ATM USING FINGERPRINT

Swati Koli
Student, NCRD's Sterling Institute of Management Studies, Nerul, Navi Mumbai
swatikoli100@gmail.com

Mahur Patil
Student, NCRD's Sterling Institute of Management Studies, Nerul, Navi Mumbai
mahurpatil10@gmail.com

Prof. Sagar Thakare
Assistant Professor (MCA), NCRD's Sterling Institute of Management Studies, Nerul
sagthakare@gmail.com

ABSTRACT:

A Fingerprint-Based Authentication Framework for ATM Machines. The security of ATM transactions has sparked widespread anxiety in several regions of the world. These issues stem from a number of constraints in the existing architecture of the various service sites. The current use of Personal Identification Number (PIN) for ATM user verification and identification has made the machine vulnerable to unauthorized access, misplacement, forgetfulness, and card eating, among other things, limiting the machine's attractiveness and patronage.

This study presents a framework for fingerprint - authenticated ATM applications. The framework is made up of modules for fingerprint enrolment, database management, and verification. The verification module is divided into three sub-modules: fingerprint enhancement, feature extraction, and matching, all of which rely on appropriate mathematical models to work. There is also a financial transaction platform, which includes withdrawal and balance inquiries. The implementation was carried out using a Windows 7 operating system, with C# and Microsoft SQL server serving as the frontend and backend engines, respectively. False Rejection Rate (FRR), False Acceptance Rate (FAR), and Average Matching Time (AMT) tests on the application illustrate the adequacy and applicability of the proposed framework for ATM user verification and authentication.

Keywords: *ATM Machine, Fingerprint panel, Desktop Application, Server, USER, Internet*

1. INTRODUCTION:

In an ATM (Automated Teller Machine) the personal identification using biometrics are preferred over the standard. Biometrics based authentication may be a potential candidate to exchange password-based authentication. Among all the biometrics, fingerprint based identification is one in all foremost mature and proven technique. Fingerprint Based ATM could be a desktop application where fingerprint of the user is used as authentication. The fingerprint minutiae features are different for every person therefore the user will be identified uniquely. Instead of using ATM card Fingerprint have ATM is safer and secure. There is no need to carry an ATM card in your wallet, and there is no risk of losing it. One critical feature of ATM security is the personal identification number (PIN) or password. A PIN or password is widely used to secure and protect clients' financial information from illegal access. PINs are frequently used for identification and authentication in access codes for buildings, bank accounts, and computer systems.

2. LITERATURE REVIEW:

N.Selvaraju, G.Sekar (2010) in their paper, ‘A Method to boost the protection Level of ATM Banking Systems Using AES Algorithm’ published in International Journal of Computer Applications explains The fingerprint image acquired from the user is encrypted within the ATM terminal for authentication. The encrypted image is transfer through secured channel to the central banking terminal. within the banking terminal fingerprint image is decrypted. The decrypted image is compared with that fingerprint templates. The authentication is valid if the minutiae matchings are successful.

Apoor Va, Priya Bh, Sowmya Vk,Mahesh Prasanna K (2013) in their project, ‘ATM Security’ published in Indian Journal of Science and Technology explains that how the verification process takes place. together with that they also explain how the user’s fingerprint data stored within the database.

Sneha Ramrakhyani, Manisha Meshram, Lata Chandani, Rasanjali Gothe, Parul Jha (2017) in their research paper, ‘Fingerprint Based ATM System: Survey’ published in Indian Journal of Innovative Research in Science, Engineering and Technology. In these paper they supply two phases to clarify fingerprint based ATM System i.e. one is Enrolment phase and second is Authentication phase. And also they survey on approximate ratio of ATM card related frauds.

S. Jathumithran, V. Thamilarasan, A. Piratheepan, P. Rushanthini, J. Mercy veniancya, P. Nirupa and K. Thiruthanigesan (2018) in their research, ‘Enhancing ATM Security Using Fingerprint’ published in ICTACT JOURNAL ON MICROELECTRONICS, author has research in field of electronics therein what quite security provide to secure their transaction. And also fingerprint module connected to the Arduino Uno R3 Board.

Melinda Don Seemanthy, Aleena Mary Varghese, Rakesh T K, Aravind Menon, Sebin Jose (2019) in their research paper, ‘Enchanced Security ATM Transaction using Iris, Fingerprint, OTP Authentication' published in GRD Journal for Global Research and Development Journal for Engineering. In these paper they use three modules that are: Fingerprint Scanning, biometric authentication, OTP Generation. In these paper they explain how the cash transaction in an ATM machine are secured by providing personal identification, by analyzing biometrics like fingerprints and iris patterns which are known for his or her steadiness and variety.

3. PROBLEM DEFINATION:

Many criminals tamper with ATMs and utilise illicit techniques to steal a user's credit card and password. Customers are even kidnapped at gunpoint and forced to divulge their bank credit card PIN, and some are held for many days until the user's account is entirely depleted. The frequency of ATM fraud and criminal activity is increasing, and immediate steps must be done to prevent criminality. The adoption of biometric fingerprints on ATM machines will protect ATM transactions and reduce criminal activity at ATM machines to practically zero percent.

