AUTHORIZING SECURE ATM TRANSACTIONS USING FACE DETECTION AND TELEGRAM

S China Ramu[1], Raman Dugyala[2], Sugandha Singh[3*], Saima Bareen Mirza[4]

Abstract

Automated Teller Machines (ATMs) are utilized for all banking transactions in the modern world. Although ATM us- age is rising, more frauds are happening in general. My proposed work focuses on giving the cardholder reliable security to lessen those frauds. A Raspberry Pi processor with a RFID module and a GSM were combined to ensure security. The work is mainly focused on authorizing secure transactions by capturing the card user's image. The cardholder will receive the recorded image through SMS for authorization. The process will either be further approved or rejected based on the cardholder's authorization. If the cardholder gives their consent, the subsequent transaction happens. Once access has been granted, a OTP will be issued on the registered number of the cardholders, and the card user can withdraw only after inputting the OTP. If the user denies the authorization, the transaction will not proceed further. In addition to the above, my work also provides security, namely fire and smoke inside the place where ATM is located. The sensor detects any smoke or flame produced by any unusual activities or actions and alerts the security personnel via the buzzer.

Keywords: Raspberry pi ATM SMS GSM RFID

[1,2,4] Department of Computer Science and Engineering, Chaitanya Bharathi Institute of Technology, Hyderabad
[3*]Department of Artificial Intelligence and Machine Learning, Chaitanya Bharathi Institute of Technology, Hyderabad

***Corresponding Author:**Sugandha Singh
*Professor, AI&ML Department, Chaitanya Bharathi Institute of Technology, Hyderabad
Email: sugandha77.cse@gmail.com

DOI: 10.48047/ecb/2023.12.si10.0035

1. INTRODUCTION

Security and maintaining the integrity of all organizations have always been prioritized. Since the ATM's invention in the 20th century, many alterations have been made to it. We intended to improve security by integrating face recognition into the system with the help of machine learning. Our culture has altered as a result of the invention, installation, and widespread use of ATM machines, which are used to withdraw cash using debit and credit cards. The cardholder's password has been used in many unauthorized attempts to access the ATM, and cash withdrawals have been done without the cardholder's knowledge. [1] Both the cardholder and the bank are faced with a serious problem as a result. We start this endeavor to provide an ATM safety mechanism to solve these kinds of problems. ATMs are the main focus of physical security, which strives to create Access Control, Authentication, and Identification [2,3]. Access control is another type of information system security consideration that is used to confirm a person's identification so that only a verified person can access the system [4,5]. With the development of banking systematization, banking has transformed. On the one hand, it has freed us from having to wait in large lines to withdraw cash, but on the other hand, it has increased the likelihood of fraud [6,7]. According to reports, using an ATM is a quick, easy, and advantageous way to handle all of our banking demands [8,9]. ATM cards or debit cards authenticate the user after the cardholder's name, card number, pin, and expiration date have been confirmed. However, if the card is lost or the PIN is known to an unauthorized user. We need a high level of security, which is why adding RFID and OTP to present technology was anticipated. OTP has become popular utilizing Telegram for extremely secure confirmation and personal authentication. The research's main objective is to defend the ATM system and ATM card more effectively by using the tried-and-true, trouble-free techniques of OTP and RFID with Telegram-enabled facial recognition. The primary objectives of this study are as follows:

- To increase system security, a fire gas sensor will be employed to find unwanted disturbances and sound an alarm.
- To make it more flexible for individuals who are inexperienced with new technologies, we give a user-friendly system by altering the current system.

Only after the transaction has been completed or after the authorized user's account has been debited is unauthorized access revealed. This project is therefore focused on a method to prevent the threat that unauthorized users bring to ATM security by granting access to the user only after the user's identity has been confirmed using a camera placed on the ATM machine. The ATM will use facial detection and face recognition to compare the person trying to withdraw money from it to the image of the account holder that is kept on file by the bank. The system will permit the transaction to proceed if the image matches the user; else, the image will be sent to the account holder's mobile number for user verification.

