OTP ATM CARD FOR SAFE AND UNTHREAT TRANCTIONS

GENTEM VARAPRASAD[#1],
Naga Sai Sanketh.P[#2],G.Naga Harsha varadan Reddy [#3],K.Murali Mohan[#4],M.G.Mohammad Nahir[#5]
Assistant Professor, Department of Computer Science and Engineering, Santhiram Engineering college, Nandyal, Kurnool Dist.[#1]
Under Graduate Students, Department of Computer Science and Engineering, Santhiram Engineering college, Nandyal, Kurnool Dist.[#2]
Under Graduate Students, Department of Computer Science and Engineering, Santhiram Engineering college, Nandyal, Kurnool Dist.[#3]
Under Graduate Students, Department of Computer Science and Engineering, Santhiram Engineering college, Nandyal, Kurnool Dist.[#4]
Under Graduate Students, Department of Computer Science and Engineering, Santhiram Engineering college, Nandyal, Kurnool Dist.[#5]
varaprasad.cse@srecnandyal.edu.in[#1],
saisanketh533@gmail.com[#2],gharsha1425@gmail.com[#3],kadiyalamurali45678@gmail.com[#4],mohammad.nazhir@gmail.com[#5]

ABSTRACT:

A self-governing ATM host has a right to use any bank. There is no security layer is implemented in the ATM card except pin number. It is very costly for the bank to include the fingerprint and Iris scanner. In this paper, we monitor the location of the ATM usage, time taken for the user to accessing the ATM machine, sequence of events processed by the user and expected amount of withdrawal by the user. All these four factors are verified for the authentication purpose of the user along with password. If any of the above said, parameter are differing and then the One Time Password is generated to the User's Mobile number for further more secure authentication system. In the modification phase, an automation user Internet recognition model is designed to enhance the user comfort and detection of the time span spend by the user in the ATM machine. If due to signal problem of the mobile One Time Password will not be received in that cause secret process is used to private ATM users.

Keywords: ATM, Transaction, Identity theft, One Time Password, Secret process.

I. INTRODUCTION

Automated Teller Machine (ATM)[1] is considered the common e-banking technology adopted by banks all over the world. ATM is a computerized machine that provides customers of banks the facility of accessing their accounts for cash withdrawal and to carry out other financial transactions without the need for a human cashier, clerk or bank teller. It combines a computer terminal, recordkeeping system, and cash vault in one unit, permitting customers to enter a financial firm's bookkeeping system either with plastic card containing a personal identification number (PIN) or by punching a special code number into a computer terminal linked to the financial firm's computerized records 24 hours a day.

ATM's has been adopted by banks because they offer considerable benefits to both banks and their depositors. The most exciting experience for customers as well as bankers is that the ATM is replacing all the difficulties of bank transactions such as personal attendance of the customer, banking hour restrictions and paper-based verification. It is quite easy to withdraw money from ATM instantaneously at any time. ATMs allow one to perform multiple banking functions such as withdrawal of cash, making balance enquiries, transferring money from one account to another, paying insurance premium, making small loans and payment of bills.

II. LITERATURE SURVEY

Identification is the establishment of identity. Authentication confirms claim by use of identity. PIN authentication technique has many problems. Biometrics is best for authentication today and is realistic [2]. Multifactor authentication technique will enhance banking transactions via ATM. Technique proposed in our work involves three authentications techniques to further enhance ATM usage and operations.

Shuffled ATM keypad method and they develop Bluetooth application to overcome the shortfalls of PIN entry was proposed by [3]. This method shows numbers in the Liquid Crystal Display keypad and communicates the password through the wireless medium.

A novel cardholder verification method was proposed by [4]. It gives the user the flexibility to add one or more extra RFID devices like smart watches, smart phones, rings, necklaces, and bracelets and select a suitable security level for use. The Black and White (BW) Method was proposed by [5]. Our popularly known numeric keypad is colored at random, part black and the other white. Only users with correct PIN digit can answer the colors. A keyboard using fake cursor that hides password entry on screen was presented by [6]. In this system, only one cursor is for actual input while others are distraction for third parties.

In the process of ATM transaction, there are different aspects that should be considered. Personal identification number has been of very great importance in the overall operation. The PIN is not printed or embedded on the card but is manually entered by the cardholder during ATM transactions. In existing system, the card will be swiped. After swiping the card, the machine will ask for amount to be transacted and user's PIN. The user has to enter the necessary details. Upon entering, the transaction will take place. The transaction would get declined if incorrect PIN is entered.

III. THREATS TO ATM SERVICES

There many threats related to ATM security as the popularity and usage increases incessantly. New ATM's are being installed in different locations daily and the users are also increasing. Some of the threats are discussed below.

A. Shoulder Surfing

Shoulder surfing is a way of looking over someone's shoulder, to get information. In a crowded environment, it is very easy and effective to stand beside a fellow and watch how PIN numbers are entered at cards terminal[7].

B. Spoofing

Spoofing is impersonation, getting access and taking advantage of someone else's account. [7].