4. OBJECTIVE:

Our system's primary goal is to make ATM transactions more secure and user-friendly. The system is utilised in ATM applications to provide biometric security via fingerprint authentication. The goal of this project is to improve the security of the present system. ATM (Automated Teller Machine) technology by integrating the user's fingerprint into the bank's database in order to further authenticate it. It is implemented to facilitate fingerprint capture and comparison, as well as to offer OTP. This is accomplished by simulating and creating an ATM system with a fingerprint scanner. This technology uses fingerprint recognition to replace regular ATM cards. As a result, there is no need to carry ATM cards to conduct transactions.

5. RESEARCH METHODOLOGY:

Biometric ATMs are self-service cash machines that employ a biometric measure to spot users and permit them to withdraw cash. The biometric check is also used because the sole customer identifier, or it's going to be utilized in conjunction with another format, like a payment card, a mobile device, or an extra security credential, like a PIN. Biometric measures will typically involve palm or finger vein print biometrics, however additional features like as iris recognition may additionally be utilised. Biometric authentication is becoming increasingly prevalent within the banking and finance industries. The fingerprint notion isn't only for security, but also to beat client misunderstanding of the ATM concept. Many drawbacks are rapidly reduced by utilising a fingerprint method. They include we wish to not carry ATM card in your wallet and no danger of card loss, CARD is stolen, passwords are frequently exchanged or, hacking many consumers are proud of our system because of speedy and superior service. The Biometric Panel of ATM Machine shown in below Fig.1.

Fig.1: Biometric Panel of ATM Machine
(Reference: https://www.google.com/biometircinatm)

One kind of biometrics technology is fingerprint scanning. We are using our fingers to access the ATM machine and make a transaction. We utilise this method since it's simple to line up. We don't need to get obviate the present ATM machine.

The verification module is split into three sub-modules:

1. Fingerprint Enhancement

2. Feature Extraction

3. Matching

The ATM fingerprint functioning procedure involves obtaining data from a server. We must first get authentication from the bank before proceeding with the method. A biometric machine is employed by a bank employee to scan his or her fingerprint. Enrolment is that the process by which a biometric equipment extracts the features of a fingerprint and stores them during a database. When a client wants to use an ATM that has been biometrically scanned, he must first place his finger at the sensor. First, the biometric scanner will scan it and compare it to the stored feature and If the feature match then the person is allowed for transaction otherwise it not process. The Scanning Process is shown below in Fig.2.

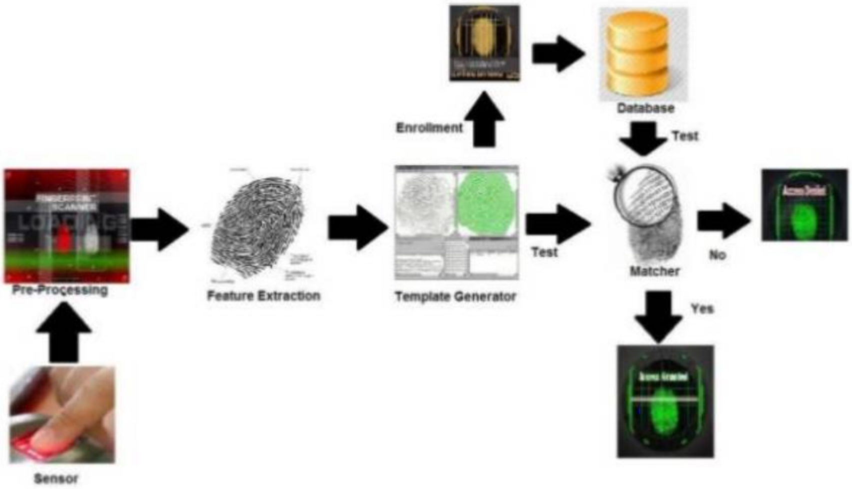

Fig.2: Fingerprint Scanner
(Reference:https://www.google.com/verificationprocessoffingerprintinatm)

Working:

The working is incredibly simple as normal ATM machine the difference is barely fingerprint scanner panel, if we suppose we forgot to hold a ATM card then it will be more useful. In Fingerprint panel, User host machine Display on ATM through internet. Using internet admin hook up with the net server from which biometric may be controlled. For giving any live update regarding name, mobile number and account number. User will get one OTP on mobile no and when user will enter OTP code that will be match so the further next process as same as normal ATM machine. After the method will end the user must select cancel and process will terminated. The OTP is valid till 2 min only. Working of ATM Using Fingerprint Scanner shown in Fig.3.

