Prototype for Card-less Electronic Automated Teller Machine using Internet of Things

Marietta J, Chandra Mohan B, Hari Haran V

***Abstract:** Automated Teller Machine (ATM's) are devices used for the personal and business financial transactions or banking functions. It can be used without the help of the banking official. The ATM's have become popular among the public for their availability and the user friendliness. Nowadays ATMs are available in many locations such as college, supermarket, gas station, banking center, airport, work location, hotels, and entertainment establishment, having a consistent high volume of user traffic. The existing ATM machine uses the ATM cards for the user access to authenticate their account in order to use the services of the ATM. There are several problems which includes card expiring, cost of maintenance, accessing customer account by others, waiting time before the issuance of the new card, card damaging, card cloning, shoulder surfing attack, skimming attack, eavesdropping attack, guessing attack. This paper presents the prototype for the card-less electronic Automated Teller Machine without the use of the card. The proposed system uses the face recognizer using the HAAR algorithm. Using the help IoT the unauthorized users could be tracked and if there is any mismatch with the authorized users the mail and SMS could be send to the registered users.*

***Keywords:** ATM card, IoT, HAAR classifier, face recognition, biometric.*

I. INTRODUCTION

These days, saving money division is an essential part of a human regular day to day reality. Keeping money offices are generally utilized by individuals for their budgetary judiciousness exercises. Customized Automatic Teller Machine (ATM) is an electronic machine which is used for getting a financial balance adjust from wherever without the help of bank staff. The client can play out a couple of keeping cash practices like cash withdrawal, money exchange with the help of ATM. It is viewed the capacity of damages identified related to ATM is extended in this manner there is a need to give improves security to ATM machine. In the current ATM machine security to exchanges for distinguishing proof of approved client isn't accessible. Be that as it may, this is limited secure connections with ATM machine. Past works concerted on biometric strategy to give upgraded safety to ATM exchange while GSM technique is executed for similar reason though, some framework utilizes a blend of the two procedures. As of now, ATM security is given to the exchanges as it were. GSM based security will be provided for in which one-time Key (WEBPAGE REQUEST) is send will selected amount to exchange. The blend of GSM Furthermore RFID advancement may be moreover used which impacts the minimum with secure over recently RFID advancement. The innovation as disadvantage along these lines, biometric innovation is presented for ATM exchange. In biometric strategy unique mark and face acknowledgment framework are utilized for ATM exchange. Unique mark acknowledgment framework for ATM
Exchange is utilized in light of the fact that every client has one of a kind finger pattern. This skeleton provides for a greater amount secure return over GSM. Face affirmation methodology will be similarly used to security previously, which face may be recognized from 3 plans for authentication reason Likewise, security is upgraded and facial acknowledgment highlights. In this framework, current face picture coordinated with put away picture and subsequent to coordinating the pictures accurately, demand will be sent to registered number client need to enter the website page ask number for finishing exchange. There are numerous frameworks accessible for securing exchanges, however there is not any specific framework to protected ATM machine. So near is a need to implement a structure which screens Furthermore control the room and place where atm machines are set. This Anti-robbery framework guarantees safe condition for card holder's ideal from opening exchange to the end. It keeps dependent upon correspondence channels with every last one of appropriate national Also widespread security working get-togethers amassed on the area and expectation of wrongdoing, whichever particularly against ATMs, or in an indirect way against ATMs through violations executed at diverse terminals. Banks pass on more ATM's to two purposes: (I) with benefit is receptive should customers whenever, anywhere. (ii) Lessen their attempting out about passing on delegates on serve customers. Billions from claiming people would making use from claiming ATMs consistently for day-today term. So Investigations and inquiries regarding are setting off ahead should upgrade those security from claiming atm exchanges. Similarly, as those amount from claiming ATM related wrongdoings, for example, burglaries, breaking under ATMs, ATM unidentified way hacking need aid setting off ahead around, the advancement must make brought out for a particular wind objective to overcome this and the rationality must a chance to be moved ahead.

Revised Manuscript Received on October 30, 2019.

* Correspondence Author
Marietta J*, SCOPE, Vellore Institute of Technology, Vellore, India Email: jmarietta1@gmail.com.
Chandra Mohan B*, SCOPE, Vellore Institute of Technology, Vellore, India Email: dr.abc@outlook.com
Hari Haran V, SCOPE, Vellore Institute of Technology, Vellore, India Email: hariharan5894@gmail.com

Banks must a chance to be that's only the tip of the iceberg careful previously, securing ATM exchanges.

In this period, the current schema incorporates card peruses, electronic cushion, ATM PIN amount and feature Cameras. Present schema furnishes customers for an ATM card What's more its PIN number. These times a PIN numbers could be hacked, also might be separated adequately toward using atm looking at gadgets and Eventually Tom's perusing camcorders. Thus, with a specific end goal to beat every one of these challenges we have set up cutting edge, shrewd great ATM safety framework. Our future system of card-less ATM System comprises of PIC-18 Microcontrollers, IR, PIR, Open CV programming, HAAR calculation, Webcam to give more solid security to ATM exchanges.

