St. Mary's University

Faculty of Informatics

Department of Computer Science

ATM Security Framework for Ethiopian Banks

By

Yeshiwork Tefera

April 2019

ATM Security Framework for Ethiopian Banks

Thesis

by

Yeshiwork Tefera

to

Faculty of Informatics

of

St. Mary's University

In Partial Fulfillment of the Requirements

For the Degree of Master of Science

in

Computer Science

Advisor: Asrat Mulatu(PhD)

April 2019

ACCEPTANCE

Accepted by the Faculty of Informatics, St. Mary's University, in partial fulfillment of the requirements for the degree of Master of Science in Computer Science

Thesis Examination Committee:

_____

Advisor

Asrat Mulatu(PhD)

_____

Internal Examiner

_____

External Examiner

_____

Dean, Faculty of Informatics

Getahun Semeon(PhD)

April 2019

DECLARATION

I, the undersigned, declare that this thesis work is my original work, has not been presented for a degree in this or any other university, and all sources of materials used for the thesis work have been duly acknowledged.

Yeshiwork Tefera
Full Name of the Student

_____

Signature

Addis Ababa

Ethiopia

This thesis has been submitted for examination with my approval as advisor.

_____

Full Name of the Advisor

_____

Signature

Addis Ababa

Ethiopia

April 2019

ACKNOWLEDGEMENTS

Next to God, I would like to give special thanks to my advisor Dr. Asrat Mulatu, for always being there whenever I need help. The thesis would not have this shape without his professional inputs, criticism, guidance and support. And also, I would like to give special thanks to Ato Tewodros Mengistu for his start up comments support and encouragement.

I would also like to extend my special thanks to surveyed banks including Commercial Bank of Ethiopia and to those private bank staff members, who took their time and resources to answer our questions, offered their ideas and comments. I would like to say thank you all.

Last but not least, I would like to extend my thanks to all my families and friends for their support, encouragement and prayer not only during my thesis work but also all the way during my study.

Yeshiwork Tefera

ABSTRACT

Automated teller machine (ATM) security is the current issue throughout the world. ATM users increase every time because it is more convenient to use rather than to go to a branch. So, many banks, including Commercial Bank of Ethiopia, are trying to install ATM machines throughout the country to facilitate financial transactions. ATM machines are located in different areas which are suitable to customers to get the service anytime and anywhere. But this may cause various security problems. ATM threat can be divided in to three major categories. Those are logical threat, physical threat and fraud commonly known as skimming. On this study we tried to investigate these threats in the local context. Based on which we proposed an improved ATM security framework.

Our preliminary survey indicated that banks do not use procedures to secure their ATM machines. The main objective of this study is, therefore, to design an improved framework that is used to secure ATM machines and, any bank can use this framework to enhance its ATM security. To validate the framework MATLAB with specific scenarios that model common ATM tasks has been executed. The result show that on the MATLAB simulation on biometric (voice and finger print) measure uniquely identify high level of security which is by far stable and secure ATM system that of the current authentication system on practice.

Keywords: ATM Security Framework, ATM Skimming, ATM Security Threats, Banking Transactions

LIST OF FIGURES

LIST OF ACRONYMS

ATM	Automated Teller Machine
PIN	Personal Identification Number
SMS	Short Message Service
DoS	Denial of Service
EAST	European Association for Secure Transactions
ISP	Internet Service Provider
PCI PTS	Payment Card Industry PIN Transaction Security
PIC DSS	Payment Card Industry Data Security Standard
DNA	Deoxyribonucleic acid
MEMS	Micro Electro Mechanical Systems
HMM `	Hidden Markov Model
HSAP	High Security Alert Password
ARM	Advanced RISC Machines: one of CPUs
GSM	Global System for Mobile communication
AES	Advanced Encryption Standard
3DES	Triple Data Encryption Standard
NFC	Near Field Communication
NCR	National Cash Register
PSS	Premier Switch Solutions

Table of Contents

CHAPTER ONE

INTRODUCTION

1.1. Background

An automated teller machine (ATM) is an electronic banking outlet, which allows customers to complete basic transactions without the aid of a branch representative or teller. There are two primary types of automated teller machines. The basic units allow the customer to only withdraw cash and receive a report of the account's balance. The more complex machines will accept deposits, facilitate credit card payments and report account information. To access the advanced features of the complex units, one will usually need to be a member of the bank that operates the machine[1].In our country we do have the basic type of ATM machine which allow a customer to withdraw cash and a few complex ones.

According to Falaye.A in [36] the continuous advances in E-Payment technology characterized by a complex and competitive environment have brought huge impact on business operations and have in particular brought about a paradigm shift in banking operations. In a bid to catch up with global development, improve the quality of service delivery, and reduce cost of transactions, the application of information and communication technology concepts, techniques, policies and implementation strategies to banking services is now a subject of fundamental necessity and concern to all banks and indeed a prerequisite for local and global competitiveness in banking.

ATM is the modern and one of E-Payment technologies which is new to our country. The cash dispenser was born almost 50 years ago. The ATM finds its origins in the 1950s and 1960s, when self-service gas stations, supermarkets, automated public-transportation ticketing, and candy dispensers were popularized.

The first cash machine seems to have been deployed in Japan in the mid-1960s, according to a Pacific Stars and Stripes account at the time, but little has been published about it since.

In 1960, Simjian managed to influence a New York City bank to take a few of his automatic-deposit machines. So that customers could trust that they would see their money again, there was a microfilm camera inside the Bank graph that took a snapshot of every deposit. Customers received a copy of the photo as their receipt. Still, the Bank graph did not catch on. “The only people using the machines were prostitutes and gamblers who didn’t want to deal with tellers face to face,” Simjian explained, and there were not enough of them to make the machines a worthwhile investment.

In 1967, a Scottish inventor named John Shepherd-Barron was sitting in the bathtub when he had a flash of genius: If vending machines could dispense chocolate bars, why couldn’t they dispense cash? Barclays, a London bank, loved the idea, and Shepherd-Barron’s first ATM was installed in a branch on Enfield High Street not long afterward. Unlike modern ATMs, Shepherd-Barron’s did not use plastic cards. Instead, it used paper vouchers printed with radioactive ink so that the machine could read them. The customer entered an identification code and took her cash maximum of £10 at a time.

Today, there are almost 3 million ATMs around the globe [32]. Although use of the machines has declined in recent years, likely because more people make purchases using credit and debit cards instead of cash, the ATM continues to have a place in modern culture. Today’s machines sell everything from airline tickets to movie tickets to medicine.

Modern banking industry in Ethiopia, which was introduced in 1905 by Emperor Minilik II, has recently started a consolidation exercise by unifying the state owned commercial bank of Ethiopia with construction bank of Ethiopia that left the country with 18 banks out of 19 banks previously in existence. In a bid to ensure customer satisfaction Ethiopian Banks have invested greatly in the development of their Information Technology (IT) infrastructure and implementing the core banking solution which completely changes there manual work to automated systems that helped them to introduce various e-banking and e-payment systems for delivering a wide range of value added products and services.

In June 2009, the Ethiopian Banks have a total number of ATM machines which is not more than 48 in number as specified in the annual reports of the banks 2014/2015[2]. Ethiopia has currently about 1235 ATM terminals and more than 3100 POS machines deployed

throughout the country[2].With gradual growth since its introduction in 2001. The use of ATMs in Ethiopia has been increased in recent years, in commercial bank of Ethiopia alone. The number of ATM and visa card users in the year 2009/10 was 15,000 and in 2014/15 increased to more than 1,604,363[3].

The use of ATM is not only safe but is also convenient, This safety and convenience, unfortunately, has an evil side that do not originate from the use of plastic money rather by the misuse of the same. This evil side is reflected in the form of "ATM frauds" The problem of ATM frauds is global in nature and its ramifications have been felt in Ethiopia as well.

In November 2010, Four Nigerian Nationals Jailed in Ethiopia over ATM Fraud who withdrew more than one million Birr from other customers' accounts in one month[4].

In European, ATM Crime Report covering the first six months of 2015 EAST[5] has reported that ATM fraud incidents were up 15% when compared to the same period in 2014.

Security in the ATM Network is very necessary because it is widely spread in all areas such as financial, network administration and other important parts of financial network which requires very sensitive handling of transmission of data. Manipulating the transmitted data, spoofing and misuse of ATM channels would be very critical in accounting system.

Security protocols are applied on untrusted networks to enhance their safety. ATM networks are one of the typical networks that need a high level of security to prevent the attacker doing malicious activities. ATM communication consists of several phases, such as authentication and authorization. So, establishing a comprehensive security in ATM infrastructure needs a lot of concerns. Lack of security even in one of the phases can lead to massive security breach.

According to the last 2011 survey in 27 European countries[5] card skimming is still the most prevalent crime, however 61% of European countries reported a decrease due to use of anti-fraud devices and implantation of Europay, EMV(EuroayMasterCard and Visa) technology embedded in ATMs providing two factor authentication which drastically lowers the risk of stolen credentials.

In the US, ATM fraud is expected to increase; this is due to the transition to EMV standards in Europe, Asia, Latin America and Canada where EMV embedded chip cards are much more difficult to counterfeit than magnetic stripe cards available in US.

There are many kinds of ATM threats. In general we do have three ATM threat or vulnerabilities: those are; Physical attack is the actual break of an ATM, logical attacks are malware and fraud are what we commonly known as skimming.

1.2. ATM Systems

The ATM system was introduced with the main objective of providing banking services to customers after banking hours and during the weekends. Therefore the automatic teller machine should provide basics banking services which were already provided by a bank's teller during office hours.

An ATM is simply a data terminal with two input and four output devices. Like any other data terminal, the ATM has to connect to, and communicate through, a host processor. The host processor is analogous to an Internet Service Provider (ISP) in that it is the gateway through which all the various ATM networks become available to the cardholder (the person wanting the cash). Here it is parts of ATM machine. [34]

Here it is the principle behind the working of ATM. It communicates with the bank via Internet by means of wireless broadband or phone lines. When the customer inserts ATM card, it reads the information contained on the magnetic strip. The magnetic strip is the hard copy of customer's account information. It waits the customer to enter PIN once the PIN is verified the ATM communicates with customer's bank to access customer account information. Depending on customer transaction request, the ATM forwards the transaction request to the hits processor which in turn routes the request to cardholder's account. If the account balance request is placed, the host processor returns a printed receipt of the account information. If cash is requested, the machine goes through the same initial steps of communicating with the host processor. [34]

Host processor then creates an electronic funds transfer from the cardholder's account. After the creation of funds transfer the host processor sends approval code to the ATM to

dispense cash. According to [35] the cash dispensing system has an electronic eye that "counts" each note as it exits the dispenser. There is also a sensor that checks the thickness of the notes being dispensed. If two notes are stuck together, they are diverted to reject bin. Even the soiled or mutilated notes are also diverted to reject bin. A record is maintained for all the notes which is called journal. Here it is parts of ATM machine.

- **Card reader** - The card reader captures the account information stored on the magnetic stripe on the back of an ATM/debit or credit card. The host processor uses this information to route the transaction to the cardholder's bank.[35]
- **Cash dispenser -** The heart of an ATM is the safe and cash dispensing mechanism. The entire bottom portion of most small ATMs is a safe that contains the cash.[35]
- **Keypad** - The **keypad** lets the cardholder tell the bank what kind of transaction is required (cash withdrawal, balance inquiry, etc.) and for what amount. Also, the bank requires the cardholder's personal identification number (**PIN**) for verification. The PIN block is sent to the host processor in encrypted form.
- **Speaker** – The speaker provides the cardholder with auditory feedback when a key is pressed.
- **Display screen** - The display screen prompts the cardholder through each step of the transaction process. Leased-line machines commonly use a monochrome or color CRT (cathode ray tube) display. Dial-up machines commonly use a monochrome or color LCD.[35]
- **Receipt printer** - The receipt printer provides the cardholder with a paper receipt of the transaction.

Beside of the above ATM machine components, ATM manufacturer like Diebold and NCR are going to manufacture new ATM machine which includes finger printer for fingerprint scanner for authentication purpose.

Different ATM threats and vulnerabilities are increase now days. The next section describes about threats and vulnerabilities of ATM and type of ATM threat.

1.3. Threats and Vulnerabilities

Threat is a possible danger that might exploit a vulnerability to breach security and therefore cause possible harm [37] it is a potential violation of security.

Vulnerability is an existence of weakness, which can be exploited by a Threat Actor, such as an attacker, to perform unauthorized actions within a computer system [36] to exploit vulnerability; an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerability is also known as the attack surface.
ATM vulnerability mean weakness in the overall system which abuse the banking operation and allows an unauthorized user to have access to any other customers' account and perform financial operation using ATM for transacting from any other customer's account.

ATMs contain huge amount of cash and process sensitive customer data to perform cash transactions and banking operations. In the past, criminals mainly focused on physical attacks to gain access to cash inside an ATM's safe. They captured customer data on the magnetic strip of an ATM card with skimming devices during insertion of the card. These days, criminals increasingly use logical attacks to manipulate an ATM's software in order to withdraw cash or to capture customer data[6].

There are a variety of ATM attacks because it is such an attractive target. We cannot list all the types, but highlights some popular ones throughout the world. Generally ATM attack can be classified into three main categories. Those are logical threat, physical threat and fraud commonly known as skimming

1.3.1 Physical Attacks

Physical attack is related to ATM manufacturing defect or weakness leaving scope for attackers or hackers to make physical changes in the manufacturing of machine. It may be external attachment of external skimming devices to read the information and make a fake card or get the secure information using these external devices[7].

Attacks that result in the physical damage of the entire ATM or a component primarily focus on stealing cash from the safe.

Physical threats to ATMs occur on an individual basis, they represent perhaps the most direct threat to those who manage and operate ATMs. Physical attacks range from pure brute force attempts to rob the vault to higher-level threats in which criminals attempt to gain access to the terminal to load malware into a machine and perhaps the network, or reprogram the machine to change dispensing rules.

Burglary: Armed criminals force customers and employees to withdraw cash.

Brute force: Criminals attempt to steal cash by physically attacking the ATM. They use mechanical tools, torches and explosives to open the safe door or make an opening in the safe walls [8].

Removal: Criminals attempt to remove the ATM from its location by using a chain attached to it and pulling it with a truck or other large vehicle, such as a forklift or earth mover.

Ram-raid: The common method is physically removing ATM from premise with vehicle or heavy truck, and then steal cashes with opening safe by force. In UK, it was reported that on May 11th, Ram-raiders who stole a cash machine from a Bingley shop caused about £30,000 of damage after repeatedly driving a car into the shutters. The masked burglars towed away a cash machine using a 4x4 vehicle.

Explosive: Criminals use solid explosive materials or combustible gases to explode with intent of gaining access to the security enclosure. The most serious is explosive not only causes cash loss, but also facilities and environment damage or casualties[8].

Physical ATM security is important in cases where cipher keys exist in terminals. In the absence of physical security, an abuser may search for a key or substitute its value. To avoid such abuses, banks should preserve the integrity of non-secret parameters as well as the confidentiality of secret parameters. ATM security should focus on protecting ATMs from physical attacks. Modern ATM security concentrates on denying access to money inside the machine to a thief, by means of techniques such as dye-markers and smoke canisters. By setting access control, intrusion detection, security guards and by implementing central monitoring station we can enhance physical ATM security.

Bead on our surveillance from the above list of ATM attack is brute force is a common one for Ethiopia banks. This is happen when different politic cause occurred. On the

other hand attacker by observing the environment they will plug the USB flash and other dives to interpret the ATM machine functionality.

