IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Volume 8, PP 20-24

Secured Tam Simulator

Geetesh Gadekar[1], Sarvesh Gadekar[2]Meghana Rahe[3], Prof. Renuka Nagpure[4]
[1](Information Technology, Atharva College of Engineering/Mumbai University, India)
[2](Information Technology, Atharva College of Engineering/Mumbai University, India)
[3](Information Technology, Atharva College of Engineering/Mumbai University, India)
[4](Information Technology, Atharva College of Engineering/Mumbai University, India)
Corresponding Author: Geetesh Gadekar

Abstract: *Security of Money, Data etc. is most important in today's world. This project is based on Security of ATM. In this project we will simulate an ATM machine where dynamic computer-generated password is provided to user for every transaction. As soon as user enters account no, user must provide his/her finger print to ATM machine using a Biometrics Finger Print Scanner, if the finger print is validated properly, a new dynamic computer-generated password will be sent to user on his/her mobile phone on the number which is registered at bank. Using that auto generated password user will be able to login into the account. After completing transaction when user log's out of the account, the password will be automatically destroyed.This way we can have a secure ATM transaction every time.*

Keywords- *Security, fingerprint, password, ATM, simulate*

I. Introduction

1.1 Aim and Objectives:

Our aim is to provide multi-factor authentication, with normal ATM facilities and additional DD facility. An Automated Teller Machine (ATM) is a safety-critical and real-time system that is highly complicated in design and implementation.

This paper presents the formal design, specification, and modeling of the ATM system using a denotational mathematics known as Real-Time Process Algebra (RTPA). The conceptual model of the ATM system is introduced as the initial requirements for the system. The architectural model of the ATM system is created using RTPA architectural modeling methodologies and refined by a set of Unified Data Models (UDMs), which share a generic mathematical model of tuples.

Our system also provides a D/D facility in a single ATM machine. The benefit of our system is that it provides multiple authentication i.e. two-way security.

1.2 Problem statement

The proposed solution is two-way authentication wherein thumbprint authentication and OTP authentication will be implemented along with DD facility.

1.3 Scope

In this system we will simulate an ATM machine where an 8-pin dynamic computer password is being generated. As soon as user enters account number and gives the fingerprint to the system a new dynamic computer-generated password will be sent to user's mobile phone on the number which is registered at bank only if the account number is correct and fingerprint is matched. Using that auto generated password user will be able to login into the account. After completing transaction when user logs out of the account, the password will be automatically destroyed. A new password is provided to user for every single transaction process. This way we can have a secure ATM transaction.

II. Review of Literature

2.1 ATM Transaction Security Using Fingerprint/ OTP [1]

This project was carried out in 2005 by Krishna Nand Pandey, Md.Masoom, SupriyaKumari and PreetiDhiman. This paper deals with the solutions related to the ATM security. That project deals with making use of fingerprint or One Time Password (OTP) verification along with the use of ATM pin. In that system, the user can have third party authentication either temporary or permanent. In the whole process, the first party I.e the banker will maintain a database of the customer including fingerprint and mobile number. The banker will provide the ATM card along with its PIN. For the transaction after entering the ATM pin, the customer will be asked to choose an option either fingerprint or OTP verification. The OTP will be sent to the registered mobile number of the customer through GSM module connected to the system. After authorized verification, the

customer will be able to proceed for transaction else after three successive wrong attempts, the ATM card will be blocked for 24 hours and a message will be sent to the registered mobile number.

2.2 Securing ATM with Biometric and OTP [2]

This project was carried out in 2015 by Mohammad Hamid Khan. ATM is an easy way to get money, you just need to insert card and password and you just got the money. But what if someone will steal your card and somehow, he/she will know your password, it will grant him/her full access to your money. That raise question on present security and demands something new in the system that can provide second level of security. One-time password (OTP) is password that validates an authentic user for only one login to the respective system. If user is unauthorized, system will not allow further access. OTP can be generated by using different cryptographic hash functions that provides a fixed string which can be used as second level security at ATM. In generation of OTP there are many factors that can make OTP unique every time it is generated. Factors that can be considered are time at when the user is accessing the machine, account number of the user, mobile number of the user, Location of the user, International Mobile Station Equipment Identity (IMEI) number which is unique for every mobile device. By taking into consideration factors like daily life problem (general problems) that is phone got switched off, battery is down; less coverage of network can affect the OTP solution etc. To avoid application-based problem this report also suggest a solution i.e. biometric security; by using biometric security the alternative security will be as same as OTP. In this report, the flow of system I am developing, topics related to ATM banking and security, about OTP and biometric solution is discussed.

