St. Mary University Graduate Studies

Security Issues in Mobile Banking Service in Commercial Bank of Ethiopia

By

Liya Areda

Advisor

Zemenu Aynaddis (Asst.Prof)

A thesis submitted to the school of Graduate Studies of St. Mary University in partial fulfillment of the requirement for the degree of Masters in Business Administration

Jul,2024

ADDIS ABABA

CERTIFICATE

This is to certify that the thesis titled "Assessing Security Issues in Mobile Banking Service in Commercial Bank of Ethiopia: " was submitted to St. Mary University for the award of the Degree of Master of Business Administration (MBA) and is a record of genuine research work carried out by Mrs. Liya Areda under our guidance and supervision.

This thesis has not been submitted to any other university or institution for awarding a degree or certificate.

Main Adviser’s Name   Date   Signature

________________________   ___________________   ______________________

Co-Advisor’s Name   Date   Signature

________________________   ___________________   _________________

DECLARATION

I hence declare that I completed my thesis named " Security Issues in Mobile Banking Service in Commercial Bank of Ethiopia: ." under the guidance and supervision of Asst. Professor Zemenu Aynaddis.

This thesis is not submitted for a degree or diploma to any university or organization. It is original.

Researcher’s Name Date Signature

St. Mary University Graduate Studies

Thesis Title

Security Issues in Mobile Banking Service in Commercial Bank of Ethiopia

By

Liya Areda

APPROVED BY BOARD OF EXAMINERS

Dean, Graduates Studies Signature

-------------------------------- --------------------------------------

External Examiner Signature

---------------------------------- ---------------------------------------

Internal Examiner Signature

----------------------------------- --

Acknowledgements

I'd want to use this opportunity to express my heartfelt gratitude and appreciation to everyone who helped me with this study. First and foremost, I'd like to thank my advisors, Asst. Professor Zemenu Aynaddis, for his help and engagement in improving my thesis. Second, this thesis would not be possible without the cooperation of CBE staff and my manager, Meron Umer, in order to collect the necessary data. As a result, I am deeply grateful to every one of them. Finally, I'd want to express my heartfelt gratitude to all of my friends and partners who have helped me in various ways.

Abstract

The mobile banking services is one of the newly introduced services designed to enable customers transact 24 hours in a day and seven days a week without the need to go to the bank's counter. The major challenges for the adoption of mobile banking technologies are customer concerns about security therefore the major objective of this study is, to assess current security practices and customer protection of mobile banking service in Ethiopian banks .Using a descriptive study, this study collected primary data from 235 respondents from the banking sector in Commercial Bank of Ethiopia. The respondents were selected using a purposive sampling technique. It was concluded that making information available would increase the number of customers using M-banking. Nowadays, mobile gadgets are an essential component of an individual's daily life. People can conduct financial transactions utilizing their mobile devices, which might introduce security threats and problems to mobile banking.

Consequently, CBE use M- banking to deliver its banking services and it is needed to enhance security issues for becoming safer and more trusted, the research recommended the M-banking app should have a minimum four-digit PIN, multi-factor authentication, and a two-step security mechanism. It should have a 2-5-minute session, a minimum active time of six months to a year, and daily verification codes. To improve security, provide unlimited verification codes for blocked apps, identify reasons for blockages, and check for fraud activities. Use encryption, SHA2 or SHA3 hashing algorithms, and set a timetable for app updates. After identifying by discussing the mechanisms to solve the problems, recommendations are discussed which aim to increase security challenges for CBE M- banking apps as a recommendation.

Key Words; Mobile Banking, Security issues and Customer protection

ACRONYMS

ATM	Automated teller machine
E-Banking	Electronic banking
ICT	Information communication technology
M-Banking	Mobile Banking
NBE	National Bank of Ethiopia
SMS	Short message sending
POS	Point of sale
USSD	Unstructured Supplementary Service Data
APK/APP	Application
NIST	National Institute of Standards and Technology
IBE	Identity Based Encryption
AES	Advanced Encryption Standard
PIN	Personal Identification Number
OTP	One Time Password

List of Tables

Table of Contents

CHAPTER ONE

1. INTRODUCTION

1.1 Background of the study

Banking is mostly a technological and mathematical in nature. As a result, it is well suited for digitization; nevertheless, its wide use and culture prevents banks from adopting technological innovation fully as needed to thrive in the digital economy (Alex Lipton & Pentland, 2016). Traditional banking activities and financial services that were previously are only available physically and the customers are inside at bank branch to seek banking services. But now such banking services have been digitized (or moved online) via digital banking services Digitalization allows banks to take customer service to the next level while also allowing for higher automation and cost efficiencies Essentially, digitalization transforms bank from product providers to continuous contextualized service providers, assisting consumers in better understanding their financial and commercial affairs and making better personal decisions.

However, there are few problems to becoming truly digital. It requires banks to operate a digital stack that is real-time, open and integrated, enabling banks to offer the right services and content with in a secure way. That is the digital banking services can integrate with third- parties, it brings security challenges to maintain the right channel at the right time and with the ability to fulfil all orders and enquiries instantly. In our country, Ethiopia banking services are adopted and provide services through private and governmental bank organizations from those Commercial Bank of Ethiopia (CBE) is one of the oldest public banks established in 1942 as a State Bank. Since the CBE has gone through different reforms and mergers coming out as one of the most reputable and biggest commercial banks in Ethiopia. To serve customers, CBE provides its services through digital banking such as online banking (Mobile Banking and Internet Banking), card banking ATM and POS), and Agent Banking (CBE Birr).

In this study we are focused on M-banking of CBE. Currently mobile phones' usage is highly elevated in the current era compared to their usage a decade before in our country Ethiopia, the numbers of mobile phones users are higher than the number of bank accounts holders. Due to such high usage level, most business organizations, the entertainment industry, banks, the education sector, and almost all fields turn towards mobile phone adaptability. People use mobile phones for shopping, transferring money, and getting various services (Waqas & Rasool, 2021). Due to that, currently almost all banks are facilitating customers to use mobile phone to get banking services.

But using digital technologies like mobile devices for financial issues strong security is needed. Because, strong security and privacy measures are critical to expanding and developing various kinds of financial products. For a person who has been living their entire life with structured financial institutions, falling victim to a security failure may permanently divert them from that particular bank service (Castle, et al., 2016).

Currently, we are focusing on Mobile banking (M-banking) channels services security as part of our study assessment. It uses Unstructured Supplementary Services Data (USSD) and application (app) based channels to deliver M-banking services for its customers.

USSD is a real-time session-oriented technology, used to provide mobile based network and banking services without Internet using USSD codes over Global System for Mobile Communications (GSM) channel (Krithiga, Lakshmi, & Ranjan, 2017). For banking services using USSD, the Mobile Network Operator (MNO) is used as an interface between the customer and his respective bank. USSD is a user interactive menu driven, cheaper and faster solution and is better than SMS with respect to cost, security and channel usage. It is platform independent, and it can be available in multiple languages and does not require any software to download. USSD is considered as a better choice for non-smartphone users of rural community to avail network services and bank payment solutions. In USSD decryption algorithm is installed at the server side. The system uses encrypted messaging protocols with deniability guarantee and message level secrecy (Krithiga, Lakshmi, & Ranjan, 2017). Therefore, the intruder cannot able to read the SMS or access it. To achieve this, symmetric encryption and identity-based encryptions are used.

Certificate Authority, key exchange sessions are failed, because of considering the cost using multiple SMS on a GSM network on a single transaction. USSD based CBE M-banking system working easily by dialing *889# through Ethio-telecom.

App based M-banking is taken into account to be one of the most necessary mobile commerce apps. Currently CBE has such types of apps to operate transactions in current market. It enables the customer interacts with a bank via a mobile device, such as a mobile phone or personal digital assistant (PDA) by downloading apps into their smartphone or tablet, allowing them to access their bank account with just a few clicks.

