Enhancing the Security Features of Automated Teller Machines (ATMs): A Ghanaian Perspective

Nana Kwame Gyamfi
Computer Science Department, Kumasi Polytechnic
Kumasi, Ghana

Mustapha Adamu Mohammed
Computer Science Department, Koforidua Polytechnic
Ghana

Kwaku Nuamah-Gyambra
Computer Science Department, Koforidua Polytechnic
Ghana

Dr. Ferdinand Katsriku
University of Ghana
Department of Computer Science

Dr. Jamal-Deen Abdulah
University of Ghana
Department of Computer Science

Abstract

The growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. Access codes for buildings, bank accounts and computer systems often use personal identification numbers (PIN's) for identification and security clearances. Conventional method of identification based on possession of ID cards or exclusive knowledge like a social security number or a password are not all together reliable. An embedded fingerprint biometric authentication scheme for Automated Teller Machine (ATM) banking systems is proposed in this paper. Over the past three decades, consumers have been largely depending on and trusting the Automatic Teller Machine (ATM) to conveniently meet their banking needs. However, despite the numerous advantages of the ATM system, ATM fraud has recently become more widespread. In this paper, we provide an overview of the possible fraudulent activities that may be perpetrated against ATMs and investigate recommended approaches to prevent these types of frauds. In particular we develop a prototype model for the utilization of biometrics equipped ATM to provide security solutions against most of the well-known breaches, from a Ghanaian perspective. To ensure that such security approach will be accepted by the majority of users, our model was tested and the users' opinions were given.

Keywords: Automated Teller Machines (ATMs), Biometric Technology, Bank Customers, Electronic, Security.

1. Introduction

Rapid development of banking technology has changed the way banking activities are dealt with. One banking technology that has impacted positively and negatively to banking activities and transactions is the advent of Automated Teller Machines (ATMs). With an ATM, a customer is able to conduct several banking activities such as cash withdrawal, money transfer, paying phone and electricity bills beyond office hours and physical Interaction with bank staff. In a nutshell, ATM provides customers a quick and convenient way to access their bank accounts and to conduct financial transactions. A Personal Identification Number (PIN) or password is one important aspect of the ATM security system. PIN or password is commonly used to secure and protect financial information of customers from unauthorized access [10]. An ATM (known by other names such as an automated banking machine, cash point, cash machine or a hole in the wall) is a mechanical system that has its roots embedded in the accounts and records of a banking institution [10] [13].

It is a computerized machine designed to dispense cash to bank customers without the need of human interaction; it can transfer money between bank accounts and provide other basic financial services such as balance inquiries, mini statement, withdrawal and fast cash among others [5]. The old saying puts necessity as the mother of invention, but in today‘s world, the relationship is sometimes reversed. Technological advances often come first and drive the search for commercial applications. This situation is true in the field of biometric identification, whereby the automated identification of people by biological characteristics such as their fingerprints or iris patterns. In the past two years, rapid decreases in price and better performance have made biometric technology practical for consumer applications such as accessing automatic teller machines (ATMs) and for governmental purposes such as confirming the identities of welfare recipients.

But a sharp debate is emerging over whether biometric technology offers society any significant advantages over conventional forms of identification, and whether it constitutes a threat to privacy and a potential weapon in the hands of authoritarian governments. The use of biological features for identification is of course not new—fingerprinting was developed in the 19th century—nor is automation of the process. Beginning in the late 1970s, defense and national security agencies that could afford it started using automatic biometric systems to check identities as a more secure alternative to photo-IDs. But more widespread applications did not emerge until greater computing power dropped the price of biometric systems.

For example, a fingerprint scanner that cost $3,000 five years ago, with software included, and $500 two years ago, costs $100 today. Similar price reductions have occurred in other leading biometric technologies, such as iris scanners. With lower prices, biometric identification systems are moving into two main application areas—banking and governmental agencies—and they have spurred growth in the new industry to nearly $250 million a year in annual sales. Several banks around the world, including Bank United (Houston, TX) and Nationwide Building Society in the United Kingdom have tested iris scanners as an alternative to personal identification number (PIN) codes for ATM access. On a larger scale, the state of Connecticut began to use fingerprint scanning in 1996 as a way to identify welfare recipients, and the U.S. Army, Air Force, and Social Security Administration are looking at various biometric recognition systems. Both the Department of Defense and the Department of Veterans Affairs plan to use finger images to verify the identity of employees and those seeking retirement benefits.