C. Skimming

This involves the use of card skimmer devices by fraudsters to get card details from the magnetic chip [8]. These devices are usually installed inside or over the top of an ATM card reader.

D. Card Trapping/Phishing

Card trapping and Phishing attempt to steal card as the customer insert it into the ATM for transaction [9]. A device is placed over or inside the card slot to capture the consumer's card. These devices are designed to prevent the card from being returned to the consumer after transaction.

E. Reply Attacks

Here, attackers spy the conversation between the sender and receiver and takes important information e.g. sharing key and then contact to the receiver with that key. In Replay attack the attacker gives the proof of his identity and authenticity.

IV. FUNCTIONAL OVERVIEW

In transaction process, consists of recording the following parameters for the transaction:

1. Type of transaction to be performed.
2. Correct States/Screen display
3. Timeout parameters based on requirement.
4. proper flow based on us-on-us and them-on-us cards.

If any misbehavior take place it will block the enter transaction. One might think that it could be very plausible to have deviation from one of these parameters on a regular basis for the original user of the ATM card. For that purpose, our model declares a transaction as fraudulent only if 3 or more of the 4 factors mentioned above are deviated from the user's record then it is Post Declaring Fraudulent /Legitimate Action.

If the transaction is declared as legitimate, the user may proceed with the withdrawal of cash from the ATM. But if the transaction turns out to be fraudulent one, which could happen with a slim possibility for the original user, the user would be sent a text message with a One Time Password to his/her mobile through the ATM's record searching ability and network connectivity. The user may then unblock the transaction with that password. In case of a fraudulent user, the original user would be notified that someone is performing an identity theft with their ATM card and would be prompted to take appropriate action after the realization of such an event. In case of signal problem occurs then use the secret quiz process to unblock the process.

V. SYSTEM ANALYSIS

The objectives of this study are to propose a authentication system on the existing ATM process for withdrawal, after entry of correct PIN and to propose authentication system in a scenario where a customer-specified withdrawal limit is attained. To perform the transaction the pin and amount has to be entered by the user. The permanent PIN number will get verified by the bank server. If the authentication is successful then the entered amount will be verified whether the amount lies within the user specified limit. Upon successful authentication the OTP will send to the pre-registered mobile device.

VI. WORKFLOW

For implementing OTP, we will make use of GSM modem to send SMS (an OTP) to user's mobile number. The idea to use mobile phones is preferred over e-mail because the people in rural areas have simple phones which can receive text messages but have no internet connections and e-mail facilities. Since mobile phones are ubiquitous, we intend to use mobile phones so that everyone can take the benefit of the new proposed system. The user will receive OTP

immediately after passing the face recognition test. Once OTP is received user has to enter the code which is of 4-digit. User gets three chances to enter the code. If the code is entered incorrectly in three consecutive attempts account gets temporarily blocked and notification is sent to registered mobile number

It gives the basic architecture of the developing project, Explained by flowchart.

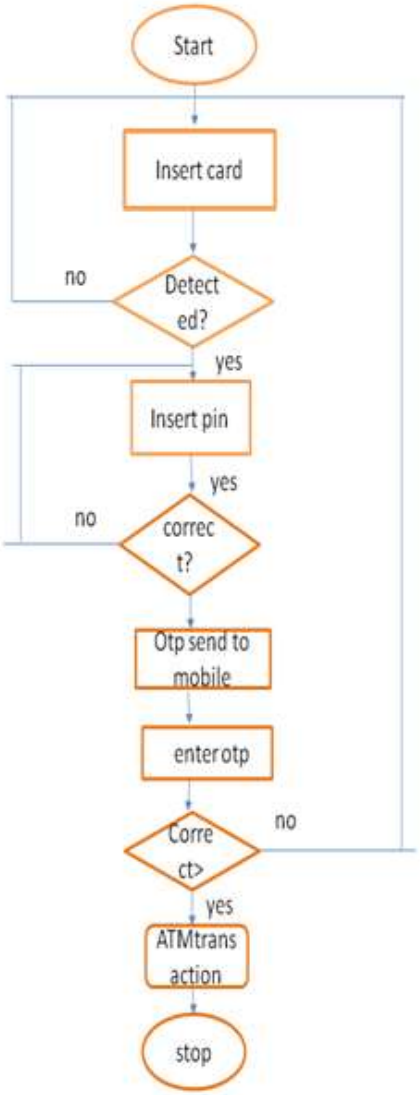

Fig.6.1 Basic Architecture of working model

VII. SYSTEM IMPLEMENTATION

In this proposed system, consist of 3 modules.

A. Admin Module

In Admin Login Module the admin can login to the application using their Username and password. Login is necessary in order to access the information. In Admin Module the admin can login to the application using their username and password. The admin will update the information related to user from time-to-time. Admin will give solutions to the queries raised by the registered students.

