IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

Double Layered Security System for Smart ATM by Fingerprint and RF Technology

Dr Kala R[1], Haritha MP[2], Sreeyuktha R[3], Vishnuprasad R[4]
Assistant Professor, Department of Computer Science and Engineering[1]
Students, Department of Computer Science and Engineering[2,3,4]
Hindusthan Institute of Technology, Coimbatore, Tamil Nadu, India

Abstract: *The crucial prerequisite in these days is to get rid of various forms of attacks. Nowadays, for financial transaction, automated teller machines (ATMs) are the mostly used gadgets in which personal identification numbers (PINs) are generally used for transaction. But personal identification numbers (PINs) are not secured from many types of threats (spoofing, eavesdropping, man-in-the middle attack etc.), which can affect the security of the confidential and private information. Due to this reason, different biometric systems gain popularity worldwide for their behavioral and physiological features. However, the current biometric systems, for example, iris, palm, faces or voice are extremely complex to use and have different disadvantages. In order to overcome these disadvantages a new concept has been introduced in this paper, for authentication in ATM a fingerprint authentication method and for information (finger print) transfer a combined approach fingerprint and RF technology scheme is used. Finger authentication system is implemented by the combination of fingerprint reader and fingerprint sensors. For the purpose of information (fingerprint) scanners work by capturing the pattern of ridges and valleys on a finger. The information is then scanners work by the device's pattern analysis. For fingerprint authentication system, the experiment shows that in proposed classification the average recognition accuracy is 99.75% and 99.92 % and the execution time is 0.168 s and 0.187 s respectively..*

Keywords: Fingerprint, RF technology

I. INTRODUCTION

The existing system is a microcontroller-based ATM in which normal cards are replaced with RFID cards that contain the card number of the user. Instead of using the PIN, the fingerprint of the user is used for authorization. Hence if the person is in the vicinity of ATM, his/her card is scanned by the RFID scanner and the system waits for the valid fingerprint of the corresponding card. If a valid fingerprint is recognized by the fingerprint sensor of the ATM, message will be sent to the phone number, registered to the card, stating that "The access is granted".

On the other hand, if an invalid fingerprint is recognized, the user of the corresponding card gets a message stating that "Access not granted! Someone has tried to access this card". Regardless of if the access is granted or not, the cardholder also gets details about the time, date, and location of the access. To minimize the storage of unwanted video feed, the images of the people inside ATM are saved in the database through a camera that helps the respective bank and the cardholder in case of theft at the ATM.

1.1 RFID

Radio Frequency Identification (RFID) refers to a wireless system comprised of two components: tags and readers. The reader is a device that has one or more antennas that emit radio waves and receive signals back from the RFID tag. Tags, which use radio waves to communicate their identity and other information to nearby readers, can be passive or active. Passive RFID tags are powered by the reader and do not have a battery. Active RFID tags are powered by batteries.

RFID tags can store a range of information from one serial number to several pages of data. Readers can be mobile so that they can be carried by hand, or they can be mounted on a post or overhead. Reader systems can also be built into the architecture of a cabinet, room, or building.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

II. OBJECTIVE

The main grail of this project is to intensify more security to the ATM system by using most trusted and effortless way that is Fingerprint and RFID System One Time Password (OTP). The major objectives of the project are: To enhance the security of the system. Finger print will be employed to detect the account holder identity. To furnish more authentication using RFID and OTP. To introduce user friendly system for those people who are less familiar with newer technologies, with very few changes in the current System. That is accomplished by using current technologies/devices like Mobile, SMS and ATM GUI etc.

III. RELATED WORK

Biometrics is a technology that helps to make your data tremendously secure, distinguishing all the users by way of their personal physical characteristics. Biometric information can be used to accurately identify people by using their fingerprint, voice, face, iris, handwriting, or hand geometry and so on. Using biometric identifiers offers several advantages over traditional and current methods. Tokens such as magnetic stripe cards, smart cards and physical keys, can be stolen, lost, duplicated, or left behind; passwords can be shared, forgotten, hacked or unintentionally observed by a third party There are two key functions offered by a biometric system. One method is identification and the other is verification.