2.3 Secure Authentication for ATM Implementing QR Code Using Mobile Devices [3]

This project was carried out in 2016 by S. Kanimozhi and D. Revathy. In that paper, they propose Security PIN Authentication for providing security for user by using ATM by connecting Smart Phones. Itis using Image Processing techniques is implemented for the user pin entry process. QR Code is the trademark for type of matrix barcode. A barcode is a machine-readable optical label that contains information about the item to which it is attached. Security PIN Authentication allows a user to scan a QR code from the screen of a point-of-service terminal and connects to the cloud-based bank's server. Security PIN Authentication server to obtain secure onetime-use PIN templates. Here, a PIN template is a sequence of digits with marked positions for the user to enter the actual PIN code. The QR code scanning is done using mobile devices. The Security PIN Authentication service can also be used with a smart phone.

2.4 SEPIA: Secure-PIN-Authentication-as-a-Service for ATM using Mobile and Wearable Devices [4]

This project was carried out in 2005 by Rasib Khan, Ragib Hasan and Jinfang Xu. In that paper, they propose Secure-PIN-Authentication-as-a-Service (SEPIA), a secure obfuscated PIN authentication protocol for ATM and other point-of-service terminals using cloud connected personal mobile and wearable devices. Their approach protects the user from shoulder-surfers and partial observation attacks, and is also resistant to relay, replay, and intermediate transaction attacks. A SEPIA user utilizes a Google Glass or a mobile device for scanning a QR code on the terminal screen to prove co-location to the cloud-based server and obtain a secure PIN template for point-of-service authentication. SEPIA ensures minimal task overhead on the user's device with maximal computation offloaded to the cloud. They had implemented a proof-of-concept prototype to perform experimental analysis and a usability study for the SEPIA architecture. ATM authentication using PIN-based entry is highly susceptible to shoulder-surfing or observation attacks. Credit/Debit cards are also not resilient to relay and other skimming and cloning attacks. In this paper, we propose the Secure-PIN Authentication-as-a-Service (SEPIA), a cloud-based obfuscated PIN-based authentication service for ATMs or point-of service terminals using personal mobile or wearable devices. We have focused the security design for SEPIA based on visual privacy of users for a one-time-use PIN template and address the security vulnerabilities in PIN-based authentication.

2.5 Experimental study of thumbprint-based authentication framework for ATM machines [5]

This project was carried out in 2014 by Iwasokun Gabriel Babatunde and Munda Josiah Lange. The system depends solely on fingerprint for human verification and identification and its architecture is presented. The Network Service serves as the operational platform for the system. The thumbprint database is available on the Network and it adopts a relational model to store information on the thumbprints of the registered customers. Stored information includes pattern type and feature characteristics. There is no due preference for the use of thumbprint as image from any of the other fingers could be designated for the same purpose. The operation of Personal Identification Number (PIN) based Automated Teller Machine (ATM) has continued to experienced challenges currently militating against its acceptance and patronage. The challenges include card swallowing, misplacement, damage or expiration. Several users are also experiencing forgetfulness of PIN and the activities of fraudsters targeted at PIN pilfering for authorized access to account. This paper presents the experimental

study of a framework for fingerprint authenticated ATM that addresses these challenges. The framework is an embodiment of different components for fingerprint processing which include enrollment, database and verification.

2.6 Automatic Demand Draft Withdrawal Machine Using Microcontroller [6]

This project was carried out in 2014 by B. Suganya1, K.V. Soundarya Devi and M. Revathi. In this automated system, the customer must insert their currency in the rupee slot and must wait for few seconds to accept it. Then within next few seconds they must feed the required details in the PC instead of writing in a form. This is then generated and the sum of amount which has been inserted will be added in the softcopy. Then they must verify once and must give print. Thus, the Demand Draft will be generated in few seconds instead of standing for hours. Thus, this system eliminates the drawbacks of the existing set-up. It is placed in the bank branches like that of ATM. In proposed system, image processing is used to count the currency. With this automation, issuing of demand draft is made easier by feeding the inputs in the input module. In our project we designed the hardware for taking the currency notes from the input slot and software is designed to generate the demand draft. The objective of this project is to design a simple, easy to install, microcontroller-based circuit to control and PC or laptop interface for generating the demand draft. The controller used here is a low power, cost efficient chip MSP430 microcontroller which communicates with the Sensor for sensing the currency note efficiently and drivers to control the rotation of notes. MSP430 also communicates with PC/Laptop for parsing the data. Also, the use of easily available components reduces the manufacturing and maintenance costs. The design is quite flexible as the software can be changed any time. It can thus be tailor-made to the specific requirements of the user. This makes the proposed system to be efficient and effective in time saving.

