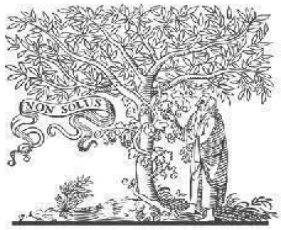
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

IJIEMR Transactions, online available on 12th Dec 2024. Link

https://ijiemr.org/downloads.php?vol=Volume-13&issue= Issue12

DOI:10.48047/IJIEMR/V13/ISSUE12/07

Title: "ATM SECURITY WITH RFID AND OTP"

Volume 13, ISSUE 12, Pages: 69- 75

Paper Authors
S. Nagajyothi, Ravu Sanjana, Soorarapu Hanvitha, Vittam VedhaSri

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper as Per UGC Guidelines We Are Providing A ElectronicBar code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

ATM SECURITY WITH RFID AND OTP

S. Nagajyothi[1] Ravu Sanjana[2], Soorarapu Hanvitha[3], Vittam VedhaSri[4]
[1,2,3,4] Department of ECE, CMR Institute of Technology, Medchal, Hyderabad, Telangana, India.
hanvithasoorarapu@gmail.com

Abstract- The need for security has increased in the recent times due to the high level of technology we use today. The most frauds performed, are financial frauds which cause loss to many individuals or organizations worldwide. ATM (Automatic-Teller-machine) It enables a bank account holder to perform transactions i.e. specially cash withdrawal in a public space without the need of any authorized bank person. But this causes a threat to the safety of the account holder as his/her card or bank account details can be skimmed easily by the intruder which creates loopholes in the security system & these loopholes are further explored by the attacker or intruder to perform unethical actions on the users bank account. So, to overcome this we have come-up with the concept of 2-way authentication which provides or creates a 2nd layer of security to the existing system & making it difficult for any types of malicious activity.

Keywords: One time password (OTP), Automatic Teller Machine(ATM), Personal identification number(PIN).

I. Introduction

To improve the security in the current ATM system we have come up with a system which ensure 2 level authentication and in turn it will make the Atm transactions more safe and secure. In this paper the proposed system ensures 2 way authentication in which the first level is the static PIN assigned to a particular card and the second level of authentication is the OTP which is sent to the user on his/her registered mobile number when intended to do a withdrawal transaction. The OTP is dynamic in nature and it is also time-bounded hence making it safe and secure to transact without any major changes to the User Experience as well as physical ATM machine. The security domain interest us because due to the technology we use today, there are many financial frauds taking place at a huge rate. Technology has mode our works easier & faster but with its drawbacks. ATM security is a major problem faced worldwide. Many People assume banks more risky than keeping the money at home or residence as banks are more likely to be robbed or hijacked. Here we saw the security domain to be to interest & worth working on. Recently there is a rise in ATM fraud cases like Card Skimming, Pin tapping, etc. Most of the attacks are performed successfully because the PIN we use to perform transactions is static & can be traced easily by the intruder. Hence we came-up with the concept of OTP (One-time- password) which will help us provide 2-way authentication.

ATM security has evolved significantly over the years to combat the growing threats of fraud and unauthorized access. One of the most innovative advancements in enhancing ATM security is the integration of RFID (Radio Frequency Identification) technology combined with OTP (One-Time

Password) authentication. This dual-layer security approach aims to provide a more secure and convenient method for cardholders to access their accounts while reducing the risk of unauthorized transactions. However, the inclusion of OTP in this system ensures that physical card access alone is not enough for transaction approval. After the user taps the RFID-enabled card, the ATM generates a unique OTP, sent to the user's registered mobile device or app. This OTP, which is valid for a limited time, must be entered at the ATM to authenticate and complete the transaction. By requiring both the card and the OTP, this system creates a robust two-factor authentication (2FA) process that significantly reduces the likelihood of fraud. Incorporating RFID with OTP enhances ATM security by combining the convenience of contactless technology with the security of a dynamic password, ensuring that only authorized users can perform transactions. This multi-layered security approach provides a stronger defense against unauthorized access, skimming devices, and other forms of cybercrime, making it a critical step toward securing financial transactions in the modern banking landscape.