I.Literature Review

The author's main objective is to defend the ATM system and ATM card more effectively by using the tried-and-true, trouble-free techniques of OTP and RFID with Telegram-enabled facial recognition. The following are the study's main goals:

- To improve system security, a fire gas sensor will be used to look for unauthorized activity and raise an alarm.
- By modifying the current system, we provide a user-friendly system that is more adaptable for people who are unfamiliar with new technology.

The major goal of the project is to improve ATM system and ATM card security by combining the tried-and-true, trouble-free OTP and RFID technologies with Telegram-enabled facial recognition. The following are the study's main goals:

- A fire gas sensor will be utilized to monitor for unauthorized activities and sound an alarm to increase system security.
- By modifying the current system, we provide a user-friendly system that is more adaptable for people who are unfamiliar with new technology.

The card cannot be used to access the account alone because the transaction additionally needs a human. Face recognition is accomplished using the Eigen face-based method. On the other hand, the Eigen face-based technique may occasionally be misled by the use of counterfeit masks or images of account holders. Due to the use of a card and PIN in the current ATM paradigm, there have been more assaults including stolen cards, statically generated PINs, card duplication, and various other risks. The facial recognition feature stops people from using stolen or fake cards to access accounts. Because the transaction also needs a person, the card cannot be used to access the account alone. The Eigen face-based method is used for face recognition. [10-14]

The Eigen face-based method has the drawback

that it can occasionally be tricked by utilizing fake masks or photos of the account holder. Financial institutions profit greatly from ATM transactions, and cards are heavily advertised. Since they attract more non-bank customers who have to pay service fees, off-premises ATMs are frequently more profitable for banks. Unfortunately, customers who use outdoor ATMs are more vulnerable to theft. Statistics on ATM attacks are gathered from regular bank inspections conducted by financial organizations. Contrary to popular belief, there was one ATM crime (including theft) for every 3.5 million operations.

There are a variety of ways to deceive an ATM, including Card Theft: Card trapping devices, which are tiny mechanical instruments inserted within the reader's stomach and coated in an opaque, transparent covering, have been employed by thieves in a number of ways to steal real playing cards. So that the customer's card cannot be retrieved after the transaction is finished, inquiries have hooks connected to them. When the user of the ATM machine expresses concern about the stolen card, the criminal, who is typically next to the ATM, will offer assistance and advise that the user enter the PIN again so that they may study the data input and memories the PIN. The criminal will then use a probe (a fishing device) to extract the card after the customer has left the vicinity, thinking the ATM has stolen their card. Once the thief has seen the customer's PIN and the card in their possession, they can quickly take money from the account of the unwary user.

This paper's major goal is to safeguard ATM transactions by reducing actions or activities that take place at ATMs. In order to reduce it, the Raspberry Pi is integrated with the Linux operating system and a low-cost, independent Embedded Web Server (EWS) relying on an ARM11 CPU. In order to prevent ATM thefts, real-time research is being done. [15]

II. Proposed Work

The Raspberry Pi has been connected to many modules, including GSM, RFID, DC motors, cameras, and buzzers. The sensors are interfaced with Node MCU as illustrated in Fig. 1. The modules are described as follows

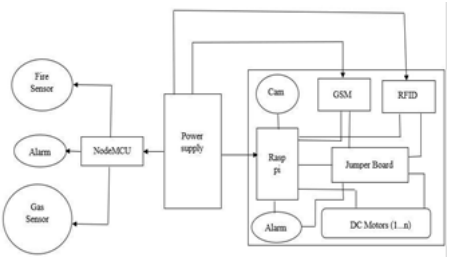

Fig. 1: System architecture of ATM

- **Raspberry Pi:** It is an ARM cortex-based board, which a single-board computer is working at a low charge. Itcan perform different functions at a time with processing speed and memory, performing like a normal PC, and hence named a Minicomputer. Raspberry Pi can perform a full range of ARM Linux distributions as well as Microsoft Windows as it has an ARMv7 processor (Fig. 2). We are using this ARM processor everywhere in our daily lives like mobile phones, computers, laptops, iPods,etc. Pi is an amazing tool for IoT. In the market, we have many dissimilar types of Raspberry Pi boards available. The most popular is Raspberry Pi 2 Model B. Raspberry Pi 3 Model B is also been launched, which is resembling RPi 2 but has some modernized features like Bluetooth connectivity, a more powerful CPU, onboard Wi-fi, etc.