In the case of banking, the advantages of biometric scanners are mainly convenience rather than security. ―Customers like the ease of just going up to the ATM and staring at it for a few seconds. Although biometric technology protects against a thief who can guess a carelessly chosen PIN code, it does nothing to prevent the more common holdups in which an ATM customer is robbed near the machine or forced at gunpoint to withdraw money. The advantages for government agencies are clearer, as biometrics make the creation of false identities harder. But this is precisely what concerns some privacy and efforts are under way to develop automatic signature identification and voice-identification systems.

In this paper, we therefore provide an overview of the possible fraudulent activities that may be perpetrated against ATMs and investigate recommended approaches to prevent these types of frauds. In particular we develop a prototype model for the utilization of biometrics equipped ATM to provide security solutions against most of the well-known breaches. To the best of our knowledge, ATMs in the Banking Industry of Ghana are not biometrically equipped, which makes our objectives for this research paper a necessity.

II. Problem Statement

Previously, cash withdrawal, cash deposit and bank account details of customers through banking activities were very tough and tedious, but nowadays various banks have implemented electronic banking activities which allow customers to use the ATM because it’s banking conveniences in relation to the above activities. Many banks worldwide has installed ATMs in various places/cities/towns/rural areas so customers of banks can easily withdraw cash and check their balance and perform any other banking transaction with ATMs.

However, users/customers of such electronic transactions have many passwords used to access their e-mails, car radios, mobile phones, computers, ATM Cards etc. and users have many cards like Credit Card, Debit Card, and Identity Card etc. Therefore, many problems are faced by users in relation to their ATM Cards and PINs, some of these problems are elaborated below:

Sometimes a lot of effort is involved when users/customers are required to remember different passwords. On many occasions users forget their passwords. Forgetting passwords sometimes create a problem of not performing a required transaction and inputting wrong password will likely lead to hacking/seizure/locking of the ATM card. ATM cards have to be mobile in order to be used. Forgetfulness of ATM cards at the point of transaction will always yield no transactions and negative results.

Sometimes users/customers use a common PIN/password for all electronic transactions things. In such cases, there are weakness and deficiency of security, because any other person who knows a common password of another can easily use his/her ATM card. In order to eradicate these types of deficiencies, we propose the ATM machine with the biometric system. Various biometric technologies such as iris, finger, voice, wrist etc. are currently being used on a global scale in developing countries. Each user has its unique identity based on physical or behavioral attributes. These attributes are never stolen by any person.

III. Types of ATM Frauds

In the last few years, there have been many reports of hacking into the electronic ATM system and this has caused losses of billions of dollars in the global banking industry. Oracle attack on authentication protocols and breaches affecting ATMs such as cloning of cards and hacking of PIN code have been increasingly been reported. Some popular ATM frauds/attacks are explained in the subsections below.

I. Skimming Attacks

This is the most popular breach in ATM transaction. In this ingenious rip-off, lawbreakers are taking advantage of technology to make counterfeit ATM cards by using a skimmer (a card swipe device that reads the information on ATM card). These devices resemble a handheld credit card scanner and are often fastened in close proximity to or over the top of an ATM‘s factory-installed card reader. When removed from the ATM, a skimmer allows the download of personal data belonging to everyone who used it to swipe an ATM card. A single skimmer can retain information from than 200 ATM cards before being re-used.

II. Card Trapping

This involves placing a device directly over or into the ATM card reader slot. In this case, a card is physically captured by the trapping device inside the ATM. When the user leaves the ATM without their card, the card is retrieved by thieves/criminals. Typically only one card is lost in each attack. The most common variant is known as the Lebanese Loop

III. Pin Cracking

Attacks on customers ‘PINs have been known to security researchers for years, e.g., [3], [9], [7]. One of the most efficient of these _PIN cracking‘attacks was discussed in [8]. How the processing system used by banks is open to abuse was explained in [8]. One of the attacks, targets the translate function in switches - an abuse function that is used to allow customers to select their PINs online. In either case, the flaws create a means for an attacker to discover PIN codes, for example, those entered by customers while withdrawing cash from an ATM provided they have access to the online PIN verification facility or switching processes. A bank insider could use an existing Hardware Security Module (HSM) to reveal the encrypted PIN codes.

In a worst case scenario, an insider of a third-party switching provider could attack a bank outside of his territory or even in another continent. Unfortunately, proposals to counter such attacks are almost nonexistent other than a few suggestions; for example, maintaining the secrecy (and integrity) of some data elements related to PIN processing (that are considered security insensitive according to current banking standards) such as the decimalization table‘and _PIN Verification Values (PVVs) /Offsets‘have been emphasized [9], [8].