1.3.2. Logical ATM Security

Logical vulnerability relates to software weakness where a software attack can easily be performed, it may be use of some virus attack or malware attack. Logical weaknesses are used to steal sensitive computer information and details of ATM cards. The information gathered is used for duplicating a card i.e. for making a fake ATM card with all genuine information of the original ATM card.

ATM malware is designed to steal cardholder data and PINs or to withdraw cash[6]. Typically, malware hides in the system to remain undetected as long as possible. It impairs confidentiality, integrity and authenticity of transaction data for its particular intention. ATM networks are based on the Internet protocol and face the same attacks as other IP-related networks, e.g., denial of service (DoS), sniffing, man-in-the-middle attacks, or eavesdropping.

Communication between ATM and host can be used as entry point to launch remote attacks. Even network devices like routers and switches can be targeted. Logical security focuses on maintaining a secure network, protecting the OS and designing a system so that intruders cannot threaten cardholder's data and software components[6].

Logical Security Measures

Network plays a key role in the functioning of ATMs since a customer swipes their card, enters the PIN and details are then sent to the database for validation. Attackers usually intercept this information to perform logical frauds. The following logical security measures can help prevent such incidents:

1. Firewall
2. Effective tracking and monitoring system
3. Encryption technologies
4. Logical access control
5. Fraud detection system
6. Protection of communication

1.4. Types of ATM Frauds

Card and Currency Fraud

Card and currency frauds include direct attacks to steal cash or cards as well as indirect attacks to steal sensitive cardholder data that is later used to create fake cards for fraudulent withdrawals. The target of these attacks is a single ATM, which may be physically manipulated for skimming, card fishing and currency trapping[9].

Card Skimming

Skimming refers to the stealing of the electronic card data, enabling the criminal to counterfeit the card. Consumers experience a normal ATM transaction and are usually unable to notice a problem until their account is defrauded. This is the most frequent type of attack reported; the criminal uses devices (skimmers) to capture cardholder data from the magnetic strip. These devices can be installing over the top of the ATM's card reader sometime installed inside the ATM. [9]

Here, the installation by a criminal of a foreign device on an ATM to capture data from the magnetic strip of a customer's card. The card details and PIN are captured at the ATM and used to produce counterfeit cards for subsequent cash withdrawals.

Eavesdropping

By installing a forging device on ATM machine the criminal easily capture customer's data. This is typically achieved via a wiretap, sniffing the functionality of the card reader, or connection to a magnetic read head within the card reader. The defining characteristic of an eavesdropping device is the use of the legitimate card reading functionality of the card reader to capture the customer's card data. [9]

Cash Shimming

The criminal installs a foreign device on an ATM to capture data from the chip of a customer's card. The defining characteristic of a card shimming device is, therefore, the targeting of the data contained on the chip on the customer's card, typically by placement of the foreign device between the customer's card and the contacts of the card reader. The placement of a card shimming device by a fraudster enables a number of possible attacks such as capturing magnetic strip equivalent data, relay and other man in the middle attack.[9]

Card Trapping

Trapping is the stealing of the physical card itself through a device fixed to the ATM. In a pre-EMV or chip-and-signature environment, the PIN does not need to be compromised. Again, contactless capability can help. The card is the physically captured at the ATM, and PIN is compromised. Later the card is lost in each attack.

ATM Malware or Cash out Attack

Malware that takes control of the ATM cash dispense functions, thereby allowing the criminals to take out cash.

Cash or Pin Data Compromise

Malware are that intercepts card and PIN data at the ATM, further allowing the criminals to copy this to create counterfeit cards.

Keypad Jamming

The fraudster jams the 'Enter' and 'Cancel' buttons with glue or by inserting a pin or blade at the buttons' edge. A customer trying to press the 'Enter/OK' button after entering the PIN, does not succeed, and thinks the machine is not working. An attempt to 'Cancel' the transaction fails as well. In many cases, the customer leaves and is quickly replaced at the machine by the fraudster. A transaction is active for around 30 seconds (20 seconds in some cases), and he is able to remove the glue or pin from the 'Enter' button to go ahead with the withdrawal. The loss to the cardholder is, however, limited by the ceiling on withdrawals, and the fact that only one transaction is possible without swiping the card again and reentering the PIN.[9]

The above listed types of ATM attack are common throughout the world specially Card Skimming. Some countries try to protect those types of attack using different techniques like biometrics. When we come to Ethiopian banks they didn't have any techniques to secure their ATM machine if one of the above type ATM frauds occurs. So this paper proposes fingerprint and voice recognition techniques for our banks to secure the ATM machine.

1.5. Biometrics Techniques

Identification and verification of a person today is a common thing; a bank sector also uses this identification and verification of a person to protect customer data. So to do this authentication not only bank but also other industries are using a biometric method. Biometric

is the most secure and convenient authentication tool. It measures individual's unique physical or behavioral characteristics to recognize or authenticate their identity.

Common physical biometrics includes fingerprints, hand or palm geometry, retina, iris, and facial characteristics. From this biometrics we are using fingerprint and voice recognition for our ATM machines to improve authentication of customer.

1.5.1. Fingerprint Recognition

Fingerprint recognition relies on the imaging of the fingertips. The structure of a fingerprint ridge and valleys (minutiae) is recorded as a picture or digital example (a simplified information, minutiae based most of the time) to be more compared with different pictures or examples for authentication or verification. Among all the biometric techniques, fingerprint based identification is a well-known technique that has been used successfully in ATM user authentication. A fingerprint could be a set of skin lines, domestically parallel, named ridges and empty area between two consecutive ridges named valleys.

Fig. 1.1: Fingerprint Ridge and Valley

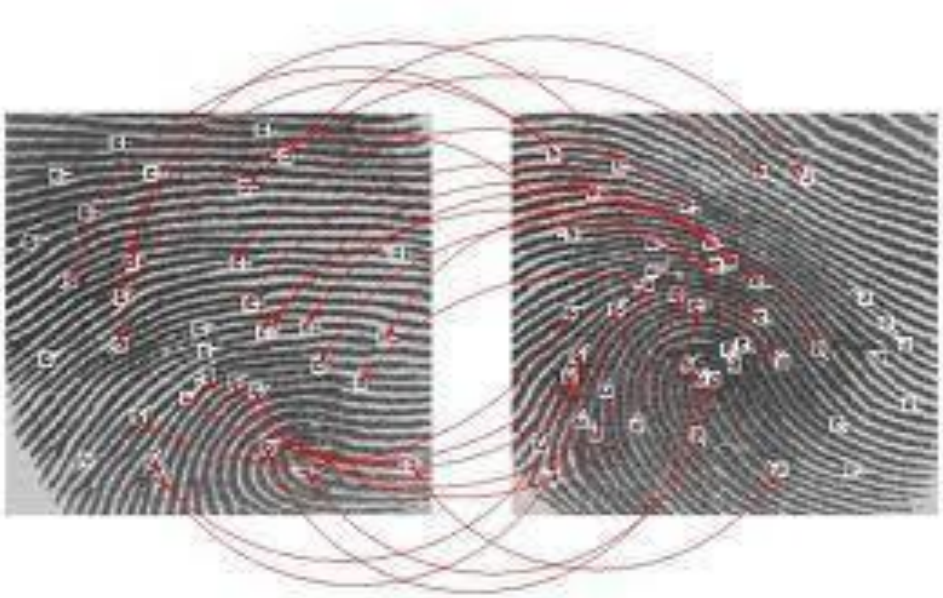

Fig. 1.2: Points Extracted from a Fingerprint

Fig. 1.2 shows points extracted from the fingerprint of a person. The pattern of extraction are enough and reliable fingerprint verification authentications in biometric method.

Fingerprint Scanner: A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching.

It supports wide range of fingerprint sensor interoperability giving you a freedom to select suitable sensor that most fits to your application. Furthermore, the fingerprint data for enrollment and verification are compatible among different sensors, even if they are based on different technologies. This feature of unification presents application manufacturers and system integrators with much more flexibility than ever before.

1.5.2. Voice Recognition

Voice recognition is the ability of a machine or program to receive or to understand and carry out spoken commands. It is generally regarded as one of the convenient and safe recognition technique. Voice verification combines behavioral and physiological factors to produce speech patterns that can be captured by voice processing technology.

In voice recognition systems, inherent properties of the speaker like fundamental frequency, cadence, nasal tone and inflection are used for voice authentication.

System require user to generate the voice sample at the time of creating account in bank. Then these data's are stored in authentication database. It work by analyzing the waveforms and air pressure patterns produced while a person talks. User speaks into the microphone. Microphone captures sound waves and generates electrical impulses and sound card coverts voice signal into digital signal.

1.5.3. Vibration Detection

To secure the ATM physically, vibration detection method is critical. Vibration sensor area unit currently conjointly fixed either within the ATM or premises housing the ATM. Vibration alarm activates once somebody attempt to cut causing vibration in the ATM machine and its premises for taking appropriate actions to defend the ATM from cutting and forestall the ATM machine from any sort of tampering with the machine.

The principle to operate vibration alarm system of the ATM is signal processing and analysis of the assorted onboard sensors then to require acceptable action within the event of a legitimate attack. Additionally, this unit features a range of dedicated inputs that support remote sensors that enhance and extend the world of coverage. Here it is some common cases for vibration.

VIBRATION: Attack by means of grinding, hammering, drilling, or thermal cutting device can trigger the VIB output.

1.6. Statement of the Problem

The problem of ATM frauds is global in nature and its consequences have been felt in Ethiopia as well. The well-known bank like bank of American in China, proposed solutions to secure their ATM machines mostly that focus on physical security also installed 80,000 biometric ATM machines. However in the case of Ethiopia banking ATM system that I identified there is no such uniform standard which is capable to challenge the level of threat that can occur during this time of era. Basically the current working ATM systems are magnetic or chip card system using a four digit PIN pass number. Both of these techniques are highly exposed to a potential level of threat based on the finding identified and stated on the survey.

Based on the finding on the research questioner the most common ATM problem in Ethiopia banks are related with a customer awareness level on how to handle and secure their ATM card, that mean the way customer handles their ATM card with that of PIN number and they may face ridiculous problem. The second problem that was identified during the survey and the research review technical issues on the four digits PIN and card are critical requirement to use ATM machine. Most ATM attacks seek out to obtain a customer's personal information, such as their card number and (PIN) attacker may use card skimmer device to skim the data from the card and use other type of fraud to customer using PIN and card.

Therefore this research intends to investigate in deep the current state of ATM security and propose an improved security framework that can secure ATM machine which fulfill a level of security demand for the period.

1.7. Basic Questions

The study's entire focus is to find answers for the bellow listed questions.

- What is the degree of vulnerability of ATM customer service channel?
- What are the potential threats and attacks of ATM services?
- How mature is user's awareness in regard to ATM security implementation?
- What factors affect the physical security implementation of ATM machines?

1.8. Objectives

1.8.1. General Objective

The main object of this thesis work is to propose a generic improved ATM Security framework for the banking industry in Ethiopia.

1.8.2. Specific Objectives

- To investigate the degree of user awareness with regard to ATM security implementation.
- To investigate the current ATM security mechanisms or frameworks.
- To examine the physical security of ATM machines.
- To examine current ATM frauds.
- To design an improved ATM security framework.
- To generate common usage scenario and validate them.

In view of this, the study will equip bank executives, policy makers of the banks and financial institutions and indeed security agencies with necessary information on ATM as a form of electronic banking with a view to making strategic decisions that would enhance effective product delivery to meet customer satisfaction, secure banking operations and improve bank efficiency in general. And also for those venders (for the manufacturer of ATMs) we contributed for our country by designing new framework that consist multilayered authentication techniques.

1.9. Organization of the Rest of the Thesis

This study is organized in seven chapters. These are:

Chapter One: introduces what ATM security is, how the ATM machine is work that mean ATM systems and ATM threats and vulnerabilities. This chapter also presents the statement of the problem and the objective of the study.

Chapter Two: is the part where literature on ATM security.

Chapter Three: this chapter presented research design and methodology which includes what research method was employed in this work selection of sample for the study, data collection techniques, and data analysis methods was stated clearly.About current statues of ATM security also presented in this chapter.

Chapter four: is the part where a new proposed ATM Framework clearly presented.

Chapter five: in this chapter we generated scenario for the proposed framework and also validate the proposed work.

Chapter six: is the part where a limitation and contribution were presented.

Chapter seven: concluding remarks and recommendations were made. And future possible study areas were also suggested.

CHAPTER TWO

REVIEW OF RELATED WORKS

In this chapter we review some related works which are done on ATM security. Most of the papers/suggest that the current authentication method is not sufficient to secure the ATM machines, which is the PIN and ATM card, like Jane [10] mentioned that this two factor authentication is not secure. Different researchers proposed various techniques to secure ATMs. Most of the researcher's center of attention was on biometric authentication techniques.

Muhammad Bello et al., in[11] put second level authentication mechanisms to secure ATMs. Second-level authentication sometimes known as two factor authentication or two step verification. This means that the user enters a verification code in addition to its username and password. Second level authentication is a security process that can be accomplished by utilizing either a mobile phone (SMS) or token device which provides a one-time password for transaction authentication.

The method adopted for this research was to develop an enhancement of the existing system by building an additional security mechanism on the existing system's security mechanism. The proposed system was found to be realistic and cost effective when compared to other proposed authentication mechanism for ATM transactions. But the drawback of this paper is that the customer always should have the cell phone with them because the system generate one time password and send to the customer cell phone.

The research works done by Deepa Malviya in[12]discussed about the survey on enhanced safety approach for ATM using face recognition technique. On this paper the researcher put an authentication method for securing ATM transactions and has been improved using biometric authentication techniques. It was face recognition from three different angles. The study aims to design a module of an ATM simulator based on face recognition from 3 different angles in order to minimize frauds associated with use of ATM systems. The system does not answer the question what if two people have the same face, like if they are identical twins?

PoojaMail et al., in[13] has proposed Multilevel ATM security based on two factor biometrics. They thought that ATM access is not securing enough using four digits PIN. They proposed new approach for existing ATM system for providing more security using biometric features which plays an important role because these are unique and not easily hack.

J.N.Oruh et al., in[10]proposed a three factor authentication technique. Two factor authentications are password (PIN) and smartcard (ATM card) which are currently used for banking transaction authentication. So he suggested that this authentication method is not successful to secure ATMs. In the current ATM system security can be breached when password is disclose to an unauthorized user or card is stolen by an impostor that a simple password is easy to guess by any impostor while difficult password may be snooped using sophisticated techniques. He suggested a biometric authentication (fingerprint) in addition to PIN number and card.

Three-factor authentication involves the use of three independent variables for authentication, which will normally include the following; Password (something known only by an individual i.e. password, pass phrase or PIN), ATM card (token held by an individual) Fingerprint (something the individual only, is). The use of three-factor authentication improves the security of any given system, making it almost impossible for attackers and hackers to break into the system without specialized aid.

Fakir Sharif et al., in[14] set two levels for securing ATM banking system. The first security level is done on the client side by providing biometric authentication scheme. The second level was using AES algorithm to secure the communication link between the client machine and the bank server. Their proposed system consists of a fingerprint-capturing device, which captures image of the client. Taken image is fed to the image-processing device within the ATM machine. The processed image is converted to 1024 bit of binary data which is the input data of the AES processor encrypting the data with the help of 4 digit decimal key that is provided by the user as password. The drawback of this paper is what if the customer fingerprint doesn't work, sometime some cutover does not get a fingerprint image when they scan their finger.