For these reasons, we consider security and privacy issues are essential issue for our bank (CBE). Because, when customers track their account through USSD and Mobile app channels, many customers and the bank itself have faced security challenges for operating banking services through those channels. Due to this, we are motivated to study ana assess the security issues of Mbanking channel services of CBE.

1.2. Statement of the problems

Security is the main issue for M-banking services (Castle, et al.'2016) and must developed when transaction is conducted between bank and the customer's mobile phone. In banking services like M-banking, improper identification, authorization and insufficient security awareness can lag the mechanism of system security and can be the source of vulnerabilities for customers or banks when they are access M-banking (Krevatin & Ivan, 2010).

Currently M-banking has security challenges which can lead loss of assets or transactions when customers are using it (Frimpong, Kwaku, & Ahenkora., 2012). This denies the banks valuable information for conducting cost benefit analysis for adopting the technology. To overcome such types of problems various researchers like (Muhammad, Ganesh, & Sankar, 2011) conduct researches on security issues of M-banking system focused on authentication method, (Al.Delaye/ &Shaymaa, 2022) study about mobile app security and (G.Ramesh and Kifle Berhane, 2016) study security protocol and cryptography that guarantees provision of confidentiality. However, as CBE also used those mechanisms to make its M-banking channel system more secure still there is a security problem to make the system more vulnerability.

To overcome such kind of problem; this study, assess security issues to fill the gap by examining the current risks facing in M-banking channels among the CBE, and recommending various strategies that would minimize M-banking risks of CBE to run its business in a safe way.

1.3. Research questions.

To gain a comprehensive understanding of the phenomenon under investigation, and to be able to provide a sufficient justification for answering that question, the following questions needs to be addressed. Based on the problem stated in this study, the research develops the following research questions.

1. How does technological trends affect the security of mobile banking service: in the case of CBE Kirkos District?
2. How effective is the current security protocol of mobile banking service: in the case of CBE Kirkos District?
3. How informed is the Customer awareness on the current security protocols of mobile banking service: in the case of CBE Kirkos District?
4. Is the current IT infrastructure of CBE is well equipped to counter the current security treats of mobile banking service?

1.4 Objectives

General Objectives

The objective of this study is to assessing and identifying security issues of M-banking of CBE, **..**

Specific Objectives

To achieve the general objective, we assess the following specific objectives.

1. Evaluate the technological trends affect the security of mobile banking service: in the case of CBE Kirkos District.
2. Evaluate how effective is the current security protocol of mobile banking service: in the case of CBE Kirkos District.
3. Assess How informed is the Customer awareness on the current security protocols of mobile banking service: in the case of CBE Kirkos District.
4. Evaluate the current IT infrastructure of CBE is well equipped to counter the current security treats of mobile banking service.

1.4. Significance of the study

The study has great significance for the organization of CBE. CBE s a commercial and governmental institution, it need greatest security for improving its trust and privacy for running its business effectively As, this study can identify security gabs and issues on online banking services (M-banking) of CBE and this can help to the organization to fill its gab and build its greatest security system to delivery of its service on M-banking channels. Such types of findings with its corresponding solutions can help for CBE to build highest trust on the customers and this can also lead to run its business insufficient and safe way for achieving its vision.

1.5. Scope of the study

The scope of this research is limited on conducting Assessment of the security issues in mobile banking service: in the case of CBE Kirkos District. From M-banking Services the research will focus on Security Protocol, Security Issues, Current IT infrastructure of CBE and the awareness of the customer on the security protocols placed. With the limited time and resource that the research will focus only on Commercial Bank of Ethiopia Limited to Kirkos Districts.

1.6. Organization of the research report

This study is organized into five chapters. In the first chapter, the general background of the study, statement of the problem, research questions, general and specific objectives, significance of the study, scope and limitations of the study were included. In the second chapter, review of related literature was incorporated. In the third chapter, the methodology part of the study. In the fourth, chapter the result & discussion were presented. Lastly in the fifth chapter, conclusion & recommendations of the study was presented consecutively.

Chapter Two

2. Literature Review

2.1. Theoretical Review

What is mobile banking?

Mobile banking allows its users to conduct financial transactions through mobile devices such as mobile phones and tablets. It is a service offered by banks and other financial institutions that allow users to obtain account balances, pay bills and transfer funds on their mobiles. However, mobile banking is different from mobile payment. Indeed, the latter is a service that allows users to pay for a product or service using a mobile device. Paying for purchases doesn't require having a bank account. It is more often added to the phone bill or paid by cash to specific agents.

Accessing banking services on a mobile device give customers a high degree of freedom. Not only this, it also enables them to do their banking independently of their location and time. In traditional banking a customer needs to be present at one of the branches of a bank and has to take into account, at the opening hours the bank has established (imran, Ashraf, & EJM, 2012). This is enhanced through M-banking as is one of digital banking services.

The study by (Muhammad, Ganesh, & Sankar, 2011) proposed security issues in M-banking and its effect on customers. Its implemented model was based on identifying security risks in Mbanking and to provide and authentication method from M-banking transaction by using bio metric mechanism for the purpose of reducing risks of fraud. And the study concludes that finger-print mechanism is more suitable than other ordinary mechanisms like login using password mechanism. Even Short message service (SMS) and USSD were not designed to transmit secured data, the study in (G.Ramesh and Kifle Berhane, 2016) was described it Is widely used to exchange sensitive information between communicating parties like Hello Cash, Ethio Gebeta, CBE Mbanking, 8100, 8400 and so much more, Due to the vulnerable nature of SMS and USSD, the study (G.Ramesh and Kifle Berhane, 2016) were proposed an alternative solution that provides a clientserver SMS and USSD security protocol that guarantees provision of confidentiality, authentication, integrity, non-repudiation, and file compression security services. The study used hybrid cryptographic scheme which is based on the Identity Based Encryption (IBE) and Advanced Encryption Standard (AES) algorithms without key distribution servers and certificate authorities to achieve more robust functionality. In order to achieve all the goals, the study proposed an introduction of independent Ethio telecom mobile app, only for smartphones who involve in the E-commerce that Ethio Telecom has setup, which will serve as a secure SMS sending agent that encrypts and sends any SMS or USSD that involves any transfer of money.

The study by (Leili & Massoud, 2016) was to review different methods of authentication in Mbanking and achieved an advanced authentication system to increase security required for mobile devices and the model with layers two security. The study was used PIN (personal identification number) code, ID / password, fingerprint and one- time password token for authentication methods. The study was focused on M-banking benefits, architecture, vulnerabilities, and different protocols of M-banking and proposed method which was more secure for M- banking system. The method had two security layers which are and proposed method which was more are Authentication and. Authorization. In addition, for preparing the security of the Network Layer, their method would authorize the Message format, which is encrypted with 'SHA-256 format. The study by (Al.Delayel & Shaymaa, 2022)deals about Mobile app security (the security layer) which is one of the most important features for the developer and users of mobile-apps. Despite all the security measures in an M-banking app, there might be a lot of vulnerabilities which affect the bank and users of the app. Due to this, this study was showed that many users of the M-banking app are not feeling safe to use it and it might put them at a risk because all of their financial information saved on the mobile device. Like any other apps, M-banking apps have various vulnerabilities hat might refer to using a Wi-Fi connection and different operating systems which affect the security methodology on each mobile OS and implies that the metrics used to evaluate the security awareness by the end user remains unquantified.

The study in (Yildirim & Varol, 2019) deals about the security threats and security measures in mobile and online banking systems The study identifies device network, and data center are the three groups of mobile threats. The study also considers what important measures to be taken for security risks and recommend using Encryption and digital certificate, logging information with Password requirements/restrictions, Session management and Two-Factor Authentication. The study also in identifies using Virtual Keyboard as weakness for security models in mobile banking and suggested using OTP to increase the security off M- banking.

(Tsai & Zhuang, 2012) Informed that for raising the security of M-banking, some banks adopt the one- time password (OTP) to remedy the possible M- banking stealing risk. In order to provide a reliable and secure M-banking process without decrease the convenience concurrently, (Tsal & Zhuang, 2012) aware using aware using one-time password (OTP) and personal biometric have been combined using with personal identification number and password for verification while using M-banking.

