International Journal of Engineering and Management Research
e-ISSN: 2250-0758 | p-ISSN: 2394-6962
https://ijemr.vandanapublications.com

Peer Reviewed & Refereed Journal
Volume-14, Issue-5 (October 2024)
https://doi.org/10.5281/zenodo.14189889

Analysis of the ATM's Security and Privacy- Preserving Mechanism

S.Jayaprakash[1*] and M.Jayanthi[2]
[1]PG Scholar , Department of Computer Science and Engineering, Kalaignar Karunanithi Institute of Technology, Coimbatore, INDIA
[2]Assistant Professor , Department of Computer Science and Engineering, Kalaignar Karunanithi Institute of Technology, Coimbatore, INDIA

[*]**Corresponding Author:** S.Jayaprakash

Received: 23-09-2024 Revised: 12-10-2024 Accepted: 30-10-2024

ABSTRACT

Through a [2] variety of methods, such as encryption, monitoring, and authentication, the ATM privacy security system ensures the security and confidentiality of users' financial and personal information during ATM transactions. The system makes an effort to thwart fraud attempts and unauthorised access by utilising such tactics. This all-encompassing security solution for ATMs is made especially to stop potential ATM theft and unauthorised access. Users who have registered an owner will receive an authorised acceptance message via a link on their registered phone number prior to being able to withdraw money; only the owner may do so. This system has an exclusive verification technique. The ATM room's occupancy is continuously monitored by the system, which also includes an overcrowding control warning that activates with a sound when more than one person enters the space. Using a vibration sensor to operate as a theft detector, the device finds any suspicious activity in the ATM and promptly alerts the neighbouring station so that swift action can be taken. The maximum level of protection is offered to bank management and ATM users by the features of the ATM Privacy System.

***Keywords*--** Privacy, Security, ATM, Confidentiality, Authorization

I. INTRODUCTION

ATMs are a vital part of modern banking systems, allowing customers to conveniently access cash and financial services. Despite its convenience, ATM fraud and theft pose a significant risk to banks and users alike. Recently, a number of methods have been developed to increase ATM security, such as using accept messages for every card transaction. This work provides a novel security system that integrates an infrared (IR) sensor-based overcrowding control alarm system with an accept messaging system. Additionally, the system has an ATM theft warning that uses a vibration sensor to alert the nearby police station.

The primary objectives of the proposed system are to deter fraud and improve ATM security, especially in high-crime regions. By requiring users to authorise each card transaction, the accept message system can prevent fraud and unauthorised access. The overcrowding control alarm system uses an infrared sensor to detect the number of individuals in the vicinity of the ATM. If the location gets crowded, an alert will go out to notify the local police station and other users. Additionally, the ATM theft indicator alert uses a vibration sensor to detect any unauthorised attempts to steal or tamper with the ATM. Should such an endeavour be identified, the police station will receive an immediate alarm. This proposed security solution has the potential to greatly increase ATM security, especially in high-crime regions. By adding an extra layer of defence against fraud and unauthorized access, these security features are integrated, guaranteeing the security of customer financial data and transactions. All things considered, the proposed security system is a significant advancement in ATM security systems, and its deployment could assist banks and consumers in averting monetary losses resulting from ATM fraud and theft.

II. EXISTINGSYSTEM

ATM Security Enhancement with Biometrics shows how the current ATM security system [2] necessitates an authorization message from a designated person for every card transaction. To increase the security of ATM transactions, the suggested solution uses biometric authentication. Before starting any transaction, the user is required to provide their biometric information, such as fingerprints or facial recognition. This is done to verify their identity. Once the user's identity has been verified, the system requests authorization or rejection of the transaction from a designated individual, like a bank teller. A surveillance camera is another feature of the system that monitors the ATM and searches for any unusual activity. An alarm system linked to the surveillance camera notifies the police or security staff in the event of any suspicious activity. The accuracy and consistency of the biometric

Peer Reviewed & Refereed Journal
Volume-14, Issue-5 (October 2024)
https://doi.org/10.5281/zenodo.14189889

authentication procedure are among the many tests that the authors have conducted on the proposed system. The results of the trials show how accurate and dependable the suggested strategy is in verifying users' identities and preventing unauthorised access.