II. Literature review

In this paper, we propose to add more security to the current ATM Systems. By using Biometric Authentication and GSM technology, we can overcome many of the flaws introduced by our current ATM system such as shoulder surfing, use of skimming device, etc. In our proposed system, Bankers will collect the customer's as well as respective nominee's fingerprint and mobile number at the time of opening the account [1]. The primary step is to verify currently provided fingerprint with the fingerprint which is registered in the Bank's database at the time of account opening. If the two fingerprints get matched, then a message will be delivered immediately to the user's mobile number which is the random 10 digit pin number called as One Time Password (OTP). This OTP can be used only once, thus this avoids various problems associated with the present system [2]. For every transaction, new OTP will be sent to account holder's mobile number, thus there will not be fixed PIN number for every transaction. Thus, PIN number will vary during each transaction assuring security. Rapid development of banking technology has changed the way banking activities are dealt with. One banking technology that has impacted positively and negatively to banking activities and transactions is the advent of automated teller machine (ATM). It is a computerized machine designed to dispense cash to bank customers without need of human interaction [3]. Today the ATM users are increasing in numbers. hey use the ATM cards for banking transactions like balance enquiry, mini statement, withdrawal, etc. The ATM machine has card Reader and keys as input devices and display screen, cash dispenser, receipt printer, speaker as output devices [4]. ATMs are connected to a host processor, which is a common gateway through which various ATM networks become available to users. Various banks, independent service providers owned this host processor. Account information of user is stored on the magnetic strip present at the back side of the ATM card. When we enter the card in the card reader, the card reader captures the account information and the information is used for the transaction purpose. And we have to insert the pin by keys.The password is the only identity so anyone can access the account when they have the card and correct password [5]. Once the card

and is stolen by the culprit and if he/she comes to know the password by any means then the culprit can take more money from the account in the shortest period, it may bring huge financial losses to the users. In the recent days, there have been many such ATM fraud cases.

Due to some of the flaws in our present ATM system such as use of static pin and ATM card, its users face many kinds of problem and there have been many issues associated with the present system. To overcome the problems associated with the present ATM System, in our project we are using biometric features [6]. Biometrics technologies are a secure means of authentication because biometrics data are unique, cannot be shared, cannot be copied and cannot be lost. Physical characteristics include fingerprint, hand or palm geometry, retina, iris and face while popular behavioral characteristics are signature and voice [7].

In this paper the ATM maintenance has be done with the help of various sensors. Sensors like smoke sensor, PIR sensor, Accelerometer, light sensor and temperature sensors act as an input devices and the relay circuit act as an output device which help to ON and OFF the external devices. Here the Raspberry Pi Microprocessor controls all the input and out devices [8]. All the values from the sensor are sent to the maintenance unit with the help of IOT server. Here we also add RFID tag and a USB Camera for verification and security purpose. The RFID is used to read the ATM card and once the card is read the USB Camera will scan the iris of the user for verification. The values from the sensors and RFID are continuously monitor by the maintenance team and if there is any change in any of those sensors, the maintenance unit can notice immediately with the help of IOT [9]. This system is much easier and reliable system compare to all the other existing system. The Internet of Things (IoT) is that the network of physical objects or "things" embedded with electronics, software, sensors, and network property, that permits these objects to gather and exchange information [10]. IoT permits objects to be detected and controlled remotely across existing network infrastructure, making opportunities for additional direct integration between the physical world and computer-based systems, and leading to improved efficiency, accuracy and economic profit. "Things," (ATMs) were 1st introduced in 1939. Nowadays, concerning three million units area unit put in worldwide. Because the variety of ATM units increase, the machines area unit susceptible to hacker attacks, fraud, robberies and security breaches. Within the past, the ATM machines main purpose was to deliver cash of bank notes and to debit a corresponding checking account. However, ATM machines have become additional difficult, and that they serve varied functions, so changing into a high priority target to robbers and hackers. Trendy ATM machines are enforced with highsecurity protection measures. They work beneath advanced systems and networks to perform transactions. robbers threaten bank patrons with a weapon to loot their withdrawn cash or account.