IV. Phishing/Vishing Attack

Phishing scams are designed to entice the user to provide the card number and PIN for their bank card. Typically, an attacker uses email representing them as a bank and claiming that user account information is incomplete, or that the user needs to update their account information to prevent the account from being closed. The user is asked to click on a link and follow the directions provided. The link however is fraudulent and directs the user to a site set up by the attacker and designed to look like the user’s bank. The site directs the user to input sensitive information such as card numbers and PINs. The information is collected by the thieves/criminals/hackers and used to create fraudulent cards. Some variants are spear phishing and Rock Phish attacks.

Traditionally, after a successful phishing attack, the criminal would extract the needed information and go into the online account and remove the victim's bank funds. This has changed for some of the more sophisticated criminals in recent years were instead of looting the victim's account; they go to the check image page, where they take a copy of the victim's check. Many financial institutions are now offering check images as part of their online banking services to their customers. The checks contain the victim's bank account number, signature, address, phone etc. The attacker can either take the copy and make paper counterfeit checks, or take that information and create PayPal accounts or other online payment accounts that will leave the victim on the hook for any purchases.

V. ATM Malware

Malware attacks require an insider, such as an ATM technician who has a key to the machine, to install the malware on the ATM. Once that has been done, the attackers can insert a control card into the machine‘s card reader to trigger the malware and give them control of the machine through a custom interface and the ATM‘s keypad. According to a report in [11], a Trojan family of malware infected 20 ATMs in Eastern Europe. The malware lets criminals take over the ATM to steal data, PINs and cash. The malware captures magnetic stripe data and PIN codes from the private memory space of transaction processing applications installed on a compromised ATM.

VI. ATM Hacking

Attackers use sophisticated programming techniques to break into websites which reside on a financial institution's network. Using this access, they can access the bank's systems to locate the ATM database and hence collect card information which can be used later to create a clone card. Hacking is also commonly used to describe attacks against card processors and other components of the transaction processing network. Most of the ATM Hackings is due to the use of non-secure ATM software.

VII. Physical Attack

ATM physical attacks are attempted on the safe inside the ATM, through mechanical or thermal means with the intention of breaking the safe to collect the cash inside. Some of the most common methods include ram raids, explosive attacks and cutting. Robbery can also occur when ATMs are being replenished or serviced. Staffs are either held up as they are carrying money to or from an ATM, or when the ATM safe is open and cash cassettes replaced. There are a variety of mechanical and physical factors that can inhibit attacks to the safe. The certification level of the safe (UL 291 Level 1 is recommended as a minimum for ATMs placed in unsecured, unmonitored locations). Alarms and sensors that will detect physical attacks on the ATM safe. Ink stains technologies that will run and make unusable any removed banknotes.

IV. Security Measures of ATMS

As technology advances and ATM applications become more ubiquitous, there is more of confidential data being transmitted over the ATM system. As more sensitive transactions are conducted, more threats breaches are reported and the challenge of securing the system becomes more urgent. Many security services in bank transactions are dependent on authenticating users such as generation of accurate audit trails, non-repudiation in communications, preserving confidentiality and other input validation techniques such as batch totals, format checks, reasonableness checks and transaction validation.

These features only ensure that certain procedures are followed and cannot tell whether the person with the card and PIN is authorized to use it, they just ensure that the data transmitted follows certain guidelines or protocols that request transactions such as cash withdrawals are made within reasonable limits, that money is transferred to the proper account, and so forth. Therefore, it is essential to develop stronger authentication and identification measures to stop criminals from committing fraudulent acts.

A. Electronic Banking System

Electronic banking which is an emerging paradigm in Ghana is a new industry which allows people to interact with their banking accounts via the Internet from virtually anywhere in the world. The electronic banking system addresses several emerging trends: customer demand for anytime, anywhere service, product time-to-market imperatives and increasingly complex back-office integration challenges. This system allows consumers to access their banking accounts, review most recent transactions, request a current statement, transfer funds, view current bank rates and product information and reorder checks. E-banking can be defined as the deployment of banking services and products over electronic and communication networks directly to customers [7].