Many researchers have been trying to develop fingerprint system which detects and verify with certain area of interest. The following text gives a brief overview.

3.1 ATM Terminal Security using Fingerprint Recognition

After testing the system developed, we came to know that ATM prototype can be efficiently used with fingerprint recognition. Since, password protection is not bypassed in our system, the fingerprint recognition done after it yielded fast response and is found to be of ease for use. Fingerprint images cannot be recreated from templates; hence no one can misuse the system. LPC2148 and FIM3030 provide low power consumption platform. Speed of execution can be enhanced with the use of more sophisticated microcontroller. The same hardware platform can be used with IRIS scanner to put forward another potential biometric security to the ATMs.

3.1.1 Disadvantages

- **System Failures** – scanners are subject to the same technical failures and limitations as all other electronic identification systems such as power outages, errors and environmental factors.
- **Cost** – it is true that fingerprint recognition systems are more cost effective than ever, but for smaller organisations the cost of implementation and maintenance can still be a barrier to implementation. This disadvantage is lessening as devices become more cost effective and affordable.
- **Exclusions** – while fingerprints remain relatively stable over a person's lifetime there are sections of the population that will be excluded from using the system. For example, older people with a history of manual work may struggle to register worn prints into a system or people who have suffered the loss of fingers or hands would be excluded.

3.2 ATM Security based on Fingerprint Biometric and SVM

In this paper, we propose a fingerprint classifier based on Support Vector Machine (SVM), a relatively new technique to train classifier that is well founded in statistical learning. A fingerprint image is a digital representation of a fingerprint pattern acquired though a scanner. The design of ATM terminal system based on fingerprint recognition took advantages of the stability and reliability of fingerprint characteristics, the recent results in pattern recognition have shown that support vector machine (SVM) classifiers often have superior recognition rate in comparison to other classification methods. Additional, the system also contains the original verifying method which was inputting owner's password. The security features were enhanced largely for the stability and reliability of owner recognition. The whole system was built on the technology of embedded system which makes the system more safe, reliable and easy to use.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

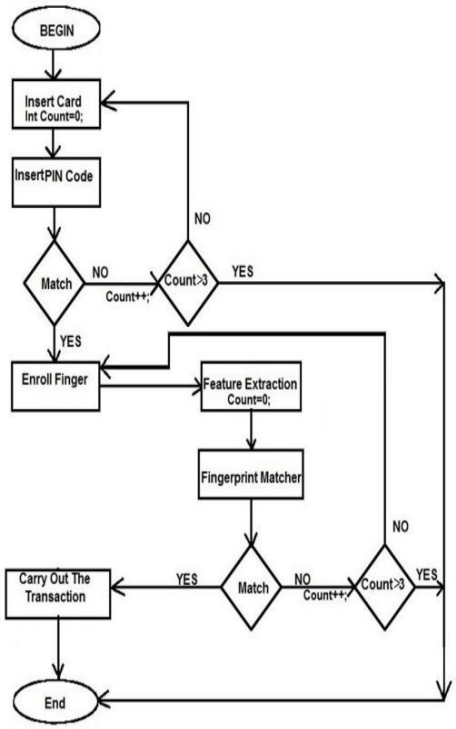
3.2.1 Disadvantages

- SVM algorithm is not suitable for large data sets.
- SVM does not perform very well when the data set has more noise i.e. target classes are overlapping.
- In cases where the number of features for each data point exceeds the number of training data samples, the SVM will underperform.
- As the support vector classifier works by putting data points, above and below the classifying hyperplane there is no probabilistic explanation for the classification.
- It does not perform well when we have large data set because the required training time is higher.