As is known that android with the highest market share and it can limit the access of apps to android features through permissions. Due to this (Cho, Han, & Seo, 2013) study Investigated and analyzed the condition of use of permissions of banking apps, which handle the most sensitive data and prepared the basic data for the preparation of countermeasures by analyzing its potential risks. Obviously, misuse of permissions can might cause serious impacts on the system and other apps. Consequently, using dangerous permissions may cause serious damages when apps were repackaged into malicious apps, which could easily avoid the user's notice. Therefore, the study informs that it is necessary to deals direct or indirect security systems through the restrictions or guides on developing the banking apps.

Based on the principles of information security (Nie & Hu, 2008) presented, issues of information security of M-banking and discussed the security protection measures such as: Encryption technology, identity authentication, Infrastructure (WPKI) technology for the problem of Virus attacks, Information leakage, loss and distort and incomplete Information.

The study by (Eyob Ketema, 2020) Was deals about that e-service quality dimensions are significant forerunner to customer satisfaction, from the perspective of security, reliability and ease of use that can have great influence on e-service quality. The study assesses the dimensions which are perceived critical by the Abyssinia Bank customers. The parameters like: reliability, efficiency, security, responsiveness, empathy, and ease of use were found to be positively influencing Abyssinia banks m-banking customer satisfaction. Thus, the study recommends that Abyssinia bank management as a service provider should pay attention to the identified dimensions specifically on ease of use and reliability of m-banking services while devising e-banking strategies to provide high service quality (security) and satisfaction to its customers.

Looking the M-banking system of some other private banks in Ethiopia like Abyssinia, Buna and awash bank, there are some situations to make them more secure than our bank (CBE). When we look Abyssinia bank (B0A), it is much more secure when we compare with CBE M-banking systems. Its authentication method is much strong. Because when customers want to login, the system obligates that the user/customers must enter OTP which is send from bank through SMS text and also does not accept password character without their combination.

Buna bank M-banking app channel also is not easily reverse engineered. Even when we reverse the M-banking app of Buna bank, data of codes are encrypted and the database classes are not seen. Sor it is difficult to find important data from the reversed code. Not only has this, Awash Bank M-bank app channel also hid the database classes from the client side This implies that, it is best practice. Because, in case of our bank CBE, the M-banking app is easily reversed engineered and we can see the database classes.

2.2. Trends in mobile banking

The introduction of the Internet has completely changed the way the financial services sector operates, giving companies access to new markets and methods for providing round-the-clock consumer care. Online banks, online brokers, and wealth managers that provide individualized services are just a few of the new companies in the financial services market that have been brought about by the capacity to conduct financial transactions online. Nevertheless, their share of the market is still quite small. The mobile and wireless sector has been one of the fastest-growing in the globe over the past few years, and it is currently expanding quickly.

A survey conducted by financial firm Celent predicts that by 2010, 35% of households with internet banking would utilize mobile banking, up from less than 1% at the moment. The number of calls to bank centers via mobile devices is expected to reach up to 70%. Users will soon be able to pay at actual points of sale using mobile banking. By 2010, "mobile contact less payments" will account for 10% of the market for contactless payments. Many people think that those who use mobile phones have just recently begun to fully exploit their data capabilities. In Europe, where mobile phone adoption is quite high (at least 80% of users use one), and in Asian nations like India, China, Bangladesh, and the Philippines, where mobile infrastructure is relatively superior than fixed-line infrastructure.

Financial organizations interested in providing value-added services now have access to enormous marketplaces. Banks may provide their clients with a multitude of services via mobile technology, including the ability to transfer money while on the go, check stock prices online, and even trade stocks while stuck in traffic. Mobile banking will be the "killer application" for the upcoming generation of mobile technology, predicts German mobile provider Mobilcom

2.3. Benefits of Mobile Banking

Benefits to Customers

The emergence of the online banking revolution has had a tremendous impact on general banking clients.

a) An online account makes a banking customer's account very accessible.

b) Customers can manage their accounts remotely from their home or workplace by using mobile banking. It is no longer necessary to visit a bank in person for any kind of financial activity.

c) Paying utility bills is made easier with the use of mobile banking. It does away with the necessity of waiting in line to pay your bills.

d) A single phone can provide most, if not all, of the services that are typically offered by the neighborhood bank.

e) Mobile banking is largely to blame for the sharp increase in the use of credit and debit cards. A customer can shop globally without any need for carrying paper currency with him.

Benefits to Bank

In addition to banking clients, Pallab S. and Munish M. (2013) have noted that the expansion of mobile and online banking infrastructure has shown to be very advantageous for banks and bank organizations as a whole for the following reasons:

a) The idea of mobile banking has greatly aided banks in keeping an eye on their particular overhead and operational expenses.

b) Banks are now more competitive as a result of the growth of mobile banking. Better opportunities and paths were made available for banking activities as a consequence.

Since the bulk of records under an e-banking setup are retained electronically, mobile banking has secured transaction transparency and made significant progress toward eliminating the paperwork requirements.

d) The network of traditional bank branches is noticeably inferior to the reach and delivery capabilities of mobile-enabled institutions.

2.4. Adoption of Mobile Banking

A significant body of research on mobile financial services has been produced during the last ten years. According to Hoehle and Huff (2009), the majority of these studies employed research methods and frameworks that have long been employed in the IS field. Information systems academics seem to embrace the Technology Acceptance Model (TAM) (Davis, 1989) the most out of all the models that have been suggested. TAM is adapted from the Theory of Reasoned Action (TRA) (Ajzen & Fishbein, 1980). According to the TAM, a user's desire to use a new information system is influenced by their views about it, which in turn determines whether or not the user adopts the system. The TAM goes on to say that the differences in users' intents may be largely explained by two beliefs: perceived utility and perceived ease of use. A significant body of research on mobile financial services has been produced during the last ten years. According to Hoehle and Huff (2009), the majority of these studies employed research methods and frameworks that have long been employed in the IS field. Information systems academics seem to embrace the Technology Acceptance Model (TAM) (Davis, 1989) the most out of all the models that have been suggested. TAM is adapted from the Theory of Reasoned Action (TRA) (Ajzen & Fishbein, 1980). According to the TAM, a user's desire to use a new information system is influenced by their views about it, which in turn determines whether or not the user adopts the system. The TAM goes on to say that the differences in users' intents may be largely explained by two beliefs: perceived utility and perceived ease of use.

According to Davis (1989), future study on technology acceptance should consider the impact of other variables on utility, simplicity of use, and user acceptability. As a result, perceived ease of use and perceived usefulness may not completely reflect behavioral intents to use mobile banking, prompting the search for other predictors of mobile banking adoption. Rogers' (1983) Diffusion of Innovation Theory provides insight into the acceptance of innovative technologies. Rogers (2003, p.175) identified five perceived features of innovation that influence favorable or unfavorable attitudes: relative benefit, compatibility, complexity, trialability, and observability.

2.5. Mobile banking in Ethiopia

According to Ethiopian history, the country's first bank, the Bank of Abyssinia, was created in February 1905 under the reign of Emperor Menelik II. In 1931, the Bank of Abyssinia was dissolved owing to foreign management dominance, and the Bank of Ethiopia was founded. However, due to a lack of trained staff in the country, foreigners continued to run the bank. The Bank of Ethiopia was superseded by the State Bank of Ethiopia shortly after the war against Italy. The latter was Ethiopia's first bank, wholly managed and owned by the government.

Meanwhile, a number of international banks had established branches in the country, with the majority of them seeking control of the country's economy. The State Bank of Ethiopia gave rise to the current Commercial Bank of Ethiopia (CBE) and National Bank of Ethiopia (NBE).

However, with the current government's takeover in 1991 and the subsequent promotion of private investment, a number of private banks formed in the country's financial industry. As a result, Monetary and Banking Proclamation No.83/1994, as well as Licensing and Supervision of Banking Business No.84/1994, established the legal framework for banking investment.