The study article similarly [1] provides another illustration of an actual ATM security system that makes use of an IR sensor and a vibration sensor. The technique outlined in this research paper combines the use of an infrared sensor and a vibration sensor to identify any unauthorised attempts to damage or steal from the ATM. The vibration sensor is mounted to the outside of the ATM, where it detects any movement or shaking of the ATM's casing. In the meantime, the user is informed by the IR sensor if there is anyone or anything nearby the ATM. Any uninvited attempts to tamper with the ATM, such as drilling, hammering, or other tampering techniques, are detected by the system. If such an attempt is discovered, a notification is issued right away to the police station or security team. The recommended system has been put to the test by the authors under a range of conditions, accounting for elements like light, humidity, and temperature.

The studies' outcomes [3] demonstrate how accurate and dependable the system is at identifying any unauthorised attempts to use the ATM. All things considered, this technology demonstrates a successful method for securing ATMs, providing an additional line of protection against fraud and unauthorised access. The utilisation of biometric authentication technology ensures that transactions can only be initiated by approved persons, while the surveillance camera and alarm system give further security measures to forest all ATM fraud and theft.

III. LITERATUREREVIEW

Iris recognition is a type of biometric identification that uses the unique, random pattern found on each iris to provide a unique solution for identity, security, and authentication. To automatically identify a person, the iris recognition system compares a fresh eye image to the human iris patterns stored in an iris template database. The iris template database is created in three stages, two of which are segmentation and feature extraction. [1]. Banks give ATM cards to customers who wish to access services including cash withdrawals, PIN changes, and balance inquiries. However, real ATM cards have a number of issues, such as loss, counterfeiting, deterioration, expiration, and hijacking. Thus, fresh ideas are needed to improve security. One such idea is a cardless transaction system using ATMs, which is now being studied by numerous researchers. In this case, we propose a modified model based on this protocol that provides the same transaction capabilities as before, but instead of using biometric fingerprints—which have a number of disadvantages—we recommend using random Personal Identification Numbers (PINs) and One-Time Passwords to determine customer authentication. [2].A popular piece of technology that facilitates everyday transactions without straining the banking system is the ATM. Nonetheless, it is vital to guarantee that these gadgets are protected against theft and other detrimental actions. PINs or smart cards with magnetic stripes and PINs are frequently used by traditional ATM systems to validate users. While this takes care of user security, the bank has to put in additional effort to secure ATMs. It is insufficient to merely place security personnel. Thus, the objective of this project is to install a sophisticated security system that can detect theft or robbery and initiate a range of preventative actions. This system uses sensors tokeep an eye on several aspects of the ATM's security, including cameras, reed switches, and ultrasonic sensors[3]. ATM cash theft is a widespread issue that costs the general public their hard-earned money in numerous countries, including India. This loss has an indirect effect on the public because less money is accessible to them. This study project uses the most efficient communication technology, the Internet of Things (IoT), to report on such occurrences. The best way to report such incidents to the authorities is through the Internet of Things (IoT), which uses internet technology that is now prevalent in ATMs. The recommended method uses IoT and an embedded system to finish the task. An ESP8266-based Internet of Things device coupled with a vibration sensor and ATMEGA 328 P PU microcontroller is used to detect ATM robberies and alert law enforcement. [4].In today's society, security systems are vital. With the advancement of security systems, iris recognition and biometric systems have emerged as crucial instruments for biometric-based identification. These innovations have substantially improved the bar for personal verification, enhancing national, international, and individual safety. This is because the iris design is a wonderful choice for really secure environments because it is solid, distinctive, and pleasant. ATMs made banking more convenient and accessible, but they also made it more likely that skilled thieves would target these machines. One potential workaround due to the advancement of biometric identification technologies, such as fingerprint and iris scanning, is to encrypt client passwords using certain article points. This approach would be quicker and mo resecure[5].This indicates a fresh approach to verifying and identifying users at ATMs. This approach uses regular authentication procedures along with body characteristics captured by a hidden camera within the ATM. The data collected from the camera is processed to compare the percentage with the stored data in order to authenticate/identify the legitimate person. If someone is thought to be suspicious, they receive the appropriate care.