3.3 Fingerprint Authentication for ATM

A smartcard based ATM fingerprint authentication scheme has been proposed. The possession (smartcard) together with the claimed user's Biometrics (fingerprint) is required in a transaction. The smartcard is used for the first layer of mutual authentication when a user requests transaction. Biometric authentication is the second layer. The fingerprint image is encrypted via 3D map as soon as it is captured, and then is transmitted to the central server via symmetric algorithm. The encryption keys are extracted from the random pixels distribution in a raw image of fingerprint. The stable features of the fingerprint image need not to be transmitted; it can be extracted from the templates at the central server directly. After this, the minutia matching is performed at the central server. The successful minutia matching at last verifies the claimed user. Future work will focus on the study of stable features (as part of encryption key) of fingerprint image, which may help to set up a fingerprint matching dictionary so that to narrow down the workload of fingerprint matching in a large database.

3.3.1 Flow Chart



3.3.1 Disadvantages

General Limitations

- Misidentification
- False Acceptance
- False Rejection

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

2. Privacy
3. Image captured at 500 dots per inch(dpi). Resolution: 8 bits per pixel. A 500 dpi fingerprint image at 8 bits per pixel demands a large memory space, 240 KB approximately à Compression required (a factor of 10 approximately).

Limitations for individual
1. Dry, wet or dirty hands.
2. For some people it is very intrusive, because it is still related to criminal identification.

3.4 Enhancing ATM Security using Fingerprint

The objective of this research are listed below Fingerprint based ATM System is more secure than ATM card. User can make transaction using his fingerprint any place and at any time, he need not have to carry ATM card. User can transfer money to various accounts by mentioning account number in case of emergency. The system can be used in various Banks. Low educated people can access easily. When our ATM card misplaces then no one use or access. It automatically blocks. No one can hack the pin code. The hackers can easily guess the 4-digit pin code.

The main focus of this paper is to develop the better security system by using fingerprint based ATM. An embedded system is a combination of software and hardware to perform a dedicated task. Some of the main devices used in embedded products are microprocessors and microcontrollers. In this research mainly concentrated in Visual studio and Arduino Uno. In this paper, a fingerprint based ATM cashbox accessing system implemented using Arduino Uno module and it is the heart of the device. Initially we store the fingerprint of bank manager and that will be verified with the fingerprint that we are giving when the time of authentication. In this system, we stored all the data in SQL database. If the fingerprints are matched then ATM cashbox will open, otherwise buzzer will give alarm. The task related instructions are loaded into Arduino, which is programmed using Arduino language. The system consists of Arduino Microcontroller Unit, Fingerprint module, LED indicators and a buzzer alarm system and microcontroller that collect data from the fingerprint module. As it is based on the fingerprint authentication there is no chance of disclosing of password or pin to the third parties. In this system, we are mainly concentrates in customer security and usage. Before introduction our system so many illiterate people cannot use the ATM machine. By introducing Fingerprint based ATM system all the people can use the ATM because of user friendly. In our system, we don't want to carry ATM card and so that loss of ATM card and charring card in wallet have been reduce. Because of that we are mainly concentrating in illiterate people. In this description we have receive the entire fingerprint with the help of Arduino Uno board. In this process an Arduino Uno board plays an important role. An Arduino board is connected with the fingerprint module to receive and checks the fingerprint and all the dates will be save in the MS SQL server. In this system we are mainly concentrated in the illiterate people because all the people are lacking in the communication between the customer and the ATM machine. In banking all the customer wants to do their transaction fast and quick. Because all the customer wants to do their transaction as soon as possible. When we introduce this system all the customers able to do their transaction quick and safe. Because when the entire customers want to deposit cash or withdraw their money, they all want to do their transaction immediately. So all are trying to save their time. Therefore, that bank introduce Automatic Teller Machine (ATM) instead of teller. This machine provides all facility like teller in the bank. Moreover, it provides better and quick process. Customer doesn't want to wait in the queue to do their transaction. We provide it as the same technique like ATM, but when all the customer wants to do their transaction banks provide some security using debit card, credit card, master card, visa card. When the customers start to do their transaction, they want to have their cards and the pin number. When the customers have poor knowledge about ATM and their function they are so much confused. Using this system, the customer can use their fingerprint to do their transaction instead of cards. We have done many researches due to this biometric system. By our research we have notice that fingerprint is unique. It's very difficult to make any duplicate fingerprint. Its shows that it is more secure than the old system. At the end of our research Fingerprint biometric system prove more percentage of security and safe system to develop our system. Arduino UNO is the most used board in the family of Arduino boards (Fig.1). In this research Arduino board function as main software. It is used for many researches in the field of electronic. This board is mainly connected to fingerprint module. Fig.1. Arduino Uno R3 Fingerprint module is an input device used for Fingerprint processing and captures a digital image of the fingerprint pattern. We are using to recognized fingerprint because it is unique.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