The Commercial Bank is essential to providing financial services to a large and varied population in Ethiopia. In line with the nation's attempts to close financial gaps, mobile banking services are being introduced, providing banking services to both urban and rural locations Economic development is thought to be accelerated by mobile banking; nevertheless, the effective deployment of these services is highly dependent on the security and reliability of the digital channels.

Security Issues with Mobile Banking: With the Commercial Bank of Ethiopia branching out into mobile banking, security issues arise that demand attention. Numerous security risks, such as identity theft, illegal access, and data breaches, can affect mobile banking services. Building and sustaining client trust, protecting financial information, and guaranteeing transaction integrity all depend on identifying and resolving these issues.

2.6. Evolution of mobile banking in commercial bank of Ethiopia

As of the end of May 2016, Ethiopia has 16 commercial and two state-owned banks in operation. Ethiopia's banking system remains undeveloped despite fast growth following financial deregulation. Checks are mostly used by government institutions, non-governmental organizations, and a few commercial firms. Commercial banks in Ethiopia continue to provide the same services and operate in the same manner as in previous decades. Deposit mobilization, credit distribution, money transfer, and safe custody are typical banking tasks performed by Ethiopia's state and commercial banks. Ethiopian banks struggle to provide exceptional customer service, provide customizable solutions, and stand out in a market saturated with similar offerings.

The evolution of mobile banking services in the Commercial Bank of Ethiopia (CBE) is likely to be characterized by a series of technological advancements, policy changes, and customer adoption patterns Commercial Bank of Ethiopia has been implementing various strategies to enhance its mobile banking services. These include the early adoption of basic mobile banking services which allow customers to check balances, view transaction history, and receive SMS notifications. As technology advanced, the bank expanded its offerings to include transactional services like fund transfers, bill payments, and mobile recharges. A dedicated mobile banking application was developed to enhance the user experience and improve security measures. 'The bank also integrated advanced security measures such as multi-factor authentication, biometric recognition, and encryption protocols to protect customer data, The bank has also expanded its mobile banking services to include internet banking, allowing customers to access their accounts across different digital platforms. It has also launched initiatives to reach unbanked or under banked populations through mobile channels. Collaborations and partnerships with mobile network operators and fintech companies have been made to expand the mobile banking ecosystem. Continuous technological upgrades and regulatory compliance are also essential to the bank's success. The bank may have conducted educational campaigns to raise customer awareness about the benefits and security features of mobile banking services. Future developments may involve exploring emerging technologies like artificial intelligence, block chain, and enhanced data analytics to further improve and innovate its mobile banking offerings.

According to the Newsletter released in 2012 by Making Finance Work for Africa, Ethiopia's financial sector is tiny and heavily influenced by the state. Public banks make up 67% of total deposits and 55% of loans and advances. The government regulates lending, interest rates, and owns the largest bank, Commercial Bank of Ethiopia (CBE), which accounts for over 70% of the sector's total assets as of April 2012. The Central Bank, the National Bank of Ethiopia, controls all foreign exchange operations and oversees all foreign exchange payments and remittances. In June 2011, Ethiopia had a private credit to GDP ratio of around 9%, lower than the sub-Saharan African average of 30%.

2.7. Mobile banking Risk Assessment

Mobile banking is a subset of mobile financial services that involve the use of mobile devices for transfers, marketing, banking, and payments. This study focuses on mobile banking due to the unique risks faced by financial institutions offering this service. Mobile banking is an emerging Information and Communication Technologies (ICT) element that has changed the operations of the banking sector. It can be classified into Short Message Services (SMS) Banking, Application (Software) oriented, and Browser (Internet) based models.

Banks are introducing m-banking to take advantage of high mobile phone penetration worldwide, particularly in Africa. However, in developing countries like Sub-Saharan Africa and North Africa, there are often obstacles to the adoption of mobile banking technology. These obstacles can be attributed to facing events or difficulties that hinder the adoption of certain technology or those contrary to it. For example, 80% of adults in Sub-Saharan Africa have no formal accounts, while 60% in North Africa have no.

To mitigate risks associated with mobile banking, bank management should complete a risk assessment based on bank-specific factors. This includes understanding the network architecture, mobile banking technology solution(s), mobile banking application design, features, threats, wireless transmission protocols, data storage and processing, and methods of attack. Additionally, they should identify controls to prevent attacks and/or data loss. By addressing these challenges, banks can effectively manage the risks associated with mobile banking and ensure the safety and effectiveness of their products and services.

2.8. Mobile Banking Security in Developing Countries

As mobile banking has advanced, it has created both new security challenges and revolutionary prospects for financial inclusion in these nations. Differentiated socio-economic environments, low digital literacy, and limited technology infrastructure all contribute to unique security considerations.

1. **Limited Infrastructure**: The dependability and security of mobile banking transactions strong building developing nations' difficulties in building strong telecommunications and internet infrastructure.

2. **Digital Literacy**: The population's varying degrees of digital literacy can result in security problems like vulnerability to phishing attacks or insufficient knowledge of safe transaction procedures.

3. **Device Security**: Because older mobile devices and feature phones are more common in some poor countries, there may be security risks because these devices may not have sophisticated protection.

4. **Regulatory Obstacles**: Emerging regulatory frameworks in poorer nations may make it difficult to enforce strict security requirements for mobile banking services.

5. **Impact on Financial Inclusion**: Although mobile banking promotes financial inclusion, trust building among unbanked populations many of whom are unfamiliar with digital financial services requires a high level of security.

2.9. Security concern in mobile banking in commercial bank of Ethiopia

Regarding mobile banking security issues in the context of the Commercial Bank of Ethiopia, it's critical to take a number of possible dangers and preventative actions into account.

CBE provides services through digital banking such as online banking (Mobile-banking and Internet banking), card banking (ATM and POS), and Agent Banking (CBE Birr) Currently, we are focusing on M-banking services security as part four assessment provided by CBE. During assessment I have identified some security gaps and I stated the vulnerabilities and our recommendations to fill the gaps as mentioned below

2.9.1. Identified vulnerability Issues on CBE M-Banking app without tools

As customers used M-banking in CBE and applying manual assessment on M-banking app, we had seen some security gaps which an bring high vulnerabilities issues. Some of them that we were identified are explained below.

1. Short PIN Length

personal identification number (PIN) is a relatively short typically 4-8 digits) numeric string that is used as a password to authenticate a user to a device in many electronic financial transactions (Menezes 1997) PIN are usually issued in association with payment cards and may be required to complete transaction and used to add additional security to the electronic transaction process. CBE M-banking uses a PIN to prove that customers have the right ta access to their data.

The issue that We identified is weak PIN. Weak PIN/ password is often cited as one of the most serious threats to M-banking system security. As a result, this can lead to vulnerability issues. It may be guessable or open to brute force attack

we have tested the PIN security of CBE M-banking apps in both android and IOS, while the PIN security of the IOS is good but in the case of Android OS, the PIN security of the system is very poor and easily vulnerable to fraud and brute force attack as it allows only single digit PIN even though the minimum secured PIN digit should be at least 4 digits. Not only this, but also the app does not allow PIN more than 4 digits in both android and IOS. In case of USSD the system also does not allows for users to use PIN length more than 4 digits

2. unlimited verification code for Blocked apps

when the app has been blocked the reason for blocking is not seen on the system at branch, whether the customer performs malfunction or not. Though when the customer arrives at the bank for the verification of his app, the bank employee has no mechanism to identify the reason or the blockage. Unlocking Customer mobile application without identifying the reason of the lock can lead to suspicious activities.

3. No restriction on Activation and verification codes

The verification code and activation code can be sent to the customer without restriction, which means there is no daily limit. This helps the intruder to perform malfunction during the time to activate the app repeatedly.

4. **The app active period without activity**

When a customer loses his device, the app remains active until he customer reports it missing. not only this, the customers are not sed the M-banking app channel for a long period of time, the app to remain active for an extended period. This may cause that create expansion of chances that the intruder to enter the internal network and make unlawfully activity. In general, this means that Fraudsters could see customers' idle accounts as a perfect cover to hide their own actions.