Fig. 2: Raspberry Pi

- **RFID:** A tracking device called RFID is utilized to identify and confirm the legitimate tags that are attached to any labels, living organisms, or objects (Fig. 3). These devices use radio waves to identify objects and people. A tag or card, which is scanned by an RFID reader and processed in accordance with the needs of the application, is the fundamental means through which an RFID system facilitates data transfer.

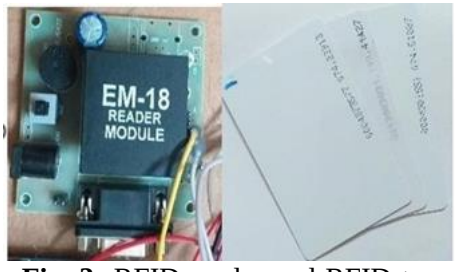

Fig. 3: RFID reader and RFID tag

- **Pi camera:** Here the camera has an image sensor quality and an inbuilt sensitive microphone. Image resolution is fitted to 25 megapixels and the focus range is 4cm to infinity.
- **GSM module:** To generate a connection between the computer and a GSM system, GSM/GPRS module isused (Fig. 4). It is a type of wireless MODEM device that is used for communication. GSM, like mobile phones, requires a Subscriber Identity Module (SIM) card to initiate a network connection. In addition, their International Mobile Equipment Identity (IMEI) number is required for identification.
- **ESP8266 Node MCU & Sensors:** The Node Micro-Controller Unit (Node MCU) is a free open-source software & hardware environment that is assembled arounda low-cost SoC named ESP8266. ESP8266 can not only connect to Wi-Fi and establish interactions with the internet, but it can also build a network of its own sothat other devices can connect directly to it.

Fig. 4: GSM Module

Making ESP8266 is more flexible. Fire sensors can detect flameor wavelength of a light source within the range of 760nm to 1100nm and with a distance of 80cm. Gas sensors have a high sensitivity and fast response. It can detect gas concentrations anywhere from 200 to 10000ppm.

IV. Working Process

- Essentially starting off by communicating with an RFID module. An RFID Module is made up of an RFID Tag, Card, and RFID Reader. A 12-digit character code can be found on the coil of an RFID card. The card is serially read by an RFID reader to identify whether or not it is legitimate when the card is brought close to the reader. A programmer then transmits the data to the Raspberry Pi.
- The Raspberry Pi is also connected to the GSM module, Camera, DC Motors, and NodeMCU with the aid of Python code.
- Assembling all the necessary code on a Raspberry Pi to launch the model's operation.
- The associated user's face is photographed and sent to the cardholder's Telegram ID when the RFID Card is recognized as valid.
- The cardholder will get given a picture of the user and be asked whether or not to grant access.
- An OTP will be produced through GSM and delivered to the relevant cardholder's registered number if the cardholder grants access.
- After entering the OTP, the appropriate user must then enter the amount of cash to be transacted; if the cardholder refuses to grant access, a buzzer alarm will sound.
- Fire/gas sensors also interface with Node MCU; as a result, an alarm is triggered whenever an accident occurs in an ATM.

V. Results

This work is mainly focused on securing ATM transactionsis performed and the respective results are as follows, This is the complete hardware kit that is used in this research work (Fig. 5).

Fig. 5: Test-bed environment

Fig. 6 shows the initial step which will verify whether the card is valid or not using RFID Reader.

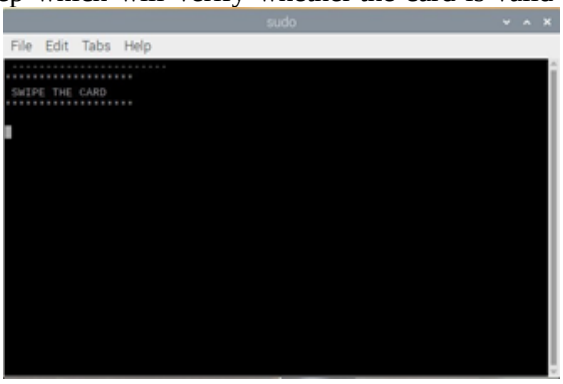

Fig. 6: Initial step

The card's detection is displayed in a window similar to that in Fig. 7 and alternately sends the cardholder's image for permission. The transaction will proceed by generating OTP as illustrated in Fig. 8 if the user is authorizing the card.