It is the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels [8]. These electronic and communication networks include Automated Teller Machines (ATMs), direct dial-up connections, private and public networks, the Internet, televisions, mobile devices and telephones. Among these technologies, the increasing penetration of personal computers, relatively easier access to the Internet and particularly the wider diffusion of mobile phones have drawn the attention of most banks to e-banking. Significant differences exist among banks in terms of their e-banking capabilities. These differences can take two main dimensions. The first is the use of electronic

B. Strengths and Advantages of Biometric Technology

Biometric technology identifiers are difficult to be lost or forgotten, difficult to be copied/shared and require the person to be authenticated to be present at the time and point of authentication (a user cannot claim his password was stolen and misused!!). Instead of passwords, biometric systems could be used to protect the strong cryptographic keys. Some strengths of biometric technology include the following:

Provision of strong authentication. Can be used instead of a PIN. Hidden or diminished costs of ATM card management like card personalization, delivery, management, re-issuance, PIN generation, help desk, and re-issuance can be avoided. It is accurate. Flexible account access allows clients to access their accounts at their convenience. The operational cost of the ATMs will ultimately reduce. For a given biometric identifier, all users have a relatively equal security level – One user‘s biometrics are no easier to break than another‘s. There cannot be many users who have ―easy to guess‖ biometrics that can be used to mount an attack against them. The commonly used biometrics are DNA, Face, Ear, Facial infrared thermo gram, Fingerprint, Gait, Hand and Finger geometry, Iris, Keystroke, Palm prints, Signature, Voice etc. which are very different amongst individuals [2].
The advantages of the biometric integrated systems in ATMs are:

This biometric integrated system of ATM is safer to the conventional ATM system. It recognizes the actual account holder nobody other than the card holder can operate the ATM. It can be only operated by the real account holder. It gives safety and security to the Bank account holders .It is 100% temper proof. It gives 100% security to the ATM card holders. If anyone obtains the pin number and other details of the ATM card holder even then it cannot be operated unless the thumb impression is matched. Biometric integrated systems in ATMs can be used in credit cards and debit cards and other online payment systems. The bank will also prefer this system with the viewpoint of security and customer care. Biometric integrated systems in ATMs will lessen the workload of the banks Biometric integrated systems in ATMs will increase the trust of the banking customer. Biometric integrated systems in ATMs can also be implemented with the CCTV surveillance and Alarms Bells to avoid the break open of the ATM Machine by the thieves. Biometric integrated systems in ATMs are useful to the illiterate person and for rural areas. With the combination of the PIN and biometric system the ATM transaction is fully secured. Biometric integrated systems in ATMs will minimize the chances of the blockage of account on account of wrong pin used by the ATM card holder.

V. Related Work

Shaikh and Rabaiotti [8] analyzed the United Kingdom (UK) Identity (Id) Card scheme. Their analysis approached the scheme from the perspective of high volumes of public deployment and they described a trade-off triangle model. They found that there are trade-offs between several characteristics, i.e. accuracy, privacy and scalability in a biometric based identity management system, where the emphasis on one undermines the other.
A Murthy and Reddy [3] developed an embedded fingerprint system, which is used for ATM security applications. In their system, bankers collect customers‘ finger prints and mobile numbers while opening accounts, and then customers only access the ATM. The ATM works in such a way that every time a customer places his/her finger on the printing module, the ATM automatically generates a different 4-digit code as a message to the mobile phone of the authorized customer through a GSM modem connected to the microcontroller. The code received by the customer is entered into the ATM machine by pressing the keys on the touch screen. After entering the received code, the ATM checks whether the code is a valid or not before allowing the customer further access and usage. Schouten and Jacobs [7] presented an evaluation of the Netherlands‘ proposed implementation of a biometric passport, largely focusing on technical aspects of specific biometric technologies (such as face and fingerprint recognition) but also making reference to international agreements and standards (such as ICAO and the EU‘s ―Extended Access Control‘‘) and discussed the privacy issue in terms of traditional security concepts such as confidentiality. Debbarma [10] proposed an embedded Crypto Biometric authentication scheme for ATM banking system.

The development and deployment phase of Belgium e-ID card has been discussed by Marein and Audenhove (2010). It has been argued that the preexistence of national register was one of the factors that have helped in the development of the Belgium e- ID card. So far eight million cards have been provided to Belgium citizens mentioning the process was smooth and straightforward (Marein and Audenhove, 2010). A discussion on security and the design of the Malaysian identity card, i.e., Mykad has been done by Raphael et al. (2003). Mykad integrates ID card, driving license, passport and ATM. Because Mykad is used for various sensitive purposes, Raphael et al. (2003) stated that its security features should be analyzed before it is deployed. It is important to consider the perceptions and response of end users while developing and analyzing biometric based identity management systems (Laurie et al., 2007).