2.7 A novel method to enhance the security of ATM using biometrics [7]

This project was carried out in 2015 by G. Renee Jebaline and S. Gomathi. The biometric authentication is the technique in which the biometric data in the database is compared with the current input data. When the authentication gets satisfied then the future process is carried out. The client's biometric image is captured, and it is encrypted using blowfish algorithm at the client's side. Before encryption the fingerprint image is processed to extract the minutiae. The image quality is highly related to the performance of the system. For a good quality image, minor preprocessing is enough for feature extraction. The minutiae extraction can be carried out with the help of two techniques. The techniques involving the minutiae extraction are Binaized fingerprint images and Gray Scale Fingerprint Images. The encrypted image is then transmitted through secured network to the server. In the server side the image is decrypted. The minutiae extraction helps us to find out the core points, and the core points are only encrypted during the transaction. When we perform encryption only with the core points identified from the input image after extraction, the transaction time can be reduced to the greater extent. During transaction the hit and miss algorithm is used to identify the core points since the image fed may vary in angle from the enrollment image.

III. System Design

"ATM simulator and server" project will be divide into two phases. First phase will concentrate on develop the back-end server, the centralization of all of the transactions. Second phase will be developed the front-end ATM. In addition, we must simulate both the interface and hardware of an ATM.

To use ATM, customer place their card into card reader and the customer then needs to give the fingerprint and after verifying the fingerprint a four-digit PIN will be sent to users registered mobile number which he/she need to input. The session is started when customer place their card into card reader and finish when customer press reject button on ATM to get the ATM card back.

ATM Client should be able to support both graphical interface and the biometric device. In order work, the project should have the reusability, follow the OO principal and keep in mind: "close for modification but open for extension".

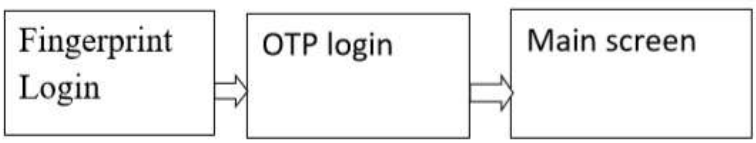

Figure 3.1: Block Diagram of ATM

The Proposed System consists of three blocks:

Fingerprint Login: There will be a fingerprint algorithm which will be used for scanning which is described below [4.1]. The hardware used is the biometrics scanner. As soon as user enters account number, user must provide his/her fingerprint to ATM machine using a Biometrics Finger Print Scanner.

OTP login: If the finger print is validated properly, a new dynamic computer-generated password will be sent to user on his/her mobile phone on the number which is registered at bank. Using that auto generated password user will be able to login into the account. The password will be provided to the user for every transaction. After completing transaction when user log's out of the account, the password will be automatically destroyed.

Main screen: On the main screen, various options will be displayed such as cash withdrawal, balance enquiry and demand draft. Cash withdrawal and balance enquiry are the two options provided to the user which a normal ATM machine has. We'll also simulate the generation of demand draft. The D/D's soft copy will be generated by the system software when the user clicks on the D/D option in the software. The D/D details will be filled by the user.

Fingerprint Recognition Algorithm:

To authenticate the user by automatically extracting minutiae from user's scanned fingerprint image, fingerprint recognition algorithm is required. The fingerprint recognition algorithm involves two main steps: -

Step 1: - Image processing step in which characteristics of scanned fingerprint are captured by having image under-going several stages.

Step 2: - Matching algorithm step in which user authentication is done by comparing feature data comprised of minutiae with Fingerprint Template captured at the time of opening account.

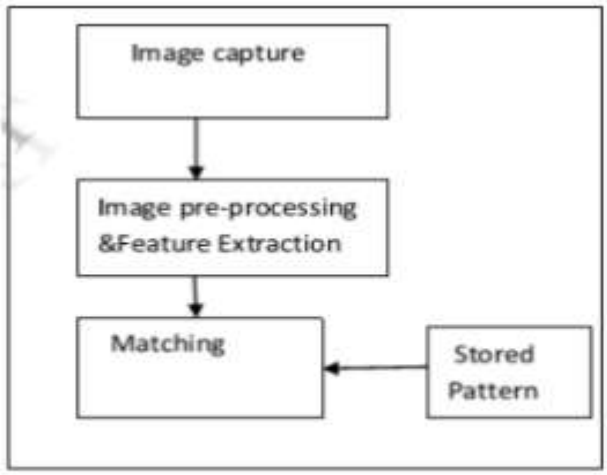

Fig 4.1: Fingerprint Recognition Process

The client side consists of following module: -

Start Session – To start using an ATM, the customer inserts their card. They only need to enter a Personal Identification Number (PIN) for verification after receiving the dynamic password on the registered mobile number. Then they also need to give their thumb impression to ensure greater security.