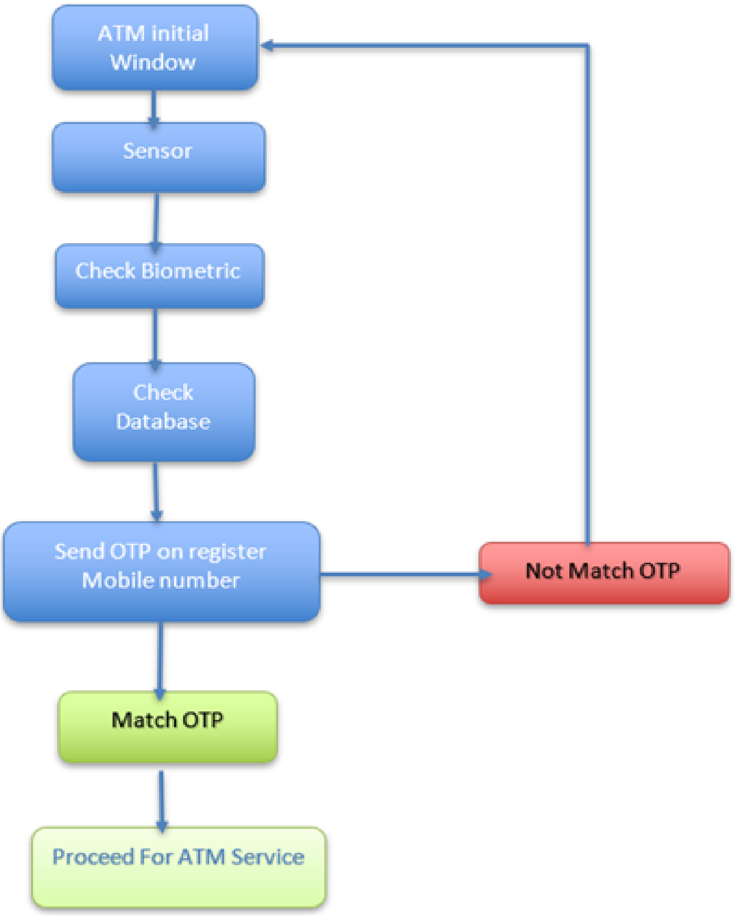

Fig.3: Block Diagram of ATM USING FINGERPRINT

6. ANALYSIS FINDING:

Earlier machines are utilized in old way which is dearer and fewer secure to use the bank services. there's more chance to hake or misuse of machine to withdraw money from another account. Now the cardboard also blocks within the machine so after completion of our service the cardboard will unblocked from machine. due to these reasons, Fingerprint panel the ATM will safer and user also use the ATM machine easily. Include the fingerprint panel of normal size. It works like pin also and after the tactic we put our figure on fingerprint panel then process will complete. there's otherwise is we've option to choose card or fingerprint, if we use fingerprint then put finger on fingerprint panel and system will find details from biometrics and further process will start. The ATM using fingerprint machine is correct for attracting customers' attention and influencing your purchases.

7. LIMITATIONS:

If the user's finger pattern is cut or damaged, the system may fail to recognise the person. After some years, we must update our biometrics at the bank. a major investment in biometrics is required for security. Breach of information - Biometric databases can still be hacked. Tracking and data – Biometric equipment, like biometric identification systems, might limit users' privacy.

8. CONCLUSION:

We shall be able to prove identify supported who we are instead of what we possess or remember by using ATMs that use fingerprints. due to the rise in electronic transactions, there's a rising requirement for quick and precise user identification and authentication. PINs are frequently used for identification and security clearances in access codes for buildings, bank accounts, and computer systems. Because a personality's biometric data is inextricably linked to its owner, is non-transferable, and unique to every individual, identity verification technology supported fingerprint identifiers is also able to overcome this problem. Biometrics isn't simply a stimulating pattern recognition research problem; if applied correctly, it's the potential to form our society safer, reduce fraud, and increase user convenience by extensively delivering functions like identification, large scale identification, and screening.

9. REFERENCES:

1. Moses Okechukwu Onyesolu and Ignatius Majesty Ezeani," ATM Security Using Fingerprint Biometric Identifer: An Investigative Study", International Journal of Advanced branch of knowledge and Applications, 2012. 4. Apoor Va, Priya Bh, Sowmya Vk,Mahesh Prasanna K,"ATM Security", Indian Journal of Science and Technology, 2013.
2. Sneha Ramrakhyani, Manisha Meshram, Lata Chandani, Rasanjali Gothe, Parul Jha,"Fingerprint Based ATM System: Survey", Indian Journal of Innovative Research in Science, Engineering and Technology, 2017.
3. Melinda Don Seemanthy, Aleena Mary Varghese, Rakesh T K, Aravind Menon, Sebin Jose,"Enchanced Security ATM Transaction using Iris, Fingerprint, OTP Authentication", GRD Journal for Global Research and Development Journal for Engineering, 2019.

4. URANG Awajionyi S. and Ojekudo Nathaniel A,"Securing automatic teller machine Machine (ATM) Transaction Using Biometric Fingerprint", American Journal of Engineering Research (AJER), 2020.