VI. Research Design and Methodology

The security feature for enhancing the Indian Banking ATM was designed using the client/server architecture. In this scenario, there is a connection between the customer identification information, customer‘s accounts and records in the bank (server). The network is designed to support a large number of users and uses dedicated server to accomplish this. The reason for choosing a Client / Server model for our proposed system is because it provides adequate security for the resources required for a critical application such as banking systems. Similarly, a descriptive conceptual approach which includes Unified Modeling language (UML) tools such as use case models, activity diagrams & sequence diagrams etc. is adapted. The work is implemented using Visual Basic 6.0 software tools, used to design the user interfaces and/or cardholder interaction with the ATM Machine.

A. Population and Method of Data Collection

The target population of this study was customers and staff of some commercial banks in Awka, Anambra State, and Southeastern Nigeria. The customers and students were randomly selected. The instrument used for this study was a 16-item questionnaire developed by the researchers. The items in the questionnaire were derived from an extensive survey of relevant literature and oral interview. The instrument has three sections. The first section deals with participants‘profile. The second section deals with participants‘use and reliability of ATM. The third section deals with the reliability of fingerprint biometric characteristic. Of the 200 copies of the questionnaire administered, 163 usable copies were returned. This represented 82 % return rate. This study was carried out over a period of four months. The items in the instrument were analyzed using descriptive statistical methods [11] [6]. The secondary sources of data were obtained from journals, the Internet and textbooks. Expert judgments were used to ascertain the validity of the items in the questionnaire. Two experts face validated all the items in the questionnaire. The wordings of items were also checked for clarity. Two items in the questionnaire were deleted for irrelevance while three ambiguously worded items were restructured to reflect clarity. After the corrections, the two experts found the items to be suitable for administration on the subjects. The reliability co-efficient of the instrument was tested by using the Cronbach alpha which is adequate for reliability measure. The instrument yielded a reliability coefficient of 0.81.

VII. Proposed Biometric (Fingerprint) Strategy for Ghana Banking System

One of the best security measures against some of the attacks mentioned above is the deployment of biometrics in the current ATM system as discussed below.

Biometric Smartcard – A prototype

Biometric identification is utilized to verify a person‘s identity by measuring digitally certain human characteristics and comparing those measurements with those that have been stored in a template for that same person. Templates can be stored in the biometric device, the institution‘s database, a user‘s smart card, or a Trusted.

Third Party service provider‘s database. There are two major categories of biometric techniques: physiological (fingerprint verification, iris analysis, hand geometry-vein patterns, ear recognition, odor detection, DNA pattern analysis and sweat pore analysis), and behavioral (handwritten signature verification, keystroke analysis and speech analysis). In [12], it was found that behavior based systems were perceived as less acceptable than those based on physiological characteristics. Of the physiological techniques, the most commonly utilized is that of fingerprint scanning. With biometrics, such fraudulent incidents can be minimized, as an added layer of authentication is now introduced that ensures that even with the correct pin information and in possession of another person’s ATM card, the user‘s biometric features cannot easily be faked.

In banking system Biometrics holds the promise of fast, easy-to-use, accurate, reliable, and less expensive authentication for a variety of applications [2]. At the time of transaction customers enrollment their fingerprint to a high resolution fingerprint scanner. The fingerprint image is transmitted to the central server via secured channel. At the banking terminal the minutiae extraction and matching are performed to verify the presented fingerprint image belongs to the claimed user in bank database. The authentication is signed if the minutiae matching are successful. The proposed scheme is fast and more secure. Fig 1 shows the whole procedures for proposed banking biometric application system in India. A basic biometric authentication system consists of five main components.

These are: sensor, feature extractor, fingerprint/template database, and matcher and decision module. The function of the sensor is to scan the biometric trait of the user. The function of the feature extraction module is to extract the feature set from the scanned biometric trait. This feature set is then stored into the template database. The matcher modules take two inputs, i.e. feature sets from the template database and feature set of the user who wants to authenticate him and compares the similarity between the two sets. The last module, i.e., the verification module makes the decision about the matching of the two feature sets. Biometrics is a rapidly evolving technology that is being widely used in forensics, such as criminal identification and prison security, and that has the potential to be used in a large range of civilian application areas. Biometrics can be used to prevent unauthorized access to ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks.

