IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

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

Mr. Aniket Jadhav[1], Dr. Vijaya Bhosale[2], Mrs. Harshada Nage[3]
Student, M.Sc.IT.[1]
Assistant Professor, Department of I.T[2,3]
I.C.S. College, Khed, Ratnagiri

Abstract: *The growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. PINs are commonly used for access codes to buildings, banks, and computer systems. Conventional methods of identification, such as possession of an ID card or exclusive knowledge, such as a Social Security number, or a password, are not always reliable.*
In this article, we propose a biometric embedded fingerprint biometrics authentication scheme for ATM banking systems. For over 30 years, consumers have relied on and trusted the ATM to meet their banking requirements. However, ATM fraud is on the rise. In this article, we explain the potentially fraudulent activities that can be perpetrated against an ATM and provide recommendations on how to prevent them. In particular, we create a prototype model of the biometric equipped ATM that provides security solutions for most of the known breaches, from Ghana's perspective. To make sure that most users will accept this security approach, we tested the model and received opinions from users.

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

I. INTRODUCTION

The rapid advancement of banking technology has drastically altered the way in which banking activities are conducted. One such banking technology that has had a positive and negative impact on banking activities and transactions has been the introduction of automated teller machines (ATMs). Through an ATM, customers can carry out a variety of banking activities, such as cash withdrawals, money transfers, payments of phone and electricity bills outside of the office hours, and even physical interactions with bank staff. Basically, an ATM provides customers with a convenient and fast method of accessing their bank accounts and carrying out financial transactions.

One of the most important aspects of an ATM security system is the use of a personal identification number (PIN) or a password. A PIN or password is used to protect a customer's financial information from unauthorized access.

An ATM (also known as an automatic banking machine, a cash point, a cash machine, or a hole-in-the-wall ATM) is a mechanical device that has its roots in a banking institution's accounts and records.

This circumstance is genuine within the field of biometric recognizable proof, whereby the mechanized distinguishing proof of individuals by natural characteristics such as their fingerprints or iris designs. Within the past two a long time, quick diminishes in cost and superior execution have made biometric innovation common sense for customer applications such as getting to programmed teller machines (ATMs) and for legislative purposes such as affirming the personalities of welfare beneficiaries.

The utilize of organic highlights for distinguishing proof is of course not new— fingerprinting was created within the 19th century—nor is automation of the method. Starting within the late 1970s, defence and national security offices that seem manage it begun utilizing programmed biometric frameworks to check characters as a more secure elective to photo-IDs. But more broad applications did not develop until more prominent computing control dropped the cost of biometric frameworks.

For illustration, a unique finger impression scanner that fetched $3,000 five a long time back, with software included, and $500 two a long time back, costs $100 nowadays. Comparable cost decreases have happened in other driving biometric advances, such as iris scanners. With lower costs, biometric recognizable proof systems are moving into two

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

primary application areas— banking and legislative agencies—and they have impelled development within the unused industry to about $250 million a year in yearly deals. A few banks around the world, counting Bank Joined together (Houston, TX) and across the country Building Society within the Joined together Kingdom have tried iris scanners as an elective to individual distinguishing proof number (Stick) codes for ATM get to. On a bigger scale, the state of Connecticut started to utilize unique mark filtering in 1996 as a way to recognize welfare recipients, and the U.S. Armed force, Discuss Drive, and Social Security Organization are looking at different biometric acknowledgment frameworks. Both the Department of Defense and the Office of Veterans Issues arrange to utilize finger pictures to confirm the personality of workers and those looking for retirement benefits.

Within the case of managing an account, the focal points of biometric scanners are primarily comfort instead of security. ―Customers just like the ease of fair going up to the ATM and gazing at it for many seconds. In spite of the fact that biometric innovation secures against a cheat who can figure a carelessly chosen Stick code, it does nothing to avoid the more common robberies in which an ATM client is victimized close the machine or constrained at gunpoint to withdraw money. The focal points for government organizations are clearer, as biometrics make the creation of untrue characters harder. But this can be absolutely what concerns a few security and efforts are beneath way to create programmed signature distinguishing proof and voice-identification frameworks.

In this paper, we hence give an diagram of the conceivable false exercises which will be executed against ATMs and examine prescribed approaches to prevent these sorts of fakes.

