Advance ATM Security System

Harsh Srivastava[1], Rahul Singh Khokhar[1], Prateek Parashar[1]

[1]*Department of Electronics and Communication Engineering, JSSATE, Noida-201301, India*

Abstract

The Idea of Designing and Implementation of Security Based ATM theft project is born with the observation in our real life incidents happening around us. This project deals with prevention of ATM theft from robbery. So overcome the drawback found in existing technology in our society. An IR sensor is used here which senses any motion inside the money tray whenever someone tries to rob. Once the IR sensor senses any motion inside the money tray, the beep sound will occur from the buzzer. Servo Motor is used for closing the door of an ATM. And we have used two doors in our project in which one door will be closed once two members enter the ATM cabin and another door will closes whenever someone tries to rob the ATM. The Stepper motor is used to leak the gas inside the ATM to bring the thief to an unconscious stage. A Wifi module is used to send the message to the nearby police station and to the corresponding bank. A LCD display is also used to show the messages. This will prevent the robbery and the person involved in robbery can be easily caught

Keywords: Security, Sensors, Module

1. INTRODUCTION

An ATM, which stands for automated teller machine, is a specialized computer that makes it convenient to manage a bank account holder's funds. It allows a person to check account balances, withdraw or deposit money, print a statement of account activities or transactions, and even purchase stamps.

Automated teller machines (ATM) have become one of the essential services nowadays as one can withdraw cash through an ATM without even going to a bank. It was in 1987, that HSBC introduced the concept of atm in India.

In the present scenario, the majority of the population uses the ATM machine to withdraw cash and these machines are easily available at airports, railway stations and market places. Now there are nearly 3 million ATMs installed worldwide.

Despite having security there are many ATM robbery cases we hear frequently. Maharashtra reported 233 cases of ATM fraud in 2018-19, the highest in the entire country, Reserve Bank Of India (RBI) data, accessed by TOI, revealed. The data showed that Delhi grabbed the second spot with 179 cases, followed by Tamil Nadu with 147 cases of ATM fraud. In Maharashtra, people lost Rs 4.8 crore to bank fraud, while in Delhi people lost Rs 2.9 crore. The country witnessed an increase in ATM fraud cases in general (up from 911 to 980).

Among the crimes for financial organizations, the cases of theft and robbery have a very high proportion of over 90% and the crime for the ATM has increased because the external ATM has been increased and it is always exposed to the crime.

2. LITERATURE REVIEW

Indranil Banerjee and Sjivangam Mookherjee[1] incorporated the developments into the current ATM systems to increase security, usability, and dependability.The security mechanism in use needs to be quick and robust. The biometric scanners used in the offered design, such as the iris scanner and the two-way check with the fingerprint scanner, give it a unique quality. The system can access the subsequent steps for the transaction because the iris scanner is the primary security check. The ATM card's inbuilt fingerprint scanner serves as the system's secondary security check. Only when the cardholder's inputted data matches what is in the database is the transaction process considered successful. It is suitable for use because it uses less energy. Comparing the proposed modified approach to the other existing classification and affirmation procedures for ATMs, it is practical and economical.

The study by Jignesh J. Patoliya and Miral M. Desai[2] suggested the idea of a smart ATM security system built on the Embedded Linux platform is put out in this article as a trustworthy security solution for the general public. The study's main objective is to design and implement an embedded Linux platform-based face detection-based ATM security system. The system is implemented on a credit card-sized Raspberry Pi board with enhanced OpenCV (Open Source Computer Vision) image processing software capabilities. Consecutive operations, like the initial system capture of the human face and check to see if the human face is detected correctly or not, give a high level security mechanism.

This work by Avinash Deshpande[3] suggested an automated ATM surveillance and control system , which can watch the ATM system for any attacks on the ATM machine or on users while they are conducting transactions in the ATM centre, stop them, and catch the intruder. The security of ATM centres will be improved by this system. To show the system's efficacy in actual ATM centres, a prototype with the required hardware is being created.

