Journal – ICON (Integrating Concepts) ISSN 2456-6071

Security in ATM using FRAME

Lorinda.E [#1] , Devaprasad.D [*2]

[#]*Master of Engineering , Dept of CSE , Sivaji College of Engineering and Technology*

[*]*Assistant Professor, Dept of CSE , Sivaji College of Engineering and Technology*

d.devaprasad233@gmail.com

***Abstract*— Automatic Teller Machine(ATM) is an electronic machine which is used for accessing bank account from anywhere without the help of bank staff. Though security is provided for ATM machines, cases of robberies are increasing. The ATM machines are not safe since security provided traditionally were either by using RFID reader or by using security guard outside the ATM. The security is not sufficient because RFID card can be stolen and can be misused for robbery. To overcome the problem, a new technology is introduced which aims to design real-time monitoring and controlling system. FRAME is the abbreviation of Fingerprint Recognized Access Management Equipment. This technology is applied on the ATM in which the user has to enter the secret code along with the finger print to reveal his database. If the fingerprint and the code are recognized then the permission is granted for transaction. If it is not recognized then the camera placed on the machine will take an image of that person. This image with the corresponding date and time of the transaction is send to the bank through email and an SMS is generated and is send to the owner. Here virtual ATM card is used.**

I.INTRODUCTION

Nowadays, banking sector is one of the most important parts of a human day to day life. Banking facilities are widely used by people for their economies activities. Automatic Teller Machine (ATM) is an electronic machine which is used for accessing a bank account from anywhere without the help of bank staff. The user can perform several banking activities like cash withdrawal, money transfer with the help of ATM. It is observed that number of crimes related to ATM is increased hence there is a necessity to provide enhances security to ATM machine. Previous technologies provide security to transactions for identification of authorized user. But this is limited for secure transactions with ATM machine. Previous works focused on biometric technique to provide enhanced security to ATM transaction whereas GSM based technique is also implemented for the same purpose. Whereas, some system uses a combination of the both techniques.

Currently, ATM security is given to the transactions only. GSM based security is provided in which One Time Password (OTP) is send to the registered number for transaction. The combination of GSM and RFID technology is also used which makes the system secure than only RFID technology. This technology has drawback in which number of crimes related to ATM is increased. The RFID cards can be stolen and can be misused for robbery. So we use virtual ATM card which will be found only in one’s email. There are some limitations in the previous technologies used for ATM security. In biometric method, fingerprint recognition method for ATM transaction. Also security is enhanced with a camera placed on the ATM machine if any one’s fingerprint is not recognized. It will take an image of the person who is in front of the ATM machine. This image is then send to the bank and an alert message is send to the owner. The owner can thus contact the bank immediately.

Our system flow contains two electronic control units. One is for biometric authentication and other is for shutter control. The biometric verification is any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits. Shutter control is when the fingerprint is not matching the process stops at once and the camera placed there takes the image of that person.

II. RELATED WORK

Frauds related to the ATM (Automatic Teller Machine)are increasing day by day which is a serious issue. ATM security is used to provide protection against these frauds. Though security is provided for ATM machine, cases of robberies are increasing. Previous technologies provide security within machines for secure transaction, but machine is not neatly protected. The ATM machines are not safe since security provided traditionally were either by using RFID reader or by using security guard outside the ATM. This security is not sufficient because RFID card can be stolen and can be misused for robbery as well as watchman can be blackmailed by the thief. So there is a need to propose new technology which can overcome this problem. This paper proposes a system which aims to design real-time monitoring and controlling system. The system is implemented using Raspberry Pi and fingerprint module which make the system more secure, cost effective and stand alone. For controlling purpose, Embedded Web Server (EWS) is designed using Raspberry Pi which serves web page on which video footage of ATM center is seen and controlled. So the proposed system removes the drawback of manual controlling camera module and door also this system is stand alone and cost effective.

III. PROPOSED SYSTEM

Automatic Teller Machine(ATM) have operated for a very long time without full exploration of all essential functions of the facility and this has baffled the minds of the public and other decision makers about the effect of ATM operations on customer demand for it. It was realized that there is high traffic intensity for ATMs use for most banks in the municipality. Also, higher educational attainment, number of ATMs per bank, convenience and security features, efficiency and low transaction charges have significant effect on influencing the usage of ATM services. It is recommended that management of these banks need to upsurge the number of quality and security of ATM services in order to increase access and usage of ATM.