II. PROBLEM STATEMENT

Already, cash withdrawal, cash store and bank account subtle elements of clients through managing an account exercises were exceptionally intense and repetitive, but these days different banks have executed electronic keeping money exercises which permit clients to utilize the ATM since it's managing an account comforts in connection to the over exercises. Numerous banks around the world has introduced ATMs in different places/cities/towns/rural regions so clients of banks can effortlessly pull back cash and check their adjust and perform any other keeping money exchange with ATMs.

However, users/customers of such electronic exchanges have numerous passwords utilized to get to their e-mails, car radios, portable phones, computers, ATM Cards etc. and clients have numerous cards like Credit Card, Charge Card, and Personality Card etc. Subsequently, numerous issues are confronted by clients in connection to their ATM Cards and PINs, a few of these issues are expounded underneath:

In some cases a parcel of exertion is included when users/customers are required to keep in mind distinctive passwords. On numerous events clients disregard their passwords. Overlooking passwords in some cases make a issue of not performing a required exchange and contributing off-base secret word will likely lead to hacking/seizure/locking of the ATM card. ATM cards need to be portable in arrange to be utilized. Absent mindedness of ATM cards at the point of exchange will continuously surrender no exchanges and negative comes about.

Sometimes users/customers utilize a common PIN/password for all electronic exchanges things. In such cases, there are shortcoming and lack of security, since any other individual who knows a common watchword of another can effortlessly utilize his/her ATM card. In arrange to annihilate these sorts of insufficiencies, we propose the ATM machine with the biometric framework. Different biometric innovations such as iris, finger, voice, wrist etc. are right now being utilized on a worldwide scale in creating nations. Each client has its one of a kind personality based on physical or behavioural properties. These traits are never stolen by any individual.

III. TYPES OF ATM FRAUDS

Within the final few a long time, there have been numerous reports of hacking into the electronic ATM framework and this has caused misfortunes of billions of dollars within the worldwide managing an account industry. Prophet assault on confirmation conventions and breaches influencing ATMs such as cloning of cards and hacking of Stick code have been progressively been reported. A few prevalent ATM frauds/attacks are clarified within the subsection's underneath.

Skimming Assaults

This is the foremost popular breach in ATM exchange. In this brilliant rip-off, criminals are taking advantage of innovation to create fake ATM cards by employing a skimmer (a card swipe gadget that peruses the data on ATM

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

card). These gadgets take after a handheld credit card scanner and are frequently affixed in near nearness to or over the best of an ATM ‘s factory-installed card per-user. A single skimmer can hold data from than 200 ATM cards some time recently being re-used.

Card Catching

This includes putting a gadget specifically over or into the ATM card peruser slot. In this case, a card is physically captured by the catching gadget interior the ATM. When the client clears out the ATM without their card, the card is recovered by thieves/criminals. Ordinarily as it where one card is misplaced in each assault. The foremost common variation is known as the Lebanese Circle

Stick Breaking Attacks

on customers ‘PINs have been known to security analysts for a long time, e.g., [3], [9], [7]. One of the most productive of these _PIN cracking ‘attacks’ was talked about in [8]. How the processing framework utilized by banks is open to manhandle was clarified in [8]. One of the assaults, targets the interpret work in switches - an mishandle work that’s utilized to permit clients to choose their PINs online. In either case, the blemishes make a implies for an assailant to find Stick codes, for illustration, those entered by clients whereas pulling back cash from an ATM given they have got to the online Stick confirmation office or exchanging forms. A bank insider seem utilize an existing Equipment Security Module (HSM) to uncover the scrambled Stick codes. In a most noticeably awful case situation, an insider of a third-party switching provider seem assault a bank exterior of his region or indeed in another landmass. Shockingly, proposition to counter such assaults are nearly non-existent other than a few proposals; for illustration, keeping up the mystery (and keenness) of a few information components related to Stick handling (that are considered security harsh concurring to current keeping money measures) such as the decimalization table and PIN Confirmation Values (PVVs) /Offsets have been emphasized [9], [8].