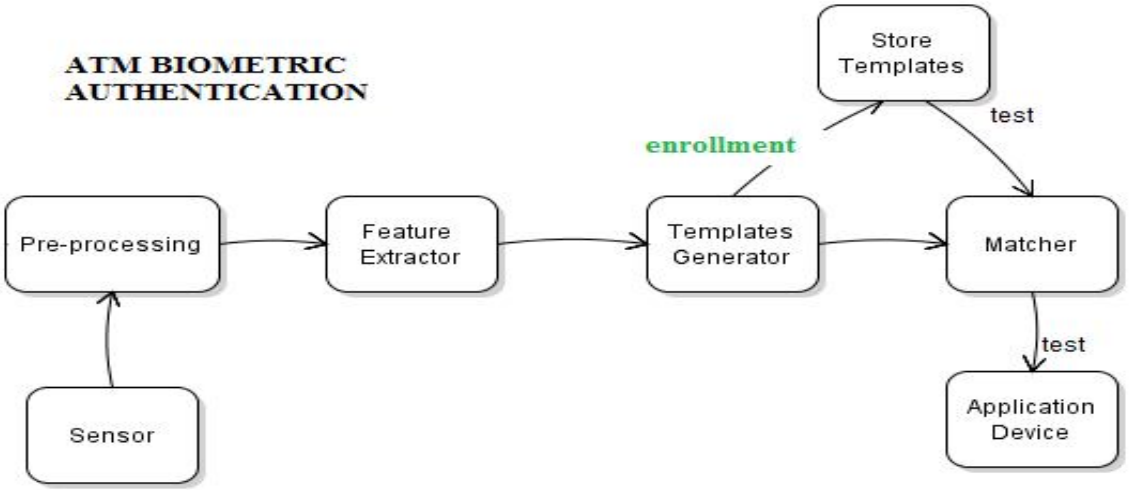

Fig 1: Working of biometric authentication

The figure 1 above shows the working of biometric authentication process.
A biometric device works on the basis of some human characteristics, such as fingerprint, voice or patter of line in the iris of your eye. These devices include handprint detectors, voice recognizers and identification patter in the retina. Authentication with such devices uses unforgivable physical characteristics to authenticate users. The user database contains a sample of user's biometric characteristics. During authentication, the user is required to provide another sample of the users biometric characteristics. This is matched with the one in the database, and if the two samples are the same, then the user is considered to be a valid user. The advantages of this may include: all attributes of the ATM cards will be maintained, counterfeiting attempts are reduced due to enrollment process that verifies identity and capture biometrics, and it will be extremely high security and excellent user-to-card authentication. These advantages are for the benefit of users as well as system administrators because the problems and costs associated with lost, reissued or temporarily issued can be avoided, thus saving some costs of the system management. On the negative side, the major risk posed by the use of biometric systems is that a malicious subject may interfere with the communication and intercept the biometric template and use it later to obtain access [4]. Likewise, an attack may be committed by generating a template from a fingerprint obtained from some surface. Although few biometric systems are fast and accurate in terms of low false acceptance rate enough to allow identification (automatically recognizing the user identity), most of the current systems are suitable for the verification only, as the false acceptance rate is too high.

The propose design uses a maximum of 8 characters, numbers or a mix of the both PIN and fingerprint as verification factors of the authentication process. ACOS smartcards and AET60 BioCARD Key development kit were used in the propose design. In the verification part, the users have to submit the correct PIN DES encrypted current session key to get access to the next level. Users have 3 successful attempts to enter the correct PIN, else the cards will be locked and render it to uselessness. Lastly, we use the fingerprint as the biometric identifiers as it takes shortest enrollment time.

Reliable, user authentication is becoming an increasingly important task in the Web-enabled world. The consequences of an insecure authentication system in a corporate or enterprise environment can be catastrophic, and may include loss of confidential information, denial of service, and compromised data integrity. The value of reliable user authentication is not limited to just computer or network access. Many other applications in everyday life also require user authentication, such as banking, e-Commerce, and physical access control to computer resources, and could benefit from enhanced security.