III. System Model

Modern ATMs are implemented with high-security protection measures. They work under complex systems and networks to perform transactions. The data processed by ATMs are usually

encrypted, but hackers can employ discreet hacking devices to hack accounts and withdraw the account's balance.

This helps to overcome the problem of complexity and provides easiest way to secure the ATM transaction. Whenever person enters account number onto the ATM machine, the system requires PIN to authenticate the user. If the PIN number gets verified, the OTP is generated and sent to user's mobile number. The transaction will succeed only if the user enters valid OTP, otherwise transaction will fail. Again the user will repeat the above steps until valid OTP was entered. If the OTP entered is wrong more than a particular limit the card will be blocked.

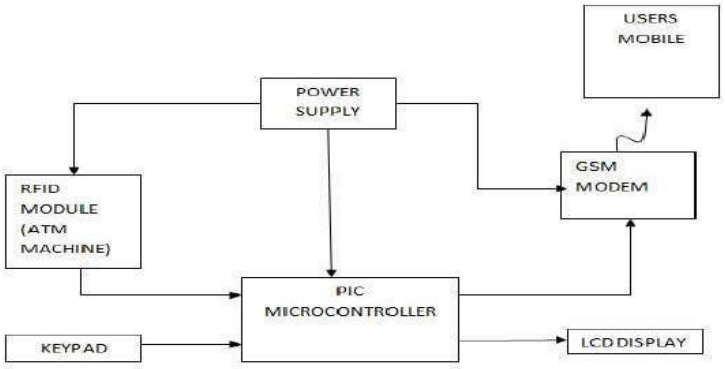


Fig 1: Block diagram of ATM Security with RFID and OTP

One-Time Passwords (OTPs) for ATM security, when combined with RFID (Radio Frequency Identification) technology, enhance the protection of transactions and user accounts. Here's how the combination of OTPs and RFID improves security:

A. Two-Factor Authentication (2FA):

OTPs add an extra layer of security to the traditional ATM PIN. In this setup, the user's ATM card may be equipped with an RFID chip, and the user must provide a one-time password (OTP) generated either by a mobile phone or a separate security token. This way, even if someone intercepts or clones the RFID card, they cannot access the account without the OTP.

B. Protection Against Skimming:

RFID-enabled ATM cards are susceptible to unauthorized scanning or "skimming," where attackers use devices to wirelessly read card information. With OTPs, even if an attacker obtains the RFID data, they cannot perform transactions without the OTP, which is valid only for a short period.

C. Enhanced Security at Contactless ATMs:

Some ATMs equipped with RFID technology allow for contactless transactions, where users don't need to insert their card physically. OTPs add an extra layer of verification for such transactions, minimizing the risk of unauthorized use.

1. **User Interaction:** The cardholder inserts their ATM card into the machine and enters their PIN as usual.
2. **OTP Generation:** After the correct PIN is entered, the system generates a unique OTP. This OTP can be sent via different channels: SMS to the registered mobile number or Email .Dedicated mobile banking app or token generator.
3. **OTP Verification:** The cardholder receives the OTP and enters it on the ATM keypad to confirm the transaction.
4. **Transaction Authorization:** Once the ATM verifies the OTP against the one generated by the bank's server, it proceeds with the requested transaction (withdrawal, balance inquiry, etc.).

IV. Result

In the paper, the objective of developing ATM security using RFID and OTP has been achieved. Thus, by using this project the security of ATM is achieved. Whenever a person tries to hack the ATM container at that time OTP is generated to our mobile and send the message to microcontroller. Modern ATMs are implemented with high-security protection measures. They work under complex systems and networks to perform transactions. The data processed by ATMs are usually encrypted, but hackers can employ discreet hacking devices to hack accounts and withdraw the account's balance.