In the study by Anjalin Roy[4], The system's main concept is that when the ATM card is inserted and verified, his image is acquired using the ATM's webcam and compared to the card owner's actual images that are already saved in the database. The user advances to the next level, where he can input the password to complete the transaction, if the taken image matches the stored photographs, proving that he is the authorised user. When the captured image and the saved image don't match, it indicates that the user is not allowed and blocks access to him.
The system may also notify the legitimate card owner of the card misuse. In order for the planned system to save and use account holders' faces in the future, account holders must train their faces to the system. The suggested system itself can perform further processing after obtaining the person's photograph linked to the card from the database, which has no impact on actual server capacity. Additionally, the proposed system may employ the already-installed cameras on ATMs to take pictures, which further lowers the cost of deployment. Consequently, this study suggests a straightforward, economical technique that adds security for ATM transactions against illegal card usages.

In the study by Raj M[5] he suggested the proposed work's goal is to use a Raspberry Pi to construct a low-cost stand-alone Embedded Web Server (EWS) based on an ARM11 CPU and the Linux operating system. It provides a reliable networking solution with numerous internet application areas. To deliver an embedded web page to a web browser, the Web server can be run on an embedded hardware with constrained resources. The proposed architecture for ATM security consists of the following modules: shutter lock authentication, web enabled control, sensors, and camera control.

The focus of the article by Bharati M Nelligani[6] is the novel strategy for securing ATM (Automatic Teller Machine) systems is described in this study. The paper's goal is to inform readers about the enhanced smart ATM security system that was created using cutting-edge technologies and embedded systems. In our suggested system, an RFID card serves as the ATM card, and an IR sensor detects the presence of cardholders and activates the fan and light. If the ATM is tampered with, an SMS is transmitted through GSM to two main stations. In the event that the cash box is stolen, GPS is used to trace the position. Authorized bank workers are identified and verified using finger prints. As a result, the suggested approach is a very secure one for ATMs

Vijay Varadharajan's[7] paper focuses on the design and administration of security services for ATM networks are covered in this article. The positioning of security services inside the ATM protocol stack is examined using a variety of methods. Following consideration of these options, it is suggested that the security layer be positioned between the AAL and ATM levels. Confidentiality, data integrity, and data origin authentication are all provided on the user plane by the proposed security layer. The study then introduces a key establishment process and an authentication scheme. During the call setup processes, this protocol is integrated with the current ATM signalling protocol. Without going against the rules now in place, the created security design can be transparently incorporated into the B-ISDN Protocol Reference Model.

The study by S.J Shepherd[8] was able to satisfy the user's desire for a wireless ATM, the system had to be enhanced. The functioning of the wireless ATM system, particularly the security component, is one of its features. When creating the wireless ATM standard, security has so far received little to no consideration. As a result, a variety of features for security functions are taken into account. This study attempted to outline the security aspects of wireless ATM networks while taking into account the features of the fixed ATM network that is now in place and the security offered by wireless networks. Instead than attempting to specify the cryptographic system, it offers a template for creating one with the necessary functionality.

According to a study by S.Shriram and Swastik B. Shetty[9] this paper describes an Automated Teller Machine (ATM) surveillance system, a smart system based on embedded technology that integrates various sensors to continuously monitor its surroundings for suspicious activities like physical attack, fraud, and theft that could endanger the ATM and people nearby. The security and safety precautions that can be put in place to stop such raids through effective surveillance are also covered. This study examines the various physical assaults against ATMs and suggests ways to foresee them, take preventative action, and alert authorities via the GSM network. It also goes through how the suggested system will be put into practise, as well as the sensors and other hardware needed to deploy the system.Thus, the suggested technique successfully increases the security of ATMs against impending attacks.

A qualitative study by Christiawan and Bayu Aji Sahar 10] introduced the idea of the Fingershield ATM, an ATM that uses fingerprints for biometric identification and is integrated with a smart card and database server. Because each fingerprint has a distinctive set of properties, fingerprint technology is a potent identifying tool. Although users must add an extra 1.5 seconds to their authentication time for fingerprint verification, the security is significantly increased and assured. The experimental descriptive method will be used in this study. With the help of this technique, ATM fraud should be reduced, giving customers a sense of security when using ATMs.based on previous implementation and test findings, Fingershield ATM functions work as intended, some security parameters passed the test, and nearly all specifications are met.