Nowadays, about 3 million units are installed worldwide. As the number of ATM units increase, the machines are prone to hacker attacks, fraud, robberies and security breaches. In the past, the ATM machines main purpose was to deliver cash in the form of bank notes and to debit a corresponding bank account. However, ATM machines are becoming more complicated, and they serve numerous functions, thus becoming a high priority target to robbers and hackers.

ATM vandals can either physically tamper with the ATM machine to obtain cash, or employ credit card skimming methods to acquire control of the user's credit card account. Credit card fraud can be done by inserting discreet skimming devices over the keypad or credit card reader. The alternative way to credit card fraud is to identify the PIN directly with devices such as cameras concealed near the keypad. Security breaches in Electronic funds transfer systems can be done without delimiting their components which are communication links ,computers , and terminals(ATM).

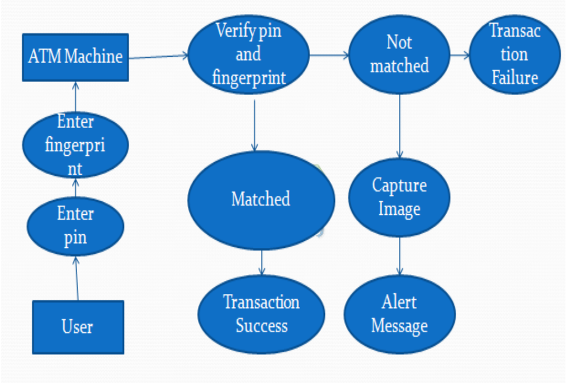


Fig. 1 : Block Diagram of Proposed System

First, communication links are prone to attacks. Data can be exposed by passive means or direct means where a device is inserted to retrieve the data. The second component is computer security. There are different techniques that can be used to acquire access to a computer such as accessing it via a remote terminal or other peripheral devices such as the card reader. The hacker had gained unauthorized access to the system, so programs or data can be manipulated and altered by the hacker. Terminal security is a significant component in cases where cipher keys reside in terminals. In the absence of physical security, an abuser may probe for a key that substitutes its value. The goal of this paper is to design a ATM system with more security using biometric authentication. The main contributions are as follows:

At first, I Introduce virtual card in which the details of the ATM card is available in the owner's email. The name, card number, cvv number, signature and the validity date will be available in the email. The virtual card is generated once the owner starts the account in the particular bank by using his personal details.

When starting the account in the bank the bank staff has to login the bank website by giving his own login ID and password. And then the user has to give his personal details to the bank. While starting the bank account the virtual card is generated and is send to the owner via email. The fingerprint of the user is also collected by the bank. Multiple fingerprint collection is also possible.

While come to an ATM machine, the user who needs to withdraw money from the ATM machine has to enter the virtual card details of card number and the secret pin which is generated when starting the account number is also entered to the ATM machine. When the pin number is verified the user has to enter his fingerprint. When the fingerprint is recognized the user can withdraw money. Otherwise the camera placed in the ATM machine will capture the image of the person who is in front of the ATM machine and will be sent to the bank database. An SMS is sent to the owners registered mobile. The fingerprint is encrypted and is saved to the bank's database. When the user enters the fingerprint to the ATM machine the data is compared with the encrypted data in bank database. If the code is matched the fingerprint is recognized. If the code is not matched, the fingerprint is not recognized and the transaction will be failed.

We the definition and the security model of the ATM machine with two technologies biometric verification and shutter control I also prove the security of my system and justify its performance by concrete implementation.

We showed the system model for cloud storage auditing with verifiable outsourcing of key updates. There are three parties in this model: the bank, user and the ATM machine. The bank is the owner of the files that are uploaded to cloud. The total size of these files is not fixed that is the bank can upload any number of files to cloud in different time points. The cloud stores the bank's files. The user has the role of withdrawing the money from the ATM machine by giving proper authentication. The user can also change the pin number of the virtual ATM by ATM machine. The third model ATM machine holds the process of cash withdrawal if fingerprint is recognized, else the process will fail and capture the image of the person and an alert message is sent to the user via SMS.