IV. PHISHING/VISHING ASSAULT

Phishing tricks are planned to allure the client to supply the card number and Stick for their bank card. Regularly, an assailant employments mail speaking to them as a bank and claiming that client account data is fragmented, or that the client has to overhaul their account data to avoid the account from being closed. The client is inquired to tap on a interface and take after the bearings given. The connect be that as it may is false and coordinates the client to a location set up by the aggressor and outlined to see just like the user’s bank. The location coordinates the client to input touchy data such as card numbers and PINs. The data is collected by the thieves/criminals/hackers and utilized to form false cards. A few variations are skewer phishing and Shake Phish assaults.

Traditionally, after a effective phishing assault, the criminal would extricate the required data and go into the online account and remove the victim's bank stores. This has changed for a few of the more advanced hoodlums in later a long time were rather than plundering the victim's account; they go to the check picture page, where they take a duplicate of the victim's check. Numerous monetary educate are presently advertising check pictures as portion of their online banking administrations to their clients. The checks contain the victim's bank account number, signature, address, phone etc. The aggressor can either take the duplicate and make paper fake checks, or take that information and make PayPal accounts or other online instalment accounts that will take off the casualty on the snare for any buys.

V. ATM MALWARE

Malware assaults require an insider, such as an ATM professional who features a key to the machine, to introduce the malware on the ATM. Once that has been done, the assailants can embed a control card into the machine‘s card peruser to trigger the malware and allow them control of the machine through a custom interface and the ATM‘s keypad. Agreeing to a report in [11], a Trojan family of malware tainted 20 ATMs in Eastern Europe. The malware lets hoodlums take over the ATM to take information, PINs and cash.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

VI. ATM HACKING

Attackers utilize advanced programming procedures to break into websites which dwell on a budgetary institution's network. Utilizing this get to, they can get to the bank's frameworks to find the ATM database and subsequently collect card data which can be utilized afterward to make a clone card. Hacking is moreover commonly utilized to portray assaults against card processors and other components of the exchange handling arrange. Most of the ATM Hackings is due to the utilize of non-secure ATM computer program.

VII. PHYSICAL ASSAULT

ATM physical assaults are endeavored on the safe inside the ATM, through mechanical or warm implies with the intention of breaking the secure to gather money interior. A few of the foremost common strategies incorporate smash attacks, unstable assaults and cutting. Theft can too happen when ATMs are being recharged or adjusted.

IV. Security Measures of ATMS

As innovation propels and ATM applications become more omnipresent, there's more of secret information being transmitted over the ATM framework. As more touchy exchanges are conducted, more dangers breaches are detailed and the challenge of securing the framework gets to be more critical. Numerous security administrations in bank transactions are subordinate on verifying clients such as era of exact audit trails, non-repudiation in communications, protecting secrecy and other input approval techniques such as batch sums, arrange checks, reasonableness checks and exchange approval.

These highlights as it were guarantee that certain procedures are taken after and cannot tell whether the individual with the card and Stick is authorized to utilize it, they fair guarantee that the information transmitted takes after certain rules or conventions that ask exchanges such as cash withdrawals are made inside sensible limits, that cash is transferred to the correct account, and so forward. In this manner, it is basic to create more grounded confirmation and distinguishing proof measures to halt hoodlums from committing false acts.

Electronic Managing an account Framework

Electronic managing an account which is an developing worldview in Ghana could be a unused industry which permits individuals to associated with their managing an account accounts via the Web from essentially anyplace within the world. The electronic keeping money framework addresses a few developing patterns: client request for anytime, anyplace benefit, item time-to-market objectives and progressively complex back-office integration challenges. This framework permits buyers to get to their keeping money accounts, audit most later exchanges, ask a current articulation, exchange stores, see current bank rates and item data and reorder checks. E-banking can be characterized as the sending of managing an account administrations and items over electronic and communication systems straightforwardly to clients [7]. It is the computerized conveyance of unused and conventional keeping money items and administrations specifically to clients through electronic, intelligently communication channels [8]. These electronic and communication systems incorporate Mechanized Teller Machines (ATMs), coordinate dial-up associations, private and open systems, the Web, tvs, versatile gadgets and phones. Among these advances, the expanding entrance of individual computers, generally less demanding get to to the Web and especially the more extensive dissemination of versatile phones have drawn the consideration of most banks to e-banking. Critical contrasts exist among banks in terms of their ebanking capabilities. These contrasts can take two fundamental measurements. The primary is the utilize of electronic