According to B.V. Prasan thiet al., [15]combine fingerprint and DNA for the enhancement of ATM System. DNA is uniquely identifying the person [15]. In this scenario

no need to remember the passwords and the reference DNA data will be digitized and converted to barcode by using barcode generator, which is stored back to the ATM card. This invention can identify the proper user of the ATM card by collating the measured DNA data and fingerprint captured by fingerprint scanner. The combination of finger print and DNA data gives more accurate and precise results than existing methods as ATM access with fingerprint. The combination of DNA barcode and fingerprint biometric authentication method is very effective in protecting information and it can be a resource in a large area of applications. Security issues related to previous methods can be solved using this technique. This limitation of this paper is the voluntariness of the customer to give the DNA data because of the lack of awareness.

Santhi B. et al., in [16] proposed a new authentication system by using hybrid technology for ATM security. On this study they compared biometric methods. Those are finger print, iris, face and voice. The objective of this work is to provide enhanced security to ATM by enhancing the already proposed biometric system and making it still secured by PII (Personal Identification Image) process. Based on their study biometrics is not enough to secure ATM machines and also they said a single biometric is not a security solution on its own. Two or more methods are to be incorporated to make it more efficient. But using biometrics such as iris identification, voice verification costs much and the maintenance will be difficult. According to [16] this makes the system more costly and complicated. Another biometric method for replacing the failure of one biometric makes the machine more complicated and cost factor is affected. The proposed algorithm provides two phase security and acts as a two tier security. User can't access others account as they have other's ATM card and knows the PII. A customer needs to have both a mobile phone and finger print too. Hence having a mobile device on hand is mandatory for such cases but the users might not have his device with him while accessing the ATM machine this can be commented as a limitation.

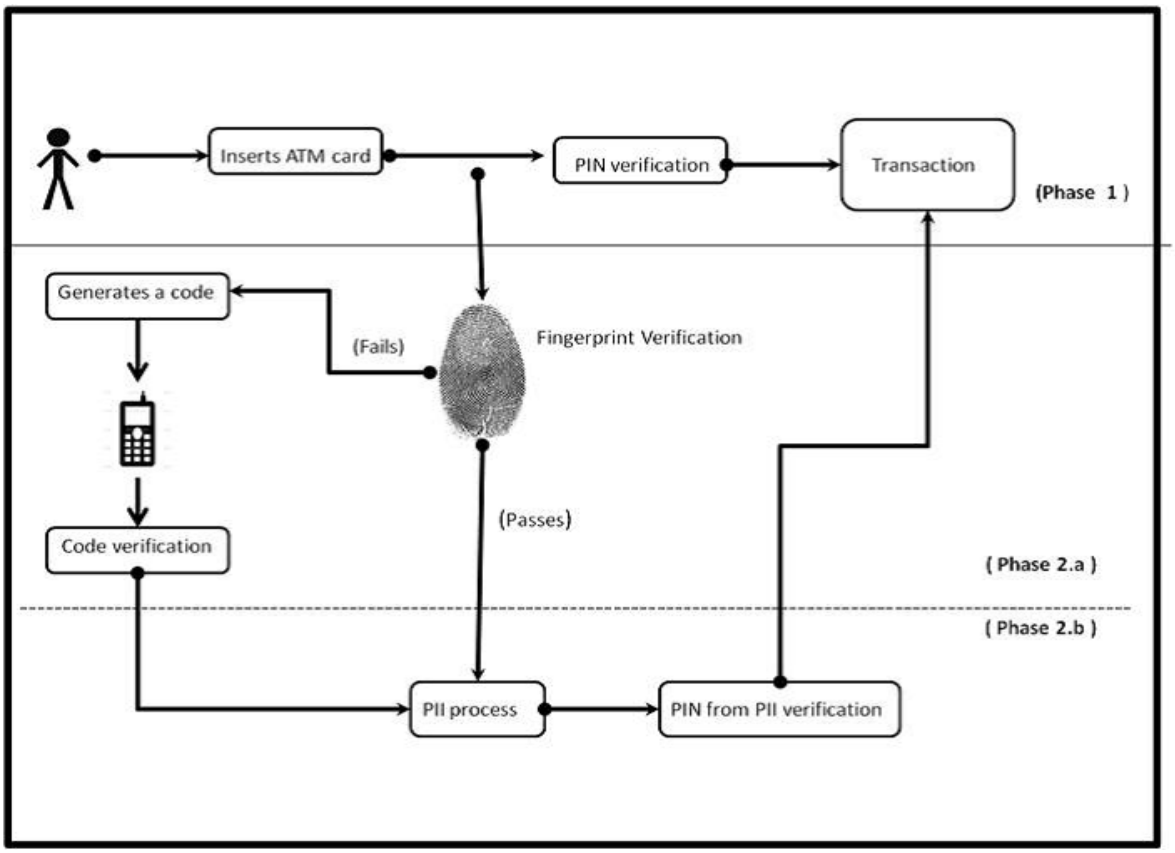

Fig.2.1: Work Flow Diagram [15]

S.P.Balwir et al., [17] in their paper stated secured ATM transaction system using micro controller.

The System uses serial communication with the computer to scan the data base of the card holder and automatically generates every time message to the mobile of the authorized customer through GSM module connected to a microcontroller 89C51. The RFID card reader is used as an identity for a particular user. If the identity (serial number of the tag) of the user is matched with the one already stored in this system, he gets immediate access through it and then the transaction is done .If the false identity is recognized then the card holder simply reply "ACTION'' then the transaction will stop and at that moment ATM door will be locked automatically by EM Lock and blow an alarm so the concerned authority can take some action. And also a message will be sent to a card holder along with the ATM machine by using GSM module.

The drawback of this work is, as we know ATM machines are placed at different areas when the ATM door locked automatically which authority is going to respond is not listed out in this work.

The researchers in [18]concentrate on the ATM security system. This paper has got the same method with that of S.P. Balwirand K.R. Katole[17].But the main difference is that whenever a thief enters and tries to touch an ATM forcefully, the movement will be observed by the MEMS sensor. While MEMS observe the movement it sends a request to the microcontroller. Microcontroller will automatically lock the door which is represented with the help of DC motor and send a message to the authority through GSM. It will produce sound with the help of buzzer to alert the security. At the same Microcontroller send the command to motor to close the door. When the switch is pressed from the outside then only door will be opened. The operation status will be shown on the LCD.

The researchers Vivek V. et al., in [19] tried to implement an advanced security model for ATM payment using Hidden Markov Model (HMM), which detects the fraud by using customers spending behavior. This Security Model is primarily focuses on the normal spending behavior of a cardholder and some advanced securities such as location, amount, time and sequence of transactions.

If the trained security model identifies any misbehavior in upcoming transaction, then that transaction is permanently blocked until the user enter High Security Alert Password (HSAP).

The main motivation of the researches in[20] is to secure the communication using secret sharing. As they said ATM networks are one of the typical networks that need a high level of security to prevent the attacker doing malicious activity. To achieve the security in the ATM network each entity customer and bank should consider the security as an important factor.

Their new framework includes a registration, authentication, and authorization system. Firstly, the user and ATM register for bank's services. The bank generates authentication information and distributes it among them. Bank also assigns some privileges to users, such

as the amount of money a customer could. Secondly, the bank authenticates user by ATM, and finally the bank authorizes user's request for a service, based on the user's privileges.

S.M. Shamsheer Daulaet al., in [21]proposed an embedded ATM security system, by using ARM processor with fingerprint recognition and GSM. On their work they stated that bankers will collect the customer finger prints and mobile number while opening the accounts. The working of these ATM machine is when customer place its finger on the finger print module automatically generates every time different four digit code as a message to the mobile of the authorized customer through GSM modem connected to the microcontroller. The code received by the customer should be entered by pressing the keys on the touch screen or keypad. After entering it checks whether it is a valid one or not and allows the customer further access. As the researchers stated that the customer should hold the mobile for every transaction which will be the drawback of the work.

Shivani A. Patil et al.,in[22] tried to seat a 3D password to secure the ATM system. User can navigate and walk through the three dimensional virtual environment and see the entities interact with the entities. The input device for interaction with entities can be mouse, keyboard, stylus, a card reader, a microphone. For example, consider user who navigates through the 3D virtual environment that is nothing but a room area.

The above research proposes different type of methods basically on biometrics. Based on our interview and physical observations in Ethiopia bank industry those ATM machines do not have any biometric authentication techniques. In this thesis work we come up with a new concept. That is we design a framework which is going to secure logical and physical threats. As we know there is no single fit for all standards for all banks to follow to secure their ATM machines. So our major objective is to designing a framework which will be common for all banks.

CHAPTER THREE

METHODOLOGY AND PRELIMINARY INVESTIGATION

3.1. Research Design and Methodology

In this chapter research design and methodology used is presented. The study was conducted using survey questionnaire, interview and observation as a method of data collection and purposive sampling is used to select those banks and employees involved in ATM operations. For interview purpose we are using IBM SPSS Statistics and Ms-excel 2007 to summarize and analyze the data collected.

The primary data sources used in this study are e-payment managers who have decision making power related to e-payment security. This is because, e-banking or e-payment departments manage all the ATM system functionalities including its security while the security experts make sure that the systems are functioning as per the established policy, procedures, and bank's requirement.

The population of the study was eighteen (18) private and government banks (headquarters) in Addis Ababa. Among those, six banks were selected based on purposive sampling mechanism. Through the aforementioned techniques rich data has been collected from 6 (six) banks. In this paper we are not going to list out the name of those banks for the cause of confidentiality.

Generally, two types of instruments for data collection were used, namely: questionnaire and interview were employed for the data collection. The primary data was collected through questionnaire (structured) and interview (unstructured).

A questionnaire was designed based on the three categories apart from demographic information as physical and environmental and logical security. The question items are open and closed on practices and status in ATM security. The questionnaires were prepared and distributed to e-payment managers and staffs of the respective sampled banks. There are60 questions in three categories. The first section dealt with personal information about the respondents. The second section inquired about the physical and environmental security of the

ATM machine and the banks. And, the third section deals with the logical security of ATM system security.

3.2. Preliminary Investigation

Interview

Informal information about interviewees' experience and knowledge has been collected by the researcher prior to conducting the interview. They possess the experience and perspective in ATM security that this research wishes to understand.

The main purpose of this interview session is to supplement and increase the validity and reliability of the information obtained through the questionnaire.

3.2.1. Interviewee's Responses

1. **What is your understand about ATM users?**

Interviewee 1 explained that most of user uses the ATM machine properly but some of them are not. When we provide the ATM card or when we register a customer we give information how to use the card; and also how to protect their PIN number.

Interviewee 2 stated that customers are aware about how to use but they did protect their PIN number. They pass their PIN number to their family member.

Interviewee 3 responded that users do not protect their card and some of the customers are response to stealing by the robbery. And some others break their ATM card

Interviewee 4 explained that currently we didn't face any problem on the side of ATM user. Because we try to give information about how to use the machine and we will give a guideline about ATM card, PIN.

2. **How do you protect the machines if the users use the ATMs unknowingly? Do you have procedures to guide the users?**

   Interviewee 1 noted that there is no formal procedure but they give information how to use the ATM machine. When the customer get ATM card, the bank provide same info how the customer insert the ATM card in the machine.

   Interviewee 2 stated that we provide service phone to call for any emergency. But we didn't have any alarm system for notification when the customers use the system unknowing.

   Interviewee 3 explained that most of the time we get common report based on this question. Many customers can't remember their PIN number because of this, customer try to guise their PIN number more than three times then the ATM machine capture the ATM card.

3. **What kind of authentication mechanisms did you use to secure the ATM transaction? Is their new enhancement to secure the ATMs?**

   Interviewee 1 says that they deployed a firewall for authentication to secure the transaction.

   Interviewee 2 until now we are using customer ATM card and PIN number as an authentication system for securing user information and to secure the entire ATM transaction.

   Interviewee 3 and 4 has got common response that they didn't use any authentication techniques because of they are under PSS.

4. **Now a day, all banks use one ATM card (Other Bank ATM) so, how do you secure users as well as the ATMs.**

   Interviewee 1 responded that if the banks connected each other that mean it didn't make any different activity on that of the previous.

   Interviewees 2, 3 and 4 have also similar explanation that the bank follows its own operational procedure. But may be on ATM machine can happen physical damage when the user operate.

5. **Do you have a framework to secure the ATMS?**

   Interviewee 1 says that under this instruction there is no any framework to follow up for securing our ATM machine. But internally we do have a procedure we are using as a framework.

Interviewee 2 sated that there is no formal developed framework which going to secure the ATM machine. The bank didn't yet design and implement compressive framework due to the following reason. These are the bank is new, lack of ATM security understanding by the top management, and lack of domain experts are some of the challenges in this bank.

Interviewee 3 noted that there is no any framework or procedures in this bank. The reason is that the bank follows the procedure of the ATM supplier. When the machine deployed, it has got its own security future.

According to Interviewer 4 there is no ATM security framework in this bank. The bank didn't yet designs implement any framework. But the bank set as plane to design a framework which has got high security.

6. **Do you follow PCI DSS standard? If your answer is yes, which of them are deploying in your Bank?**

Interviewee 1 explained that the bank does not follow the PCI DSS standard the reason is that we don't have master card and VIS card.

Interviewees 2, 3 and 4 stated that PSS meet PCI standard because of that indirectly we are following the PCI standard. But we can't list out which of them because this bank is work with PSS. We don't have a department for ATM security.

7. **How do you monitor the system? Is there any monitoring system? If your answer is yes, what monitoring system do you use?**

Interviewee 1 noted that no monitoring system since now. But now we are developing a system which is going to monitor the ATM machine. It is house made program we called it "zeber".

Interviewee 2 no monitoring tool or system but we can monitor the ATM system whether the ATM machine is down or not, and when the machine is finished the money in each case. For the cause of security we don't have monitoring system, which mean there is no any way of detecting log source, if any attack or event happen on the ATM machine.

Interviewee 3 responded that the bank do have a monitoring system. The tool which that we have is going to monitor the ATM status and security parts.

Interviewee 4 stated that the bank monitor the ATM. Like which ATM machines are working properly. Which of them need maintains, which of them finished the money and the like we can monitor but in the case of security what kind of attempt happen to the bank ATM machine is not monitor yet.

3.3. Physical Security

Banks were asked about their ATM physical security and where they locate those ATM machine and the result is summarized as shown Fig3.1 below.

Those banks locate their ATM machine in different area like near to branches, near to hotels, near to malls, near to hospitals and near to different university.

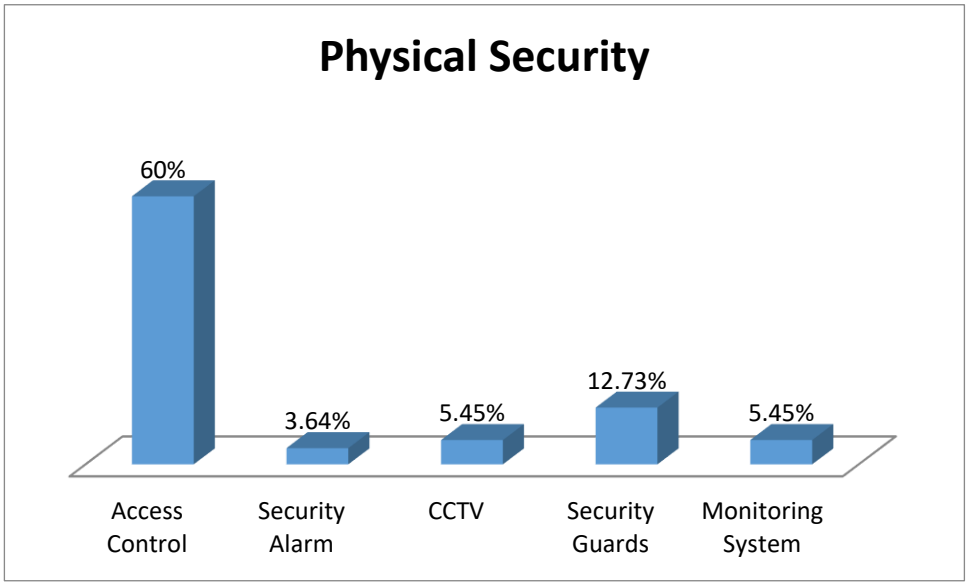

Fig.3.1 : Physical Security System

Fig.3.1 shows that 60% of the banks surveyed do have access control and 27.3% banks use security alarm, CCTV, security guards and monitoring system to secure their ATM machine against physical attack.