Figure 1

3.4.1 Disadvantages

- It has no room for technological improvements.
- The embedded systems are hard to maintain.
- It is complicated to take back up of the embedded files.
- The embedded systems have less power supply durability if it is battery operated.

One of the disadvantages of ATM machines is that they are both physically and electronically vulnerable. This makes them an easy target for criminals. Malware can be used to access people's cash. Skimming devices and small cameras can be fitted onto Automated Teller Machines. Other criminals can physically destroy an ATM in order to access cash. People risk being robbed using ATM machines especially in isolated areas. This is a huge disadvantage of ATM Machines.

An Automated Teller Machine like any other machine is bound to break down, although this is rare. Some machines may fail to recognise bank cards or can run out of cash. At other times the ATM system goes offline. Also, there is a limit to the amount of cash one can withdraw from an ATM which can be an inconvenience if you require more funds. So the other disadvantage of Automated Teller Machines is that they may breakdown. Setting up ATM machines can be affordable for financial institutions, but it is not the same for the users. Banks and machine owners obtain a lot of revenue from ATM machines in the form of fees that users are charged for using them. The transaction costs are a huge disadvantage of ATM Machines. Lack of personal service is a disadvantage of ATM Machines. There are no bank assistants to help you or to ask questions to.

IV. EXISTING SYSTEM

In our modern world, all the people used to do truncation in banking like deposit money and withdrawing money. For that, the customers will be standing in queue to withdraw money from bank. All the customers felt like waiting for withdraw cash. Therefore, that bank introduces ATM (Automated teller machine) to help the customer to withdraw money quick. In that ATM system, they introduce CARDS (Credit, Debit, master, Visa) to the customer to withdraw cash by using them. Main advantage is quick cash providing by the ATM system. The customer feels happy and they will not waste time to withdraw cash by standing. but it has the disadvantage like, smart cards and physical keys, can be stolen, lost, replicated, or left behind; passwords can be shared, forgotten, hacked or accidentally observed by a third party. The banks required a better system to maintain security for the customer to do the transaction in their banks. To overcome these problems, the developed this fingerprint based ATM system. Everyone used to do banking like storing cash and withdrawing cash. The clients will be in line to extract cash from the bank. The clients felt like biding one's time to withdraw money. That bank proposes an ATM (Automated teller machine) to aid the client extract cash quickly. In such an ATM, they propose CARDS (Visa, Credit, master, Debit) to the client to extract money through their usage. Major merit is fast money provided by the ATM. The customers feel joyful and they shall not throw away time to take out money being in queue. Still it has a main limitation like, physical keys and smart cards, may be theft, misplaced, duplicated, or forgotten; passwords may get distributed, unremembered, hacked or seen by some third party. Banks needed a good mechanism to manage protection for the clients to make the transaction in the banks. To get rid of issues, we have brought this fingerprint based ATM system.