The study by Kande Archana [11], tells the concept starts with the detection of ATM theft from robberies and then uses current technologies to address the issue in our society. When a theft happens, a PIR sensor is utilised to detect human motion, and an alarm is triggered, resulting in a beeping sound from the ATM. To process the real-time data gathered by the PIR sensor, this system uses an embedded ARM controller. Once the alarm goes off, a beep sound is made. The ATM door is then shut by a DC motor, and a stepper motor is utilised to let gas within the machine seep out, rendering the burglar unconscious. The video feed from the camera is continuously sent to the computer for later surveillance. Then use GSM to send a message to the closest police station and the appropriate bank, and use GPS to transmit footage to the same banks and police stations immediately after. Here, LCD monitors show the message's output along with streaming video. It will stop robberies where the perpetrator can be quickly apprehended.Here, the full application is run using the keil tool.

In the Swathi H research paper [12] suggested that for identity verification, ATM systems now only use an access card, which typically has a magnetic stripe (magstripe), and a fixed Personal Identification Number (PIN).In some additional circumstances, a chip and PIN are used, occasionally with a backup magstripe in case the chip fails. This approach is not particularly safe and is likely to lead to a rise in criminal activity. Thus, the requirement for an innovative, user-friendly, and secure access method is essential. In the current approach, the user generates a PIN, and the ATM system is provided with this PIN via a Subscriber Identity Module (SIM) in the user's mobile phone. This data is sent to a Global System for Mobile Communications (GSM) module that is integrated into the functional architecture of the ATM. Compared to the current conventional approaches, this security method is more reliable. The User Defined PIN (UDPIN) may be modified during each transaction, making the approach given dynamic. The user is no longer greatly inconvenienced by losing the access card, and there is no longer a requirement for fast deactivation. It can also be improved by adding additional security features without requiring many changes. This security function has been implemented in a straightforward prototype, and the outcomes are confirmed. The proposed solution has undergone thorough testing and has shown to be an easier and more effective security mechanism.

This article by Prajakta S. Patil and Swamini S. Lokhare[13] claims that Automated Teller Machines In many places, ATMs are utilised to withdraw money. In everyday life, this machine is crucial. The convenience of financial services comes with a high danger of thefts; even the presence of CCTV cannot prevent theft. As a result, we support this project because it gives ATMs a built-in security system. Raspberry Pi is used in this project as well to cut costs. This system's primary goal is to provide the ATMs with theft control, security, and periodic monitoring. The technology uses a variety of sensors to detect the unsettling atmosphere in the ATM booth. In our suggested solution, the door is unlocked using a face-recognition algorithm. When a robbery happens, sensors detect the suspicious environment, the siren sounds, and the door immediately locks. Additionally, text messages will be used to inform all owners. As a result, taking the essential action will be simpler.

The research by PNB Swamy and A. Sathi Babu [14] suggests to store the biometric information of the individual who entered the ATM room and offers biometric registration for ATM room entry. The biometric information is helpful in robbery situations. By using a buzzer, location sharing, sending notifications, and a door locking mechanism, we may further enhance the security of the ATM pin in this system. Here, a MEMS sensor is employed to detect ATM machine vibration and to send out fire alerts. To handle the real-time data gathered by the sensors, this system utilises an embedded system based on the ARDUINO controller platform. The system will issue voice alarms if it detects something suspicious or unauthorised. The door of the ATM is closed using a servo motor. The gas is released inside the ATM using a spray mechanism, rendering the robber unconscious. Additionally, use IOT to notify the closest police station and the relevant bank when a robbery occurs. Hear the LCD display board displaying the message output continually. The suggested technique additionally cleverly informs clients of the status of the ATM by flashing RED and GREEN lights.