This result implies that even if those banks try to secure their bank ATM using different control method but not enough. Since those security systems are not working effectively.

During our interview we get this information, that in one of our banks one or two skimmers try to skim same ATMs during nigh time, so all banks and customer should be aware.

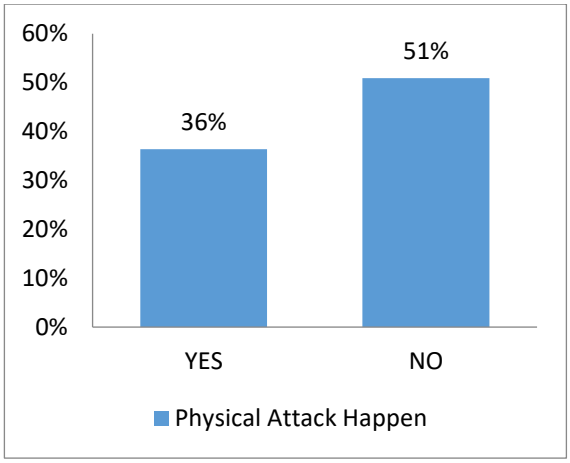

Fig.3.2: Physical Attack in Ethiopia

Fig. 3.2 shows that 36% of the respondents indicate that physical attack happen on ATM machine and 51% show that banks does not list type of any attack. Which is any physical attack was not record on their bank. Even if it is occurs they don't want to notify.

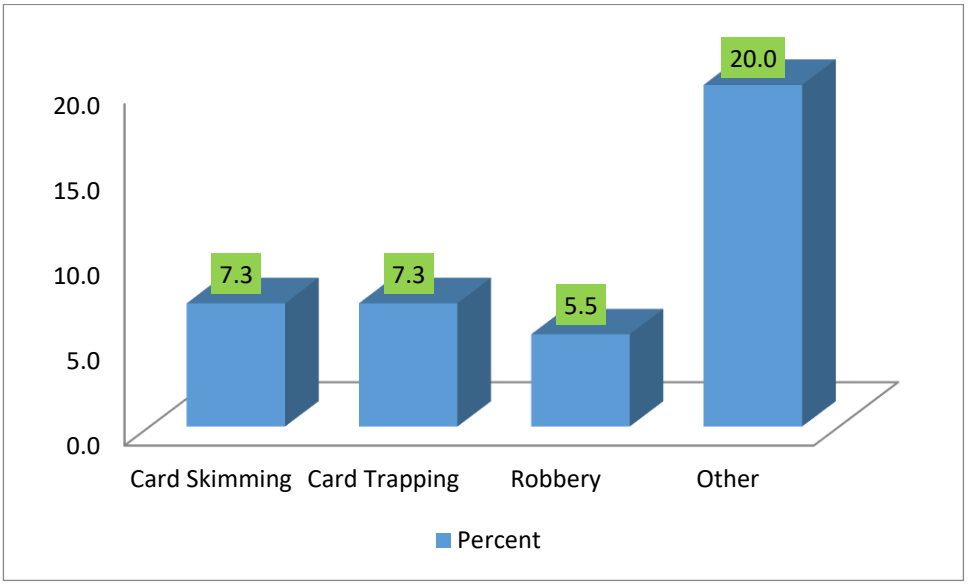

Fig.3.3: Types of Physical Attacks

Fig. 3.3 indicates type of physical attacks that occur in different banks ATM machine. 7.3% of the banks surveyed reported card skimming and card trapping was happening. 5.5% of the attacks were robbery and the 20% are list in different type of physical attack.

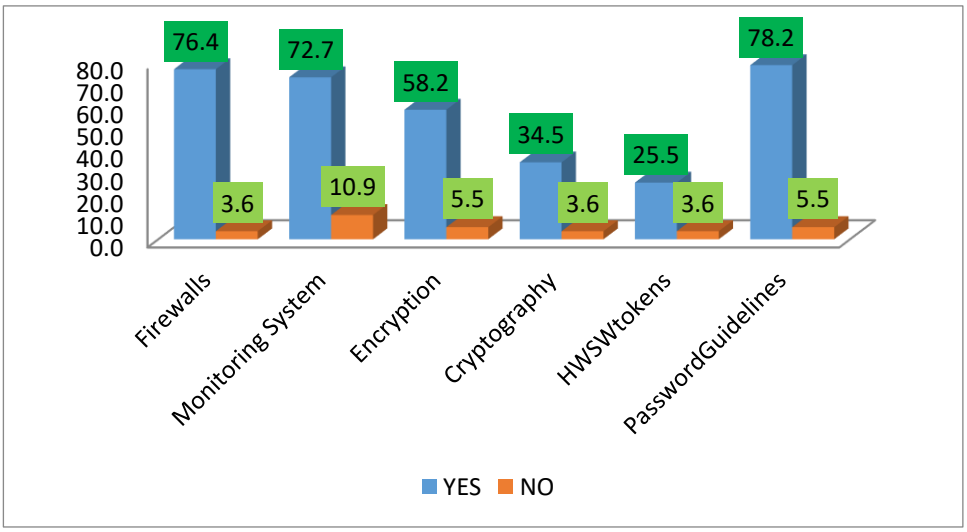

Fig.3.4: Protection Techniques

Fig.3.4 shows that banks use firewall, monitoring system, cryptography and password protection techniques to protect their ATM systems. 76.4% of the surveyed banks used firewalls for their ATM system. 72.7% of the surveyed banks used monitoring system, but the monitoring system is not monitoring the security issues. It monitors the status of the ATM whether the ATM machine has money or not. 78.2% of the surveyed banks have password guidelines and 58.2% implemented encryption techniques.

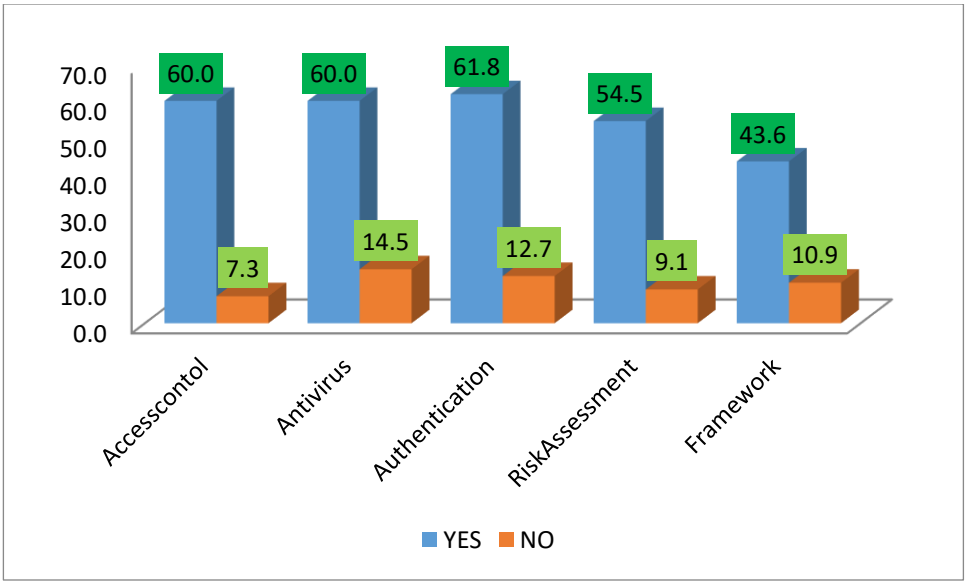

Fig.3.5: Access Control, Antivirus, and Framework

Fig.3.5 shows that banks have access control and authentication system round 61%, but the authentication techniques are PIN number and card only. 60% of the surveyed banks used antivirus. However, they are not upgrading their antivirus regularly. 43.6% of the surveyed banks do have a security framework. Based on the answers the framework is not standard.

3.4. Current Status of ATM Security

ATM security is the current issue for financial institution throughout the world. Since ATM system more simple to use then hacker using this simplicity can create different hacking techniques to penetrate the system. ATM security may focus on either securing the hardware components or any combination of them the software (OS) or the communication network, or financial institutions follow different security techniques to protect from security threats that are related from hardware components, OS or networks. Attackers search for vulnerabilities in their attempt to hack the system. When any type of attack occurs on financial institution then banks find equivalent security solution. Hackers installed skimming device on ATM machine like fake keypad. By aware this type of attack banks using anti skimming device on ATM machine to protect from skimmer. In our country this type of attack is not common but happened in one of the banks. To protect this skimming our banks didn't use any security techniques until now.

To secure ATM networks while data transfer take place host computer banks use cryptographic techniques. Those banks in Ethiopia also use this data securing method. Some of them are using DES and the others are using3DES. DES is a symmetric key block cipher published by the National Institute of Standards and Technology (NIST). A block cipher meaning a cryptographic key and algorithm are applied to a block of data simultaneously rather than one bit at a time. 3DES is the same as that of DES but 3DES using three different keys is still considered secure.

To sum up, Ethiopian banks focus on physical security to secure their ATMs. They locate the machine in secure place like near to the banks, near to hotels and they assign security guy. The other security techniques used by limiting the amount of money to be withdrawn within a day also they set a method which is blocking the connection of ATM and holding back the card when the customer try to enter their PIN number three times. All these types of securing techniques are using all banks to protect their ATM. But they didn't use any other security system like alarming system and other authentication methods like biometrics voice recognition and vibration sensors.

3.5. Standardization Issues

For the time being banks doesn't have common security standard for securing their ATM system. Even they didn't adopt a common a framework. They put their concern on ATM vendors because when the ATM machines deployed they include PIC DSS standard. Based on our observation, our banks have less attention for ATM security. Based on the responses "the reason is that in our country hacker don't exist, people are not more intelligent mean don't have knowledge for hacking the system so we are not more focus for ATM security." That is why, when we go to for data gathering some of the bank doesn't have a department for ATM security. Around six banks from 18 banks share the same switch which is PSS (Premier Switch Solutions). So those banks give their security parts to the PSS department.

Those six banks ATM are connected with the PSS. To establish the connection banks send official letter to the PSS. The PSS resend a unique terminal ID which is used to define or link with the core banking system. Internet service provider which is our Ethio-Telecom provides IP address, default gateway and subnets. Using IP address port number and host IP

which is PSS server by applying NDC+ protocol (NDC is ATM transaction processing protocol formulated by NCR Company.) PSS and ATM terminal are connected. When we came to security part beside of NDC+ protocol there is key (double DES) it has 16 digit lengths.

Once this connection is stipulated, the card holder can use one of those six banks ATM terminals. ATM machine send PAN (Primary Account Number) which is severed from the ATM card then to PSS. Using BIN (Bank Identification Number) the PSS send the request that came from the ATM terminal to the bank that has the information about the card holder. In general Ethiopian's banks have less attention to ATM security.

3.6. Future plan

Some of Ethiopian banks believe that they have secured the system because they understand that the cause is worldwide.

Banks get information about the current hacking news from different international banks though letters just for creating awareness. Our banks don't have this kind of experience that means if any attack happen on their system, they hide instead of reporting the type of attack for the sack of confidentiality. Now days, they have a plan to design security system but they didn't define what kind of security system they are going to design. So that the following PCI compliance is the standard which is going to support to design the secure system for all the banks.

3.7. PCI Compliance

The PCI Data Security Standard (PCI DSS) is a set of rules meant to ensure that all companies safely accept, process, store, or transmit cardholder data (i.e., credit card information).

PCI DSS is managed by the PCI Security Standards Council, an independent body founded by the five largest credit card brands; American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa. It was launched in 2006 to

improve the security of the transaction processes and payment technology life cycles as a whole.

The PCI Council and the five credit card brands believe that sellers and organizations that accept credit cards are primarily responsible for the security of those transactions which is why it's crucial that highly secure technologies and measures are in place to prevent theft of cardholder data.

The PCI DSS applies to all entities that store, process, and/or transmit cardholder data. It covers technical and operational system components included in or connected to cardholder data. It consists of common sense steps that mirror security best practices and build and maintain a secure network

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters. Protect Cardholder Data
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks.
5. Maintain a Vulnerability Management Program
6. Use and regularly update anti-virus software or programs
7. Develop and maintain secure systems and applications
8. Implement Strong Access Control Measures
9. Restrict access to cardholder data by business need to know
10. Assign a unique ID to each person with computer access
11. Restrict physical access to cardholder data
12. Regularly monitor and test networks
13. Track and monitor all access to network resources and cardholder data
14. Regularly test security systems and processes
15. Maintain an Information Security Policy maintain a policy that addresses information security for all personnel

Based on our observation Ethiopian's bank do not fulfill this PCI compliance. Even the monitoring system is not monitor the security level of the ATM machine it just monitor the status of the machine. So that as a common standard (as a framework) the policymaker influence to all banks to follow up the PCI DSS beside of propose framework which is enhance the ATM security.

3.8. Global Security Issues

In this section we list out some ATM security issue that occurs in different countries.

- For a long time, Germany was a target for most fraudsters. Credit cards normally used abroad for self-service transactions traditionally promised far greater gain for criminals. Losses from such attacks in Germany are only around one-tenth of the 95 million Euros lost every year in the United Kingdom to card fraud[23].
- Hackers targeted at least eight ATMs in Russia and stole $800,000 in a single night, but the method used by the intruders remained a complete mystery with CCTV footage just showing a lone criminal walking up to the ATM and collecting cash without even touching the machine[24].
- In the U.S., ATM skimming is considered the most severe threat, with 68 percent of executives classifying it as a very severe or severe threat. Cybercrime is seen as the next most critical threat, with 49 percent of executives grading it as very severe or severe.

  Sixteen percent of respondents view the physical threat to ATMs as no threat at all; this category is most likely to have a geographic component since this is primarily a big city problem. Forty-four percent of executives believe card and cash traps are a moderate threat[25].

- ATM related fraud attacks increased by 26%, up from 18,738 in 2015 to 23,588 in 2016. This rise was mainly driven by a 147% increase in Transaction Reversal Fraud (up from 5,104 to 12,581 incidents). The downward trend for card skimming continues with 3,315 card skimming incidents reported, down 20% from 4,131 in 2015. This is the lowest number of skimming incidents reported since 2005.

Losses due to ATM related fraud attacks were up 2% when compared with 2015 (up from €327 million to €332 million). The Asia-Pacific region and the USA are where the majority of such losses were reported. Domestic skimming losses rose 24% over the same period (up from €44 million to €53 million)[26].

According to our investigation Ethiopian banks do not have any ATM fraud report that realize on any source. Most banks do not announce the type of the attack even if it happens. They were going to hide the event. The main reason was they need to protect the customer's confidence on their banks.

Because of the above ATM security issues some countries implement biometric on their ATM machines and the manufacturer also add up the biometric authentication system on the new ATM machines. Here are some of them which implement the biometric authentication system.

- More than 80,000 biometric ATMs have been installed in Japan since 2006, when legislation was passed in that country requiring banks to pay for fraudulent charges[25].

- In June 22, 2016 report, Bank of America is outfitting some of its ATMs with Apple Pay support and the ability to withdraw cash using it. Bank of America is highlighting the new feature heavily on supported ATMs, making users aware that they are able to withdraw cash from the bank machine using their Smartphone.

  This feature only works with Bank of America cards and Bank of America is rolling this feature out slowly so even machines that show NFC support may not be updated to support Apple Pay yet[27].