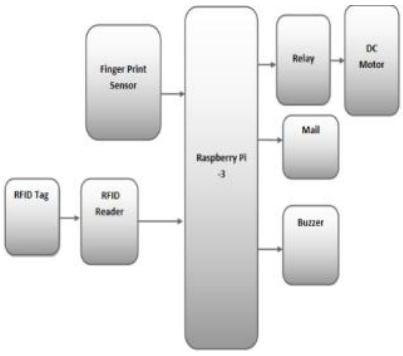
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

V. PROPOSED SYSTEM

These are the proposed Method

Finger Print Recognition based user authentication system with mail alert. Only the authentication person can use the ATM.· OTP has sent to the authority mail.· We can control the fraud access

5.1 Block Diagram of Proposed System



In the proposed system, finger print and RFID based ATM system implemented by IoT technique is done. This system could be more secure by adding the concept of soft biometrics, making biometric essential in both cases of low and high cash withdrawal. A third person is also allow to access this system with user permission. The RFID tag contains information about customer and store data's into system. The Customer read Tag into RFID reader, the tag is matched and then process fingerprint verification using Fingerprint Module. The fingerprint is matched and then OTP is send to respective person mail id. The OTP is correctly entered, then process cash withdraw.

If anyone is miss matched and alarm sound is produced and notification send to mail id. Thus this proposed system uses the RFID card and the user's fingerprint for authorization. In the case of multiple accounts, different RFID cards can be used for each bank accounts. The card closest to the proximity of the card reader will be considered for the current operation. It enhances the security by sending notifications to the mail.

Since the fraud in fingerprint recognition has increased, to ensure security towards this issue in the proposed system, use of safety measures like fingerprint detection OTP generation can be added.

VI. METHODOLOGY

In present scenario, ATM has become one of the most important facilities in our day to day life. This facility enables us to withdraw the money from the authorized account at any time. Security is the major aspect, as the need of ATM is increasing day by day. Security systems are the demands of the day, which helps to avoid theft. Although the banks are deploying security personnel at the ATM spots, but the security arrangement is not quite good enough to secure the facility in case a group of thieves tries to stole the ATM machine. Recently we have seen many cases wherein a group of people entering into ATM and overpowering the security personnel and stole the money from the ATM

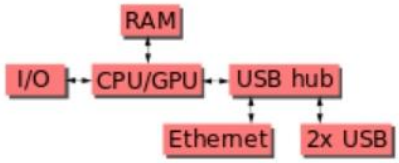
Generally a single person is unable to handle the gang of robbers. Thus an automatic security system plays very important role to avoid robberies. The Idea of Designing and Implementation of Security Based ATM Security Alert project is born with the observation in our real life incidents happening around us. In this project we are going to design system that will help in catching the thieves when an attempt is made to stole the ATM. This system will also act as a security barrier for the ATM facility.

VII. HARDWARE

6.1 Raspberry Pi - 3

The Raspberry Pi hardware has evolved through several versions that feature variations in the type of the central processing unit, amount of memory capacity, networking support, and peripheral-device support.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252



This block diagram describes models B, B+, A and A+. The Pi Zero models are similar, but lack the ethernet and USB hub components. The Ethernet adapter is internally connected to an additional USB port. In Model A, A+, and the Pi Zero, the USB port is connected directly to the system on chip (SoC). On the Pi 1 Model B+ and later models the USB/Ethernet chip contains a five-port USB hub, of which four ports are available, while the Pi 1 Model B only provides two. On the Pi Zero, the USB port is also connected directly to the SoC, but it uses a micro USB (OTG) port. Unlike all other Pi models, the 40 pin GPIO connector is omitted on the Pi Zero, with solderable through-holes only in the pin locations. The Pi Zero WH remedies this.

6.2 RFID Reader and Tag

Radio-frequency identification (**RFID**) use electromagnetic fileds to automatically identify and track tags attached to objects. An RFID system consists of a tiny radio transpoder, a radioreciver and transmitter. When triggered by an electromagnetic interrogation pulse from a nearby RFID reader device, the tag transmits digital data, usually an identifiying inventory number back to the reader. This number can be used to track inventory goods.

Passive tags are powered by energy from the RFID reader's interrogating radio waves. Active tags are powered by a battery and thus can be read at a greater range from the RFID reader, up to hundreds of meters.

