International Journal of Research in Engineering, Science and Management
Volume-3, Issue-2, February-2020
www.ijresm.com | ISSN (Online): 2581-5792

Security for Building and ATM Machine

Anjali Jaiswal[1], Nawaz Kapadia[2], Aman Wadia[3], Adarsh Goyal[4], Poonam Vengurlekar[5]
[1,2,3,4]*Student, Department of Computer Engineering, Thakur Polytechnic, Mumbai, India*
[5]*Professor, Department of Computer Engineering, Thakur Polytechnic, Mumbai, India*

***Abstract*: Better and Protective security is the need in today's world at the places such as buildings and ATM machines. There are many drawbacks of using the debit card at ATM machine so to overcome this we are implementing the withdrawal and deposits through Aadhar Verification. Since every ATM room has a CCTV camera installed so if the theft takes place we can get the details of the person since he entered the room through aadhar verification. To secure the entrance of the society so that no outsider can enter the society without verifying himself through aadhar verification.**

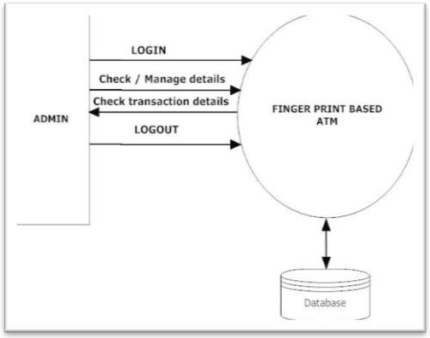
Biometric system is a identification system that recognizes an individual by determining that person. Fingerprint is dependable biometric trait as it is dedicated. It is a technology that is increasingly used in various fields like forensics and for the security purpose. The main objective of our system is to make ATM transaction more secure using aadhar no and user friendly. This system replaces traditional ATM cards with fingerprint. Therefore, ATM cards will be replaced by the biometric verification through aadhar. The money transaction can be made more secure without worrying about the card to be lost. In our system we are using embedded system with biometrics i.e. r305 sensor and Arduino uno microcontroller. The Fingerprint and the name of all users are stored in the database. Fingerprints are used to identify whether the Person is genuine and to protect ATM frauds.

***Keywords*: Security for buildings, Security for ATM machine's, Secure way to protect buildings, ATM machine.**

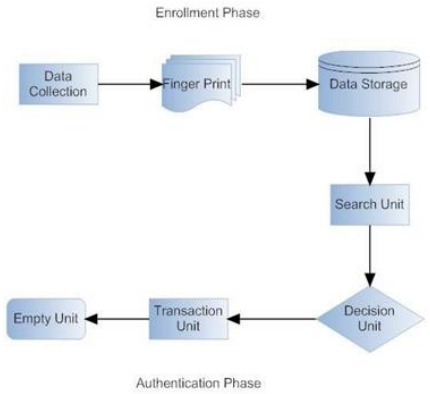
1. Introduction

In building there is the provision of entering the details which is also called as manual security but in manual security there is lot of disadvantages such as lack of security proof, unethical practices , lack of details & Same in the ATM user have to enter all of his details to transect money for ATM machine so sometimes there may happen crimes so, to overcome this problem we have come up with the project which is the combination of both software and hardware in this project we are going to use some of the important hardware and software devices like biometric scanner, Aadhar number verification & mobile verification through OTP and all this information will be stored in the master database.

Which means whenever the outsider/guest is entering the building for the first time he/she have to properly follow all this steps. Once he has followed all the steps then the guard will allow him/her to go in the building this is for building and same is for ATM machine also he/she have to enter his/her details for verification purposes. suppose if the person is disabled he/she can only verify their mobile number through OTP and they can go inside the ATM machine and in the building.