This paper by Aravind R and Edwin Raj K[15] proposed a system in which the manner of transactions was revolutionised.For a straightforward money withdrawal, there were no lengthy queues of people waiting in front of the bank. The quantity of ATMs a bank has may be taken into account when evaluating its strength. As there are more ATMs, there are also more fraudulent activities taking on inside of them.The primary goal of this initiative is to improve the security of ATM usage. Static key (PIN) security is used with the current procedure. The suggested method incorporates Face-id as a key with the present method. The fact that each person's face ID is unique and cannot be used by anyone else except the user is one of the benefits. The machine learning and image processing algorithms (Eigenface algorithm) are employed to implement the face-id scan.

The study by Jacintha V. and J. Nagarjana[16] discusses about the current situation where the vast majority of people use ATMs to withdraw cash. Even if CCTV cameras are installed in the ATM facility, there have been numerous ATM robberies that have taken place in various locations. Therefore, it is necessary to update the security system. We provide a protection system for ATM theft utilising a clever and efficient technology to help decrease these types of robberies. This method also evaluates different ATM physical assaults. In the technique we've suggested, a face-recognition camera is used to record the individual entering's face. To find abnormal behaviours performed on the ATM machine, tilt and vibration sensors are used. The temperature sensor's job is to ascertain the level of heat present in the ATM booth. The major objective of our suggested system is to use IOT and GSM networks to send an alarm through social media sites like Facebook, Twitter, and Gmail.To distribute the chloroform and render the thief asleep, use liquidator chloroform. This technology offers effective control and monitoring.

C. Bhuvaneswari and T. Malini work [17] discusses about the ATM fraud has become a pretty prevalent occurrence. Even while technology has advanced in many ways, it is still being utilised in a variety of inappropriate ways to steal money from ATMs. Many thieves have created ATM skimming and trapping technology.Many ATMs now have a recognition-based verification mechanism in place for security reasons. This work focuses on biometric identification techniques including face and fingerprint recognition.The Internet of Things has also been utilised to improve money security and provide timely notifications. The user will also receive a one-time password to confirm their identification. Proteus is used to simulate the task, and the findings are then confirmed by actually implementing them with hardware.

The authors of the work, K. John Peter and G. Nagarjana, [18] suggested a facial recognition system is a computer programme that uses a digital image or a video frame from a video source to automatically recognise or confirm a person. The proposed article uses face recognition technology for ATM system verification. There are two different kinds of comparisons used for facial recognition. The first step is verification, where the system matches the provided person to who they claim to be and makes a yes or no determination. The next step is identification, which involves comparing the provided person to every other person in the database and providing a prioritised list of matches. Face recognition software examines each individual's distinctive form, pattern, and placement of facial features. Face recognition is a fairly sophisticated technique that is primarily reliant on software. For each type of biometric equipment, this biometric methodology creates an analysis framework using PCA techniques. Face recognition begins with a picture and looks for a person in it.This can be done in a number of ways, such as through movement, variations in skin tone, or hazy human forms.

The authors of the research, Gokul S., Kukan S. and Vishnu Priyan S S[19]tells that the use of ATMs to withdraw cash has grown in the modern world. In addition, there have been more instances of theft and robbery, which highlights the necessity for highly secure ATMs with extra security elements. The goal of this effort is to create a security-based smart ATM with access controlled by fingerprint and RFID technology. The user's RFID number and fingerprint information are collected, and then the recognised card number, authorization status, and access location are sent to be verified with database information. The appropriate account holder receives a message indicating whether the authorisation is legitimate or not once the information has been verified using the database details that were retrieved. The account holder is also alerted of the access's location, time, and date. By installing vibration and flame sensors that instantly alert in case of fire and breaking, this also improves security. In order to establish total security, a camera within the machine records the user's face as well as the time and date of the access, which can be used as evidence in the event of a suspicion.

This paper by Claudio Porretti [20] discusses the purpose of this paper is to outline a novel idea for ATM security management that the GAMMA project has put out and that is being carried out by its "core" prototype, the Security Management Platform.GAMMA is an FP7 project whose objective is to create tools for managing new ATM vulnerabilities. In order to design a solution based on the self-protection and resilience of the ATM system, with the ability of sharing security information in a distributed federated environment, the GAMMA vision acknowledges the prospects presented by a collaborative framework for managing security.