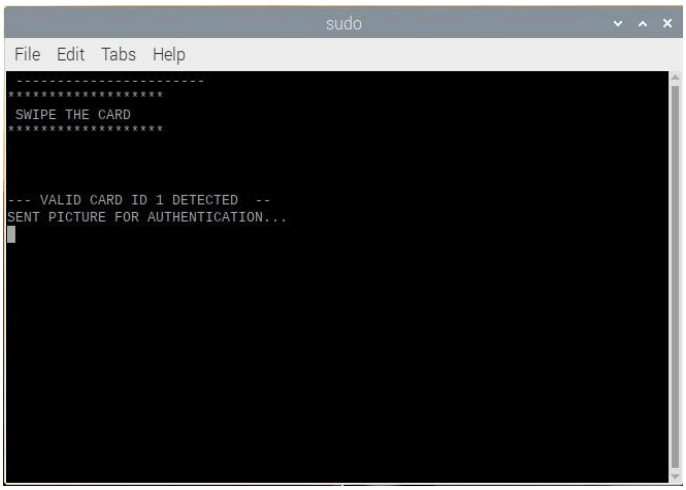

Fig. 7: Picture sent for authentication

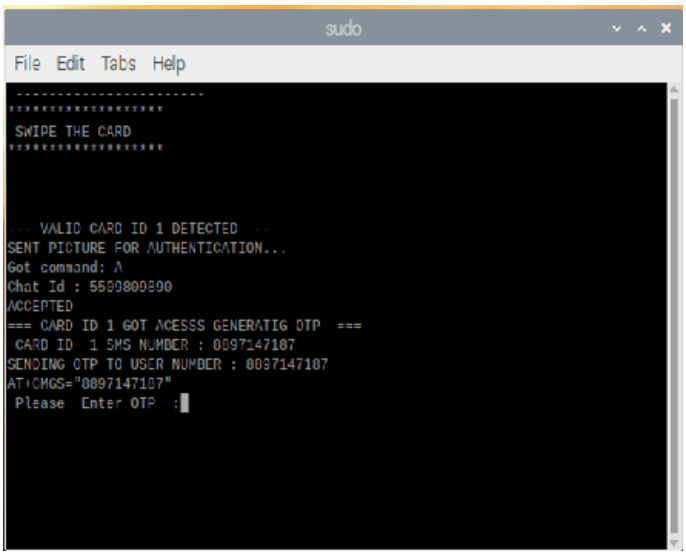

Fig. 8: Picture accepted

The OTP is received as an SMS on the registered number of the cardholder, as shown in Fig. 9. It will check to see if the OTP entered is accurate or not. If so, Fig. 10 will appear, instructing you to input the amount you wish to trade. As indicated in Fig. 11, the system will prompt you after entering the amount to proceed with the transaction in which currency denomination.

