WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

"ATM Using Fingerprint"

[1]Mr. Gyanprakash Singh, [2] Prof. Pragati Goel

[1]MCA Semester-VI, Sterling Institute of Management Studies, Nerul, Navi Mumbai shivsingh5128@gmail.com
[2] Asst. Professor, MCA Sterling Institute of Management Studies, Nerul, Navi Mumbai 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 unauthorised 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

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 based 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.

Literature Review

N.Selvaraju, G.Sekar (2010) in their paper, 'A Method to Improve the Security 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 in the ATM terminal for authentication. The encrypted image is then transmitted over the secured channel to the central banking terminal. In the banking terminal fingerprint image is decrypted. The decrypted image is compared with the 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. Along with that they also explain how the user's fingerprint data stored in 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 provide two phases to explain fingerprint based ATM System i.e. one is Enrolment phase and second one 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 in that what kind of security provide to secure their transaction. And also fingerprint module connected to the Arduino Uno R3 Board.

Melinda Don Seemanthy 2Aleena Mary Varghese 3Rakesh T K 4Aravind Menon 5Sebin 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, Iris Scanning, OTP Generation. In these paper they explain how the money transaction in an ATM machine will be secured by providing personal identification, by analyzing biometrics like fingerprints and iris patterns which are known for their steadiness and diversity.

Problem Definition

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.

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.

Research Methodology

The propose of the system to increasing the safe and secure the ATM service by introducing fingerprint system. When the fingerprint scanner of the machine scan the fingerprint of user then Real-time user data extracted from the net using data scraping techniques, where the system searches the appliance programming interface (API) http and therefore the API returns the specified data on the desktop application of ATM machine. The advantage of finger-scan technology is accuracy. By using fingerprint system many disadvantages are rapidly, reduce. They are we want to not carry ATM card in your wallet and no chance of loss card, CARD is stolen, passwords are often shared or, hacking many shoppers are satisfied by our system due to quick and better service. Moreover, initially we store the fingerprint of manager which verified with the fingerprint that we are giving when the time of authentication. If the fingerprints are matched also receive a OTP on registered number and fill in screen, if its match then user can do the transaction, otherwise not. Fingerprint based ATM System is safer than ATM card. User can make transaction using his fingerprint anywhere and at any time he needn't must carry ATM card.

Conceptual Framework Development stages:

1. Research
2. Back-end Development
3. Front-end Development

1) Research:

One of the most crucial steps in the creation of any system is research. We investigate current technology utilised to generate a fingerprint panel on an ATM machine, as well as market trends. We made the decision to develop a fingerprint solution for each end user. We are not developing a distinct application since it would be incompatible with other software platforms and would be inefficient. As a result, we decided to construct a fingerprint panel using a desktop application, which can be operated on any workstation with an Internet connection. Furthermore, web development makes updates and new programme releases simpler and easier to use.

2) Back-end Development:

The system's back-end development includes the MySQL web server and a control panel web page where the fingerprint can be configured. 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.

3) Front-end Development:

C# or PHP are used for front-end development. C# fonts, colours, margins, lines, height, width, background image, advanced position, and many other things can be customised.

Block Diagram:

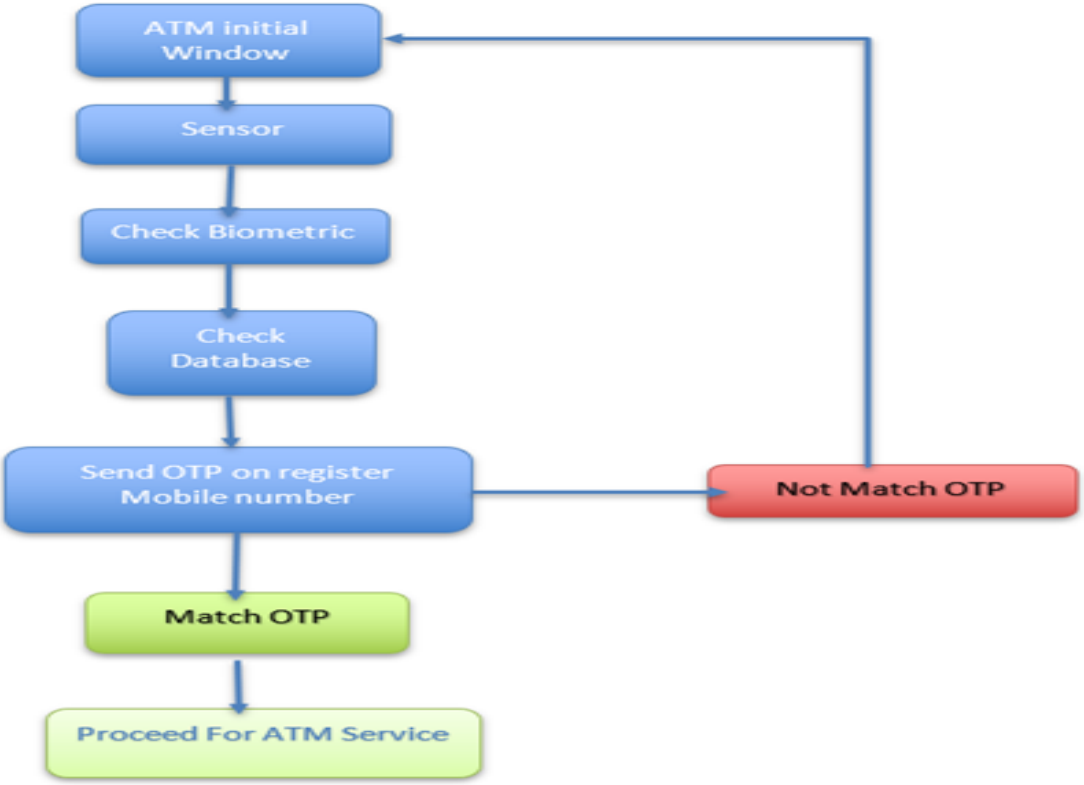

Fig 2: Block Diagram of ATM USING FINGERPRINT
(Reference: http://www.indjst.org/index.php/indjst/article/download/109854/82717)

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 can host machine Display on ATM through internet. Using internet admin hook up with the net server from which biometric may be controlled and in a very server all back-end development of the system done by MySQL. For giving any live update regarding name, mobile number and account number. respected API is employed. Again through internet all the information is transfer in JSON format to desktop application where all the code associated with the user details and every one is written in PHP(front-end). User will get one OTP on mobile when user will enter OTP code will match and also 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.

Analysis Findings

Earlier machines are utilized in old way which is dearer and fewer secure to use the bank services. There is 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. Because of 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 method we put our figure on fingerprint panel then process will complete. There is otherwise is we've choice 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 right for attracting customers' attention and influencing your purchases.

Limitation

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

Conclusion

We shall be able to prove identify based on who we are rather than what we possess or remember by using ATMs that use fingerprints. Because of the increase in electronic transactions, there is 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 person's biometric data is inextricably linked to its owner, is non-transferable, and unique to each individual, biometric identification technology based on fingerprint identifiers may be able to overcome this problem. Biometrics is not simply an interesting pattern recognition research problem; if applied correctly, it has the potential to make our society safer, reduce fraud, and increase user convenience by extensively delivering functions such as positive identification, large scale identification, and screening.

References

- https://en.wikipedia.org/wiki/Biometric_device
- http://www.ijirset.com
- http://www.kscst.iisc.ernet.in/spp/37_series/spp37s/synopsis_exhibition
- http://ethesis.nitrkl.ac.in
- http://www.ajer.org/papers/Vol-9-issue-9
- https://www.researchgate.net
- https://www.grdjournals.com
- http://ictactjournals.in