3. PROPOSED METHODOLOGY

1. Door Closing Mechanism: This security system will allow only two persons to enter the ATM cabin. The IR sensor will count the number of persons and when the count becomes two the system will automatically lock the glass door (door-1) and whenever someone tries to temper the ATM for robbery purpose, in that case the system will close another door (door-2).

2. ATM Tampering Detection Mechanism: The vibration sensor and temperature sensor are there to detect any kind of tampering on the ATM. If any tampering is detected, in that case the whole security system will be activated.

3. Unconscious Gas Releasing Mechanism: Whenever someone tries to rob the ATM, in that case the security system will release some chemical gas like chloroform which will make the thief unconscious for some time.

4. To Inform the Police and Bank on Time: This security system uses the wifi module to transmit the alert message to the nearby police station and bank at the time of robbery.

4. FUTURE SCOPE

The ATM security system safety has various techniques to avoid the robbery and ATM tampering problem. In future the security system can be advanced according to the requirements. In future we can enhance the system by adding retina scan, Palm scanner and other devices of biometric credential. More sensors such as an updated advanced temperature sensor, anti-break glass door sensor, etc. can be added to the system to ensure safety of the ATM. The most important thing is that people follow the rules and regulations related to this system to improve the security of this approach. This system can also be used at various places where access control has to be maintained and monitored

5. CONCLUSION

As we all know, these days most of the ATMs have been attacked by robbers. Also gradual increases the theft of ATMs year by year.

This paper demonstrates how an automation of “ATM THEFT” prevention from robbery (or) thief can be implemented using Node MCU ESP 8266, IR Sensor, LCD Display, Servo Motor, vibrating sensor, Temperature Sensor, buzzer and batteries for power supply.

By implementing this project we can catch thieves on time and this will decrease the robberies very much and also we can save our precious time

References

[1]. Indranil Banerjee , Sjivangam Mookherjee,2022 . Advanced ATM system using IRIS Scanner.

[2]. Jignesh J, Patoliya , Miral M. Desai,2017. Face Detection based ATM security system using Embedded Linux Platform.

[3]. Avinash Deshpande , Balwant K. Patil, Sateesh N. Dodamani,2018. Development of Advanced ATM Surveillance and Security system.

[4]. Anjalin Roy,Caren Babu, D Abraham Chandy,2021.Enhanced Security Mechanism for ATM Machines.

[5]. Raj M,Anitha Julian 2015. Design and Implentation of Anti-Theft ATM Machine using Embedded Systems.

[6]. Bharati M Nelligani, Dr, NV Uma Reddy, 2017 .Smart ATM Security System using FPR,GPS,GSM.

[7]. Vijay Vadharjana,Rajan Shankaran . Security for ATM Networks.

[8]. D. Patiyoot,S.J Shepherd.Security issues for Wireless ATM Networks.

[9]. S.Shriram,Swastik B. Shetty,2016.Smart ATM Surveillance System.

[10]. Christiwan,Bayu Aji Sahar,Fingershield ATM- ATM Security System using Fingerprint Authentication.

[11]. Kande Archana,Dr. P. Bhasakara Reddy,2017. To Enhance the Security for ATM with the help of Sensor and Controllers.

[12]. Swathi H.,Suraj Joshi,2018. A Novel ATM Security System using a User Defined Personal Identification Number with the aid of GSM Technology.

[13]. Prajakta S. Patil,Swamini A. Lohkare,2020.ATM Surveillance and Security using Image Processing,

[14]. PNB Swamy,A. Sathi Babu,2020.Smart ATM Security using IOT.

[15]. ARAVINDH R.,EDWIN RAJ K.,2021.Enhanced Security Feature of ATM through Facial Recognition.

[16]. Jacintha V.,J.Nagarjana,An IOT based ATM Surveillance System.

[17]. C. Bhuvaneswari,T. Malini,2021.Biometric and IOT Technology based safety transactions in ATM.

[18]. K John Peter,G.Nagarjana,Improving ATM Security via Face Recognition.

[19]. Gokul S.,Kukan S.,2020.Biometric based Smart ATM using RFID.

[20]. Claudio Porretti,Denis Kolev,2016.A New Vision for ATM Security Management.