- Iris recognition firm Iris ID, has entered into a strategic memorandum of understanding (MOU) with South Korea's Woori Bank to jointly develop a pilot project to enhance financial security. Woori Bank will use Iris ID's iris recognition technology to authenticate clients at ATMs, safety deposit boxes and for access control. If the project is successful, Woori Bank's 20 million customers will be able to register at one of the bank's 967 Korean branches to use the biometric authentication system[28].

- China Merchants Bank said it has implemented nine of its facial recognition enabled ATMs in the city of Shenzhen, adjacent to the China Hong Kong border, according to a report by South China Morning Post. The company said it will soon expand the rollout of the ATMs with facial recognition software throughout the city, with plans to update the bank's 12,000 ATMs. The feature will enable customers to have their picture be captured in real time by the machine, which will then compare the image to a verified photo of the individual stored in the bank's database.

  Once verified, users will be required to enter their phone number and PIN as an additional security measure before they are able to make a cash withdrawal.

  The facial recognition software uses a highly-accurate algorithm that analyzes facial characteristics and shape, as well as the angle at which the image was captured, said China Merchants Bank. The bank has also tested the facial recognition technology by using it as a secondary measure to aid bank tellers in verifying customer's identity [29].
- Diebold announced it has released its new 5500 series of ATMS, which is designed to help financial institutions deliver full availability, low total cost of ownership, and advanced security features and technologies. Diebold says the 5500 series can help financial institutions address various business objectives, such as managing security risks, driving efficiencies and lower cost of ownership, and appease customers.

  The patent-pending Diebold Active Edge card reader, which curbs all forms of skimming, is a standard feature in the 5500 series. Other available features include biometric finger-vein readers, security camera provisioning, encryption technology, and monitoring services.

  The newly developed Active Dispense technology enhances the ATM's uptime as well as optimizes its dispensing performance.

  Additionally, Active Power intelligent power management controls power to individual modules during servicing, ensuring that users will not have to turn off the entire unit.

It also cuts down energy consumption by up to 60 percent, reducing the total cost of ownership [30].

3.9. Summary of Exiting ATM Security Problems

Today, ATM has become a unique communication and service channel between banks and cardholders due to its fast, convenience and human resource saving advantages; we can easily find ATMs in branches, convenience stores, airports, and shopping malls.

To build safe ATM use environment, maintain bank's brand image and protect bank assets, all the involved organizations, institutions, and persons must research, develop and takes measures using ATM, and provide a set of advice and countermeasure on how to identify and fight against to meet the challenges faced by ATM crimes.

Based on our observation we found the following ATM security related problems:

1. **User have less awareness about ATM security (staff of the banks)**

ATM cards have become the most convenient form for purchasing our everyday needs. They have replaced the actual need to carry cash and should be treated like cash. Based on our surveillance, bank users are having less understanding about ATM security. This may cause users fold up for unnecessary ATM attacks. Even the bank employees are victim to ATM threats. Most banks give awareness to their customer about how to use the ATM machine like how to insert the care to ATM machine, how to protect their PIN numbers and card. But banks do not give any information about ATM attack so, the consumer must be educated to be observant and inspect the ATM before using it.

2. **Banks hide any incident which is happening to their system.**

If there is any incident that occurs on ATM system, most banks does not announce the type of attack. The reason is banks want to protect their customer's confidence on banks.

3. **Banks does not have common framework to secure the system.**

When we contact some banks through interview and through questionnaire they didn't have any framework which is used to security their ATMs. They think they are secure because when banks purchase an ATM machine from ATM venders all ATMs equipped with PCI DSS.

Most banks purchase the machine from different ATM venders, like NCR and Diebold, which follow different standards.

4. Banks does not have monitoring system.

Monitoring System is the most essential system for secure any system. Network monitoring is a vital and demanding task within network security operation. Network monitoring is a retrospective approach network administrators adopt to deal with performance issues and security incidents. Any transaction which is performed by an ATM machine should be monitored. Based on our observation, only one bank have a standard monitoring system but the rest banks have in-house monitoring system developed by their employees. But these in house monitoring systems monitor the status of the ATM whether the ATM is down or not, whether ATM finished money for those caskets.

5. All banks use only PIN authentication techniques.

PIN and card are the most critical requirement to use the ATM machine. Many ATM attacks seek to obtain a consumer's personal information, such as their card number and (PIN). Attacker may use card skimming and other type of fraud to customer using customer's PIN and Card. so PIN authentication techniques is not enough to secure ATM. So we have to add up other authentication techniques to enhance our ATM security. By using different biometric like fingerprint we can prevent current ATM frauds.

6. All banks affected by common type of attack, that is PIN and card theft.

As we know that our entire ATM machines verify the customer using PIN authentication techniques only. Because of this, most of financial institutions are victim of the same attack. Card users have less awareness about ATM security; they place their PIN numbers with their card in inappropriate places.

By providing awareness to the card user about the current ATM threats and by improving the current security techniques like biometrics techniques we can prevent this type of attack.

CHAPTER FOUR

PROPOSED FRAMEWORK AND ITS IMPLEMENTATION

4.1. Proposed Security Model

The current ATM machine has got those components like cash dispenser, display, keypad, network interface, receipt printer, log device and card reader. On the existing ATM system we add up four major components that will be used improve security of the current ATM systems. Those are fingerprint module, voice recognition, pre-verification SMS system and vibration sensor module.

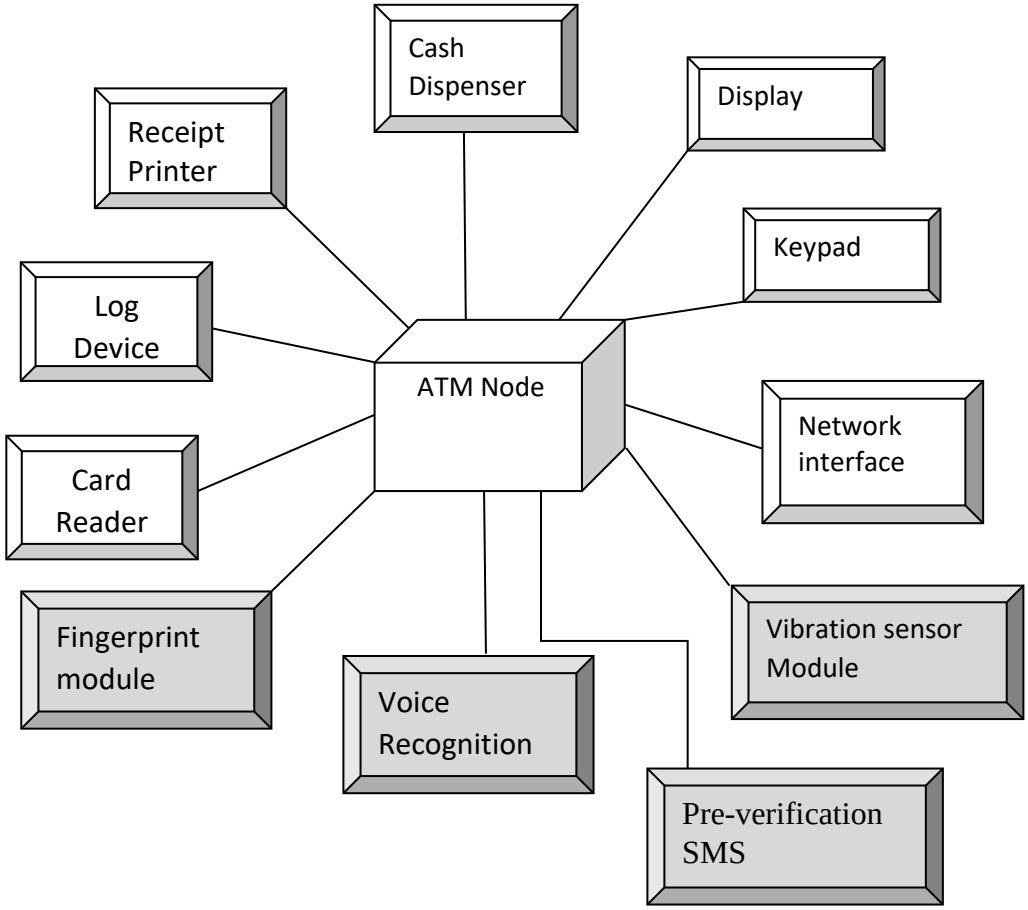

Fig.4.1: Components for the Propose System

The proposed system framework on ATM integrated with fingerprint and voice biometrics authentication as designed as follows.

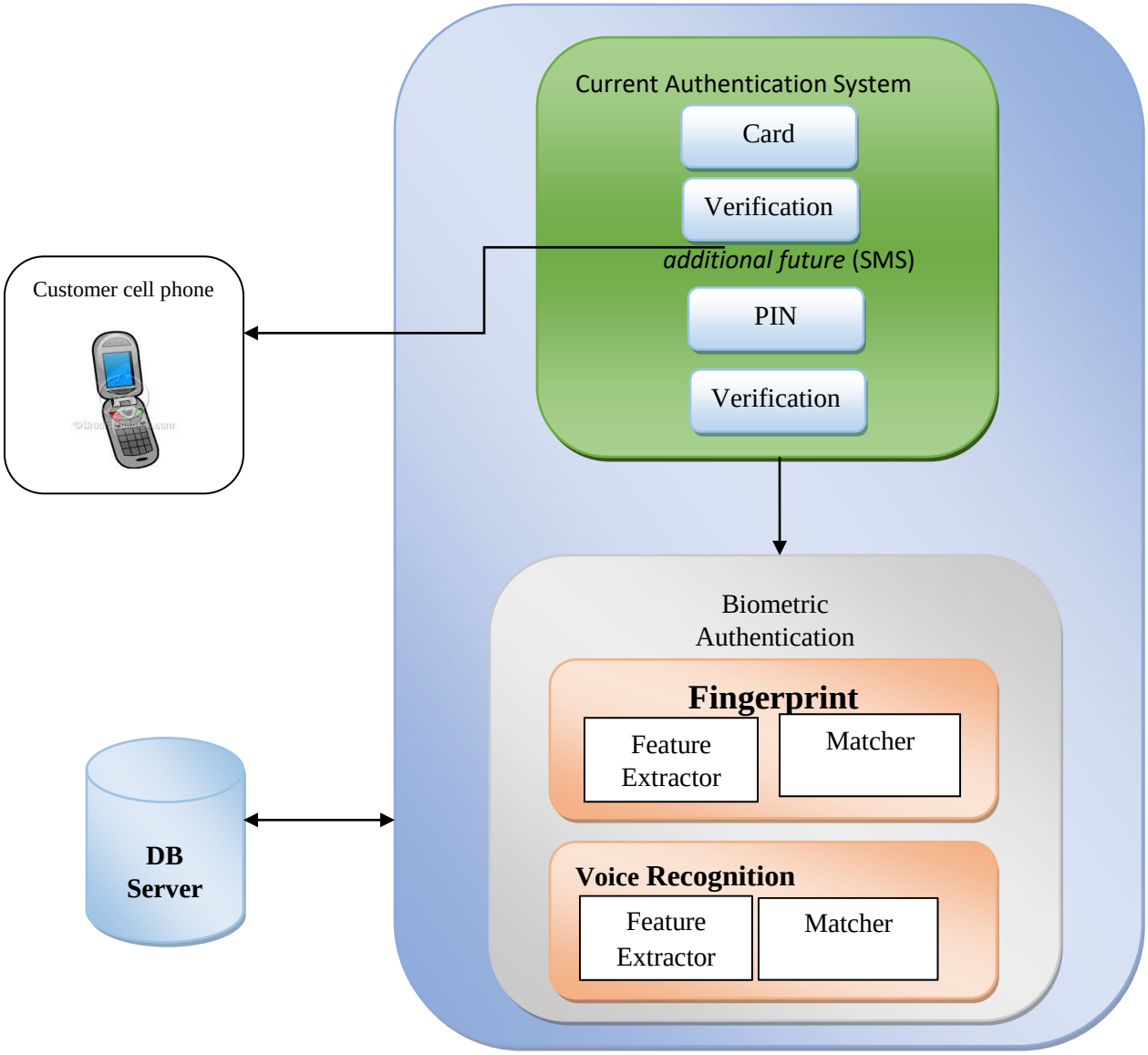

Fig.4.2: The proposed system framework architecture

The function of those components is newly introduced in this work is discusses as follows.

Pre-verification SMS – this is where the customer will get SMS when he/she enters the card before PIN has entered and processed further. So the customer will be aware about the any transaction made upon their card.

Fingerprint validation–fingerprint sensor is a biometric authentication on customer's fingerprint. Using the fingerprint device customer's will be verified upon the database. Under this study the fingerprint validation is mainly done when the PIN authentication failed to progress.

-Feature extraction from fingerprint biometrics

In both fingerprint identification and finger print verification, the image has been extracted using feature extraction method. It has following steps. [33]

Image acquisition, here the image is captured using the fingerprint reader and extract the features into machine readable format.

Normalization: it enhances the contrast of image by transforming the values in the fingerprint image it distinguishes the ridges and valley of an image.

Ridge orientation: it is used to obtain the angles of an image and calculated by 168 16 block size.

Gabor filter: it is used to remove the noise from an image and it preserves ridges and valleys.

Binarization: it is used to convert the grey level image into binary image using threshold values. The pixels with higher values more than the threshold value as white other pixel values are black [33].

Minutiae extraction: In minutiae extraction. It is to count the number of ridge pixels, every ridge pixel on the thinned image is surrounded by and depending on the rule and we can assign the untiae points to pixels. It is to match the minutiae obtained from two sample fingerprint image and test whether they are from the same fingerprint or not. [33]

Voice Recognition A type of security authentication that relies on person unique voice patterns for identification in order to gain access on ATM. It is additional biometric authentication undergo and this validation process will applied when the fingerprint authentication is failed.

Database – The backend data warehouse which enables to store the specified customer information for both PIN and the biometrics record. This is used to identify and verify each customer's validity based on either PIN or their biometrics records which is stored on the database.

As we know ATM is an automatic banking machine which allows customers to complete basic transactions without any help of bank representatives. The customer accesses their account through special type of plastic card that is encoded with user information on a magnetic strip.

The magnetic strip on the back of the card may look like a solid black line, but it's actually composed of millions of tiny magnets, each one magnetized either north or south, which two magnetic readers understand like a binary code. The first reader confirms the card is real, while the second reads your account number and PIN, checking this against the code that you entered on the keypad. The customers insert the card into card reader.

The card reader is an input device that reads data from a card .The card reader is part of the identification of your particular account number and the magnetic strip on the back side of the ATM card is used for connection with the card reader. The card is swiped or pressed on the card reader which captures user account information i.e. the data from the card is passed on the host processor (server). The host processor thus uses this data to get the information from the card holders.

The card is recognized after the machine asks further details like your personal identification number, withdrawal and your balance enquiry Each card has a unique PIN number so that there is little chance for some else to withdraw money from your account. There are separate laws to protect the PIN code while sending it to host processor. The PIN number is mostly sent in encrypted form.

The speaker provides the audio feedback when the particular key is pressed.

The display screen displays the transaction information. Each steps of withdrawal is shown by the display screen. A CRT screen or LCD screen is used by most of ATMs.

The receipt printer print all the details recording your withdrawal, date and time and the amount of withdrawn and also shows balance of your account in the receipt.

The cash dispenser is a heart of the ATM. This is a central system of the ATM machine from where the required money is obtained. From this portion the user can collect the money. The duty of the cash dispenser is to count each bill and give the required amount. If in some cases the money is folded, it will be moved another section and becomes the reject bit. All these actions are carried out by high accuracy sensors.