Qualities and Points of interest of Biometric Innovation

Biometric innovation identifiers are difficult to be misplaced or overlooked, troublesome to be copied/shared and require the individual to be verified to be display at the time and point of verification (a client cannot claim his watchword was stolen and abused!!). Rather than passwords, biometric frameworks can be utilized to ensure the solid cryptographic keys. Some strengths of biometric innovation incorporate the taking after: Provision of solid confirmation. Can be utilized rather than a Stick. Covered up or reduced costs of ATM card administration like card personalization, conveyance, administration, re-issuance, Stick era, offer assistance work area, and reissuance can be maintained a strategic distance from. It is exact. Adaptable account get to permits clients to get to their accounts at their comfort. The operational fetched of the ATMs will eventually diminish. The focal points of the biometric coordinates

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

frameworks in ATMs are: This biometric coordinates framework of ATM is more secure to the routine ATM framework. It recognizes the real account holder no one other than the card holder can work the ATM. It can be as it were worked by the genuine account holder. It gives security and security to the Bank account holders .It is 100% mood verification. It gives 100% security to the ATM card holders. In the event that anybody gets the stick number and other subtle elements of the ATM card holder indeed at that point it cannot be worked unless the thumb impression is coordinated. Biometric coordinates frameworks in ATMs can be utilized in credit cards and charge cards and other online installment frameworks. The bank will too incline toward this framework with the perspective of security and client care. Biometric coordinates frameworks in ATMs will reduce the workload of the banks Biometric coordinates frameworks in ATMs will increment the believe of the keeping money client. Biometric coordinates frameworks in ATMs can moreover be implemented with the CCTV surveillance and Alerts Chimes to dodge the break open of the ATM Machine by the hoodlums. Biometric coordinates frameworks in ATMs are valuable to the uneducated individual and for provincial ranges. With the combination of the Stick and biometric framework the ATM exchange is completely secured. Biometric coordinates frameworks in ATMs will minimize the chances of the blockage of account on account of off-base stick utilized by the ATM card holder.

V. RELATED WORK

Shaikh and Rabaiotti [8] analyzed the identity card (Id) system of the United Kingdom. His analysis approached planning from a general distribution perspective and described a trade triangle model. They found a trade-off between several aspects: accuracy, privacy and scalability of bio-based identity management systems. Here, emphasizing one trait weakens another. Murthy and Reddy [3] developed a fingerprint system embedded in ATM security applications. In these systems, banks collect the customer's fingerprint and mobile phone number when opening an account, and the customer simply enters the ATM. After entering the received code, the ATM verifies that the code is correct before sending it to the customer and using it. Schouten and Jacobs [7] presented a review of the Netherlands' proposal to implement a biometric passport, focusing on the technical aspects of specific biometric technologies (e.g. facial recognition and fingerprinting) and also referring to international agreements and standards (eg ICAO).). and EU"""""s Extended Access Control) and discuss privacy issues from the perspective of traditional security concepts such as privacy. Debbarma [10] proposed an integrated clinical biometric authentication scheme for ATM banking systems. The development and distribution phases of the Belgian electronic ID card have been discussed by Marein and Audenhove (2010). It has been argued that the existence of a national register was one of the factors that helped the development of the Belgian electronic ID card. So far, 8 million cards have been issued to Belgian citizens and the process is simple and straightforward (Marein and Audenhove, 2010). A discussion on the security and design of Malaysia's identity card, namely Mykad, by Raphael et al. (2003). Mykad integrates ID, driver's license, passport and ATM. Since Mykad is used for several sensitive purposes, Raphael et al. (2003) suggested that safety factors should be analyzed before deployment.

VI. RESEARCH DESIGN AND METHODOLOGY

Indian Bank ATM security features are designed to harden the network by connecting customer identification information (CII), customer account information (CA), and bank (ERP) records. This network is intended to support a high volume of users and utilizes dedicated servers to accomplish this. The Client/Server architecture has been selected for this proposed system due to its ability to provide adequate security for resources necessary for critical applications, including financial systems. Additionally, the visual conceptual approach is implemented, which incorporates Unified Modeling Languages (UML)-based tools such as Use Case Models, Functional Diagrams, Sequence Diagrams, etc. This work is completed using Visual Basic Version 6.0, which is utilized to design the UI and cardholder interactions with the ATM.