II. LITERATURE SURVEY

In South America already, the finger print technology has been introduced and it has been embedded with the ATM machines in replacement to the PIN numbers. This prevents accessing the customer account by others. In India this technology embedding the finger print with the ATM is not implemented.

Currently Personal Identification Number (PIN) is used as the authentication technique in ATM. The PIN numbers could be easily hacked by the attackers. The 4-digit PIN could be hacked using the finger prints plated in the number box. The bar code of the card could be hacked by the attacker using the detector. So, the secure authentication techniques are required to overcome the problems.

Kumaresan et al. [1] proposed shuffled keypad in ATM to prevent the device attackers. In this method the shuffled numbers in the Liquid Crystal Display Keypad prevents the hackers from hacking the PIN number. Through the wireless medium the Bluetooth application is developed to use between the ATM and the user. The linear Feedback Shift Register is used to generate the random numbers.

Alhothaily et al. [2] proposed a method to prevent various security attacks such as multi-possession factor authentication with a distance bounding technique. This technique is suitable for the personal RFID devices which include smart watches, rings, necklace, smart phones.

Lee et al. [3] proposed a method where the regular keypad is colored at random where half is black and half is white.

De Luca et al. [4] proposed a method to hide the password entry in the on-screen keyboard. He also uses various cursors in the screen so that the attacker could be distracted, as fake cursor moves differently from the different cursors.

Guo et al. [5] introduced the technique for manipulating the magnetic stripe cards data. This can be used to prevent the data skimming.

Sujith et al. [6] the crimes and robbery in the ATM could be prevented by monitoring the motion features for different abnormal activities that happen in the ATM locations. The multiple object detection methods and various event detection techniques of computer vision could be used for tracking the abnormal activities that can be segmented from videos. Oko et al. [7] proved that the finger print technique for the authentication of the user may not allow the user to access his account if his hands are dirty from the natural environment. So, the authors proved that the technique is in efficient to be implemented in the ATM.

Few other techniques like the iris and retina as the identification technique. There is disadvantage that the users might not like the laser beamed into their eyes for every time the user needs to access ATM to withdraw money. Thus, this method is also considered as the inefficient authentication technique. For authenticating the user voice could be used as the biometric identification. But the drawback is that two users may have the same voice and the user can hack the other user's account with the voice.

These days, individual's quest for quick and advantageous lifestyle, quick and helpful administration of ATM is made for individuals to abstain from holding up in line at the bank for quite a while. So as to serve individuals helpfully, it is a need to screen the ATM hardware to ensure its typical operation, and manage the startling issues in time. In this manner, Cheng et al. [8] forms a cloud stage for caution benefit, does some alert investigation, which shows up at various circumstances in various areas of the ATM machine. This can give better support of ATM clients.

III. PROPOSED METHOD

Considering the entire drawbacks in various authentication techniques this paper aims at providing authentication using face recognition. In order to prevent the ATM from robbers and the attackers few ideas have been provided. Real-time monitoring system for the ATM has been developed with various sensors which includes accelerometer sensor, camera module, and face recognition based on the camera module is proposed.

Here we are using Raspberry Micro controller inside that controller more software are in built to find the face recognition for the person. Also, we are using the OPENCV advance image processing software to get more reliable result. This will help to find the authorized person to withdrawal the money. The block diagram shows IR & PIR sensors. IR sensor is used to detect the object in front of the door. Then PIR sensor is used to find the human detection in front of machine, once the machine detection done it will direct to login page then the webcam captures the object automatically and matches with our database images. In these process HARM Algorithm approach takes place to find out the authorized person then it allows to access the withdraw screen for transaction cycle.

the content as a separate text file. Complete all content and

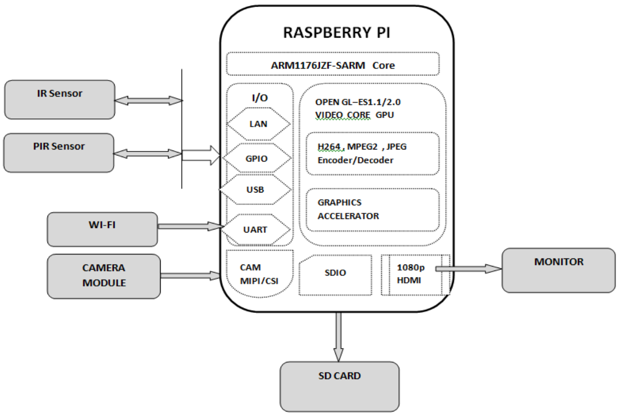

Fig 1. Proposed method

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

IV. RESULT & DISCUSSION

The motion detection is done using the PIR sensor and the IR sensor. If the motion is detected the open selection page is opened for the user authentication. The camera which is placed in front will take the picture automatically. The image which is stored is taken is then compared with the image which is stored in the database. We analyze the different percentage of the face recognition by giving different images. The authentication of the user to access the account in the ATM could be done using the HAAR classifier algorithm.