Once the PIN is confirmed, the machine automatically connects to bank's network which relays a signal back to the built-in vault, giving it a specific set of instructions. The ATM will then complete the transaction that has been requested. If you forget to take your cash for whatever reason, modern cash machines will swallow the money within a short period of time so you won't be out of pocket.

A flow chart is designed for the proposed system as shown in fig. 4.3. The flow chart shows how the improved framework adds the security of ATM systems by using multiple layers of security mechanisms that are combination of PIN, SMS, fingerprint system and voice recognition mechanism and vibration sensor system.

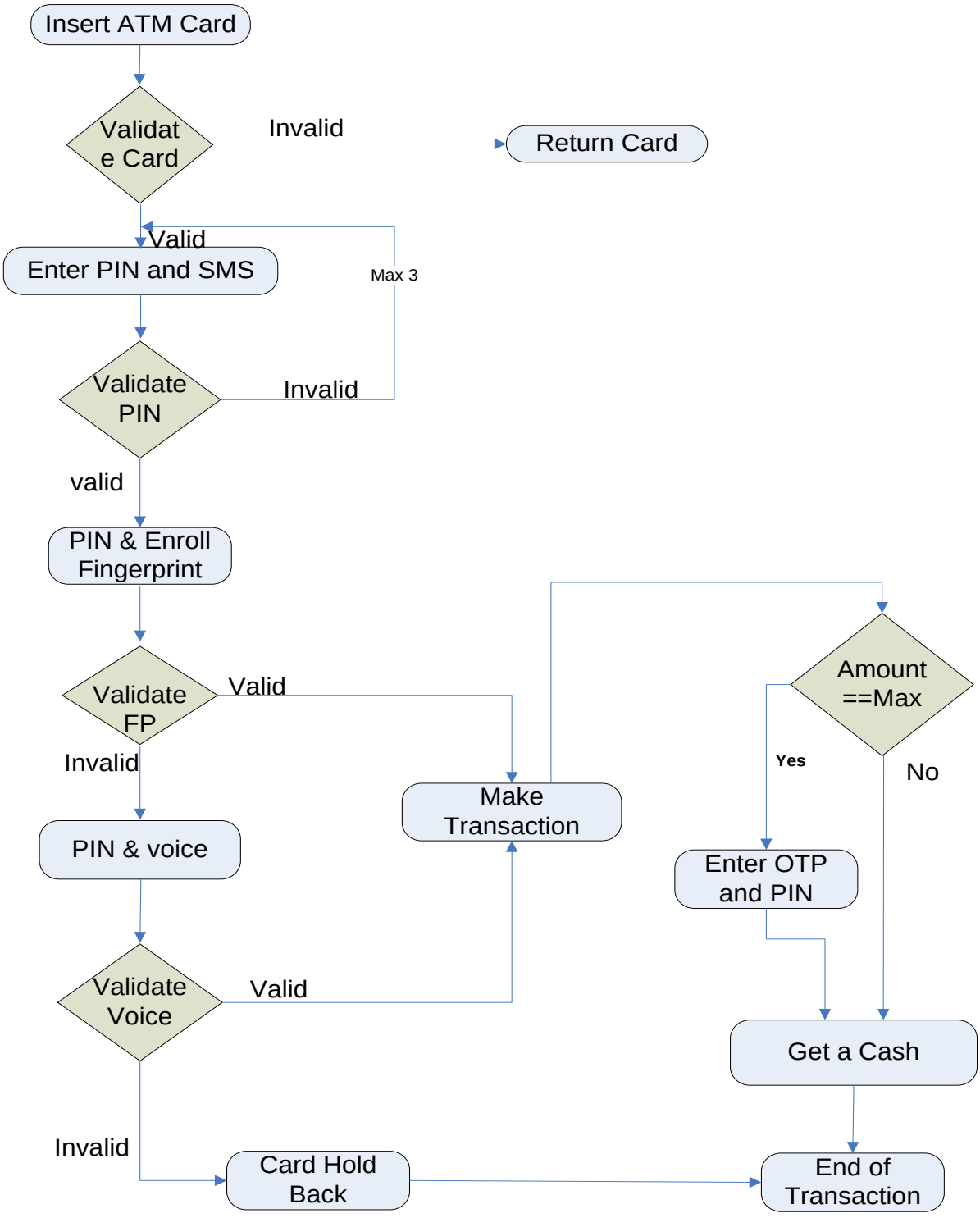

Fig.4.3: Flow Chart for Propose System

CAHPTER FIVE

SCENARIO GENERATION AND VALIDATION

In this chapter typical user scenarios have been generated which are going to emphasize the functionality designed in the framework and validate the scenarios using MATLAB simulation software.

A user inserts ATM card into ATM machine and the machine read the magnetic strip from the card and then identify the user with his/her bank account. After the card validation, if the card information doesn't match with the database then the machine will return the card to the customer. But if the user information does match with that of the database then the ATM machine will ask the user to enter the PIN. After this phase we list out some scenario here under.

5.1.Typical Usage Scenarios

Scenario I: Using PIN with SMS notification

The current ATM machines authenticate the customer using PIN number only that means the customer enters the card into the card reader where it verifies the card then she/he enters the PIN number. This authentication technique allows the customer to enter the PIN only three times. But if the customer enters incorrect PIN number for three times then the machine will take the card.

In our improved system the machine does not go to straight and ask to enter the PIN number for the second time. When the customer enters the card for the first time then the ATM machine will send SMS to the card holder for pre-notification. Then a chine will check the PIN number if it is correct. The user will make any transaction. But when the customer tries to withdraw the money more than half of the maximum allowed limitation (for example commercial bank of Ethiopia set 6000 birr as a withdrawal maximum limitation) then the customer will get one time password. So, the card holder should have and enter from her/his mobile this one-time password which is generated by system using soft token.

Scenario II: PIN and fingerprint recognition

In this case the card holder should enter correct PIN number for first time but if she/he enters incorrect PIN then she/he try to enter the PIN number for the second time then the machine should enforce to check her/his fingerprint. In this case the system will authenticate the PIN number and fingerprint of the customer for verification. If the PIN is correct then customer will make the transaction, but if the PIN is incorrect the system will enforce to check voice instead of PIN. In this scenario the fingerprint is also validated, if the fingerprint match with the image found in the database, then the customer will get the cash. If the fingerprint doesn't match, then the system will ask the customer to insert her/his voice using microphone. The system also sends SMS during every authentication to the card holder.

Scenario III: PIN and Voice Recognition

This scenario will be performed when the card holder enters the PIN number and she/he scan her/his finger and the system if not authenticate the fingerprint then the system will promote other authentication which is voice recognition techniques. In this case the voice of the customer will be checked. If the voice doesn't match with the voice which is found in the database then the system will generate one time password and send it to the customer's mobile. The customer will insert the OTP in addition to the fingerprint. When the voice is valid using the OTP which it got from the system can get the cash dispensed.

Scenario IV: Finger and Voice recognition

If the card holder enters the PIN number for the third time then the system asks to enter the card holder fingerprint and voice to recognize the customer. Fingerprint and voice recognition both are a biometric authentication methods. They uniquely identify customers.

Scenario V: Pre-verification to the customer using SMS

When the card holder using the ATM machine and after entering the PIN number when it verifies then the system will send SMS to card holder cell phone.

Scenario VI: Vibration Sensor Module

This vibration sensor is used to secure the physical part of the ATM from physical damage. This module will measure the vibration rate; if it is above the threshold then it will send the

alarm to security guard. In this scenario it works independently because it used to protect the external part of the ATM machine.

5.2. Validation of Scenarios

For validation of the above listed scenarios we used MATLAB software. In this part we tried to implement the proposed system that contains fingerprint, voice recognition and vibration detection methods.

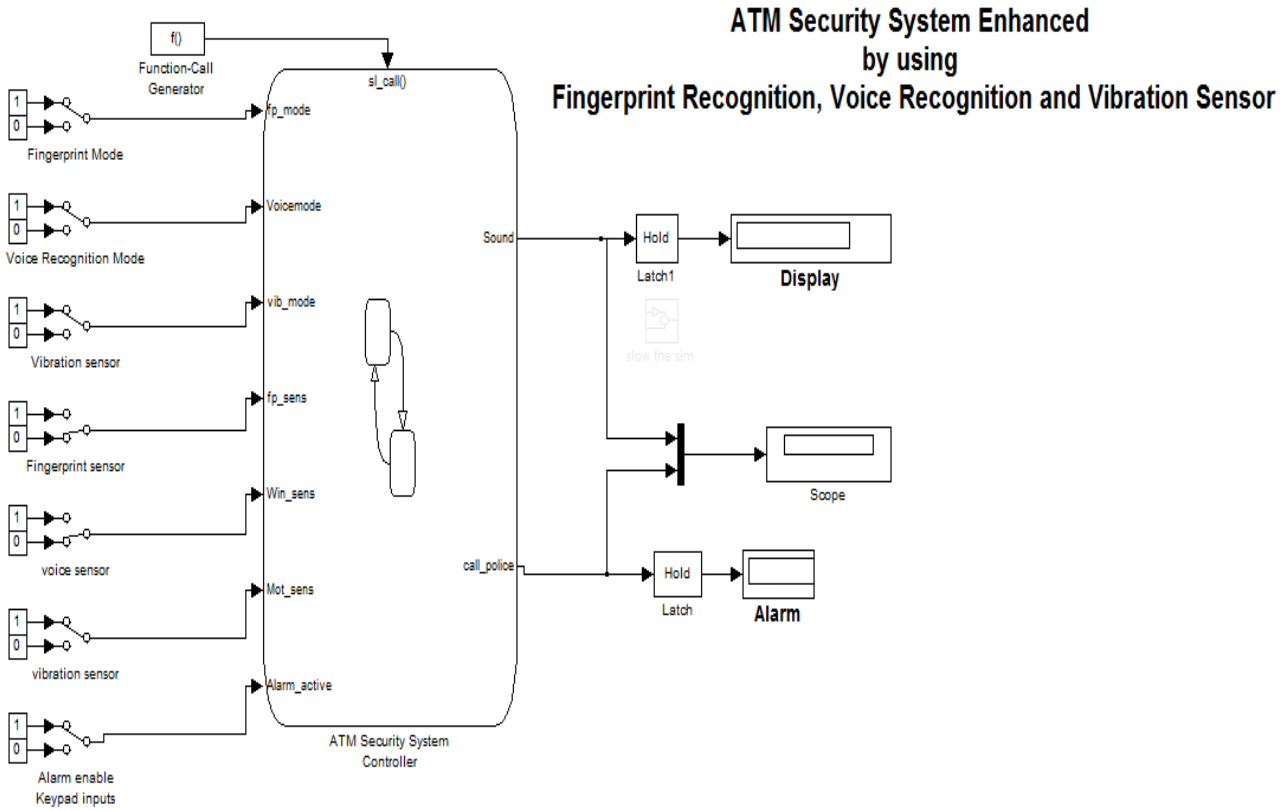

Fig. 5.1: Proposed System Implementation using Matlab

Fig. 5.1 shows that how the proposed systems work. In each scenario the system generates an alarm. But in this case each input which is fingerprint, voice recognition and vibration detection generate the binary signal (0's and 1's) by swapping the bits, it generate the alarm if it detect any intrusion.

If the fingerprint doesn't match with that of fingerprint which is stored in the database, the system will generate alarm. And it will swap to the next scenario that is voice recognition mode.

On this section the two modes were simulated which are fingerprint and voice recognition using MATLAB. Under this validation part we are adding some sample snapshots which is taken from MATLAB system.

Login page

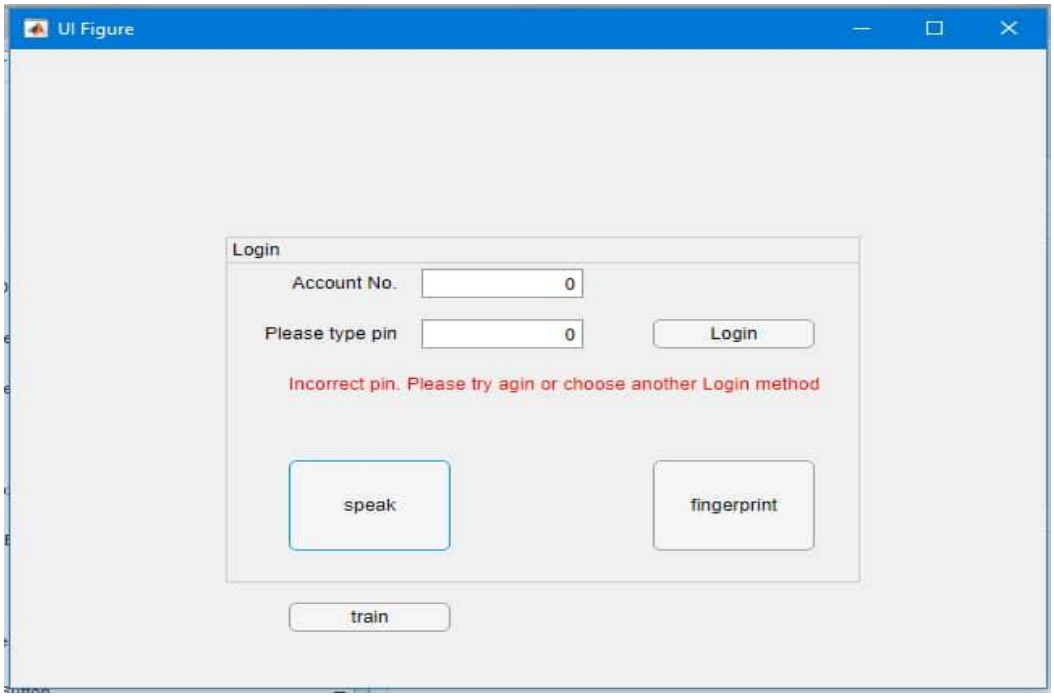

Fig. 5.2: Login Page

Fig. 5.2 is login page which is showing that when the user input was wrong password. Here the user speech and fingerprint authentication options appear and the user chooses with the button.

Fig. 5.3 shows voice listening page if the user clicks speech recognition button. It records for 10 sec. Then it finds if there is a match from trained codebook. If the user matches with registered voice it will invoke its username, welcomes and allows the user for account access

and operation like balance, withdrawal transfers, and so on. If the voice doesn't match it will allow 2 or 3 trials.