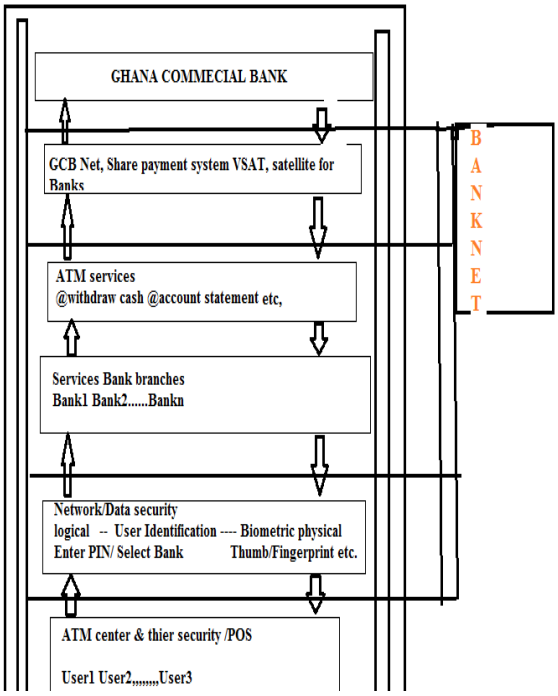

Fig 2: Conceptual ATM model

The prevailing techniques of user authentication, which involve the use of either passwords and user IDs (identifiers) or identification cards and PINs (personal identification numbers), suffer from several limitations. Passwords and PINs can be illicitly acquired by direct covert observation.

Once an intruder acquires the user ID and the password, the intruder has total access to the user‘s resources. In addition, there is no way to positively link the usage of the system or service to the actual user, that is, there is no protection against repudiation by the user ID owner. For example, when a user ID and password is shared with a colleague there is no way for the system to know who the actual user is. A similar situation arises when a transaction involving a credit card number is conducted on the Web. Even though the data are sent over the Web using secure encryption methods, current systems are not capable of assuring that the transaction was initiated by the rightful owner of the credit card. In the modern distributed systems environment, the traditional authentication policy based on a simple combination of user ID and password has become inadequate. Fortunately, automated biometrics in general, and fingerprint technology in particular, can provide a much more accurate and reliable user authentication method. Biometrics is a rapidly advancing field that is concerned with identifying a person based on his or her physiological or behavioral characteristics.

Biometric readings, which range from several hundred bytes to over a megabyte, have the advantage that their information content is usually higher than that of a password or a pass phrase. Simply extending the length of passwords to get equivalent bit strength presents significant usability problems.

It is nearly impossible to remember a 2K phrase, and it would take an annoyingly long time to type such a phrase (especially without errors). Fortunately, automated biometrics can provide the security advantages of long passwords while retaining the speed and characteristic simplicity of short passwords.

Fig3: Biometric ATM

Even though automated biometrics can help alleviate the problems associated with the existing methods of user authentication, hackers will still find there are weak points in the system, vulnerable to attack. Password systems are prone to brute force dictionary attacks. Biometric systems, on the other hand, require substantially more effort for mounting such an attack. Yet there are several new types of attacks possible in the biometrics domain. This may not apply if biometrics is used as a supervised authentication tool. But in remote, unattended applications, such as Web based e-commerce applications, hackers may have the opportunity and enough time to make several attempts, or even physically violate the integrity of a remote client, before detection.

A problem with biometric authentication systems arises when the data associated with a biometric feature has been compromised. For authentication systems based on physical tokens such as keys and badges, a compromised token can be easily canceled and the user can be assigned a new token. Similarly, user IDs and passwords can be changed as often as required. Yet, the user only has a limited number of biometric features (one face, ten fingers, and two eyes). If the biometric data are compromised, the user may quickly run out of biometric features to be used for authentication. Crime at ATMs has become a nationwide issue that faces not only customers, but also bank operators and this financial crime case rises repeatedly in recent years [1]. A lot of criminals tamper with the ATM terminal and steal customers‘card details by illegal means. Once the users‘bank card is lost and the password is stolen, the users‘account is vulnerable to attack. Traditional ATM systems authenticate generally by using a card (credit, debit, or smart) and a password or PIN which no doubt has some defects [2]. The prevailing techniques of user authentication, which involves the use of either passwords and user IDs (identifiers), or identification cards and PINs (personal identification numbers), suffer from several limitations [3]. Passwords and PINs can be illicitly acquired by direct covert observation. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes.

Despite warnings, many people continue to choose easily guessed PIN's and passwords - birthdays, phone numbers and social security numbers. Recent cases of identity theft have heightened the need for methods to prove that someone is truly who he/she claims to be. Biometric authentication technology may solve this problem since a person‘s biometric data is undeniably connected to its own, is nontransferable and unique for every individual. The system can compare scans to records stored in a central or local database or even on a smart card.
Biometrics can be defined as a measurable physiological and behavioral characteristic that can be captured and subsequently compared with another instance at the time of verification. It is automated methods of recognizing a person based on a physiological or behavioral characteristic [9]. It is a measure of an individual's unique physical or behavioral characteristics to recognize or authenticate its identity [7]. Common physical biometric characteristics include fingerprint, hand or palm geometry, retina, iris and face while popular behavioral characteristics are signature and voice. Biometrics technologies are a secure means of authentication because biometrics data are unique, cannot be shared, cannot be copied and cannot be lost.