Unlike barcode, the tag does not need to be within the line of sight of the reader, so it may be embedded in the tracked object. RFID is one method of AIDC.

RFID tags are used in many industries. For example, an RFID tag attached to an automobile during production can be used to track its progress through the assembly line, RFID-tagged pharmaceuticals can be tracked through warehouses, and implanting RFID microchips in livestock and pets enables positive identification of animals. Tags can also be used in shops to expedite checkout, and to prevent theft by customers and employees.

Since RFID tags can be attached to physical money, clothing, and possessions, or implanted in animals and people, the possibility of reading personally-linked information without consent has raised serious privacy concerns.[2] These concerns resulted in standard specifications development addressing privacy and security issues.

6.3 Finger Print Sensor

Everyone has patterns of friction ridges on their fingers, and it is this pattern that is called fingerprints. Fingerprints are uniquely detailed, durable over an individual's lifetime, and difficult to alter. Because there are countless combinations, fingerprints have become an ideal means of identification.

There are four types of fingerprint scanners:[1] optical scanners, capacitance scanners, ultrasonic scanners, and thermal scanners. The basic function of every type of scanner is to obtain an image of a person's fingerprint and find a match for it in its database. The measure of the fingerprint image quality is in dots per inch (DPI).

Optical scanners take a visual image of the fingerprint using a digital camera.

1. **Capacitive or CMOS scanners** use capacitors and thus electrical current to form an image of the fingerprint. This type of scanner tends to excel in terms of precision.
2. **Ultrasonic fingerprint scanners** use high frequency sound waves to penetrate the epidermal (outer) layer of the skin.
3. **Thermal scanners** sense the temperature differences on the contact surface, in between fingerprint ridges and valleys.

All fingerprint scanners are susceptible to be fooled by a technique that involves photographing fingerprints, processing the photographs using special software, and printing fingerprint replicas using a 3D printer.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

6.4 Motor

Electric motor is an electrical machine that converts electrical energy into mechanical energy. Most electric motors operate through the interaction between the motor's magnetic field and electric current in a wire winding to generate force in the form of torque applied on the motor's shaft. An electric generator is mechanically identical to an electric motor, but operates with a reversed flow of power, converting mechanical energy into electrical energy.

Electric motors can be powered by direct current (DC) sources, such as from batteries, or rectifiers, or by alternating current (AC) sources, such as a power grid, inverters or electrical generators.

Electric motors may be classified by considerations such as power source type, construction, application and type of motion output. They can be powered by AC or DC, be brushed or brushless, single-phase, two-phase, or three-phase, axial or radial flux, and may be air-cooled or liquid-cooled.

Standardized motors provide convenient mechanical power for industrial use. The largest are used for ship propulsion, pipeline compression and pumped-storage applications with output exceeding 100 megawatts.

Applications include industrial fans, blowers and pumps, machine tools, household appliances, power tools, vehicles, and disk drives. Small motors may be found in electric watches. In certain applications, such as in regenerative braking with traction motors, electric motors can be used in reverse as generators to recover energy that might otherwise be lost as heat and friction.

Electric motors produce linear or rotary force (torque) intended to propel some external mechanism, such as a fan or an elevator. An electric motor is generally designed for continuous rotation, or for linear movement over a significant distance compared to its size. Magnetic solenoids are also transducers that convert electrical power to mechanical motion, but can produce motion over only a limited distance.

Electric motors are much more efficient than the other prime mover used in industry and transportation, the internal combustion engine (ICE); electric motors are typically over 95% efficient while ICEs are well below 50%. They are lighter, physically smaller, mechanically simpler and cheaper to build, more durable, can provide instant and consistent torque at any speed, can run on electricity generated by renewable sources and do not emit carbon into the atmosphere. For these reasons electric motors are replacing internal combustion in most applications.

6.5 Buzzer

A **buzzer** or **beeper** is an audio signaling device,[1] which may be mechanical, electromechanical, Typical uses of buzzers and beepers include alarm devices or timer and confirmation of user input such as a mouse click or keystroke.