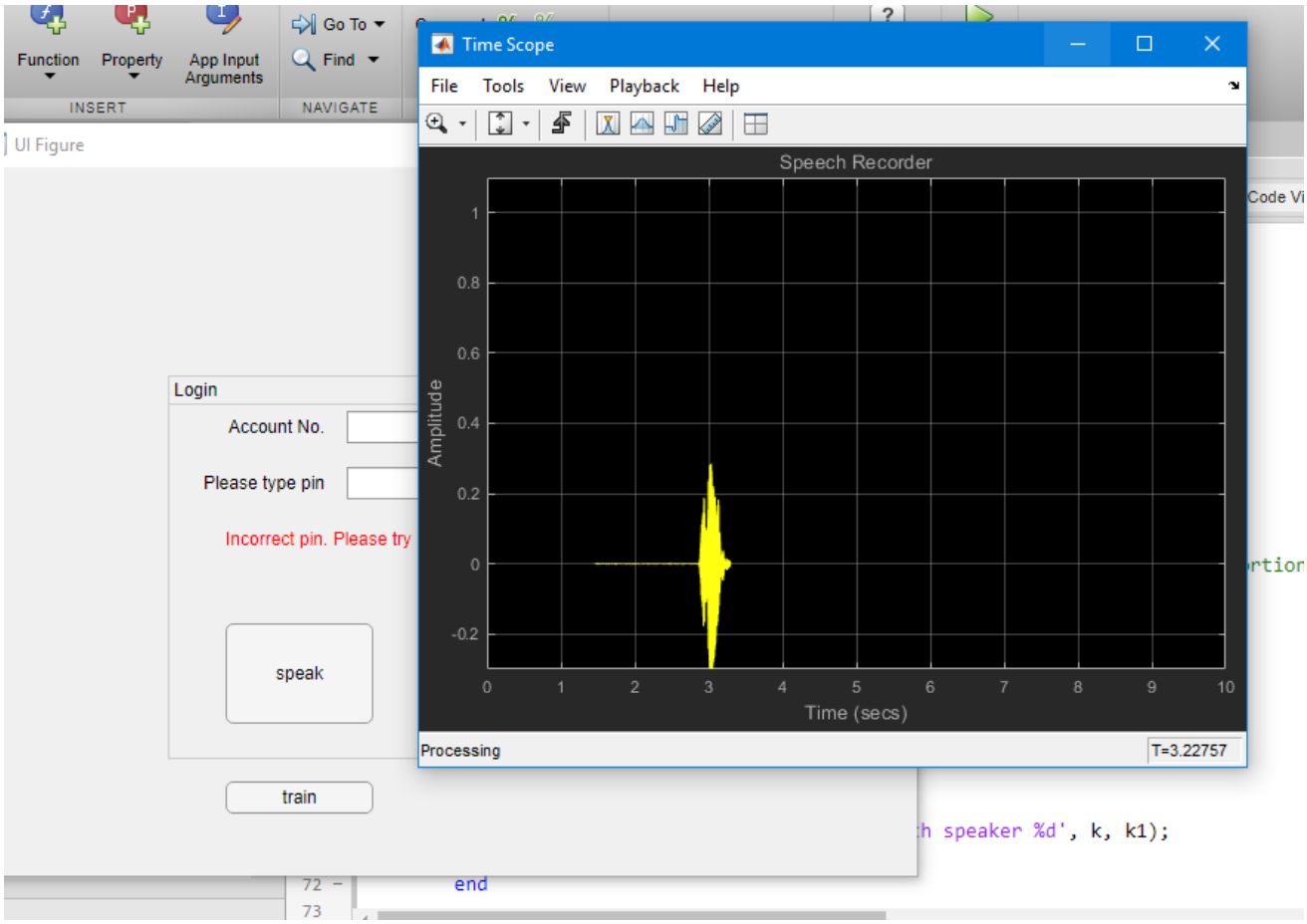

Fig. 5.3: Voice Recorder

Fig. 5.3 shows the application that registers the user's voice and fingerprint. This registration application is to be used by bank officers/clerks.

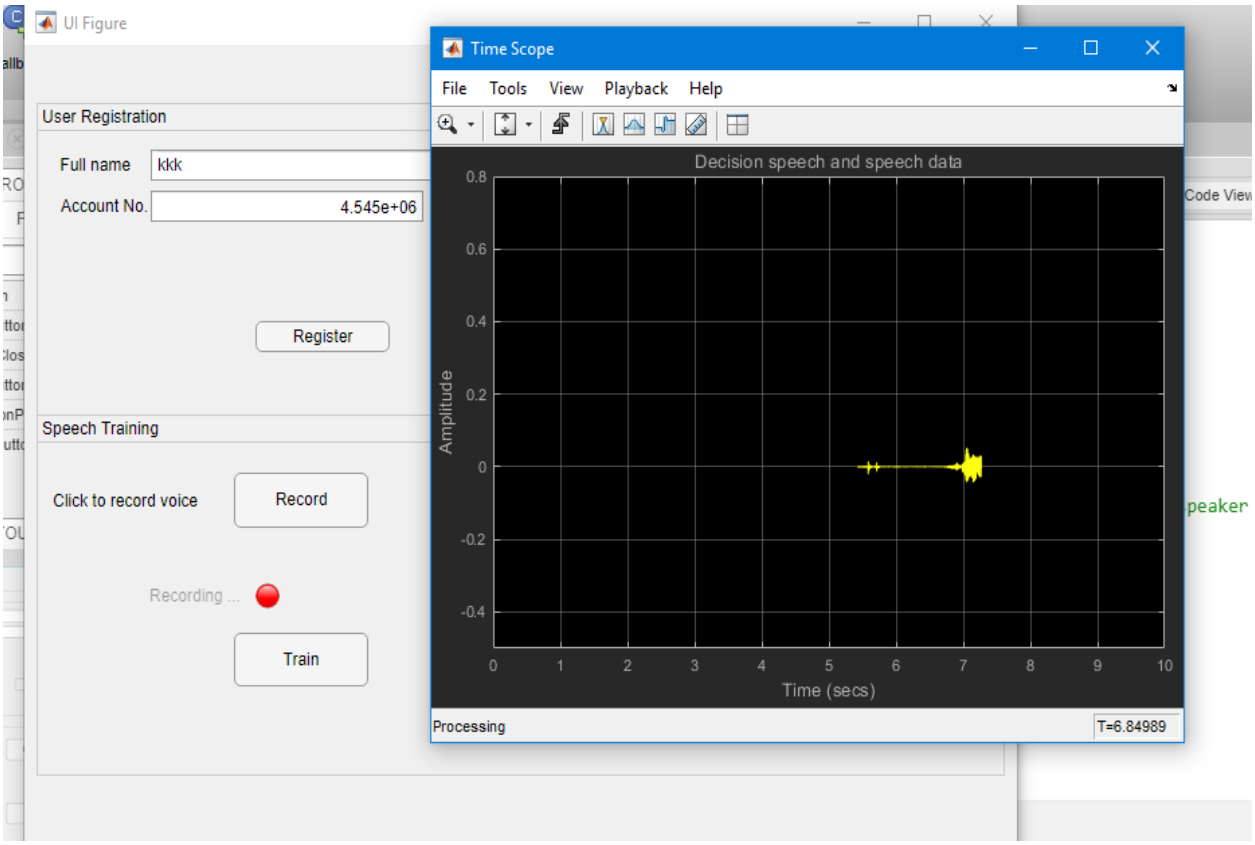

Fig. 5.4: Voice Registration

Fig. 5.4 is at the voice registration stage when the user registers her/his voice for the first time. It waits for 10 sec.

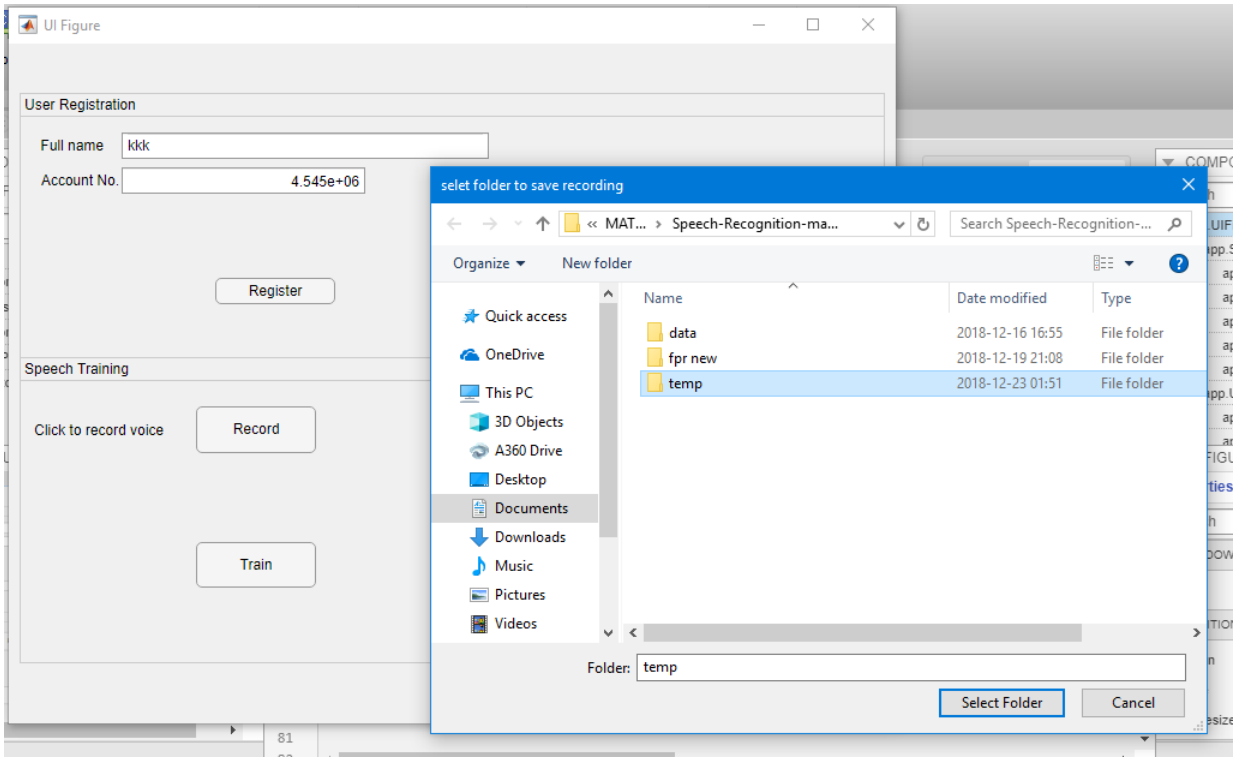

Fig. 5.5: File Browser Path

Fig. 5.5which prompts the clerk/bank users account manager to choose folder path for storage of recorded voice for future use. Actually the voice is stored for backup only the matching software uses only the voice features stored as a code book and similarly fingerprint image is stored for reference only the fingerprint matcher uses fingerprint features.

This system mainly focuses on two types of user authentications (fingerprint and voice recognition). Those authentication systems are a huge system by themselves. But here I used the block code just to show that which can be implement on ATM machine for enhancement. So that, this system can registers users fingerprint and voice on the database for the first time while they request to ATM card. And then it verifies the data which are stored in the database with that of the current user fingerprint and voice.

So that we can enhance ATM security by implementing those authentications system to the current ATM machine by using external input output device like USB flash drive, for finger print scanner and for voice recorded but it may cost for additional cost. And those banks when they deploy a new ATM machine, those machines should have this biometric future.

Hence I need to pass a suggestion to those banks, when they deploy ATM machines they can put this authentication system as a mandatory basic requirement. Not only those techniques but they have to enforce that ATM machine should include vibration detection system this is important to secure the ATM machine form physical attach

CHAPTER SIX

6. LIMITATIONS AND CONTRIBUTIONS

6.1. Limitations

In this section we mention the limitations which and the contributions of our work. This study entirely focuses on one state owned commercial bank and five private banks which give ATM services.

The study will not cover all commercial banks because of resource constraint. We only design the framework which is going to enhance ATM security while the user interacts with ATMs. The main limitation is to develop the new security system and test it on a real world ATM system equipped those hardware equipments are expensive and the tools are not available in our country easily. It needs huge amount of budgets to implement practically and to design the system. The other limitation is that the public doesn't have that much knowledge of using ATM and the lack of awareness is the main key to challenge in using additional methods (biometrics) for more security and safety. Due to the step introduced in authentication process timing is very high but it ensures inclusive security to users.

6.2. Contributions

This research work tried to investigate threats, vulnerabilities, and physical security issues and it came up with ATM security framework. This work also identifies the existing problems and suggests equivalent solutions to those problems. These proposed solutions are to be used in the customer biometric authentication like fingerprint and voice recognition. Besides the work also suggested vibration detection methods which are going to secure the ATM machine physically. This work also gives customer awareness about general ATM security.

CHAPTER SEVEN

CONCLUSIONS, RECOMMENDATIONS AND FUTURE WORKS

1.1. Conclusions

In today's technology in the bank industry, security is a very important part. Business partners, suppliers, customers, and vendors require high security system from each corner.

Today banking system is changing and innovating for quick and safe transactions at minimum cost and the banking sector is in no way left behind from the other industries. But when we came to our banks this enhancement is not reflected. Banks ability to take advantage of new opportunities often depends on its ability to provide open, accessible, available, and secure network connectivity and services. As stated on the statement of the problem and identified through this study the current ATM system has feasible vulnerabilities. Though this research study tries to find a solution that can fill those gaps using an integrated biometrics framework that can co-side with PIN based ATM system. Based on the proposed framework and the prototype tested, embedding biometrics mainly fingerprint and voice to the ATM definitely boost the security level a step forward.

The conclusion that needs to be emphasized mainly for banks of Ethiopia this is right time to realize the cost benefit analysis and make a progressive decision in order to address traits and hazards standing on the way.

At the same time I recommend to banks in Ethiopia better to realize the risk factor ahead of time on their ATM service. And make a biometrics supported system to the ATM machine that is far more secure in addition to the current PIN based system. Even if this new embedded system may have its own expense especially on the direct machine cost and infrastructure issues but this will be a long run investment in order to get customer trust and secure system at it best.

1.2. Recommendations

The following recommendations are stated to improve to the secure implementations of ATMs in Ethiopia and beyond.

1. All banks must announce while implementing those biometric techniques to all system users through Media.
2. For efficient use of the system, the administration should give intensive training for the system administrator and for the bank user.
3. The software's and other tools must be installed by skill full professionals.
4. All banks should immediately implement such a system to overcome the different security problems.
5. To use the banks standardized ATM security framework.

1.3. Future Works

Some aspects of ATM security framework that are beyond the scope of this thesis research are recommended for future research. In this work we did not implement the framework in real world scenarios, so we suggest implementing this framework. Looking into other biometric methods which can be useful for our country is an open area would also be an interesting endeavor.

Furthermore, ATM systems enables with vibration sensors would be an open and demanded features in the industry as many of the security challenges are physical attacks. This vibration sensor is used to secure the physical part of the ATM from physical damage. This sensor will measure the vibration rate; if it is above the threshold then it will send the alarm to security guard.

REFERENCES

[1] Julia Kagan website, “Automated Teller Machine-ATM.” http://www.investopedia.com/terms/a/atm.asp#ixzz49M9IGEgj.08-Jun-2016.

[2] Ayana Gemechu, 2012 “Adoption of Electronic banking system in Ethiopian Banking industry:’ Barriers and Drivers,”

[3] CBE, “Profile of the commercial bank of Ethiopia (CBE).” 2014.

[4] All Africa website, “ATM Fraud.” Available: http://allafrica.com/stories/201103040726.html,http://ethiofact.com/4974/four-nigerian-nationals-jailed-in-ethiopia-over-atm-fraud/. [Accessed: 10-Jun-2016].

[5] Lachlan Gunn, E.A.S.T, “European ATM crime report.”2016.

[6] J. Braeuer, B. Gmeiner, and J. Sametinger,“ATM Security A Case Study of a Logical Risk Assessment,” 2018, pp. 355–362.

[7] N. Sharma, “Vulnerability and security issues in Auto teller machine transactions.”

[8] G. Equipment, “Best Practice for ATM Security,” 2011.

[9] IASSCORE, “Types of ATM Fraud.” Available: http://iasscore.in/national-issues/types-of-atm-fraud. [Accessed: 23-Nov-2016].

[10] J. N. Oruh, 2014 “Three-Factor Authentication for Automated Teller Machine System,” vol. 4, no. 6, pp. 160–166.

[11] M. E. Alhassan, 2015 “An Enhanced ATM Security System using Second-Level Authentication,” vol. 111, no. 5, pp. 8–15.

[12] D. Malviya, 2014 “Face Recognition Technique : Enhanced Safety Approach for ATM,” vol. 4, no. 12, pp. 1–6.

[13] S. Salunke, R. Mane, and P. Khatavkar, 2012 “Multilevel ATM Security Based On Two Factor Biometrics,” vol. 1, no. 8, pp. 1–6.