A. Population and Method of Data Collection

This study sought to assess the reliability of the use of ATMs and fingerprints biometrics by randomly selecting customers and students from the target population of commercial banks in Anambra, Awka, and Southeast Nigeria. The participants' profiles were derived from extensive literature surveys and oral interviews, and the tool was designed with

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

16-item, three-part sections. Of 200 usable copies, 163 returned (82%) to the study, which was conducted over a period of four months. The items were evaluated through descriptive statistical methods, and expert judgements were applied to ensure accuracy. The items were face-validated, wordings were reworded for clarity, and two experts removed two items for non-revisional purposes. Following these corrections, the items were deemed suitable for use on subjects.

VII. Projected Biometric (Fingerprint) Policy for Ghana Banking Technology

One of the most effective security measures against some of the attacks mentioned is the implementation of biometric authentication within the existing ATM system, as discussed below.

Biometric Smartcard – A model

Biometric recognizable proof is utilized to confirm a person‘s personality by measuring carefully certain human characteristics and comparing those estimations with those that have been put away in a layout for that same individual. Formats can be put away within the biometric gadget, the institution‘s database, a user‘s keen card, or a Trusted. Third Party benefit provider‘s database. There are two major categories of biometric strategies: physiological (unique finger impression confirmation, iris examination, hand geometry-vein designs, ear acknowledgment, odor location, DNA design examination and sweat pore investigation), and behavioural (transcribed signature confirmation, keystroke investigation and discourse examination). In [12], it was found that behaviour based frameworks were perceived as less satisfactory than those based on physiological characteristics. Of the physiological strategies, the foremost commonly utilized is that of unique finger impression checking. The work of the highlight extraction module is to extricate the include set from the filtered biometric characteristic. This highlight set is at that point put away into the format database. The matcher modules take two inputs, i.e. include sets from the layout database and highlight set of the client who wants to verify him and compares the similitude between the two sets. The final module, i.e., the verification module makes the choice approximately the coordinating of the two include sets. Biometrics may be a quickly advancing innovation that's being broadly used in forensics, such as criminal recognizable proof and jail security, which has the potential to be utilized in a expansive extend of civilian application regions.

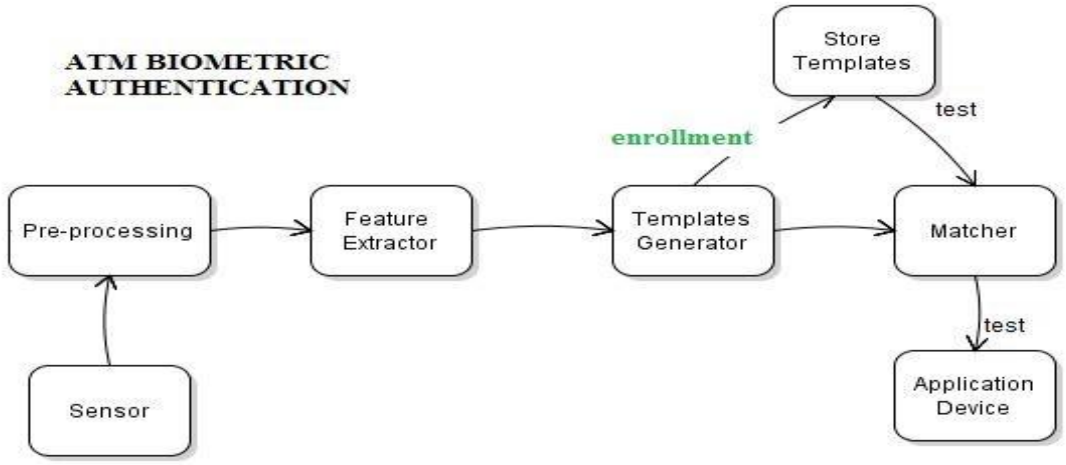

Fig 1: Working of biometric verification

The figure 1 overhead shows the working of biometric authentication process. A biometric gadget works on the premise of a few human characteristics, such as unique mark, voice or patter of line within the iris of your eye. These gadgets incorporate handprint locators, voice recognizers and distinguishing proof patter within the retina. Confirmation with such gadgets employments reprehensible physical characteristics to verify clients. The client database contains a test of user’s biometric characteristics. Amid confirmation, the client is required to supply another sample of the clients biometric characteristics. Usually coordinated with the one within the database, and in the event that the two tests are the same, at that point the client is considered to be a substantial client. The points of interest of

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

this may incorporate: all attributes of the ATM cards will be kept up, forging endeavours are decreased due to enrolment process that verifies character and capture biometrics, and it'll be amazingly tall security and fabulous user-to-card verification.