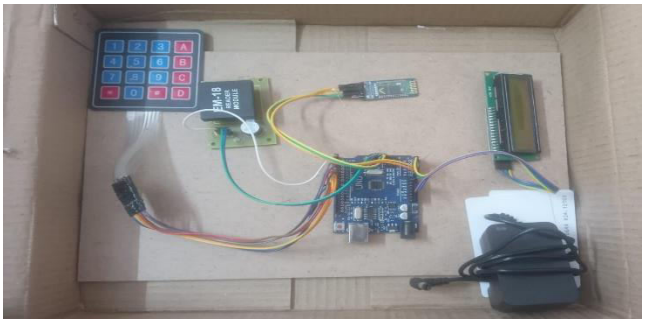


Fig 2: Kit and the process of ATM Security with RFID and OTP

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

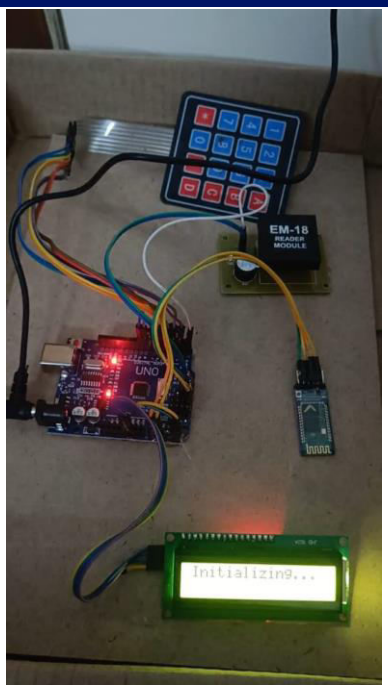


Fig 2.1(Initialization)

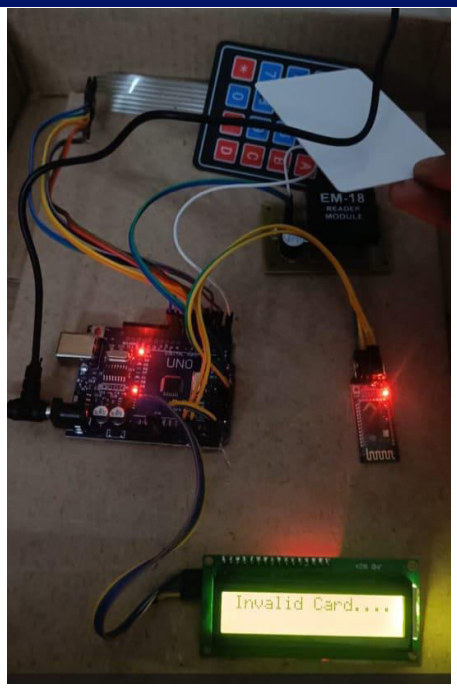


Fig 2.2 (Invalid Card..)

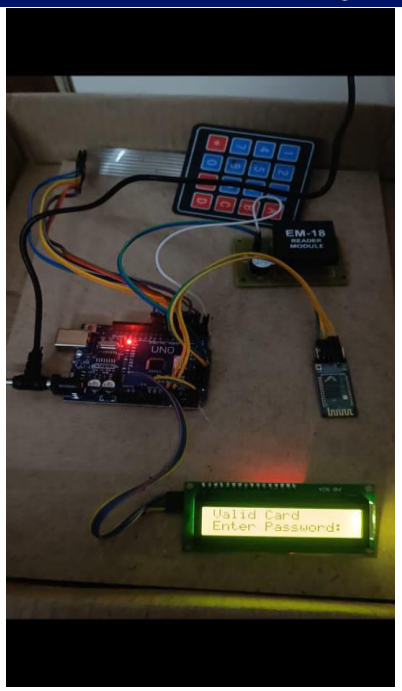


Fig 2.3 (Valid Card -Enter Password)

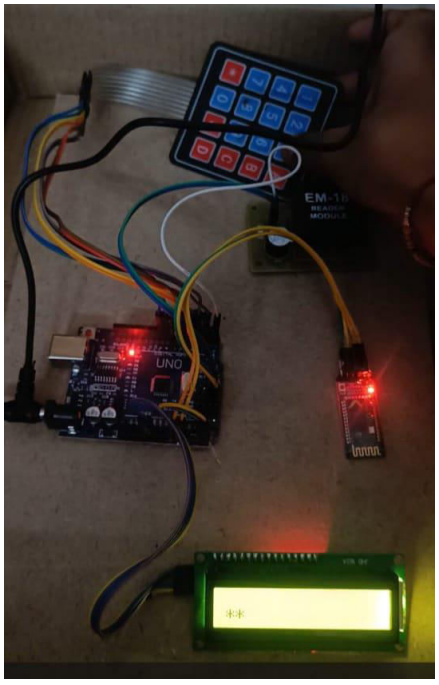


Fig 2.4 (enter pin -****)