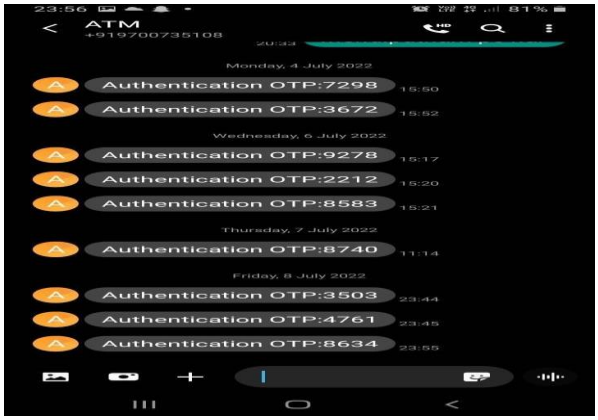

Fig. 9: OTP received on the registered number

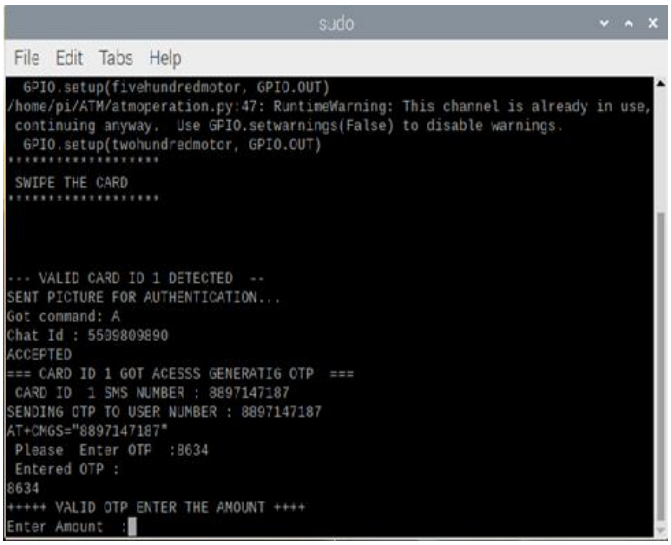

Fig. 10: Valid OTP entered

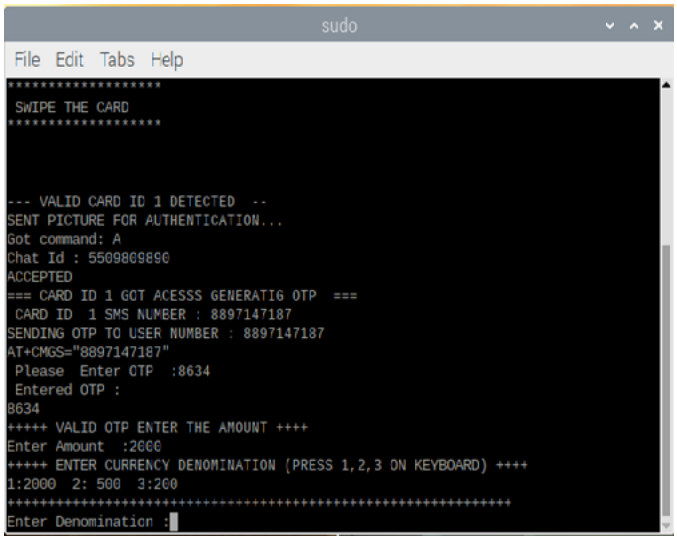

Fig. 11: Entering currency denomination

Finally the transaction in which the carduser wanted to proceed with the cardholder's authorization is successful.

Working on fire & gas sensors

Here, in Fig. 12, the fire sensor detects the flame within the range of 760nm-1100nm from the light source. As soon as the sensor senses the flame, the buzzer starts beeping to alert the corresponding.

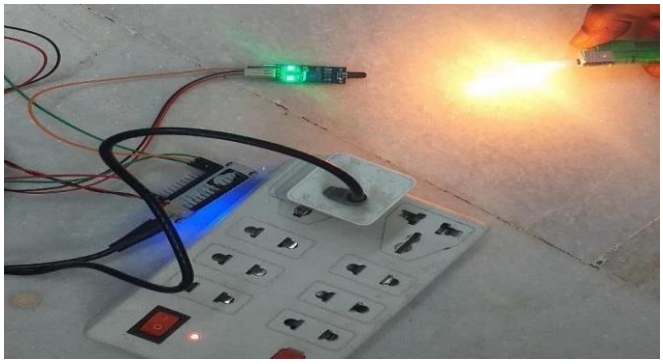

Fig. 12: Testing of fire sensor

As shown in Fig. 13, the Gas sensor is tested by keeping the concentration from 200 (0.02%) to 10000 (1%) ppm.

Fig. 13: Testing of gas sensor

VI. Conclusion

Since everyone frequently uses an ATM for banking activities, there is a chance that the frequency of ATM scams may rise. In order to reduce the amount of frauds, the suggested work improves security by validating the card user's image in addition to the OTP. Therefore, depending on the cardholder's judgement provides total security. Additionally, sensors that detect smoke and fires will be used to secure the area around the ATM.

VII. Future Scope

By improving the following characteristics, the implemented project's future scope can be expanded:

- A GPS module can be fitted to pinpoint the exact location of the ATM given that there are many ATM centers in one area.
- The Telegram app may be made more secure to prevent hacker access.
- Gas chambers and vibration sensors may also be added into the ATM machine.