5. **long session of the app**

A session is the amount of time in which a user is actively engaged with either an app in the foreground or with an open website.

In the mobile ecosystem, a session begins when the app is opened in the foreground and ends when it goes into the background with no events occurring during a predetermined time window, dependent on the mobile measurement provider.

Session timeout is a fairly popular option that needs to be used carefully. It is used to determine how long a device may remain authenticated on a switch port before it must perform authentication again.

In the case of the CBE M-banking app, the session time-out is too long, which can lead t external persons performing financial transactions if the customer's mobile device is active. That is if there is no session security, no limit on app exposure when a user leaves the mobile device unattended for a while still logged in, and there is also risk of attacks, such as when one customer attempts to use another customer's session

6. **Insufficient knowledge of M-banking users**

In our country Ethiopia, it is known that most people are very far from technology products and they are not skillful to manipulate those technology products. Due to that, the customers of M-banking users are not fully aware about how to use the system and what kind of event make their system to be vulnerable for attackers. This leads to that the customers can be easily vulnerable by social engineering attacks. As a result, the customers may blame the bank (CBE) and dis-trust it and start to leave from the bank (CBE). Not only this, to give awareness how to use M-banking, there is no delegated person to show customers who have not sufficient skill on using M-banking.

2.10. Technological Trends and Security Implications in mobile banking Security

The field of mobile banking has experienced a major evolution in technological trends, bringing with it both benefits and concerns related to security. The use of distinct biometric IDs for biometric identification and the integration of AI for fraud detection and risk assessment through machine learning and artificial intelligence are two prominent themes. Block chain technology is being investigated for transparent and safe transactions; nevertheless, scalability and regulatory uncertainty remain obstacles. Mobile banking is being made easier by the Internet of Things (IoT), but there are more attack surfaces and security mechanisms that are required as a result, although 5G technology is being used for quicker and more dependable mobile communication, its enhanced encryption also improves network security.

Although contactless payments and mobile wallets are becoming more and more common, there is a chance that fraudulent transactions might occur due to device theft or unwanted access. Although cloud computing is being utilized for processing and storing data, worries regarding data security and privacy in cloud settings still exist. Virtual assistants and chatbots are being used for customer service, but there is a chance that they might be misused or accessed without authorization. Although Near Field Communication (NFC) and QR codes are utilized for smooth transactions, there is a chance that they may be tampered with. The trend is toward continuous authentication, which improves security by constantly confirming user identification and striking a balance between security and user ease. Lastly, sophisticated security measures that improve user identification and authorization are being created for mobile banking apps.

CHAPTER THREE

3. RESEARCH METHODOLOGY

3.1. Research Design

Research design is a blueprint of a scientific study. It includes research methodologies, tools, and techniques to conduct the research. helps to identify and address the problem that may rise during the process of research and analysis.

As a result, the research used a descriptive research methodology to examine the security issues in M banking service evaluation. The information was gathered from 235 sample workers who are now employed by the Commercial Bank of Ethiopia in eighteen branches located in Addis Ababa Kirkos district.

3.2. Research Approach

Both qualitative and quantitative methods I were used in this study (mixed method approach). The core claim of a mixed methods approach is that, in comparison to either quantitative or qualitative data alone, the integration of both types of data offers a deeper knowledge of a study problem. Procedures for gathering, evaluating, and combining quantitative and qualitative data in a single research or in a multiphase series of investigations are known as mixed methods designs (John W. Cresswell, 2014). Therefore, the research would guarantee the strength of the findings towards its purpose and aid in generalizing to the full population by implementing the mixed method technique.

3.3. Data collection methods

A survey research design was selected for this study, and data was gathered using both closed- and open-ended questions. The validity of the survey results hinges on whether the sample size used to gather the data is large enough to account for the population and free from bias.

3.4. Sampling Design

The Target Population of this study will be Commercial Bank of Ethiopia .employees that are currently working in the mobile banking security services and customers who are using the service.

3.5. Target Population

According to the Commercial Bank of Ethiopia .Human Resource Report, there are currently 1514 employees working in 49 branches that are under the district's management in Addis Ababa City. Thus, the 569 employees who work in this district made up the study's target population. 35 employees from the Sarbet branch, 38 from the Kirkos Kebele branch, 49 from the Gofa Sefer branch, 50 from the Senga Tera branch, 31 from Populare branch, 24 from Abinet branch, 12 from Tekaegeno branch, 19 from Pushkin branch, 24 from Kera branch, 15 from Tegbared branch , 43 from Gofa Gebril, 23 from meshualkiya, 18 from mechare, 32 from lideta mariam ,18 from Africa mnged , 45 from gofa mazoria ,55 from temenja yazi, 38 from stadium branch are the employees used as the target population in the respective branch.

3.6. Sampling Frame and Sampling

Sampling Frame is list containing all sampling units is known as sampling frame consists of a list of items from which the sample is to be drawn. (Chittagong-4203, Bangladesh). However, sampling location is a place where a research is conducted. In this research, source of materials consisted of 235 clerical employees who are working in different branches under the kirkos District.

3.7. Sampling technique

Sampling is the process of selecting a sufficient number of elements from the target population so that by studying the sample, and understanding the properties or the characteristics of the subjects, the research is to generalize the properties to the population elements. The research has employed judgmental sampling technique to select sampling location, which is .and research participants as representative of commercial bank of Ethiopia for the study.

3.8. Sample Size Determination

The researcher used a sufficient sample size to enhance the study's reliability and findings, considering factors like the target population's size, research purpose, population variability, confidence, and precision in sampling.

Yamane's 1967 sample size determination formula, a significant contribution to Japanese statistics, was used to determine sample size when the population is finite and known. Yamane also recognized that for large target populations, his sampling method with an error of 5% and confidence coefficient of 95% would estimate the true population value within the range of precision, with 95 out of 100 samples having the true population value within the precision range. As the result, the researcher has determined the total sample size as follows

Where;

- n is the sample size,

- N is the target population size, and

- e is 5% the level of precision.

- 95% confidence level

$$n = \frac{N}{1 \pm N(e)^2} = \frac{569}{1 \pm 569(.5)^2} = \frac{569}{570 * 0.0025} = 235$$

The sample size was calculated as 235 clerical staff working at .using the formula above. Kothari (1990) reports that the questioners were distributed to the 18 branches using proportional allocation, which was based on the established sample size. 235 participants were given questionnaires, which the researcher collected in full.

3.9. Source of Data Collection

The sources of the data were both primary and secondary. Both closed-ended and open-ended questionnaires were used to gather data from the primary sources. On the other hand, books, various published and unpublished journals, manuals, reports, research papers, and online sources were used to gather secondary data.

The research collected data from both primary and secondary sources to understand the concept of CBE service accessibility. Primary data was collected through questionnaires, which were cost effective and time-efficient. The structured questionnaires, which included both close and open ended questions, were used to gather relevant information. Secondary data sources included published and unpublished materials such as company manuals, reference books, company reports, annual reports, National Bank reports, and journal articles. These sources helped fill knowledge gaps and provide a better understanding of concepts, definitions, and theories related to CBE service accessibility.

The researcher developed a study questioner based on literature on security issues in M-banking services. The four-page questionnaire was written in English, allowing easy comprehension for clerical employees. The first section required respondents' demographic data, while the second section focused on security issues in M-banking service questions, including both closed-ended and open-ended questions. The questionnaire was designed for easy comprehension and response.

3.10. Data Analysis Method

The research collected and analyzed surveys using SPSS 20 and provided appropriate interpretations. Descriptive statistics included frequencies, percentages, and tables, and the data was cleaned, arranged, and analyzed.

3.11. Validity and Reliability

Validity is the degree to which a measurement tool accurately measures what it is supposed to measure. It is used to evaluate the findings' accuracy from the perspective of the participant, research, or readers' narrative. In this study, the content validity of the research questions was examined to ensure high quality. Ass.pro Zemenu Aynaddis confirmed the questioners by examining the propriety of the questions and measuring scales. Peer discussions with scholars and specialists, including Yegzeru Belete, the Manager of digital banking at Kera branch CBE, were conducted to verify the questions' phrasing, length, structure, and clarity. This test provided valuable feedback to help the research change some of the questions.