Biometric authentication has become more and more popular in the banking and finance sector [13]. The idea of fingerprint is not only for security but also to overcome the lack of customer understanding of ATM concept. We proposed ATM with biometric, a fingerprint security system, in order to meet its customers‘ needs whom many of them have a savings account and need to have access to their money during non-banking hours.

Operated using only a smart card and a fingerprint scanner, the machines offer excellent security to card holders since there is a very low possibility of fraud. If a customer loses the card, it is difficult for another person to use it because of the digital fingerprint. By using fingerprint recognition customers are more comfortable with the idea of saving their money in the bank because they understand that if they lose their ATM card, no one can replicate their fingerprint and take their money. Fingerprint authentication is the most popular method among biometric authentication, fingerprint based identification is one of the most mature and proven technique [10].

Recently the Government of India also proposed varieties of Identity Card using Biometric based applications. Besides this we can also use this strategy in different field Government or non-Government in different applications. A Unique Identification is merely a string assigned to an entity that identifies the entity uniquely. We plan to assign a Unique ID to every person residing in India. Biometric identification system and checks would be used to ensure that each individual is assigned one and only UID and the process of generating a new UID would ensure that duplicates are not issued as valid UID numbers [9]. Recently Government in India started a biometric based ID card i.e. Unique Identification Authority of India; it provides a unique identity to persons residing in Ghana.

An embedded Crypto-Biometric authentication scheme for ATM banking systems is proposed in our paper. In this scheme, cryptography and biometric techniques are fused together for person authentication to ameliorate the security level [3].

VIII. *Conclusion*

ATM provides financial services to an increasing segment of the population in many countries. Fingerprint scanning, continues to gain acceptance as a reliable identification and verification processes. This paper identifies a model for the modification of existing ATM systems to economically incorporate fingerprint scanning PLUS blood group; and, outlines the advantages of using such system. It should be noted that the customers‘perception cannot be generalized as it was highly affected by the tradition or culture of the users involves.

IX. References

[1] ATM Market Place. (2009a) ―ATM scam nets Melbourne thieves $500,000‖, Retrieved December 2, 2009. [www.atmmarketplace.com/article.php?id=10808]

[2] ATM Market Place. (2009b) ―Australian police suspect Romanian gang behind $ 1 million ATM scam‖, Retrieved November 13, 2009, [www.atmmarketplace.com/article.php?id=1 0883]

[3] BBC News. (2009) ―Shoppers are targeted in ATM scam‖, Retrieved July 11, 2009, [http://news.bbc.co.uk/2/hi/uk_news/englan d/tees/4796002.stm]

[4] F. Deane, K. Barrelle, R. Henderson, & D. Mahar (2005) ―Perceived acceptability of biometric security systems‖. Computers & Security, Vol. 14, N. 3, pp. 225-231

[5] Global ATM Market and Forecasts (2013), Retrieved May 7, 2010, [www.rbrlondon.com]

[6] Luca, S. Bistarelli, S. &A. Vaccarelli, ―Biometrics authentication with smartcard‖, IIT TR-. 08/2002

[7] M. Bond and P. Zielinski (2003) ―Decimalisation table attacks for PIN Cracking‖, Technical report (UCAM-CLTR-560), Computer Laboratory, University of Cambridge

[8] M. Bond and P. Zielinski (2004) ―Encrypted? Randomized? Compromised? (When cryptographically secured data is not secure)‖ in Workshop on Cryptographic Algorithms and their Uses, Gold Coast, Australia

[9] M. Bond (2004) ―Understanding security APIs‖ Ph.D. Thesis, Computer Laboratory, University of Cambridge

[10] NetWorld Alliance, ―Timeline: The ATM's History‖, 2003

[11] O. Berkman and O. M. Ostrovsky (2007) ―The unbearable lightness of PIN cracking‖ in Financial Cryptography and Data Security (FC), Scarborough, Trinidad and Tobago

[12] SpiderLabs (2009) ―ATM Malware Analysis Briefing‖ retrieved May 15, 2010, [www.trustwave.com/spiderLabspapers.php]

[13] www.atm24.com/NewsSection/Industry%20 News/Timeline%20%20The%20ATM%20History.aspx