IOP Conf. Series: Materials Science and Engineering **263** (2017) 042032 doi:10.1088/1757-899X/263/4/042032

Enhanced way of securing automated teller machine to track the misusers using secure monitor tracking analysis

Jayakumar Sadhasivam[1], Alamelu M[2], Radhika R[3], Ramya S[4], Dharani K[5] and Senthil Jayavel[6].
[1]School of Information Technology and Engineering, VIT University, Vellore-632014, Tamil Nadu, India.
[2,3,4,5,6] Kumaraguru College of Technology, Coimbatore, Tamil Nadu, India.

E-mail: jayakumars@vit.ac.in

Abstract Now a days the people's attraction towards Automated Teller Machine(ATM) has been increasing even in rural areas. As of now the security provided by all the bank is ATM pin number. Hackers know the way to easily identify the pin number and withdraw money if they haven stolen the ATM card. Also, the Automated Teller Machine is broken and the money is stolen. To overcome these disadvantages, we propose an approach "Automated Secure Tracking System" to secure and tracking the changes in ATM. In this approach, while creating the bank account, the bank should scan the iris known (a part or movement of our eye) and fingerprint of the customer. The scanning can be done with the position of the eye movements and fingerprints identified with the shortest measurements. When the card is swiped then ATM should request the pin, scan the iris and recognize the fingerprint and then allow the customer to withdraw money. If somebody tries to break the ATM an alert message is given to the nearby police station and the ATM shutter is automatically closed. This helps in avoiding the hackers who withdraw money by stealing the ATM card and also helps the government in identifying the criminals easily.

1. Introduction

An ATM card is any payment card issued by all the financial institutions that enables a customer to access ATM to perform transaction such as deposits, withdrawals, etc. Most of the people rely on ATM's than banks. They cannot imagine their day to day activities without ATM that was realized recently. But the security features of ATM still need improvement. The first level of security as of now is the pin number. But the rural people who do not have sufficient knowledge of ATM they will rely on somebody to withdraw the cash for the first time, even though they can manage it later. At that time, their pin number is leaked to the third person. There arises the lack of security. Therefore, the security features should be enhanced. ATM hackers are not afraid because they cannot be traced easily.

Moreover, ATM has its advantages and disadvantages. As the multiple location accessibility, the ATM service has been quickly accessed by the customers. The user has the option of changing the pin numbers whenever required. Frequently the money withdrawal and deposit become easier than the regular processing procedures followed in the bank. In parallel, if the user lost the pin number it is difficult to use the ATM machine. For the rural peoples should learn more training to use the ATM

machine. To focus on the overall advantages and disadvantages the quick accessible ATM machine should enhance with more security features for people's daily usage.

2. Related Work

Anushasalam et al,(2014) proposes multilevel security of ATM transactions gives an insight into how ATM works and how to enhance the security in ATM. In this concept, the author discuss by creating an android App and the user is supposed to login into the App with a password. Then the card should be swiped and the pin number is entered. The pin number and the password of the App is stored the data base and they are checked for symmetry. After verification, the users should enter the transaction id in the mobile application and all the process is carried out in the mobile phone itself. Only the cash is withdrawn in the ATM. There occurs a problem if both the pin number and password of the App is leaked, then it can be hacked easily. This method improves the alert to the customers to use the ATM cash transactions.

Jane NgoziOruh, (2014) designed a fingerprint systems in ATM. Even the finger print system fails, there is a chance of taking the finger prints also. So, the author proposed a three-factor authentication system which includes smart card, biometrics and the pin number. In this approach, the Authentication algorithm included as first level, Biometric system operation as the second level and user third factor authentication as the third level of security. Using this approach, the ATM system enhance its security with the three levels of execution.

3. Automated Secure Tracking System

In Figure.1.the proposed method "Automated secure Tracking System" process started the processing with the PIN number verification. Once the number verification has done card transaction has done with the two way of secure analysis method. Such as Finger print verification and eye ball detection. This method has been executed with the proposed algorithm "Secure Monitor Tracking Analysis". In this technique, the finger prints as well as the eye ball moving positions are detected.

4. Secure Monitor Tracking Analysis – Algorithm

(1). The user enters the four-digit PIN Number.
(2). PIN number executed for all types of verification.
(3). Customer selects the processing to any types of transactions. Such as withdrawal or deposit or balance enquiry.
(4). After the verification, the Bio metric has been recognized from the user with the eye ball movement.
(5). The eye ball movement been recognized for the straight view, left view and the right view.
    i. Straight view recorded for -> 90 Degree
    ii. Left view recorded for -> 180 Degree w.r.t 90 (straight view)
    iii. Right view recorded for -> 180 Degree w.r.t 90 (straight view)
(6). The three views are recorded and that matched with the record (bank) database. Such as the customer essential data verification of Aadhar card/Ration Card/ Passport/Voter Id.
(7). Once the finger print + eye ball detection + Customer essential Id verification matched the message have been sent to the customer mobile number.
(8). If any one of the data has not matched the process get stopped and it started from the beginning.

With the secure monitor analysis process the security has been enhanced with the three ways of verification. Three types of security have been elaborated with the finger print rectification, eye ball detection with three views and customer data verification. By the proposed method the Automated

Secure Tracking system only executes if it matches all these three conditions. The Eye ball view movement has monitored with the straight view, left view and right view. If the three views are recorded then the detection gets recorded in the iris system.