Reliability and accuracy are correlated, and the Cronbach alpha coefficient is a measure of reliability. It is commonly used to assess the internal consistency or dependability of an instrument. Reliability is considered good when it exceeds 0.80, acceptable when it falls between 0.70 and

0.80, and terrible when it falls below 0.60. Cronbach's Alpha was calculated using a 5-point Likert response scale for each statement in the study.

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.836	.819	24

Table 1. Cronbach's Alpha result

The research Questioners were developed from related studies and conceptualizing based on research questions and objectives, and hence the questioners are consistent with the objective of the study and are also reliable.

3.12. Ethical Consideration

The strict regulations and source of direction for the researcher on ethical problems will be the research code of ethics. As a result, the respondents' private values will remain confidential. Respondents will not be asked for their names, phone numbers, or exact addresses in order to protect the privacy of their personal data. Moral reflection

The strict regulations and source of direction for the researcher on ethical problems will be the research code of ethics. As a result, the respondents' private values will remain confidential. Respondents will not be asked for their names, phone numbers, or exact addresses in order to protect the privacy of their personal data.

CHAPTER FOUR

4. RESULTS AND DISCUSSIONS

4.1. **Overview**

The study's primary goal was to look into security concerns with Commercial Bank Ethiopia's mobile banking service in the Kirkos District. As a result, the final conclusions and the methodology used to arrive at them will be covered in this chapter. The descriptive analytic techniques used in the statistical methods of analysis comprised frequencies, percentages, means, and standard deviation.

In the instance of Kirkos district, the statistical analysis was conducted using the Statistical Package for Social Science (SPSS version of 20.0) to evaluate the security concerns of mobile banking service in CBE. To make the analysis easy to understand, tables, graphs, and charts were also used. 235 questionnaires in all were given to the professional respondents in the sample for Commercial Bank of Ethiopia .in eighteen selected Addis Ababa city branches. Sarbet branch, Kirkos Kebele, Gofa Sefer, Senga Tera, Populare, Abinet, Tekaegeno, Pushkin, Kera, Gofa gerbil , mechare, lideta mariam, Africa mnged , gofa mazoria , temnja yazi , stadium ,meshualikiya and Tegbared branch are the names of the branches.

By mid-March 2024, the researcher had made a significant effort to gather all 235 questioners from all branches and respondents. There was a 100% response rate overall. Because of this, the number of questionnaires that were collected provides the basis for this research's analysis. Apart from the survey questionnaire, the researcher examines certain bank papers that are accessible concerning CBE .m banking sector.

The research findings are connected to the outcomes that were developed to evaluate the potential, strength, and driving force behind security vulnerabilities in mobile banking services. These issues were identified and carefully examined based on specific measurement components.

4.2. Demographic Information of the Respondents

The study conducted a descriptive analysis of demographic data collected from M-BANKING users using a questionnaire. The analysis revealed the demographic profile of respondents, including educational level, gender, age, and working experience, and was conducted using SPSS.

The results are presented in Table 4.2.

Variable	Category	Frequency	Percentage
Gender	Female	104	44.3
	Male	131	55.7
	Total	235	100
Age	18-25	127	54.0
	26-35	93	39.6
	36-50	15	6.4
	51-65	0	0.0
	≥ 66	0	0.0
	Total	235	100
Educational level	Diploma	9	3.8
	BA	174	74.0
	MA	52	22.1
	Total	235	100
Work experience	1-3 years	87	37.0
	4-6 years	112	47.7
	7-10 years	28	11.9
	≥ 10 years	8	3.4
	Total	235	100

Table2 . Demographic characteristics of the respondents

(Source: Primary Data, Collected by the Researcher, 2024,)

Overall, 131 (55.7%) of respondents are male, while 104 (44.3%) are female respondents. This indicates that the overall number of male responses outnumbers female respondents. Furthermore, the survey found that male and female workers are not proportional in the banking business.

Regarding the respondents' ages, 127 (54.0 %) fall between the ages of 18 and 25; 93 (39.6 %) fall between the ages of 26 and 35; 15 (4.4 %) fall between the ages of 36 and 50; and the ages of 51 and 65 and ≥ 66 years, where there are no respondents. The bulk of responders to this survey are young and in the security services age range.

In terms of educational level, 9 (3.8%) respondents have a diploma, 174 (74.0%) have a BA (BSC), and 52 (22.1%) have a Masters of Art degree. According to the poll, most bank employees possess degrees. The majority of responders, 226 (96.1%), possess a first degree or above, while only a few hold a diploma. This indicates that they offer greater service to the tested district.

The bank's respondents have varying levels of work experience: 87 (37%) have 1-3 years, 112 (47.7%) have 4-6 years, 28 (11.9%) have 7-10 years, and 8 (3.4%) have more than 10 years. The majority of respondents have 4-6 years of experience in a bank or business banking operation (BBO level), while the fewest have worked for 10 years or more. This bank lacks experienced employees, hindering its competitiveness in Ethiopia's banking business. Additionally, there is limited talent and capacity sharing practice.

4.3. Descriptive statistics analysis of security issues in mobile service

In this part, descriptive statistics in the form of frequency and percentage were presented to illustrate the level of agreement of the respondents in CBE .after collecting and encoding the data using SPSS. The responses for the variables indicated below were measured on five-point Likert scale with: 1=strongly disagree, 2= disagree, 3 = neutral, 4= agree and 5= strongly agree.

S.N	ITEM	1		2		3		4		5	
		F	%	F	%	F	%	F	%	F	%
1	Absolute trust in the security features	20	8.5	40	17.0	40	17	112	47.7	23	9.8
2	Money laundering and other financial crimes are difficult to commit using mobile banking;	17	7.2	41	17.4	79	33.6	77	32.8	21	8.9
3	Users have faith via M-banking technology supplied by banks	7	3.0	33	14.0	88	37.4	88	37.4	19	8.1

4	The customer assumes no risk while using M-banking technology	21	8.9	32	13.6	80	34.9	86	36.6	16	6.8

Table 3. M-banking security service with regard to technology

(Source: Primary Data, Collected by the Researcher, 2024)

According to the survey, 57.7% of participants have confidence in the security features of M-banking Security services, compared to 17% who have no opinion and 25.5% who disagree about the technology's potential for strength. The majority of respondents think that M-banking technology makes it difficult for criminal activities like money laundering. Consumers who use m-banking technology have a trust rating of 107 (45.5%), 88 (37.4%) are neutral, and 17% do not believe that m-banking security services can be as strong as they could be. While 80 respondents (34.0%) are neutral and 22.5% of customers think that the delivery of m-banking security services at CBE is at risk, many respondents (42.8%) think that m-banking technology can make services deliverable and accessible without danger.

Based on the above table, it can be concluded that M-banking Security service's potential strength effect is that it uses technology to reduce criminal activity, increase user trust, and help users become more confident about security issues while posing little danger.

4.3.2 M-banking security service with regard to Organizational factors

S.N	ITEM	1		2		3		4		5	
		F	%	F	%	F	%	F	%	F	%
1	A highly developed level of customer awareness regarding mobile banking security services;	18	7.7	36	15.3	90	38.3	71	30.2	20	8.5
2	Technical and administrative proficiency in the use and utilization of mobile banking technology;	13	5.5	26	11.1	80	34.0	95	40.4	21	8.9

3	Minimal implementation costs for m-banking, including those associated with software, hardware, networks, and reorganization	10	4.3	38	16.2	66	28.1	90	38.3	31	13.2

Table 4. M-banking security service with regard to Organizational factors (Source: Primary Data, Collected by the Researcher, 2024,

Based on the above table, it can be seen that 91 respondents (or 39%) agreed that customers' awareness of m-banking security service is well developed, 90 respondents (or 38.3%) were neutral about m-banking security, and 54 respondents (or 23%) disagreed. This suggested that CBE .'s clients are aware of its online banking offerings.