IV. ALGORITHMS

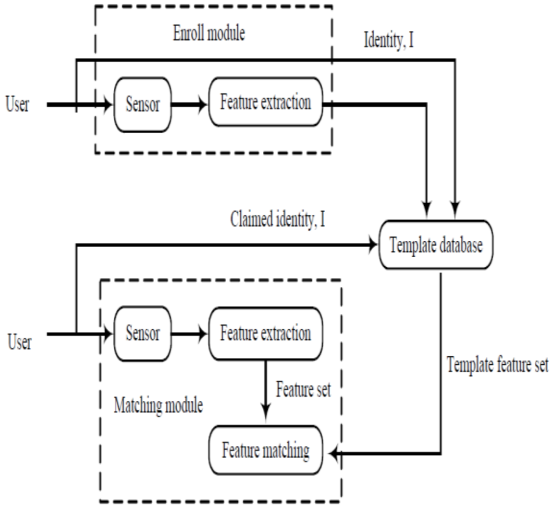
In this section, we overview the concepts that form a foundation for our research. These include SHA encryption and md5 algorithm.

A. SHA ENCRYPTION

In cryptography, **SHA-1** (Secure Hash Algorithm **1**) is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest – typically rendered as a hexadecimal number, 40 digits long.

SHA-1 produces a 160-bit hash value or message digests from the inputted data (data that requires encryption), which resembles the hash value of the MD5 algorithm. It uses 80 rounds of cryptographic operations to encrypt and secure a data object. Some of the protocols that use SHA-1 include:

- Transport Layer Security (TLS)
- Secure Sockets Layer (SSL)
- Pretty Good Privacy (PGP)
- Secure Shell (SSH)
- Secure/Multipurpose Internet Mail Extensions (S/MIME)
- Internet Protocol Security (IPSec)



SHA-1 is commonly used in cryptographic applications and environments where the need for data integrity is high. It is also used to index hash functions and identify data corruption and checksum errors.

Within the family of secure hash algorithms, there are several instances of these tools that were set up to facilitate better digital security. The first one, SHA-0, was developed in 1993. Like its successor, SHA-1, SHA-0 features 16-bit hashing.

The next secure hash algorithm, SHA-2, involves a set of two functions with 256-bit and 512-bit technologies, respectively. There is also a top-level secure hash algorithm known as SHA-3 or "Keccak" that developed from a crowd sourcing contest to see who could design another new algorithm for cybersecurity.

All of these secure hash algorithms are part of new encryption standards to keep sensitive data safe and prevent different types of attacks. Although some of these were developed by agencies like the National Security Agency, and some by independent developers, all of them are related to the general functions of hash encryption that shields data in certain database and network scenarios, helping to evolve cyber security in the digital age.

B. MD5 ALGORITHM

The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of security applications. It is also commonly used to check data integrity. The 128-bit (16-byte) MD5 hashes (also termed message digests) are typically represented as a sequence of 32 hexadecimal digits. MD5 was designed by Ron Rivest in 1991 to replace an earlier hash function, MD4. MD5 is one in a series of message digest algorithms designed by Professor Ronald Rivest of MIT (Rivest, 1992). When analytic work indicated that MD5's predecessor MD4 was likely to be insecure, MD5 was designed in 1991 to be a secure.

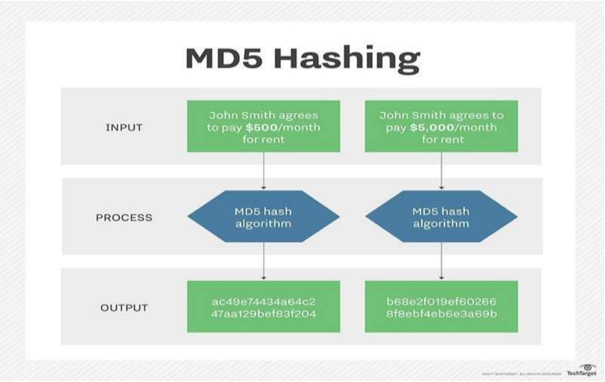

MD5 Hashing
INPUT
John Smith agrees to pay $500/month for rent
John Smith agrees to pay $5,000/month for rent
PROCESS
MD5 hash algorithm
MD5 hash algorithm
OUTPUT
ac49e74434a64c2 47aa129bef83f204
b68e2f019ef60266 8f8ebf4eb6e3a69b
TechTarget