Biometric system is an identification system that recognizes an individual by determining that person. Fingerprint is dependable biometric trait as it is dedicated. It is a technology that is increasingly used in various fields like forensics and for the security purpose. The main objective of our system is to make ATM transaction more secure using aadhar no. and user friendly. This system replaces traditional ATM cards with fingerprint. Therefore, ATM cards will be replaced by the biometric verification through aadhar. The money transaction can be made more secure without worrying about the card to be lost. In our system we are using embedded system with biometrics i.e r305 sensor and Arduino uno microcontroller. The Fingerprint and the name of all users are stored in the database. Fingerprints are used to identify whether the Person is genuine and to protect ATM frauds.



A Fingerprint scanner is used to acquire the finger print of the individual, after which the system requests for the OTP (One Time Password). If the fingerprints do not match further

authentication will not be proceeded further for the process, it will return back to reenter the aadhar number. After the verification is completed the data will be stored in the system database, the user is authenticated further to make transactions.

Data collection unit: The most important requirement for this stage is of an optical sensor i.e. r305optical scanner. The fingerprints of the user will be stored in this unit. This unit adds a fingerprint of the user to database unit and further returns a byte every newly added user/customer. The return values range from 0x00 to 0xFE. The return code is 0xFF i.e. error executing function in case when there is an error, i.e. no finger is placed on the sensor.

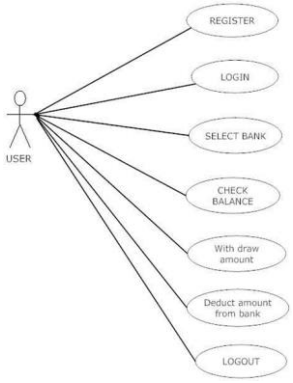
Image preprocessing unit: As the input is taken by the scanner as image preprocessing is done on the image in the scanner during the processing time, and the image is tested in the form of analog that is converted into digital form and if the quality of the preprocessed image is sufficient then the image is converted into the template.

Data storage unit: Each preprocessed image is of certain default template size i.e. approximately 512 bytes per template and the template will be stored into the database for further use. This unit allows the user to store the fingerprint data in the module and further configure it in next mode for storing an individual's fingerprint.

Search unit: As a finger is placed on the fingerprint sensor the search function will be called. The existing memory is then checked and returns a matching name of the customer if found.

Decision unit: This system compares the input image with the stored images of the database. The database image is stored after several processes, so it would be easier during the next transaction. Stored template and test image is compared and the needed resolution of the test image will be 500dpi (dot per inch) by default. When the image comparison gets satisfied, then the user of the input is an authorized user and will be allowed to make further transactions.

Transaction unit: if the decision making unit authorizes the user then the transaction is successfully carried out further Truncate function: This function is used to clear the database containing fingerprints and the other information stored in it. After executing this function, you will get following as message: 0xCC if operation was successful.0xFF in case of error. There are various ways to authenticate the biometric data feed. Combination of biometric data along with the OTP number is used to increase the security. Since the biometric data cannot be stolen or forget, the transaction would be safe and secured. The transaction time of the proposed system is about 15 seconds. The concepts of Cryptography and Steganography are known used in fingerprint based ATM system, they intend to use the finger print image captured by the fingerprint scanner as the BASE image and get the data and will stored it in the database. Using the concept of Steganography, they hide the AES256 encrypted code (OTP) inside the fingerprint image.



2. Requirement analysis

There will be a several types of devices like in hardware we will need 1) Biometric scanner for finger print 2) Arduino-UNO 3) DOT NET language for Front end 4) SQL server for Back end

Software requirement: DOT NET Language, Arduino UNO knowledge, SQL Database knowledge

A. Abbreviations and Acronyms

- IoT: Internet of things
- ATM machine: Automated Teller Machine
- SQL: Standardized query language
- DPI: Dot Per Inch
- OTP: One Time Password

B. Further Improvement

- we can implement retinas scanner for proper security purpose
- To achieve full time automation, A real time system should be employed and a Closed Circuit Television (CCTV) system that should provide for proper monitoring and security purpose in the building and the ATM machines.