Peer Reviewed & Refereed Journal
Volume-14, Issue-5 (October 2024)
https://doi.org/10.5281/zenodo.14189889

To improve outcomes, the investigation looked at face and fingerprint recognition as two physical traits. The Olivetti Research Laboratory (ORL) face database and the Extended Cohn-Kanade database (CK+) were both used for fingerprint analysis and face recognition. MATLAB was used to conduct the experiments, and the results of the recommended approach [6]. Combining a Face Recognition System with an OTP during the identity verification process and user identification at ATMs can improve system security and reduce the possibility of misuse from remote locations. [7]. the data's security and integrity by restricting access permissions, revealing only a limited amount of file information, and encrypting the data with a secret key. This implies that a user will not be able to view or alter the data without the required authorizations, even if they are not authorised to access it. The secret key authentication method, which uses both symmetric and asymmetric mechanisms, along with the three-tier authentication methodology, offer a reliable and highly secure way to limit access to important files and data. This helps prevent unauthorised access in addition to guaranteeing that the data is protected and secure from any threats. [8]. In order to electrically connect facial recognition for automated teller machines with a security paradigm and to physically combine an access card, a Deep Convolutional Neural Network is utilised. Using certain fully-fledged artificial intelligence agents, a face identification verification portal is developed for remote certification and made accessible to the end user to confirm the authorization of an unauthorised user. Thus, the technology will play a major role in breaking the account security paradigm by allowing the actual account to be used. [9]. A deep learning-based miniatureface recognition device was developed to verify the identity of the user without requiring a large infrastructure, costly servers, or cloud servers. The person's facial privacy will be protected by using smart card memory to store and retrieve the encoded information. Deep learning models for face detection and identification are available in the System on Module (SoM). [10].A network of physically connected internet-connected things is known as the Internet of Things (IoT). This project makes advantage of the Internet of Things to remotely control a load through the internet. The Internet of Things (IoT) is a network of interconnected gadgets that have sensors integrated into them that have the ability to automatically collect and send data. In this study, Google Assistant is used to execute the output and cloud computing is used to store the data. The cloud computing system makes it easier to access everything at any time and from any location by facilitating the linking of neighbouring devices. This system is designed to be cost-effective and allows for the control of several devices. [11]. Biometric authentication is used by automated securitysystems, although contact-based biometrics can spreaddiseases like COVID-19. In order to authenticate people,this research suggests a non-contact biometric techniquethat examines the , crypt, iris pigment spot and wolflinnodules. Several feature extraction techniques, including BRISK, SURF, FAST, MinEigen, MSER, and Harris, are used to extract the features from each of these locationsafter segmenting the features into rectangular shapes. Inorder to determine the best feature extraction technique for each area, a statistical analysis is conducted. The trained and untrained categories of the input data aresplit60:40. The trained and test features are put through afeature matching procedure, and the number of feature matches is examined[12]. The World Health Organization (WHO) advises keeping a safe physical distance of six feet as asocial remedy to stop the transmission of the virus in the ongoing COVID-19 epidemic. But people frequently neglect to pay attentionto those who are behind them. The system includes an Arduino UNO with PIR and ultrasonic sensors. The ultrasonic sensor monitors the space between persons when the PIR sensor notices motion. The device will sound an alarm to alert anyone within six feet of it. Abuzzerwillsoundtoalert youtothepresenceofaninfected person if the distance is less than six feet. This project's primary goal is to make sure of safe and secured society[13].