Regarding the adoption and usage of m-banking technology, 116 respondents (or 49%) agreed, 80 respondents (or 34%) were neutral, and 36 respondents (16.6%) disagreed. This suggests that the majority of respondents possess the administrative and technical skills necessary to deploy and operate m-banking technology within CBE Kirkos District.

Of the respondents, 121 (52%) agreed that the cost of m-banking implementations is cheap at CBE Kirkos District, 66 (28.1%) were neutral, and 48 (20.5%) disagreed. This suggests that the expenses associated with implementing m-banking service items, specifically the cost of ICT equipment, networks, software, and reorganization, are not very high.

4.3.4 M-Banking security Service with Regard to Environmental Factor

S.N	ITEM	1		2		3		4		5	
		F	%	F	%	F	%	F	%	F	%
1	The government's job is to encourage consumers' willingness to	15	6.4	32	13.6	79	33.6	88	37.4	21	8.9
2	Establish more favorable legal regulations for mobile banking;	11	4.7	22	9.4	85	36.2	93	39.6	24	10.2

3	Provide adequate network infrastructure and internet-related support services;	24	10.2	38	16.2	74	31.5	78	33.2	21	8.9
4	Acquire computer literacy experience;	15	6.4	39	16.6	82	34.9	80	34.0	19	8.1
5	No ICT infrastructure restrictions;	18	7.7	43	18.3	71	30.2	81	34.5	22	9.4
6	In the context of m-banking, have strong enough coordination, contact, and cooperation between banks and other decision-making centers;	9	3.8	46	19.6	88	37.4	73	31.1	19	8.1
7	Existence of financial networks connecting several banks;	16	6.8	31	13.2	69	29.4	89	37	30	12.8
8	Regular blackouts have not occurred;	14	6.0	38	16.2	78	33.2	77	32.8	28	11.9
9	Banks are required by law to utilize a uniform software platform;	11	4.7	31	13.2	85	36.2	84	35.7	23	9.8

Table 5. M -banking security service with regard to Environmental factors

(Source: Primary Data, Collected by the Researcher, 2024)

The table shows that 39% of respondents agree that there is sufficient internet-related support service and networking infrastructure for M-banking security services in CBE Kirkos District. However, 74.5% of respondents are neutral, and 26.4% disagree. The role of the government in supporting M-banking is also considered, with 46.3% agreeing that government policies and strategies play a significant role in expanding security services.

The legal framework on M-banking is considered conducive, with 49.8% agreeing and 36.2% neutral. Computer literacy experience for M-banking security services is also considered, with

42.11% agreeing and 34.9% neutral. There is no ICT infrastructure limitation for M-banking security services expansion in CBE Kirkos District.

Coordination, interaction, and cooperation between CBE .and decision-making centers are considered strong, with 39.2% agreeing and 37.4% neutral. A strong financial network linking different banks is also agreed upon, with 50.7% agreeing.

Frequent power disruptions are not considered as a concern, with 33.2% neutral and 22.2% disagreeing. Most respondents believe that there is no frequent power fluctuation, resulting in smooth operation of M-banking security services in commercial banks in Ethiopia Kirkos District.

The legal platform to use common software platforms is also considered, with 45.5% agreeing and 36.2% neutral. Overall, the majority of respondents agree that a legal platform is necessary for Mbanking security services implementation, operation, and improvement.

4.3.5 The Assessment of m-banking security service in operational benefits.

S.N	ITEM	1		2		3		4		5	
		F	%	F	%	F	%	F	%	F	%
1	Less paperwork;	17	7.2	17	7.2	24	10.2	131	65.7	46	19.6
2	Cheaper per transaction.	11	4.7	11	4.7	69	29.4	112	47,7	32	13.6
3	Enhance banking industry productivity;	11	4.7	12	5.1	54	23.0	116	49.4	42	17.9
4	Improve the production of foreign currency	6	2.6	21	8.9	54	23	114	48.5	40	17
5	Improve dependability and transaction error-free;	7	3	17	7.2	66	28.1	99	42.1	46	19.6

Table 6. M-banking security service in operational benefits (Source: Primary Data, Collected by the Researcher, 2024)

According to the above table, 177 respondents, or 85.3%, agreed that m-banking reduces paper work; 24 respondents, or 10.2%, were indifferent to this idea regarding m-banking products; and 34 respondents, or 14.4%, disagreed with this statement regarding the operational benefit of m-banking products and services. This suggests that the majority of respondents thought m-banking reduced the amount of paperwork.

The majority of respondents (144 out of 144) believe that M-banking reduces transactional costs, increases productivity in the banking industry (67.3%), and increases foreign currency earning (65.5%). Additionally, 61.7% of respondents believe that M-banking services and accessibility increase reliability and reduce errors in transactions. This indicates that M-banking services and accessibility support banking operations, reducing paper work, enhancing productivity, enhancing foreign currency generation, and increasing reliability and error-free transactions. The results suggest that M-banking services and accessibility provide operational benefits in the banking industry, such as reduced paper work, enhanced productivity, and increased foreign currency generation. The majority of respondents also believe that M-banking services and accessibility can lead to more efficient and reliable banking operations. Overall, the results suggest that M-banking services and accessibility are essential for the success of the banking industry.

CHAPER FIVE

5. SUMMARY, CONCLUSION AND RECOMMENDATIONS

This section presents the major findings, conclusions drawn and recommendations suggested based on the study.

5.1 Summary of the Major Findings

The research will assess security vulnerabilities in mobile banking services at the Commercial Bank of Ethiopia, with a focus on the Kirkos area. 235 employees from 18 branches completed open and closed-ended surveys. The majority of responders were men, aged 23 to 30, with BA degrees and 1-5 years of job experience. According to the findings, technology plays an important role in promoting m-Banking security by increasing consumer confidence, reducing criminal activity, creating trust, and lowering risks. It also raises client awareness of new products, lowers infrastructure costs, and encourages qualified experts to deploy e-banking in the banking business. The government's involvement in fostering customer willingness is also emphasized. M-banking lowers paperwork, has low transaction costs, boosts productivity, and improves dependability and error-free.

5.2. Conclusions

In simplest terms, M-banking is a technology that allows clients to engage with a bank via their mobile devices and perform financial transactions. In this study, we investigate the security issues of CBE's M-banking and make recommendations to address the security holes.

The study offered numerous ways for identifying security gaps or weaknesses and announcing study recommendations for CBE M-banking. The existing authentication mechanism is inadequate, and it should be replaced with two-step verification or multi-factor authentication techniques with a strong PIN to increase security, trust, and convenience of use. The app channel also employed poor hashing techniques and was readily reverse engineered, making it accessible to hackers. The majority of M-banking customers are also unaware of how to utilize it and what circumstances render them vulnerable. This may be reduced by educating and advising clients through various channels. In the future, it would be preferable to introduce an M-banking app authentication technique that supports other types of characters rather than just PINs.

5.3. RECOMMENDATIONS

To enhance the security issues of M-banking of CBE we are going to suggest the following recommendations.

The redesigned M-banking app should offer a minimum four-digit PIN to protect against brute force attacks. Users can also establish more complicated PINs and modify password policies to match organizational requirements. Multi-factor authentication, including fingerprints, passwords, and face ID, can be utilized in CBE's M-banking. A two-step security mechanism should require account verification before logging in and verifying transactions.

One-time Password (OTP) is a secure method for securing accounts with two-factor authentication. It allows for fast and reliable account authentication, with high-quality service and the ability to select preferred channels and backups. CBE's M-banking app uses OTP for authentication and confirmation, providing an extra layer of security. The app should have a 2-5 minute session and be disabled if not used for at least six months to a year.

The text emphasizes the importance of providing daily verification codes and unlimited verification codes for blocked apps to protect users from intruders. It also suggests that apps should include security guidelines, such as proper password selection, regular data backup, and regular password changes. The app should also educate users about data security and the need to avoid suspicious requests and websites to prevent fraud. This will help users stay safe and secure on the app.