Fig 2: Architecture of MD5 hashing

The goal of any message digest function is to produce digests that appear to be random. To be considered cryptographically secure, the hash function should meet two requirements: first, that it is impossible for an attacker to generate a message matching a specific hash value; and second, that it is impossible for an attacker to create two messages that produce the same hash value. MD5 hashes are no longer considered cryptographically secure, and they should not be used for cryptographic authentication. In 2011, the IETF published RFC 6151, "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms," which cited a number of recent attacks against MD5 hashes, especially one that generated hash collisions in a minute or less on a standard notebook and another that could generate a collision in as little as 10 seconds on a 2.66 GHz Pentium 4 system. As a result, the IETF suggested that new protocol designs should not use MD5 at all, and that the recent research attacks against the algorithm "have provided sufficient reason to eliminate MD5 usage in applications where collision resistance is required such as digital signatures."

V. DESIGN

The computer and fingerprint module is connected usingWi-Fi router. RF transceiver is used for switching ON/OFFAC whenever any user enters in the ATM center. This system is real-time monitoring system and efficient as compared to the previous systems. In the proposed system, R305 fingerprint module has been used for authentication. Whenever the user wants to enter theATM center, he has to verify his identity by placing his finger on fingerprint module. Fingerprint module is interface with PIC controller. This fingerprint module has UART serial communication. The storage capacity of this fingerprint module is 256 bytes. Verification speed required less than 1 second and scanning speed is less than 0.5 second.

Fig 3: Fingerprint sensor module

VI. CONCLUSION AND FUTURE WORK.

In this project high security for ATM machines are used and is analyzed and implemented. The biometric verification is used as each person has variable biometrics. Key updates are outsourced to the banking sector. In addition, a camera is used to take the instant photograph of the frauds is taken and is given to the bank. The proposed system gives the formal security proof and the performance simulation of the proposed scheme.

Even though, the proposed system gives the formal security proof, we can also improve the security by proposing other biometric verification such as hand geometry, earlobe geometry, retina and iris patterns, voice waves, DNA and signatures.

REFERENCES

[1] Arjun Kumar Mistry, Suraj Kumar and Vicky Prasa, "Secured Atm Transaction Using Gsm", International Journal of Electrical and Electronic Engineering & Telecommunication, Vol. 2, No. 3, July 2013.

[2] Soniya B. Milmile, Amol k. Boke "Review Paper On Real Time Password Authentication System For Atm", IJAICT, Vol. 1, November2014

[3] G. Renee Jebaline, S. Gomathi, "A Novel Method to Enhance the Security of ATM using Biometrics", International Conference on Circuit, Power and Computing Technologie, 2015.

[4] Mr. Mahesh A. Patil Mr.Sachin P.Wanere Mr.Rupesh P.Maighane Mr.Aashay R.Tiwari, [5] "

[5] Deepa Malviya, "Face Recognition Technique: Enhanced Safety Approach for ATM", International Journal of Scientific and Research Publ ications, Vol. 4, December 2014.

[6] Mohsin Karovaliya, Saifali Karedia, Sharad Oza, Dr.D.R.Kalbande "Enhanced security for ATM machine with OTP and Facial Recognition features", International Conference on Advanced Computing Technologies and Applications, 2015

[7] Ajaykumar M (2013). "Anti-Theft ATM Machine Using Vibration Detection Sensor" International Journal of Advanced Research in Computer Science and Software Engineering, pp: 23-28

[8] R. Gross, J. Shi, and J. Cohn. Quo Vadis Face Recognition? Third Workshop on Empirical Evaluation Methods in Computer Vision, December, 2011.

[9] D. Beymer. Pose-Invariant Face Recognition Using Real and Virtual Views. M.I.T., A.I. Technical Report No.1574, March 1996.

[10] T. Vetter and T. Poggio. Linear Object Classes and Image Synthesis from a Single Example Image. A.I.Memo No.1531 (C.B.C.L. Paper No.119), March 1995