IV. BLOCK DIAGRAM

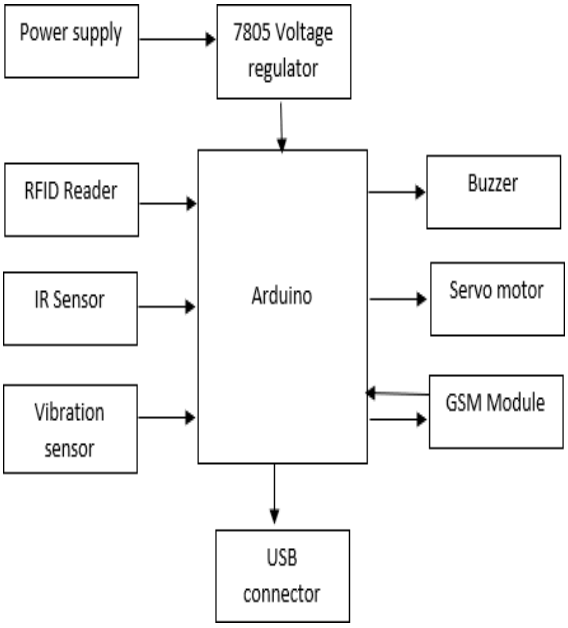

Figure 1: Block diagram

Peer Reviewed & Refereed Journal
Volume-14, Issue-5 (October 2024)
https://doi.org/10.5281/zenodo.14189889

A. Arduino

With the Arduino platform, the ATmega328 microcontroller chip is frequently used. Digital and analogue input/outputpins, timers, and serial communication interfaces are amongits many functionalities. The ATmega328 chip can be easily programmed to create unique electronic systems and devices to the Arduino platform's user-friendly programming features.

Figure 2: Arduino

Depending on their purpose, the pinsonan Arduino board can be divided into many categories. For instance, DigitalI/OPins, which are labeled D0 through D13 on most Arduino boards, are used for digital input or output. Contrarily, analog signals from sensors used to measure temperature, light, and sound are read using analogue inputpins, which have the numbers A0 to A5.

PWM pins, which hmay generate analogue output signals, are typically used toregulate motor speed or LED brightness, and are identifiedby a tilde () symbol next to the digital pin number. PowerPins, which include 5V and 3.3V, are also present and supply power to external components and the Arduino board alsoincludes Ground Pins. By setting up the device to receiveinput from the RFID receiver, the device can communicate with the authorized cardholder's device by sending a confirmation request message for the transaction.

B. Rfidtag and Reader

An object with an RFID tag can be identified and tracked via radio waves thanks to RFID(Radio Frequency Identification), a wireless communication technology. Thesetags have an antenna and microchip that transmit data whenthey are near an RFID reader. RFID tags could be used as part of ATM privacy systems to improve security and prevent unauthorized access to ATMs. A typical implementation would involve issuing RFID tags to customers, who would carry the month eirperson. An ATM's RFID receiver is where the cardholder would tap their RFIDtagtostartatransaction.

Figure 3:.RFIDReader

Utilizing radio frequency signals, an RFID receiver is capable of extracting data from RFID tags. An RFID tag communicates its unique identifying code to the receiver ach time it is in close proximity to the receiver. A connected system or device, such as an Arduinomicro controller, receives the data from the receiver, which then interpretsit.

C. Irsensor

Devices made of electronics called infrared (IR) sensors areused to detect infrared radiation. Both inanimate objects andliving things emit a form of warmth known as radiation. Thenumber of people using the ATM booth could be countedusing IR sensors in the case of an ATM privacy system. Analarm system would sound if there were too many peoplepresent. To identify people entering and leaving the ATMbooth, in-and-out IR sensors could be installed at the doors and exits. Here is a succinctex plan at ionof how in and out IR sensors could be used in an ATM privacy system.

D. Gsmmodule

There are many advantages to using a GSM module in anATM system, including the ability to establish two-factorauthentication and remote access control. Users requiringtwopiecesofidentityinordertoaccesstheATMundert wo-factor authentication. This is accomplished by employing anRFID tag as one form of identification and a confirmationvia SMS or a mobile app as a second form.

A further feature of the GSM module is remote access control, which enables authorized users to grant or prohibit access to the ATM from a distance. In environments with high security or where there is a risk to users, having a GSM module integrated into an ATM system can provide a number of advantages. Additionally, the module can be configured to immediately notify authorized users whenever there is any suspicious activity, such as attempted unlawful entry, system manipulation.

E. Servo Motor

Servo motors are designed to lock the door which can provide accurate control over a mechanical device's motion and position, making them ideal for applications that call for precision positioning and motion control.

