES, is the service beneficial to you?

☐

Strongly agree Agree ☐ Neither ☐ Disagree ☐ Strongly Disagree ☒

vi. If your answer on (ii) above is NO, why? (tick the appropriate box)

I don't have access to internet ☐

Online banking is complex and I don't understand it ☐

I prefer to go personally to the bank and carry out banking transactions ☐

vii. Please comment about the login process.....
.....
.....

Authentication issues

i. Do you share your password or PIN with anyone?

YES

NO

ii. Do you feel that the bank shares your login credentials with a third party?

Strongly agree ☐ Agree ☐ Neither ☐ Disagree ☐ Strongly disagree ☐

Near-Field Communication (NFC) functionality

i. Do you have a smart phone? (Tick the appropriate box)

Yes ☐

No ☐

ii. If your answer to question (i) is YES, does your smart phone have NFC functionality?

Yes ☐

No ☐

Appendix B

Appendix B: 1 Open up bank site use case

Use Case Name: Open up bank site		ID Number : 2	
Short Description: The customer types in her username in the PC			
Trigger: Customer through the established https.			
Type: External			
Major Inputs		Major outputs	
Description	Source	Description	Destination
a) An https session is established between the bank and the PC.	Bank server	The server sends a form to the browser with customer user name	PC/Browser
b) Bank server sends a form to the browser with Customer login field	Bank server	Customer types in the user name on the form	PC/Browser
<u>Major Steps Performed</u>			Information for steps
1. The PC resolves the <u>url</u> and opens up the bank's site.			Bank server
2. The server sends a form to the browser with the customer login field			
3. The customer types in the username in the PC			Customer Coordinates

Appendix B: 1 shows a full description of the open up bank site use including the inputs outputs involved. In this use case, the customer through his or her browser opens the banking site after establishing a connection with the bank server.

Appendix B: 2 Send response use case

Use Case Name: Send Response		ID Number : 3	
Short Description: The customer sends the response to the server			
Trigger: Customer			
Type: External			
Major Inputs		Major outputs	
Description	Source	Description	Destination
a) Customer starts the bank app	Customer	Log in page displayed on the phone	Phone
b) Customer types her PIN number on the phone	Customer	Customer types the challenge in the phone	Card
c) The phone sends the challenge and PIN to the card	Phone	A cryptogram is obtained from the card	Server
d) The Customer sends the response to the server	Customer	Phone generated code is displayed on the screen	
Major Steps Performed 1. Server replies a challenge 2. The Customer starts the bank app on the phone 3. The customer selects the login mode and types the challenge 4. The customer types her PIN 5. Phone Sends the challenge to the card and obtains a cryptogram 6. Phone generates a code on its display 7. Customer sends the response to the server			Information for steps Bank server Customer Coordinates

Appendix B 2 shows a description of how the customer starts up his or her mobile app on the smartphone and uses the app to respond to the challenge from the bank server. The app scans a two dimensional code shown on the PC.

Appendix B: 3 Reply to the challenge use case

Use Case Name: Reply to the Challenge		ID Number : 4	
Short Description: The server checks that the received response corresponds to the issued challenge			
Trigger: Server			
Type: External			
Major Inputs		Major outputs	
Description	Source	Description	Destination
a) Server checks that the received response corresponds to the issued challenge	Server	The customer sends the response to the server by typing it in the web form in the PC	Server
<u>Major Steps Performed</u> 1. Response sent to server 2. Server checks the received response 3. Server returns a value			Information for steps Bank server Customer Coordinates

Appendix B: 3 shows a description of how the bank server responds to the confirmed challenge. The bank card confirms the challenge received by the mobile phone, the phone returns the same to the bank server. After receiving the challenge the server confirms that it is the same as the challenge that was sent out and a value is returned.

Appendix B: 4 Present account details use case

Use Case Name: Present account details		ID Number : 5	
Short Description: The server presents the customer with her account summary			
Trigger: Server			
Type: External			
Major Inputs		Major outputs	
Description	Source	Description	Destination
a) Server checks that the response is valid b) The server presents the appropriate transaction options	Server	The server checks that the received response corresponds to the issued challenge.	PC/Browser
<u>Major Steps Performed</u> 1. Response confirmed by the server 2. The server presents the customer with the account details 3. The presents the customer with the transaction options.			Information for steps Bank server Customer Coordinates

Appendix B: 4 shows a description of the processes involve after the response challenge is returned to the bank server for action. The server presents the customer with his or her account details together with transaction options such as funds transfer, standing order placement and statement printing.

Appendix C: Letter of Introduction from Strathmore University



FACULTY OF INFORMATION TECHNOLOGY

Our Ref.: FIT/MSIS/RL/16/45

16th March, 2017

To whom it may Concern:

Re: Esther Omondi Akinyi - 083419

This is to confirm that the above named is a student at Strathmore University pursuing *Master of Science in Information Systems (MSc.IS)* since May 2014.

Esther is a research scholar who is currently in her 2nd (final year) of study and is doing a research pertaining her masters degree which is entitled: **Near Field Communication Model for Transaction Authentication in Online Banking.**

This research being mandatory requirement towards successful completion of her studies, it would be great if you accord Esther the necessary support that she may need from your organization to enable her complete this task.

Any assistance accorded her shall be highly appreciated.

In case you would wish to clarify any issues with us, please feel free to do so.

Yours faithfully,

Brebner Momanyi (Mr.)
Administrator, Faculty of Information Technology.
bmomanyi@strathmore.edu