Check Balance – Get the balance of an account. The user can also get a balance of all accounts linked to the card.

Withdraw Cash – A customer can withdraw cash from an account. An exchange is required if the currency withdrawn isn't the same as the account being withdrawn from. If the customer has multiple accounts, the customer is able to choose which account to withdraw from.

Issue Demand Draft– The customer can issue a demand draft from with help of ATM machine.

Book fixed deposit– The current account can be converted into fixed deposit account with the help of ATM machine.

Request new check book – a new check book can be issued by the user.

Request check status – the status of an issued check can be viewed via this module.

Mini statement – a printed statement slip is received after every transaction.

Money transfer – money can be transferred from one account to another with the help of our ATM system.

Recurring deposit activation – a recurring deposit. Account can be activated using ATM.

Bill payments – bills can be paid through ATM system.
Finish Session – When the customer is finished using the ATM, they can choose to finish their session. The ATM will return their card.
The admin side consists of the following module: -
Register account – a new account/user is being registered by the admin at the back end.
Update account – all the transactions of the user are being updated and saved by the admin.
Delete account – account can be deleted on request.
View fixed deposit log – the admin keeps the track of the fixed deposit account and on request create new fixed deposit for the user.
View check book request - checks any new requests for check book.
View Check status – checks the status of an issued check.
Bill details – processes the payments of bills requested by the user.

IV. Expected Output

This approach provides two-way authentication to the ATM system. So, the security is enhanced. The user will be able to check his/her balance and issue a demand draft as well. The hard copy of the demand draft can be made available through printout if required.

V. Conclusion

Using fingerprint and OTP for ATM process enhances the security and decreases the chances of theft and fraud. Also including the demand draft banking operation through ATM increases the usability of bank and timings as ATM is available 24X7X365.

VI. Future Scope

The system can also be enhanced by using a Mobile Application. This authentication mechanism can be further enhanced by adding/implementing a retina scanner in the system, thus making it a three-way authentication mechanism. The user can also receive digital currency such as bitcoin.

Acknowledgement

It gives us great pleasure in presenting this paper titled: "Secured ATM Simulator".
We express our gratitude to our project guide Prof. Renuka Nagpure, who provided us with all the guidance and encouragement and helped us in finding our mistakes and improving it. We also would like to deeply express our sincere gratitude to Project coordinators.

We are eager and glad to express our gratitude to the Head of the Information Technology Dept. Prof. Neelima Pathak, for her approval of this project. We are also thankful to her for providing us the needed assistance, detailed suggestions and encouragement to do the project.

We would like to deeply express our sincere gratitude to our respected principal Prof. Dr. Shrikant Kallurkar and the management of Atharva College of Engineering for providing such an ideal atmosphere to build up this project with well-equipped library with all the utmost necessary reference materials and up to date IT Laboratories.We are extremely thankful to all staff and the management of the college for providing us all the facilities and resources required.

References

[1] Krishna Nand Pandey, Md.Masoom, SupriyaKumari and PreetiDhiman, "ATM Transaction Security Using Fingerprint/ OTP". Available at: inpressco.com/wp-content/uploads/2015/04/Paper1031157-1159.pdf
[2] Mohammad Hamid Khan. "Securing ATM with Biometric and OTP."Available at: www.ijritcc.org/download/1429768516.pdf
[3] S. Kanimozhi and D. Revathy. "Secure Authentication for ATM Implementing QR Code Using Mobile Devices."Available at: www.ioirp.com/Doc/IJIRCSE/V2_I4/1ICISET218.pdf
[4] Rasib Khan, Ragib Hasan and Jinfang Xu. "SEPIA: Secure-PIN-Authentication-as-a-Service for ATM using Mobile and Wearable Devices."Available at: http://ieeexplore.ieee.org/document/7130868/
[5] Iwasokun Gabriel Babatunde and Munda Josiah Lange. "Experimental study of thumbprint-based authentication framework for ATM machines."Available at: http://ieeexplore.ieee.org/document/6918235/
[6] B. Suganya1, K.V. Soundarya Devi and M. Revathi. "Automatic Demand Draft Withdrawal Machine Using Microcontroller."Availableat: https://giapjournals.com/index.php/ijsrtm/article/download/182/176
[7] G. Renee Jebaline and S. Gomathi. "A novel method to enhance the security of ATM using biometrics."Available at: ieeexplore.ieee.org/document/7159391/