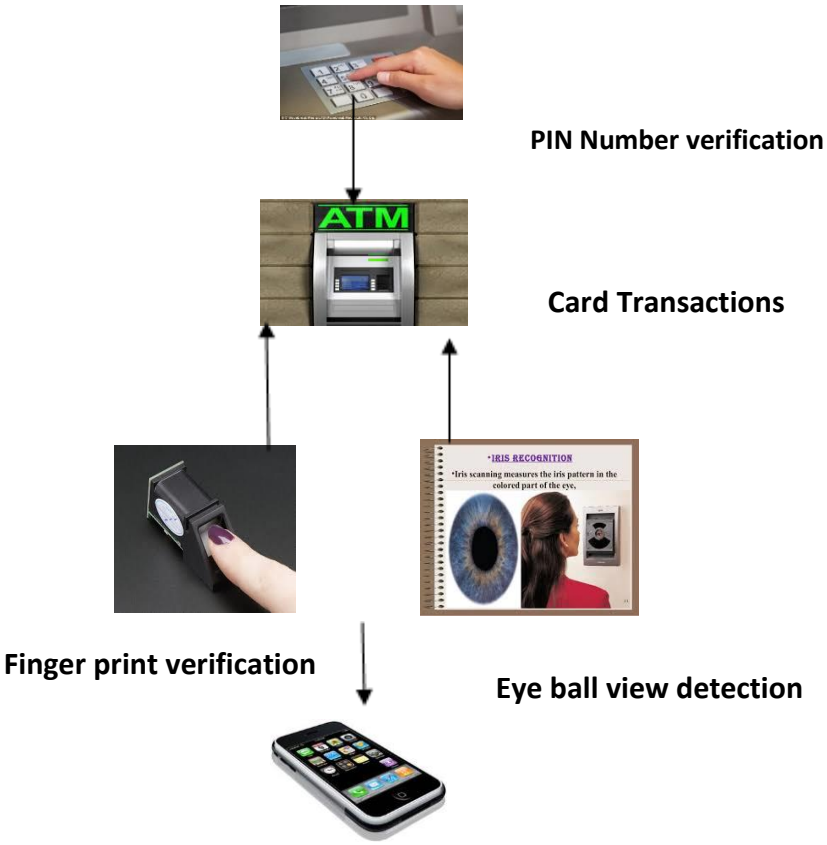

Figure.1. AUTOMATED SECURE TRACKING SYSTEM

The iris scanner scans the user's eye ball view movement. The recorded view signal is send to the Micro controller which activates the driver circuit and enables the transaction. If the iris does not match then the signal to the microcontroller will recognize that something went wrong and it will track the given iris in the bank database. In the meanwhile, if the matching has not been recognized the unmatched person photo has captured and send as the alert message to the cardholder. Other than the system improves its security with the Alert Notification. If somebody tries to break the ATM machine and try to take the money an Alert Notification is sent to the nearby police station and the door of the room is closed automatically.

5. Conclusion

The proposed Automated Secured Tracking system provides a three-way security in the form of finger print verification, Eye ball view detection and message alert notification for a ATM customer. The advantage of processing this proposed system will lead the customer to withdraw, deposit the amount in a secured way. The proposed system also leads the three-view eye ball detection to match with the customer database. This technique will prevent the unauthorized person to hack the PIN number and misuse of ATM card. In future, the work was enhanced with the agent based techniques for message alert notification using mobile applications.

6. References

[1] Salam A and Ali A 2014 Multi-Level Security for ATM Transaction 27–29
[2] Oruh J N 2014 Three-Factor Authentication for Automated Teller Machine System **4(6)** 160–176
[3] Cheng R G, Al-Taee F M, Chen J and Wei C H 2015 A Dynamic Resource Allocation Scheme for Group Paging in LTE-Advanced Networks *IEEE Internet Things J.* **2(5)** 427–434
[4] Chen Y *et al* 2014 A vision of IoT: Applications, challenges, and opportunities with China Perspective *IEEE Internet Things J.* **2(5)** 1
[5] Ujikawa H, Yamada R, Suzuki K I, Otaka A, Nishiyama H and Kato N 2016 Stand-Alone and Cooperative Deep Sleep for Battery-Driven Optical Network Unit *IEEE Internet Things J.* **3(4)** 494–502
[6] Lin S C and Chen K C 2016 Statistical QoS Control of Network Coded Multipath Routing in Large Cognitive Machine-to-Machine Networks *IEEE Internet Things J.* **3(4)** 619–627
[7] Sun Q *et al* 2016 A Comprehensive Review of Smart Energy Meters in Intelligent Energy Networks *IEEE Internet Things J.* **3(4)** 464–479
[8] Kermarrec A 2014 Online Appendix to : Personalizing Top-k Processing Online in a Peer-to-Peer **13(4)** 1–5
[9] Alhosban A, Hashmi K, Malik Z, Medjahed B and Benbernou S 2015 Bottom-up fault management in service-based systems *ACM Trans. Internet Technol.* **15(2)**
[10] Yao L, Sheng Q Z, Ngu A H H and Li X 2016 Things of Interest Recommendation by Leveraging Heterogeneous Relations in the Internet of Things *ACM Trans. Internet Technol.* **16(2)** 1–25