These focal points are for the good thing about clients as well as framework chairmen since the issues and costs related with misplaced, reissued or briefly issued can be dodged, in this way sparing a few costs of the framework administration. On the negative side, the major chance postured by the utilize of biometric frameworks is that a noxious subject may meddled with the communication and captured the biometric format and utilize it afterward to get get to [4]. Moreover, an assault may be committed by producing a layout from a unique mark gotten from a few surface. In spite of the fact that few biometric frameworks are fast and exact in terms of moo untrue acknowledgment rate sufficient to permit distinguishing proof (consequently recognizing the client character), most of the current frameworks are appropriate for the confirmation only, as the untrue acknowledgment rate is as well tall. The propose plan employments a greatest of 8 characters, numbers or a blend of the both Stick and unique finger impression as confirmation components of the verification handle.

ACOS smartcards and AET60 BioCARD Key advancement unit were utilized within the propose plan. Within the verification portion, the clients need to yield the right PIN DES scrambled current session key to get get toanother level. Clients have 3 effective endeavours to enter the correct Stick, else the cards will be bolted and render it to futility. In conclusion, we utilize the unique finger impression as the biometric identifiers because it takes most brief enrolment time. Reliable, client confirmation is getting to be an progressively imperative assignment in the Web-enabled world. The results of an unreliable confirmation framework in a corporate or endeavour environment can be disastrous, and may incorporate misfortune of secret data, refusal of benefit, and compromised data astuteness. The esteem of dependable client confirmation isn't restricted to just computer or arrange get to. Numerous other applications in lifestyle moreover require client confirmation, such as managing an account, e-Commerce, and physical get to control to computer assets, and might advantage from upgraded security.

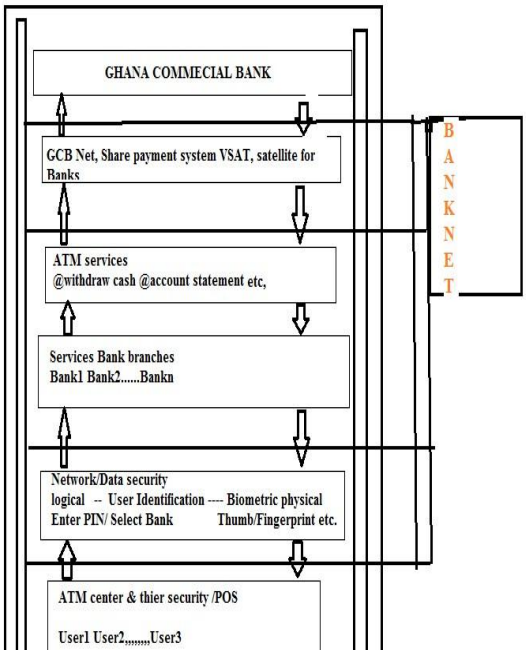

Fig 2: ATM model

Code word, IDs, ID cards, and PINs, which are commonly used for authentication, have a number of drawbacks. These include the potential for unauthorized access to resources due to direct covert surveillance, as well as the inability to link the user to the actual system or service. Furthermore, there is no guarantee that the user ID will not be refused by the owner. For instance, if a user shares a username and password with another user, the system will not be able to determine the identity of the real user.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

A similar situation occurs when a transaction related to a credit card number is made online. Although the information is sent over the network using secure encryption methods, current systems cannot verify that the transaction was initiated by the legitimate owner of the credit card. In the modern distributed system environment, the traditional authentication policy based on a combination of username and password has become insufficient. Automated biometrics, particularly fingerprint technology, offer a more precise and dependable approach to user authentication. Biometrics are a rapidly advancing field that is designed to identify individuals based on their physical or behavioural attributes. The advantages of biometrics, which range from a few bytes to a large number of megabytes, are that their information contents are typically larger than those of a password or passphrase. Increasing the length of a password to obtain the appropriate bit strength can lead to significant usability issues. For example, two thousand sentences are nearly impossible to recall, and the process of writing them will take a considerable amount of time (especially when errors occur). Automated biometrics provide the security advantages of a long password while still allowing for the speed and simplicity of a short password.