Peer Reviewed & Refereed Journal
Volume-14, Issue-5 (October 2024)
https://doi.org/10.5281/zenodo.14189889

Furthermore, servo motors have a reputation for having a quick response time, which enables them to react swiftly to changes in input signals, Because to their quick response times, servo motors can quickly adjust to changes in position and speed. Most Arduino boards run at 5V, which is also enough to power the majority of servo motors. However, some industrial-grade or high-torque servo motors may need higher voltage inputs, often between 6V and 12V. In certain situations, it might be essential to use a different power source or voltage regulator to supply the servo motor with the requisite voltage.

Figure 4: Servomotor

F. Buzzer

An electro-mechanical device called a buzzer emits a sound either continuously or infrequently when it receives an electrical signal. Depending on the programme running on the Arduino, it can be integrated with a board to produce a variety of noises or alert tones. It is possible to switch on or off the buzzer by programming a digital signal to the output pin in the Arduino IDE.

Figure 5: Buzzer

G. Vibration Sensor

A vibration sensor is a little gadget that can detect movements or vibrations and convert them into electrical impulses. It can be used in conjunction with an Arduino board to detect motions or vibrations and trigger particular actions or events inside of a programme.

Figure 6: Vibration Sensor

The customer of the ATM will be entering into the ATM room that will be counted using the IR sensors fixed directionally to monitor the number of entries inside. If more than one entries are detected the buzzer gives alert message. The customer inserts the ATM card followed by entering the pin number and amount then the message link will be sent to the authorized persons mobile to grant the access for transaction. If in case any unauthorized person operates the owners card the transaction would be declined which helps in resisting amount theft. And the system also develop to detect the theft by breaking ATM, which will be detected using vibration sensor that alerts to the nearby stations and the ATM room door will be locked to lock the thieves inside the room itself.

Figure 7: Flow chart

V. ADVANTAGES

Enhanced Security: The ATM privacy system provides more security since it uses a number of components to control access to the ATM. Only those with an RFID tag are allowed access, and the system employs IR sensors and vibration sensors to detect any unwanted entry attempts or efforts to tamper with the system.

Improved Convenience: By including a GSM module, the system makes it possible for approved cardholders to authorise ATM access and receive

Peer Reviewed & Refereed Journal
Volume-14, Issue-5 (October 2024)
https://doi.org/10.5281/zenodo.14189889

notifications via SMS or mobile apps, leading to a more streamlined access procedure and shorter wait times for users.

Reduced Overcrowding: When the ATM location is getting too busy, the system's IR sensors can identify it and warn the necessary authorities. This function improves safety around the ATM and helps to reduce crowding.

Customizable: The system can be modified to meet the needs of various ATM sites and their unique differences. For instance, based on the location of the ATM, the system can be designed to warn certain stakeholders and the vibration sensors can be customised to detect particular sorts of tampering.

Real-Time Alerts: By enabling the fast detection and reaction to potential security concerns, the system's capacity to provide authorised users real-time notifications can help prevent theft, vandalism, and other illegal acts.

VI. RESULT

Real-time monitoring should be used to swiftly identify and address any suspicious behaviour at the ATM. This will aid in the prompt prevention of fraud and unauthorised access. The selection of Arduino ATmega 328 on this paper is for a number of reasons, including its flexibility to various sensors and modules and its ease of programming. The microcontroller ATmega 328 has a wide variety of input/output pins and may be easily connected to a variety of sensors and devices. It can perform a number of tasks necessary in the ATM privacy security system, including encryption, authentication, and monitoring, thanks to its reasonably fast processing speed and big memory capacity. It is important to take the ATM Privacy Security System's specific requirements into account when choosing an IR and vibration sensor. Considering few things such as Sensitivity, Range, Response time and Power consumption IR and Vibration sensor is choosed and it played a major role.

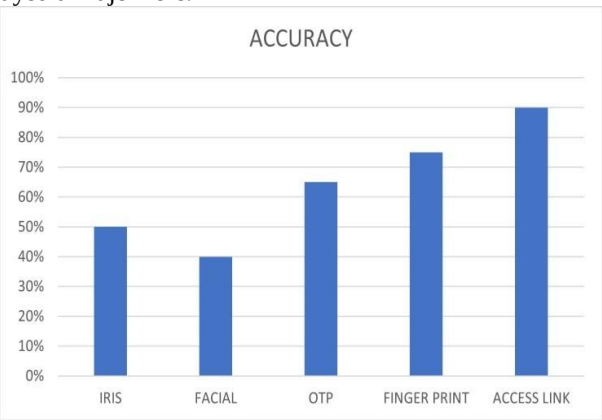

Figure 8: Accuracy

Fig. 8 shows the percentage graph of different methods. This paper resulted with high accuracy.