References

1. R, Kavitha & Kumar, Logesh & M, Chandrasekar, "Smart ATM Access and Security System using RFID and GSM Technology" International Journal of Scientific Research and Education, 2016 Doi: 10.18535/ijsre/v4i06.13.
2. Sugandha Singh, Navin Rajpal, Ashok Sharma, Ritu Pahwa, "Policy based decentralized group key security for Mobile Adhoc Networks", International Journal of Computer Science Issues, Vol 7, Issue 3, Pp 45-49, 2010, ISSN 1694-0784
3. G Udaya Sree M. Vinusha, "Real Time SMS-Based Hashing Scheme for Securing Financial Transactions on ATM Terminal", International Journal of Scientific Engineering and TR, Vol.02, Issue.12, Pp:1223-1227, September-2019.
4. Neha Gulia, Sugandha Singh, Luxmi Sapra, "A Study on different classification model on Knowledge Discovery", International Journal of computer science and mobile computing, Vol 4, Issue 6, Pp 241-248, 2015, ISSN 2320-088X
5. M. R. Dineshkumar, M.S. Geethanjali,"Protected Cash Withdrawal in ATM Using Mobile Phone", International Journal of Engineering and Computer Science, Volume 2 Issue 4 April 2017 Page No. 1346-1350, ISSN: 2319- 7242
6. Singh, S., Rajpal, N. & Sharma, A. Address allocation for MANET merge and partition using cluster based routing. *SpringerPlus* **3**, 605 (2014) https://doi.org/10.1186/2193-1801-3-605
7. Nara Ida Joslin and B. Vamsi Krishna, "Secured ATM Card Accessing System Using RFID", International Journal of Computational Science, Mathematics and Engineering, Volume-2, Issue- 11, Pp 16-18, November 2015. doi: 10.18645/IJCSME.211.005
8. Sri Vasu, Subash, Sharmila Rani, Udhayakumar, "ATM Security using Machine Learning techniques in IOT", International Journal of Advance Research, Ideas and Innovations in Technology, Volume 5, Issue 2, pp. 150-153, 2019
9. Gade Swetha1, M. Santhosh Kumar, "Secured ATM Transaction System Using Enbedded Systems", International Journal of Scientific Engineering and Technology Research, Volume 5, PP 7381-7384, April 2014.
10. Murugesan M, Santhosh M, Sasi Kumar T, Sasiwarman M, Valanarasu I, "Securing ATM transactions using Face Recognition, International Journal of Advance Trends in Computer Scienec and Engineering, Pp.1295-1299, 2020 , ISSN 2278 – 3091 Doi:10.30534/ijatcse/2020/59922020
11. Kopparapu, Srivatsa & Madamshetti, Yashwanth & A.Parvathy, "RFID & Mobile Fusion for Authenticated ATM Transaction" International Journal of Computer Applications. Vol 3. Doi: 10.5120/731-1025.
12. E.Derman, Y.K.Gecici and A.A.Salah, "Short

Term Face Recognition for Automatic Teller Machine (ATM) Users", in International Conference on Electronics, Computer and Computation, Pp.111-114, 2013. Doi: 10.21172/1.841.20

13. Mr. S. Ramana, S. China Ramu, N. Bhaskar, M. V. Ramana Murthy, "A TwoLevel Authentication Protocol for Secure M-Commerce Transac- tions using Encrypted OTP", International Journal of Mechanical Engineering, Pp 3836-3841, Volume-7, March-2022. ISSN: 0974-5823
14. Shubhra Jain, "ATM Frauds-Detection & Prevention", International Journal of Advances in Electronics and Computer Sciences Volume 4, Issue 10, Pp 82-89, October 2017. Doi: IJAECS-IRAJ-DOIONLINE-9551
15. S. Ramana, S. China Ramu, N. Bhaskar, M. V. Ramana Murthy, C. R. K. Reddy, "A Three-Level Gateway protocol for secure M-Commerce Transactions using encrypted OTP", International Conference on Applied Artificial Intelligence and Computing, Pp 1408-1416, 2022. Doi: 10.1109/ ICAAI C539 29.2022.9792908