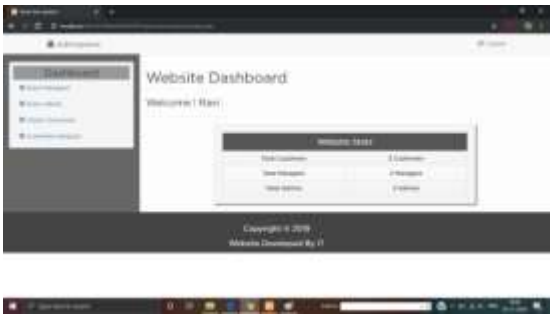

Fig.7.1 Admin Login Module

B. Manager Login

In Manager module, The manager will enter the details of the customers. The manager will register the details of the customers. The details such as customer name, customer username , Password, Mobile number ,ect. The Manager also check the transaction details of the customer . The manager will add new customers to the bank and register the customers .but The Admin only confirm the customer.

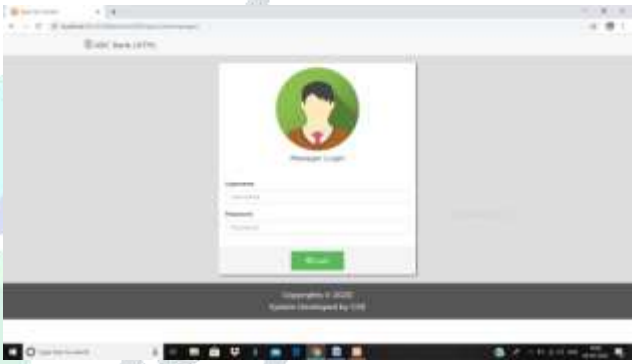

Fig.7.2 Manager Login Module

C. User Login

The user Login page contains the card no and password. If these two are correct the it will send the "OTP" to the register Mobile no. Then we will enter the OTP to the next field in the page and click on the verify button.

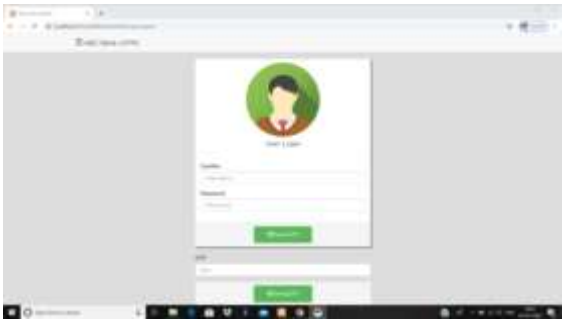

Fig. 7.3 User Login

VIII. CONCLUSION & FUTURE ENHANCEMENT

Usual ATM systems do not contain the OTP feature for money withdrawal. If an attacker manages to get ATM card and the pin number, he may easily use it to withdraw money frequently. Our project

proposes a secure ATM system using a card scanning system along with OTP system. The user may scan his card and login to the system. But after user is through with his authentication, he may view details but is asked to enter OTP as soon as he clicks money Withdrawal option. At this stage the system generates and sends a OTP to the user mobile phone. He now needs to enter the OTP in the system in order to withdraw money. Thus, our system provides a totally secure way to perform ATM transactions with two level security structures.

We also implement the graphical password authorization scheme along with the pattern recognition mechanism and RSA-ID identification, so that the security level will be further increased.

IX. REFERENCE

1. G.Jayandhi , S.Elphin SamueL, A.Govardhan, A.Vishnukumar, "Secure Pin Authentication as a Service for ATM", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 7, Issue 3, March 2018.
2. K. Laudon, and C.G Traver, E-Commerce Second Edition, Pearson Education Pvt. Ltd, Singapore, July 2005,237- 239.
3. Ojekudo Nathaniel1, Macarthy Osuo-Genseleke2, "A Comparative Study of PIN Based and Three-factor Based Authentication Technique for Improved ATM Security", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 05 Issue: 05 | May 2018.
4. A. Abdulrahman, A. Arwa, C. Xiuzhen, and B. Rongfang, A novel verification method for payment card systems, In Springer-Verlag London, May 2015,pp. 1145-1156.
5. L. Mun-Kyu, "Security Notions and Advanced Method for Human Shoulder-Surfing Resistant PIN Entry," In IEEE Transactions on Information Forensics and Security, August 2014,pp. 1556-6013.
6. A.D. Luca, E.V. Zezschwitz, L. Pichler, and H. Hussmann, H, "Using Fake Cursors to Secure on-screen Password Entry," in Proceedings of CHI, June 2013, pp. 2399–2402.
7. A.D. Luca, E.V. Zezschwitz, L. Pichler, and H. Hussmann, H, "Using Fake Cursors to Secure on-screen Password Entry," in Proceedings of CHI, June 2013, pp. 2399–2402.
8. T.P. Bhatla, V. Prabhu, and A. Dua, Understanding Credit Card Frauds," Cards Business Review, January 2003.
9. M. Roland, and J. Langer, "Cloning credit cards: A combined pre-play and downgrade attack on EMV contactless," In Proceedings of the 7th USENIX Workshop on Offensive Technologies, June 2013, pp. 324-348