Table: 1 Comparison table of different methods
This paper results as method of access link with high accuracy and with high confidentiality.

Methods	Accuracy	Performance	Only-Owner can use	Flaws	Confidentiality
Traditional	Low	High	No	Theft	Low
Finger Print	Medium	Medium	Yes	Unclear print	High
Facial	Low	Medium	Yes	Lighting	Medium
OTP	Medium	High	No	Takes time	Medium
Access Link	High	High	No	-	High

REFERENCES

[1] V. Ammisetty. (2023). Novel based hybrid security model for bank atm theft detector using internet of things. *3rd International conference on Artificial Intelligence and Signal Processing (AISP)*, pp. 1-5, DOI: 10.1109/AISP57993.2023.10134783.

[2] Panimalar, S.P., Kumar, M.A. & Rohit, N. (2023). *ATM theft detection using artificial intelligence*. In: Rathore, V.S., Tavares, J.M.R.S., Piuri, V., Surendiran, B. (eds) Emerging Trends in Expert Applications and Security. ICE-TEAS 2023. Lecture Notes in Networks and Systems, vol 681. Springer, Singapore. https://doi.org/10.1007/978-981-99-1909-3_45.

[3] Gunalan, K.V., Sashidhar, R.A., Srimathi, R., Revathi, S. & Venkatesan, N. (2023). *Enhanced ATM security using facial recognition, fingerprint authentication, and web application*. In: Subhashini, N., Ezra, M.A.G., Liaw, SK. (eds) Futuristic Communication and Network Technologies. Lecture Notes in Electrical Engineering, vol 966. Springer, Singapore. https://doi.org/10.1007/978-981-19-8338-2_22.

[4] M. S. Sri, J. K. Chaithanya & N. Dhruthiee. (2022). Design and implementation of smart atm under idle application. *7th International Conference on Communication and Electronics Systems (ICCES)*, pp. 1410-1417, DOI: 10.1109/ICCES54183.2022.9835767.

[5] B. Sricharan, J. U. Sanjana, T. V. Vani & C. N. Sujatha. (2022). RFID based atm security system using IOT. *International Conference on Intelligent*

Controller and Computing for Smart Power (ICICCSP), pp. 1-6, DOI: 10.1109/ICICCSP53532.2022.9862486.

[6] A. S, S. K N & A. Chalil. (2022). An IOT based system for securing ATM machine. *8th International Conference on Advanced Computing and Communication Systems (ICACCS)*, pp. 1764-1768. DOI: 10.1109/ICACCS54159.2022.9785243.

[7] Hossain, M. N., Sayeed, M. S. & UzZaman, S. F. (2022). Utilizing the internet of things, monitoring and protecting system for automated teller machines. *Asian Journal For Convergence In Technology (AJCT)*, 8(3), 17-21. https://doi.org/10.33130/AJCT.2022v08i03.004

[8] Takkar, S., Rakhra, M., Ratnani, A., Protyay, D.S., Pandey, P. & Arora, M. (2021 September). Advanced ATM security system using Arduino Uno. In: *9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, pp. 1-5. IEEE.

[9] Thirumoorthy, D., Rastogi, U., Sundaram, B.B., Mishra, M.K., Pattanaik, B. & Karthika, P. (2021). An IoT implementation to ATM safety system. In: *Third International Conference on Inventive Research in Computing Applications (ICIRCA)*, pp. 744-749. IEEE.

[10] M. Navin Kumar, S. Raghul, K. Nirmal Prasad & P. Naveen Kumar. (2021). Biometrically secured atm vigilance system. *7th International Conference on Advanced Computing and Communication Systems (ICACCS)*, pp. 919-922. DOI: 10.1109/ICACCS51430.2021.9441975.