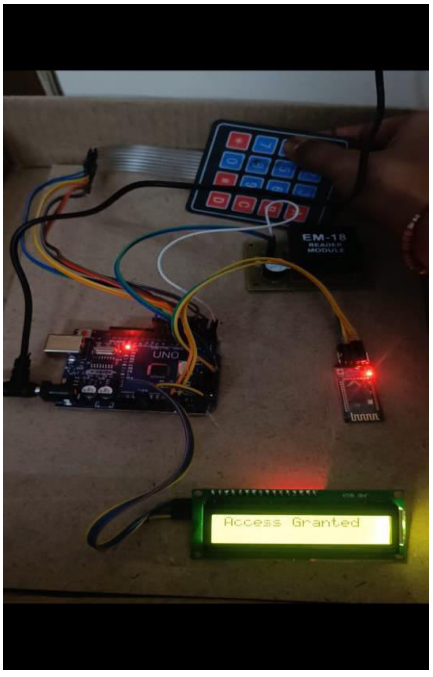


Fig 2.5 (Access Granted)

V. Conclusion

In this work, we conclude that ATM security is a major problem in banking system. Now a day's security system used in ATMs is completely based on PIN security system which is vulnerable. Banks provide four digits PIN to the user which can be changed later by the user. After first use, user usually changes the password and keeps password quite guessable. This is the main drawback of this PIN type ATM system. When ATM card is lost or stolen it is required to close the ATM card by contacting the bank immediately. The paper indicates the strong authentication of ATM card with the help of One Time Password (OTP) on mobile device.

REFERENCES

1. K. Radhakrishna, D. Satyaraj, H. Kantari, V. Srividhya, R. Tharun and S. Srinivasan, "Neural Touch for Enhanced Wearable Haptics with Recurrent Neural Network and IoT-Enabled Tactile Experiences," 2024 3rd International Conference for Innovation in Technology (INOCON), Bangalore, India, 2024, pp. 1-6,
2. Karne, R. K., & Sreeja, T. K. (2023, November). Cluster based vanet communication for reliable data transmission. In AIP Conference Proceedings (Vol. 2587, No. 1). AIP Publishing.
3. Karne, R., & Sreeja, T. K. (2023). Clustering algorithms and comparisons in vehicular ad hoc networks. Mesopotamian Journal of Computer Science, 2023, 115-123.
4. Karne, R. K., & Sreeja, T. K. (2023). PMLC-Predictions of Mobility and Transmission in a Lane-Based Cluster VANET Validated on Machine Learning. International Journal on Recent and Innovation Trends in Computing and Communication, 11, 477-483.
5. Mohandas, R., Sivapriya, N., Rao, A. S., Radhakrishna, K., & Sahaai, M. B. (2023, February). Development of machine learning framework for the protection of IoT devices. In 2023 7th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1394-1398). IEEE.
6. Kumar, A. A., & Karne, R. K. (2022). IIoT-IDS network using inception CNN model. Journal of Trends in Computer Science and Smart Technology, 4(3), 126-138.
7. Karne, R., & Sreeja, T. K. (2022). Routing protocols in vehicular adhoc networks (VANETs). International Journal of Early Childhood, 14(03), 2022.
8. Karne, R. K., & Sreeja, T. K. (2022). A Novel Approach for Dynamic Stable Clustering in VANET Using Deep Learning (LSTM) Model. IJEER, 10(4), 1092-1098.
9. RadhaKrishna Karne, D. T. (2021). COINV-Chances and Obstacles Interpretation to Carry new approaches in the VANET Communications. Design Engineering, 10346-10361.
10. RadhaKrishna Karne, D. T. (2021). Review on vanet architecture and applications. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(4), 1745-1749.