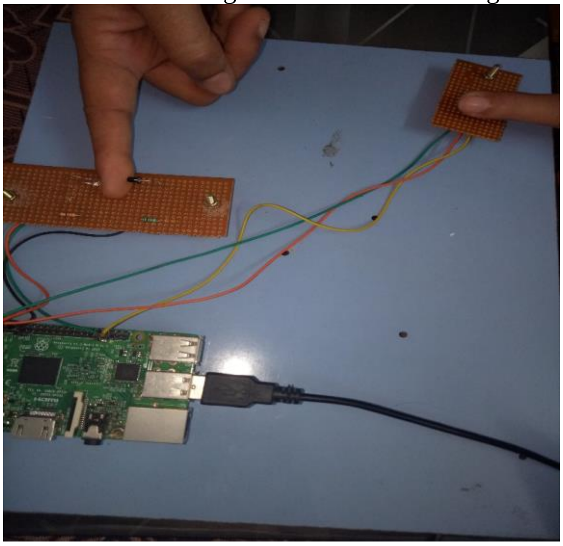

Fig. 2. IR sensor and PIR sensor used for tracking the motion of the object

The user will be authenticated if the image matches with the stored image. After the successful authentication of the user he will be allowed to withdraw the amount from the ATM machine. If the image does not match then the system considers the person as the attacker and an alert mail will be triggered to the user. If a unauthorized user try to access the account the mail will be triggered with the image of the hacker to the authorized user.

V. CONCLUSION

These days, a large portion of the ATM has been assaulted by the thefts. In this paper, a constant observing framework for ATM security in view of accelerometer sensor, camera module, and face acknowledgment in light of camera module is proposed. Along these lines the propose work gives a protected method for getting to an ATM by approved people utilizing face acknowledgment module. This additionally takes out that exists in the current frameworks by controlling the cameras. The proposed framework is financially savvy with the current manual strategies.

REFERENCES

1. Kumaresan, S., Kumar, G. D., & Radhika, S. (2015, March). Design of secured ATM by wireless password transfer and shuffling keypad. In *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)* (pp. 1-4). IEEE.
2. *Alhothaily, A., Alrawais, A., Cheng, X., & Bie, R. (2015). A novel verification method for payment card systems. Personal and Ubiquitous Computing, 19(7), 1145-1156.*
3. Lee, M. K. (2014). Security notions and advanced method for human shoulder-surfing resistant PIN-entry. *IEEE Transactions on Information Forensics and Security*, *9*(4), 695-708.
4. De Luca, A., Von Zezschwitz, E., Pichler, L., & Hussmann, H. (2013, April). Using fake cursors to secure on-screen password entry. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2399-2402). ACM.
5. Guo, H., & Jin, B. (2010, September). Forensic analysis of skimming devices for credit fraud detection. In *2010 2nd IEEE International Conference on Information and* Financial Engineering (pp. 542-546). IEEE.
6. Sujith, B. (2014). Crime detection and avoidance in ATM: a new framework. International Journal of Computer Science and Information Technologies, 5(5), 6068-6071.
7. Oko, S., & Oruh, J. (2012). Enhanced ATM security system using biometrics. *International Journal of Computer Science Issues (IJCSI)*, *9*(5), 352.
8. Cheng, Y., Shang, W., Zhu, L., & Zhang, D. (2016, June). Design and implementation of ATM alarm data analysis system. In *2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS)* (pp. 1-3). IEEE.

AUTHORS PROFILE

Mrs. Marietta Johnson received her Bachelor Degree in Computer Science and Engineering from Anna University in the year 2012 and Master of Technology from BITS Pilani, Rajasthan, India in the year 2015. She worked in the software industry (Cognizant Technology Solutions, Bangalore, India) for 3 years. She was Research Associate at VIT, Vellore, India from 2016 to June 2017. Currently she is a Research Scholar at VIT, Vellore, India. Her present research includes Internet of Things, network and machine learning

Dr. B. Chandra Mohan received his B.Tech Degree in Information Technology, Master degree in Computer Science and Engineering from Madras University and Anna University in the years 2003 and 2006 respectively. He completed his doctorate degree in the field of Heterogeneous Next Generation Network at Anna University in the year 2012. He worked both in industry and academics, in India and Abroad, about 14 years. Presently he is serving as Associate Professor in VIT University, Vellore, Tamilnadu, India. His experience includes as Teaching Faculty in Anna University Chennai, India; as a professor in VelTech Engineering College, Jaya Engineering College and Pallavan Engineering College, India. He has published a dozen of papers in International Conferences, Journals and Book series. His paper is awarded as top 25 most cited articles by Expert System with Applications, Elsevier. His research interest in Networks, Data Mining, Swarm Intelligence, IoT and Big Data. He is serving as Research Supervisor in VIT University, Anna University and AMET University

Hari Haran received his Bachelor Degree in Computer Science and Engineering from Anna University in the year 2016 and Master of Technology from Vellore Institute of Technology, Vellore, India in the year 2018. His present research includes Internet of Things.