3. Objective

The main objective of the system is that reducing the theft that is taken place in the ATM room and in the buildings.

- The members leaving in the society will be secured.
- The ATM machines will be more secured.
- One cannot enter the room or in a building before the verification process is completed and the person is successfully verified to enter.
- As the transaction is completed one has to logout the user interface before exiting the ATM room.
- One can view the transactions made throughout a month using the feature of mini statement.
- E-receipt of the transactions made throughout a month can be generated on the Mail at the end of every month.
- One can invest in the investments using the investment feature of the ATM interface.
- To propose authentication and verification process on the

existing, ATM machine to make a successful and secure transaction. The main objective of this project is to provide fingerprint as authorized identity and to design a more secure ATM system. In this, ATM machine work as when the customer place finger on biometric scanner of ATM and if the finger match is found it will display the name of customer on ATM machine. If Fingerprint match not found, it does not allow any transaction. The objective of this study is as follows:

1. To propose the authentication system on the existing ATM process for withdrawal after the entry of a correct OTP.
2. In second level authentication system in a scenario where customer specified withdrawal limit. 1. To propose the authentication system on the existing ATM process for withdrawal after the entry of a correct OTP.
3. To propose second level authentication system in a scenario where customer specified withdrawal limit.

4. Limitation

- The limitations of IOT in extreme situation are still not tested.
- Legal instruments.
- Limited facilities for real-time information exchange
- Limited facilities for real-time information exchange

5. Conclusion

As the person come at the ATM room he has to get himself verified through aadhar to enter in the ATM room to use the features of ATM interface such as with drawls, Deposits, Top up, Investments, opening a new account, Mini Statements & etc. and for building also the person have to enter all him/her details to enter in the system because of security purpose to fully secure the building for any unethical behaviour & robbery guidelines to prepare the project Security for ATM & building.

It is essential that to first understand the basic of a biometric based security system. The implementation of ATM security system by using biometric method it is very important method. As well as very challenging and difficult. But for security purpose or control the criminal records it is very important to that produce this method. I think for future work it will implement also various technologies such that unique cards or any other method.

Acknowledgement

Thanks to Mrs. Vaishali Rane the HOD of Computer Department of Thakur Polytechnic to give us the opportunity to work on this project under the guidance of Mrs. Poonam Vengurlekar.

References

[1] A. Q. M. S. U. Pathan et. al, “Finger print authentication security: An improved 2-step authentication method with flexibility,” International Journal of Scientific & Engineering Research, Volume 10, Issue 1, January 2019.
[2] https://www.buildings.com/article-details/articleid/20606/tie/9-keys-to-building-security
[3] https://en.wikipedia.org/wiki/Retinal_scan
[4] V. Vijayalakshmi, R.Divya and K. Jaganath, ”Finger and Palm print based Multibiometric Authentication System with GUI Interface” International conference on Communication and Signal Processing, April 2013 IEEE.
[5] O. A. Esan and S. M. Ngwira “Bimodal Biometrics for Financial Infrastructure Security” I. O. Osunmakinde School of Computings, College of Science, Engineering and Technology, University of South Africa, UNISA Pretoria, South Africa, IEEE 2013.
[6] Rishigesh Murugesh, “Advanced biometric ATM machine with aes 256 and steganography implementation”, IEEE Fourth International Conference on Advanced Computing, ICoAC 2012 MIT, Anna University, Chennai. December 13-15, 2012 IEEE.
[7] Rajesh. V and Vishnupriya. S, “IBIO-A New Approach/or ATM Banking System” 2014 International Conference on Electronics and Communication Systems (ICECS-2014), Feb.13-14, 2014, Coimbatore, INDIA.
[8] G. Renee Jebaline and S. Gomathi, “A Novel Method to Enhance the Security of ATM using Biometrics”, 2015 International Conference on Circuit, Power and Computing Technologies [ICCPCT], IEEE 2013.