To ensure the safety of M-banking software, it is crucial to educate users and employees on the importance of using it safely. This can be achieved through training, knowledge sharing, and a designated person demonstrating how to use Fintech technologies. Many clients are hesitant to use M-banking due to their lack of familiarity with technology. To protect the app from reverse engineering, code containing database classes must be hidden or encrypted using methods like uploading confidential files to a server or using C/C++ programming language. The use of the strongest hashing algorithms, such as SHA2 or SHA3, can improve security. Additionally, a time table should be set when the app is updated to cross-check the completion of any updates.

REFERENCE

AI.Delayel & Shaymaa. (2022). Security Analysis of Mobile Banking Application in Qatar. arXiv e-prints.

Alex Lipton, S., & Pentland. (2016). Digital banking manifesto: the end of banks. Massachusetts Institute of Technology

Castle, Sam, Pervaiz, G., Weld, F., Roesner, R., & Anderson. (2016). Evaluating the security challenges of mobile money in the developing world. IEEE In Proceedings of the 7th Annual Symposium on Computing for Development, 1-10.

cho, T. Y, Han, & Seo, S.-H. (2013). Potential vulnerability analysis of mobile banking applications. IEEE International Conference on ICT Convergence.

Ebisa, B. (2020). Adoption and Challenges of Mobile Banking Systems in Ethiopia: The Case of Cooperative Bank of Oromiya. African Conference on Information A Systems and Technology.

Elkhodr, M., Shahrestani, S., & Kourouche, K. (2012). Proposal to Improve the Security of Mobile Banking Applications. Tenth International Conference on ICT and Knowledge Engineering (pP.260-265). Sydney, Australia: IEEE.

Eyob Ketema. (2020). The impact of M-banking quality service on customers satisfaction during Covid-19 lock down, The case of Bank of Abyssinia, Ethiopia. African Journal of Marketing Management, pp. 21-37.

Frimpong, Kwaku, & Ahenkora. (2012). Internet banking security strategy: Securing customer trust.". Journal of Management and Strategy, 3(4).

Rogers, M 2003, Diffusion of Innovations, 5th edition, New York: Free Press.

Kothari, C. . (1990). Research Methdology, methods and Techniques.

JOHN W. CRESWELL. (2014). Researchn Design qualitative, quantitative and mixed approaches.

G.Ramesh and Kifle Berhane. (2016). A Security Protocol for mobile-Banking and payment using SMS and USSD in Ethiopia. International journal of research and application, 3(10).

Imran, Ashraf, R., & EJM, m. R. (2012). Mobile Banking Security.

Krevatin, & Ivan. (2010). Biometric recognition in telecom environment. IEEE 14th International Conference on Intelligence in Next Generation Networks, (pp. 1-6).

Krithiga, K., Lakshmi, H. G., & Ranjan,). (2017). USSD Architecture analysis, security threats, issues and enhancements . International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS)IEEE.

Leili, N., & Massoud, B. (2016). A review of authentication assessment of Mobile-Banking. 7th Annual Information Technology, Electronics and Mobile Communication Conference, 1-5.

Menezes, A. P. (1997). handbook of Applied Cryptography. CRC Press ,Boca Raton, FL.

Muhammad, Ganesh, B., & Sankar. (2011). Trust and security issue in mobile banking and its effect on customers. sweeden: Blekinge Institute of Technology.

Nie, J., & Hu, X. (2008). Mobile banking information security and protection methods. IEEE International Conference on Computer Science and Software Engineering.

Tsai, C.-L., & Zhuang, D.-). (2012). Secure OTP and biometric verification scheme for mobile banking. IEEE Third FTRA international Conference on Mobile, Ubiquitous, and Intelligent Computing, pp. 138-141.

Waqas, & Rasool, J. N. (2021). Security in Next Generation Mobile Payment Systems: A Comprehensive Survey. IEEE.

Yildirim, & Varol, A. (2019). A research on security vulnerabilities in online and mobile banking systems. IEEE 7th International Symposium on Digital Forensics and Security (ISDFS), 1-5.

Appendix I

Questionnaire

St. MARY’S UNIVERSITY

SCHOOL OF GRADUATE STUDIES MBA PROGRAM

Dear Sir/Madam,

I am a graduate student at St. Mary's University in Addis Abeba, studying Master of Business Administration (MBA). Currently, I am conducting research on 'security issues in Mobile Banking service in commercial bank of Ethiopia: .'. This study aims to evaluate the present security issues of Mobile Banking Services in Kirkos district, Ethiopia.

The information you offer in this respect will be used solely for academic purposes; no individual replies will be identifiable, and the identities of those answering will not be disclosed to anybody. So, its privacy is virtually ensured. Your honest and insightful response contributes significantly to the quality of research outcomes.

Thank you in advance for your kind cooperation.

Liya Areda

Tel Phone +2519 66795676

General Instruction

This questionnaire contains two sections and 3 pages that will be expected to take approximately 10 to 15 minutes to complete. Please provide your responses to the questions based on the instructions under each section. If you have comments or if you want to provide further explanations, please use the space provided at the end of the questionnaire.

Please put the tick mark (√) on the appropriate space as per your choice for each closed ended question and the appropriate reason for open-ended questions.

Part I: Demographic profile of respondents

Please indicate the following by ticking (√) on the spaces in front of the response options:

1. Gender: Male ☐ Female ☐
2. Age: 18-25 ☐ 26-35 ☐ 36-50☐ 51- 65 ☐ ≥ 66 ☐
3. Educational level: Diploma ☐ First degree ☐ master's degree and above ☐
4. Working experience: 1-3 years ☐ 4-6 years 7-10 ☐ years above 10 years ☐

Part II: Research related questions

The following questions are presented on a five-point Likert scale. If that aspect is much better than you hoped it could be chosen 5 (strongly agree), if that aspect is even better. than you expected it to be choose 4 (agree) if that aspect were what you would like it to be choose 3 (neutral), you would like to choose 2 if it to be somewhat poor (disagree) and if that aspect is much poorer that you would like it to be choose 1 (strongly disagree).

Please put (√) in the place where the choice is appropriate for you.

Key: 5= Strongly Agree, 4=Agree,3= Neutral, 2=Disagree, 1=Strongly Disagree

No.	**Statement**	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
		5	**4**	**3**	**2**	**1**
Technological trends affect the security of mobile banking service						
1	CBE strives for continuous mobile Cyber & Engineering compliance for the field					
2	CBE employ latest Technological trends on mobile banking security service					
3	CBE have infrastructure to utilize and apply the latest security protocol on the field					
4	CBE provides and encourages biometric or multifactor authentications					
current security protocol of mobile banking service						
1	CBE Delivers convenient, safe banking experiences					
2	CBE Adopts modern user needs					
3	CBE provides and encourages biometric or multifactor authentications					
4	CBE have well developed security protocol for mobile banking service					
Customer awareness on the current security protocols of mobile banking service						
1	CBE have Well developed customer awareness about m-banking products					
2	CBE allows Personalized and customized mobile banking service					

3	CBE allows customer-centric and secured mobile banking experiences					
4	CBE advises customers best usage of Mobile banking					
current IT infrastructure of CBE						
1	CBE Uses mobile banking technologies build Certified Secure mobile banking apps					
2	CBE Build, monitor and respond in one mobile app defense platform					
3	CBE have a technical and managerial skills in implementation and of m-banking technology					
4	CBE have well developed IT infrastructure suitable for mobile banking service					

Part 2 . Open Ended Questions

1. Describe your bank's future security plans for mobile banking services.

____

2. How to evaluate the security technique used for mobile banking?

____

3. Describe the problem and problems that are impeding the security process?

____

4. How do you handle problems that impede the security process?

____

5. Is there a system in place to safeguard customers from fraudulent mobile banking activity?

____

6. What type of security risk occurred in the mobile banking service? How do I handle it? What methods have you used?

____

7. How do you determine the amount of customer service protection?

____