6.5.1 Types

6.5.1.1 Electro Mechanical

Early devices were based on an electromechanical system identical to an electric bell without the metal gong. Similarly, a relay may be connected to interrupt its own actuating current, causing the contacts to buzz (the contacts buzz at line frequency if powered by alternating current) Often these units were anchored to a wall or ceiling to use it as a sounding board. The word “buzzer” comes from the rasping noise that electromechanical buzzers made

6.5.1.2 Piezoelectric

A piezoelectric element may be driven by an oscillating electronic circuit or other audio signal source, driven with a piezoelectric audio amplifier. Sounds commonly used to indicate that a button has been pressed are a click, a ring or a beep. A piezoelectric buzzer/beeper also depends on acoustic cavity resonance to produce an audible beep.

VII. Literature Survey

7.1 Anti-Theft Mechanisms in ATM Centres Using Different Sensors

Even though there are various sensors accessible, the security issues are still not captured. Its developing with new innovation creation. Pulse sensors is by all accounts powerful for execution which can recognize the burglary interruption effortlessly and can alert closest police headquarters or encompassing zone of ATM focuses all together to catch the aggressor. In future, I trust this may be conceivable with upgraded innovation.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

A. Merits

Increasing security in internal and external. Different types of sensor are used

B. Demerits

If we are using different type of sensor, we cannot get the exact information about person.GSM module to send message, So immediately cannot get the solution.

7.2 Smart ATM Security Using IoT

Based on the results obtained, the objective of implementing ATM security system using GSM & vibration sensor has been achieved. This project is used to provide security to ATM. Whenever a person tries to distract the ATM, the sensor which senses the vibrations & send a signal to the microcontroller. Once the controller receives signal, it locks the door of ATM room by sending signal to the dc motor and sprinkler sprinkles the chloroform to make the thief unconscious. At the same time, the buzzer also gets activated. Simultaneously, the controller will provide the status of ATM machine whether it is working or out of order with the of the YELLOW and RED LED lights.

Merits

Increasing security using fingerprint sensor .To find the theft using vibration sensor

Demerits

We are using vibration sensor, so we cannot get the exact information about person.

7.3 RFID and GSM based ATM Money Transfer Prototype System

This whole implementation ensures us a secured and authenticated transaction through RFID and GSM technique with lowest cost and minimum maintenance. Mankind will utilize new and secured type of money transactions. The only thing is that initial cost of RFID conversion of the entire system is the required one time investment. Account holder will utilize atm card by entering password through his predefined mobile number for bank. The value added service that this system provides increases the credibility of the financial institutions, the banks improves the convenience to its customer. Hence as the world progresses through the inevitable and an indomitable quest for knowledge, the aspect of security bound systems are bound to concede with the growing innovations and obviously more vulnerabilities. Hence our application might well solve the aspect of transaction security to a precise and great extent.

Merits

Increasing security using RFID. The notification and OTP send to respective person and buzzer alert provided.

Demerits

If we missing the RFID tag, Other person easily withdraw our money. Anytime to carry the RFID tag.

7.4 Anti-Theft Mechanisms in ATM Centres Using Different Sensors

This project is developed on the basis of more need of security in ATM banking system. Now-a day's ATM is getting less secure with emerging ways to hack/crack ATM PIN or ATM card. The ATM user's cash transaction is secured by adding the RFID reader, Tag and OTP to the existing system. The individual with the RFID tag can tap the tag along with individual must have to type the OTP generated to enter the door and to stats the system. This constraints helps to improve the safer transaction of clients Along with this ATM system is also secured. 1f rom the fraud attacks by using the Metal sensor and IR Sensor.1if any unauthorized person try enter the system and even carrying any metal objects thus immediately process gets terminated and security voice commands given by the speaker module. This ensures safety of the both ATM machine and the clients. So it has been able to prove that the RFID based ATM is practicable and could be implemented in the security of ATM systems.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

Merits

Increasing security using RFID. The notification and OTP send to respective person and buzzer alert provided. The metal is detected alert the system using metal detector sensor.