Fig3: Biometric ATM

Despite the warning signs, many individuals still opt for PINs and passwords that are easy to guess, such as birthdays, cell phone numbers, and social security numbers. Recent cases of identity theft have necessitated the development of methods to verify that a person is who they claim to be, and biometric authentication technology can provide a solution to this issue. The biometric data is uniquely linked to the individual, transferable, and individualized, and can be compared to a central database, a local database, or even a smart card record. Biometric data is an automated method of identifying an individual based on their physical or behavioural characteristics, and can be used to confirm or identify an individual.

Biometric identification is a secure method of authentication, as it is unique and cannot be shared, copied, or lost. Physical biometric features such as fingerprints, hands or palm geometry, irises, and faces are common, while behavioral features such as signature and voice are also popular. Biometric identification is becoming increasingly popular in banking and financial industry[13]. The introduction of fingerprint recognition was not only for security purposes, but also to meet the need of customers for ATM concepts. An ATM with biometric fingerprint security was offered to meet the requirements of customers, who often have savings accounts and need access to their funds outside of banking. These machines are only compatible with smart cards and fingerprint sensors, providing excellent protection for cardholders as the risk of fraud is very low. If a customer loses their ATM card, it will not be possible for anyone else to use it due to the digital fingerprint. This makes customers more likely to save their money in a bank, as they understand that no one can replicate their fingerprint and steal their money.

The Indian Government has recently implemented a variety of identity cards that use biometric technology. This strategy can be applied to a variety of industries, both governmental and non-governmental. Identifiers are simply strings assigned to an individual or group of individuals that uniquely identify them. The Government of India intends to issue a single identity card to all individuals residing in India, which will be verified by biometric identification systems.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

VIII. CONCLUSION

At the conclusion of this term paper, it is clear that the security of ATMs is of paramount importance in protecting the financial resources and personal data of customers. As technology advances, so do the tactics employed by cybercriminals. This paper has examined various methods and recommendations to improve ATM security, recognizing the need for a comprehensive and multilayered approach. The implementation of biometric verification, cordless exchange, and endpoint encryption is a significant step forward in providing client distinguishing proof and exchanging information. Not only do these innovations help to prepare for verification, but they also reduce the risk of physical assaults, like card skimming. Furthermore, the implementation of anti-skim innovation and regular physical assessments can help to identify and prevent alteration with the ATM card reader.

Real-time exchange checking and inconsistency location frameworks, as well as secure communication conventions, are essential in distinguishing and reducing potential security risks. The importance of nonstop inaccessible surveillance and administration cannot be overstated, providing a proactive approach to security episodes and specialised issues promptly.

The security of ATMs requires a comprehensive approach to ensure that they remain secure from cyber threats. Physical security measures, such as surveillance cameras, alerts and well-maintained areas, are supplemented by computerized shields to deter criminal activity. Regular upgrades and patches of the computer program are essential to address any vulnerabilities in the working framework or third-party program, ensuring that the ATM system remains strong. User instruction is a fundamental element of ATM security, and providing clients with information such as keypad protection, being aware of their environment and reporting suspicious activity increases the overall security posture.

Furthermore, the integration of multiple-factor confirmation (MFA) ensures that the ATM system is secure when exchanging customer data, such as PIN, card and biometric information. To stay ahead of the ever-changing security landscape, it is essential to collaborate with ATM administrators to implement and maintain a strong and secure ATM system. Regular testing and overhauls to meet security conventions, as well as a commitment to remain informed of the latest cybersecurity advancements, are essential for a secure ATM system.

[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 (UCAMCLTR-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 NetWorld Alliance, ―Timeline: The ATM's History‖, 2003

[10]. O. Berkman and O. M. Ostrovsky (2007) ―The unbearable lightness of PIN cracking‖ in Financial

[11]. 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