[14] F. S. Hossian, A. Nawaz, and K. Grihan, 2013 “Biometric Authentication Scheme for ATM Banking System Using Energy Efficient AES Processor,” vol. 2, no. 4, pp. 57–63.

[15] B. V Prasanthi, U. P. Jyothi, S. Bonthu, and T. V. Krishna, 2014 “International Journal of Advanced Research in Computer Science and Software Engineering Security Enhancement of ATM System with Fingerprint and DNA Data,” vol. 4, no. 12, pp. 477–479.

[16] A. I. Technology, 2012 “NOVEL HYBRID TECHNOLOGY IN ATM SECURITY USING,” vol. 37, no. 2, pp. 217–223.

[17] S. P. Balwir, M. K. R. Katole, R. D. Thakare, N. S. Panchbudhe, and P. K. Balwir, 2014 “Secured ATM Transaction System Using Micro-Controller,” vol. 4, no. 4, pp. 1358–1362.

[18] V. E. R. E. M. Aram, M. I. S. Ajid, A. L. I. B. Aig, and N. A. R. Eddy, 2015“Advanced Security Management System for ATM â€TM s using GSM and MEMS,” vol. 3, no. 3, pp. 343–345.

[19] V. V Jog, 2014 “Advanced Security Model for Detecting Frauds in ATM Transaction,” vol. 95, no. 15, pp. 47–50.

[20] V. I. A. S. E. S. Haring, 2015 “SFAMSS : A S ECURE F RAMEWORK F OR ATM M ACHINES,”

vol. 7, no. 2, pp. 71–78.

[21] S. M. S. Daula, 2012 “An Embedded ATM Security Design using ARM Processor with Fingerprint recognition and GSM,”.

[22] S. A. Patil and S. A. Hage, 2015 “Improving ATM Security Using 3D Password,” pp. 8308–8312.

[23] Atmmarketplace, “New ATM security measures tackle fraud.” Available: https://www.atmmarketplace.com/articles/new-atm-security-measures-tackle-fraud/.

[24] The hacker new, “Hackers stole $800,000 from ATMs using Fileless Malware.” Available: http://thehackernews.com/2017/04/atm-fileless-malware.html.

[25] ATM Marketplace, “ATM fraud by the numbers.”

[26] European ATM Crime Report, “Card Skimming.” Available: https://www.association-secure-transactions.eu/tag/card-skimming/. [Accessed: 24-May-2017].

[27] Stephen Mayhew, “BoA supports ATM withdrawals using Apple Pay.” Available: http://www.biometricupdate.com/201606/boa-supports-atm-withdrawals-using-apple-pay. [Accessed: 23-Dec-2016].

[28] Stephen Mayhew, “Biometric authentication technology by Iris ID for South Korea’s Woori Bank.” Available: http://www.biometricupdate.com/201512/biometric-authentication-technology-by-iris-id-for-south-koreas-woori-bank. [Accessed: 23-Dec-2016].

[29] Justin Lee, “China Merchants Bank launches ATMs with facial recognition.” Available: http://www.biometricupdate.com/201510/china-merchants-bank-launches-atms-with-facial-recognition. [Accessed: 03-Nov-2016].

[30] Stephen Mayhew, “Diebold launches new 5500 ATM series with biometric finger-vein reader.” lable: http://www.biometricupdate.com/201410/diebold-launches-new-5500-atm-series-with-biometric-finger-vein-reader. [Accessed: 23-Dec-2016].

[31] B. V Prasanthi, U. P. Jyothi, S. Bonthu, and T. V. Krishna, 2014 “International Journal of Advanced Research in Computer Science and Software Engineering Security Enhancement of ATM System with Fingerprint and DNA Data,” vol. 4, no. 12, pp. 477–479.

[32] https://en.wikipedia.org/wiki/Automated_teller_machine

[33] Mr.P.Akilan1 , Mr.K.Gunasekaran2 , M.Tech. Mr.D.Saravanan 3 ,, 2014 “International Journal of Innovative Research in Science, Engineering and Technology Design of Two Tier Security ATM System with Multimodal Biometrics By Means of Fuzzy Logic ,” vol. 3, no. 1, pp. 2347–6710.

[34] https://money.howstuffworks.com/personal-finance/banking/atm2.htm

[35] https://www.techulator.com/experts/3526-How-does-an-ATM-work.aspx

[36] Falaye A., Adepoju A, 2014 “Journal of Internet Banking and Commerce, A Survey of ATM Security Implementation within the Nigerian Banking Environment ,” ISSN: 1204-5357.

[36] https://en.wikipedia.org/wiki/Vulnerability_(computing)

[37] https://en.wikipedia.org/wiki/Threat_(computer)

APPENDIX A: Questionnaire

Introduction for the Respondent

Dear respondents:-

This questionnaire is as part of towards a thesis on ATM security. It is expected to be filled out by different stakeholders in your organization: IT management, Network admin, E-Payment staffs, ATM support and so on.

The outcome of the study will be used, primary to pin point the major security issues in the ATM systems. We kindly request you to spend your precious time to fill this questionnaire as candidly and reasonably as possible.

NB: Be sure that all the information you provide will remain confidential and will be used for the research purpose only. So, please be confident and frank to give your responses to the best of your knowledge. Ahead of time, we thank you for your cooperation!

Instruction: Please put a **"√"**sign in the square bracket [ ] for each item. You can also write your opinion or justification for open ended questions.

A. General Background of Respondents

I. **Demographic Information**

The following questions concern your position and other personal information.

1. What is your gender? Male [ ] Female [ ]
2. What is your age group?

   21 to 25 [ ] 26 to 30 [ ] 31 to 35 [ ] 36 to 40 [ ]
   41 to 45 [ ] above 45 [ ]
3. What is your Job Title? _____
4. Qualification

   10+2 [ ] 12+2 [ ] BSC/BA [ ] MSC/MA [ ] PhD [ ]
5. Year of service in this bank

   Less than 1 year [ ] 1 to 2 years [ ] 2 to 5 year [ ]

5 to 10 years [ ] more than 10 years [ ]

6. Year of service in your current position?

   Less than 1 year [ ] 1 to 2 years [ ] 2 to 5 year [ ]

   5 to 10 years [ ] more than 10 years [ ]

7. How frequently do you use your ATM card?

   [ ] Daily

   [ ] 3-5 times per week

   [ ] 4-6 times within 15 days

   [ ] Once or twice per month

   [ ] Never used my ATM card.

   [ ] I don't have an ATM card

8. If your answer for question #7 is "Never used my ATM card" or "I don't have an ATM card", what your major reason for those point? Please specify.

   _____

   _____

   _____

   _____

Part II. Physical and Environmental Security

1. How Many ATM Machines does the Bank have? _____
2. How does the Bank Locate those ATM Machine?

2.1. Near to Branches [ ] Yes [ ] No

2.2. Near to Hotels [ ] Yes [ ]No

2.3. Near to Malls [ ] Yes [ ] No

2.4. Near to Hospitals [ ] Yes [ ] No

2.5. Other Public Places [ ]Yes [ ]No

2.6. Any other, please specify _____

3. What kind of security enforcement is/are used to protect ATMs.
    3.1. Access control [ ] Yes [ ] No
    3.2. Security Alarm Terminal [ ] Yes [ ] No
    3.3. CCTV [ ] Yes [ ] No
    3.4. Security Guards. [ ] Yes [ ] No
    3.5. Central Monitoring Station [ ] Yes [ ] No
    3.6. Any other, please specify_____
4. Does your ATM have USB sockets or Pot? [ ] Yes [ ] No
5. Does any Physical attack occurred? [ ] Yes [ ] No
6. What kind of physical attack happens in your banks?
    6.1. Card Skimming [ ] Yes [ ] No
    6.2. Card Trapping [ ] Yes [ ] No
    6.3. Robbery [ ]Yes [ ] No
    6.4. Using Explosive Gas [ ] Yes [ ] No
    6.5. Any other, please specify _____
7. How often do those attacks happen in your bank history?
    [ ] 1- 3 [ ] 3 -7 [ ] 8- 12 [ ] above 12
8. How do you extract the threat, if you are using a system what system is being used?

    _____

    _____

    _____
9. What security measures are being rolled out to stop the flood of ATM crime and help to deal with customer queries?

    _____

    _____

    _____

Part III. Logical security

1. What Operating System is installed on your ATM?

1.1. Windows

1.2. Linux [ ]

1.3. Any other, please specify _____

2. Do you have firewalls that protect the ATMs from attackers and cyber threats?
[ ] Yes [ ] No

3. Does the bank have effective tracking and monitoring system? [ ] Yes [ ] No

4. What kind of monitoring tool does the bank have? _____

5. How frequently does the monitoring system work? [ ] 24/7 [ ] Daily [ ]weekly

6. How does the transmission going on, which means does data is used encryption during transmission across open or public networks? [ ] Yes [ ] No

7. What kind of encryption technologies does the bank follow? _____

8. Is there formally defined user access control policy document for granting access to multi-user information systems and services? [ ] Yes [ ] No

9. Do you use regular update of antivirus software? [ ]Yes [ ] No

10. If your answer for question #9 is yes, at what interval do you update it?

_____

11. Do you adopted or developed security software to control your ATM infrastructure?

[ ] Yes [ ] No

12. Does the bank has formal user registration and de-registration procedure document?

[ ] Yes [ ] No

13. Do you have any procedure to review user access rights at regular intervals?

[ ] Yes [ ] No

14. If your answer for question #13 is yes, how often do you conduct the review?

_____

15. Does the bank has password guidelines (about its complexity, change period, password reset, access attempt and lockout ...etc.) for users in selecting and maintaining of passwords [ ] Yes [ ] No

16. Do you have any authentication mechanism for challenging external connections? [ ] Yes [ ] No

17. If your answer to question # 16 is yes, which of the following mechanisms are used?

a. Cryptography based technique (Encryption &Digital signature) [ ] Yes [ ] No

b. Hardware or software tokens [ ] Yes [ ] No

18. Are security requirements derived from a business risk assessment? [ ] Yes [ ] No

19. Is there a culture of conducting security requirement study before systems development and test its security related issue in your bank? [ ] Yes [ ] No

20. Do you have a framework which is used as a system view or model to manage and administer the banks ATMs? [ ] Yes [ ] No

21. If your answer for question #20 is yes, what framework are you using?

_____

_____

_____

22. What suggestion do you have about ATM security in general and in Ethiopia in particular?

_____

_____

_____

APPENDIX B: Interview Questions

8. What is your understand about ATM users?
9. How do you protect the machines if the users use the ATMs unknowing? Do you have procedures to guide the users?
10. What kind of authenticate mechanisms do you used to secure the ATM transaction? Is their new enhancement to secure the ATMs?
11. Now days, all banks use one ATM card (Other Bank ATM) so, how do you secure users as well as the ATMs.
12. Do you have a framework to secure the ATMS?
13. Do you follow PCI DSS standard? If your answer is yes, which of them are deploying in your Bank?
14. How do you monitor the system? Is there monitoring system? If your answer is yes, what monitoring system do you use?

APPENDIX C:SampleMATLABcode

```
% Main---- project beigns here
varargin=op;
if op==1
Fingerprint_matcher();
elseif op==2
voice_recognition();
else
Fingerprint_matcher();
end
datafolder = fullfile('C:\Users\Dell\Desktop\Thesis_proj\Speech-Recognition-
master3','data','train');

ads = audioexample.Datastore(datafolder, ...
'IncludeSubfolders',true, ...
'FileExtensions','.wav', ...
'LabelSource','none', ...
'ReadMethod','File')
function recorder(trainpath)
tvoice=ls(trainpath);
[n,~] = size(tvoice);
deviceReader = audioDeviceReader;
setup(deviceReader);
scope = dsp.TimeScope(1,'SampleRate',44100, ...
'BufferLength', 80000, ...
'YLimits', [-0.3 1.1], ...
'ShowGrid', true, ...
'Title','Decision speech and speech data', ...
'TimeSpanOverrunAction','Scroll');
rvoice = sprintf('%ss%d.wav',trainpath,n);
fileWriter = dsp.AudioFileWriter(rvoice,...
'FileFormat','WAV');
disp('Speak into microphone now.')
tic;
whiletoc< 10
acquiredAudio = deviceReader();
fileWriter(acquiredAudio);
scope(acquiredAudio);
end
release(scope);
release(deviceReader);
end

functioncodebk = vqCodeBook(d, k)
```

```
e = 0.0001;
codebk = mean(d, 2);
distortion = int32(inf);
numOfCentroids = int32(log2(k));

fori=1:numOfCentroids
codebk = [codebk*(1+e), codebk*(1-e)];
while(1==1)
dis = distance(d, codebk);
      [m,ind] = min(dis, [], 2);
      t = 0;
lim = 2^i;
for j=1:lim
codebk(:, j) = mean(d(:, ind==j), 2);
         x = distance(d(:, ind==j), codebk(:, j));
len = length(x);
for q = 1:len
            t = t + x(q);
end
end
if (((distortion - t)/t) < e)
break;
else
distortion = t;
end
end
end
```

```
function d = distance(x, y)
[M, N] = size(x);
[M2, P] = size(y);

if (M ~= M2)
error('Matrix dimensions do not match.')
end

d = zeros(N, P);

if (N < P)
copies = zeros(1,P);
for n = 1:N
d(n,:) = sum((x(:, n+copies) - y) .^2, 1);
```

```
end
else
copies = zeros(1,N);
for p = 1:P
d(:,p) = sum((x - y(:, p+copies)) .^2, 1)';
end
end

d = d.^0.5;



function listener(trainpath)
deviceReader = audioDeviceReader;
setup(deviceReader);
scope = dsp.TimeScope(1,'SampleRate',44100, ...
'BufferLength', 80000, ...
'YLimits', [-0.3 1.1], ...
'ShowGrid', true, ...
'Title','Decision speech and speech data', ...
'TimeSpanOverrunAction','Scroll');
rvoice = sprintf('%ss%d.wav',trainpath,currentspeaker);
fileWriter = dsp.AudioFileWriter(rvoice,...
'FileFormat','WAV');
disp('Speak into microphone now.')
tic;
whiletoc< 10
acquiredAudio = deviceReader();
fileWriter(acquiredAudio);
scope(acquiredAudio);
end
release(scope);
release(deviceReader);
end


function m = melFilterBank(p, n, fs)
f0 = 700 / fs;
fn2 = floor(n/2);

lr = log(1 + 0.5/f0) / (p+1);

bl = n * (f0 * (exp([0 1 p p+1] * lr) - 1));

b1 = floor(bl(1)) + 1;
b2 = ceil(bl(2));
b3 = floor(bl(3));
```

```
b4 = min(fn2, ceil(bl(4))) - 1;

pf = log(1 + (b1:b4)/n/f0) / lr;
fp = floor(pf);
pm = pf - fp;

r = [fp(b2:b4) 1+fp(1:b3)];
c = [b2:b4 1:b3] + 1;
v = 2 * [1-pm(b2:b4) pm(1:b3)];

m = sparse(r, c, v, p, 1+fn2);


function c = mfcc(s, fs)
N = 256;
M = 100;
len = length(s);
numberOfFrames = 1 + floor((len - N)/double(M));
mat = zeros(N, numberOfFrames);
fori=1:numberOfFrames
index = 100*(i-1) + 1;
for j=1:N
mat(j,i) = s(index);
index = index + 1;
end
end

hamW = hamming(N);
afterWinMat = diag(hamW)*mat;
freqDomMat = fft(afterWinMat);

filterBankMat = melFilterBank(20, N, fs);
nby2 = 1 + floor(N/2);
ms = filterBankMat*abs(freqDomMat(1:nby2,:)).^2;
c = dct(log(ms));
c(1,:) = [];
```