Demerits

If we missing the RFID tag, Other person easily withdraw our money. Anytime to carry the RFID tag. The IR sensor can detect all the obstacle, so exactly get the information.

7.5 Anti-Theft Mechanisms in ATM Centres Using Different Sensors

The growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. Access codes for buildings, banks accounts and computer systems often use PIN's for identification and security clearances. Conventional method of identification based on possession of ID cards or exclusive knowledge like a social security number or a password are not all together reliable. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Despite warning, many people continue to choose easily guessed PIN's and passwords birthdays, phone numbers and social security numbers. This paper may solve this problem and useful for detecting a fraud . It is used in Bank sector and any ATM related security. It is also called as thief tracking system. As there is a scope for improvement and as a future implementation we can add a tracking chip on ATM card for tracing the location of card which will help in providing users assistance.

Merits

Increasing security using camera. The buzzer alert provided.

Demits

In this paper only theft is identified.

VIII. Inference from Literature Survey

We concluded that this literature survey Security and theft is identified. The security is less secure because of using RF Technology. In proposed system using Double layered security using RF and Fingerprint Verification.

The paper proposes the idea of an ATM system with multilayer security that provides protection against both physical ATM counter attacks and ATM related fraud attacks. The components used and connection between individual components in proposed system. The working of the proposed system is described under authentication and monitoring sections which help to prevent ATM related fraud attacks and physical attacks respectively.

IX. Limitations of Existing System

- If problem with credit card you cannot withdraw your money.
- If someone watches or hacks an ATM machine your details may be taken if you forget your PIN number you cannot use the card.
- Cannot be provided in rural areas: In a country like India, where banks are having large number of rural and non-computerized branches, ATM services cannot be provided.
- Limitation of cash withdrawals: Again there is a limitation of cash withdrawals from ATM. For example, many banks do not permit withdrawal of more than 25,000 at a time.
- Cash deposit facility is not safe: Similarly cash deposit facility is restricted and not safe as dropping of envelope and ATM is not advisable.
- Possibility of misusing ATM card: ATM card, if misplaced, lost or stolen, may be misused. There are number of such reported incidences now a day.
- Loss of personal touch with the Banks: Last but not the least; customers lose personal touch with their bankers.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

REFERENCES

[1]. Vikas Tripathi, Durgaprasad Gangodkar, Vivek Latta, and Ankush Mittal, "Robust Abnormal Event Recognition via Motion and Shape Analysis at ATM Installations", Journal of Electrical and Computer Engineering Volume 2015 (2015), 19 January 2015(https://www.hindawi.com/journals/jece/2015/502737)

[2]. http://www.ijera.com/special_issue/SCEVT/PART-1/N4850.pdf

[3]. A. Juels, "RFID Security and Privacy: A Research Survey, "RSA Laboratories, 28 September 2005.

[4]. "Secured ATM Transaction System Using Micro Controller" by Mrs. S. P. Balwir. Ms.K.R.Katole, Mr.R.D. Thakare, Mr.N.S.Panchbudhe, Mr.P.K.Balwir. International Journal of Scientific Engineering Research Volume 4, Issue 4, April 2014.

[5]. Kannamma, M. Barathi, B. Chanthini, and D.Manivannan. "Controlling and monitoring process in industrial automation using Zigbee." Advances in Computing, Communications and Informatics (ICACCI), 2013 International Conference on. IEEE, 2013.

[6]. Hong, L., Wan, Y. and Jain, A. Fingerprint Image Enhancement: Algorithm and Performance Evaluation.

[7]. IEEE Transactions on Pattern Analysis and Machine Intelligence,1998.

[8]. Bhanu Bir, Tan Xuejun, Computational Algorithms for Fingerprint Recognition.

[9]. Kluwer Academic Publishers, 20 Das, K. Design and Implementation of anEfficient Thinning Algorithm.