Suganthi.S. International Journal of Engineering Research and Applications
www.ijera.com
ISSN: 2248-9622, Vol. 12, Issue 5, (Series-I) May 2022, pp. 19-24

RESEARCH ARTICLE OPEN ACCESS

A Literature Survey on Automated Teller Machine [ATM] Theft Security Systems

Suganthi.S[1]
[1](*Assistant Professor, Department of Computer Science, Tagore Government Arts and Science College, Puducherry, India,605008).*

ABSTRACT
An automated teller machine (ATM) is an electronic banking outlet that permits customers to complete basic transactions without the assistance of a branch official. ATMs are convenient, allowing consumers to perform fast self-service transactions like deposits, cash withdrawals, bill payments, and transfers between accounts. Therefore, Automated Teller Machine (ATMs) security plays a vital role in day-to-day life, providing protection against physical and electronic theft from ATMs and protecting their installations is much considerable since people usage is increasing steadily now a days. This analysis paper principally deals with the implementation of security system in ATMs through totally different strategies to reinforce their safety.

Keywords **-** Automated Teller Machine, Intruder, Microprocessor, Security, Sensors

---

Date of Submission: 25-04-2022 Date of Acceptance: 07-05-2022

I. INTRODUCTION

Automated Teller Machines (ATM) provide valuable payback to the banks and also the customers. The ATMs allow bank customers to withdraw cash conveniently anytime and anywhere aside from actual bank location by automating few of banking transaction services. The customers also get real time assistance on other services like balance enquiry, short statement, application for cheque book, e-cash transfer to other account, and more to customers. How, and by whom, these services are to be used it decide by bank and people. There are two forms of automated teller machines (ATMs). The fundamental one allows the customer to only draw cash and receive a report of the account balance. Another one could be more complicated machine that accepts the deposit, provides credit card payment facilities and reports account information.

1.1 History of ATM

For many, this was the primary tangible evidence that retail banking was changing; the introduction of the ATM marked the dawn of latest digital banking. In 1960, an American named Luther George Simjian invented the Bankograph, a machine that allowed customers to deposit money and checks into it. The primary ATM was set upon in June 1967 on a street in Enfield, London at a branch of Barclays bank. A British inventor named John Shepherd-Barron is attributable with its invention. The machine allowed customers to withdraw a maximum of GBP10 at that moment. In 1970, a British engineer, James Goodfellow, proposed the idea of a personal identification number (PIN), which machine-driven verification of the identity of customers, therefore marking a landmark moment within the growth of self-service banking. In 1977, National Register, a software and technology company within the U.S., launched the NCR Model 770, an easy-to-operate ATM that allowed the banks to supply services 24/7. The advanced model (5070 ATM) launched in the early 1980s proved to be more reliable, flexible, and customer-friendly. By 1984, the sum of ATMs installed worldwide totalled a hundred thousand. In India, the development of ATMs was lethargic as a result they were launched in the early 1990s to the Indians and favoured through foreign banks. As of 2018, there have been than 3 million ATMs operational round the world. According to the consulting firm, Retail Banking analysis, that figure is projected to cross four million by 2021. Even though digital payment services are gaining popularity in the 21st century, money still is the popular transaction mode in most parts of the world. ATMs, bank branches, mobile banking, and net banking are expected to enrich one another within the predictable future.

1.2 Block diagram of ATM

The block diagram of the automated teller machine consists of primarily 2 input devices and 4 output devices. The input devices like card reader and keyboard while the output devices are speaker, display screen, receipt printer, and cash depositor. The card reader is an input device that gathers data from a card. It is a part of the recognition of your specific account number and the magnetic strip on the posterior side of the ATM card is utilized for connection with the card reader. The card is swiped or pressed on the card reader which arrests your account. The host processor thus uses this information to get the data from the cardholders. Each card has a distinctive PIN in order that there is very little chance for someone else to withdraw cash from your account. There are separate laws to defend the PIN code while sending it to the host processor. The PIN is often sent in encrypted form.

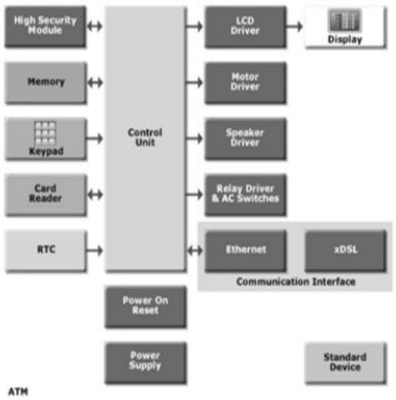


Fig.1 Block Diagram of ATM

The speaker produces audio feedback when a particular key is pressed. The display screen opens the transaction information. Each step of withdrawal is displayed by the display screen. A CRT screen or LCD screen is employed by most of the ATMs. The receipt printer prints all the details reporting your withdrawal, date and time, and the amount of withdrawal and also displays the balance of your account in the receipt. The cash dispenser is a fundamental system of the ATM from where the desired money is obtained. From this portion, the user can collect the cash. The cash dispenser must count each bill and give the appropriate amount. All these actions are executed by high precision sensors.

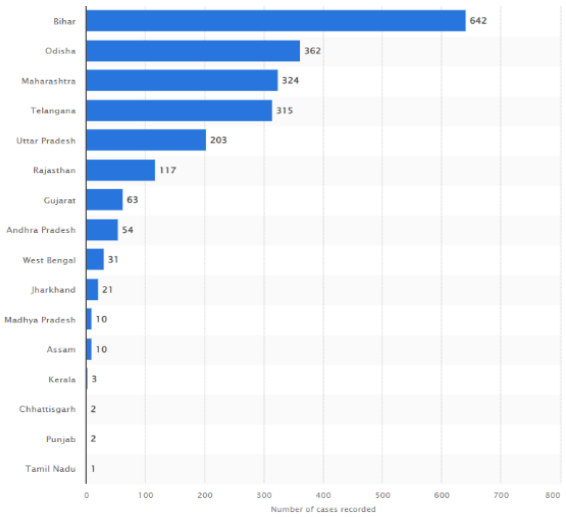
1.3 Working Principle of ATM

The automated teller machine is commonly a data terminal with two inputs and four output devices. These devices are incorporated with the processor. All the ATMs operating round the world are established on a centralized database system. The ATM should associate and communicate with the host processor (server). The host processor is corresponding with the internet service provider (ISP). It is the portal through all the ATM networks accessible to the cardholder. Once a cardholder wants to do an ATM transaction, the user provides essential information through a card reader and keypad. The ATM forwards this data to the host processor. The host processor enters the transaction demands to the cardholder bank. If the cardholder demands the money, the host processor takes the money from the cardholder's account. Once the funds are transferred from the customer account to the host processor bank account, the processor sends the confirmation code to the ATM and also the approved machine to dispense the cash. The ATM network is completely based on a centralized database environment.

II. SECURITY OF ATM

The first decade of the 21st century saw a increase within the number of ATM frauds via sophisticated malware or technologies, like skimming devices. To remain one step ahead, banks developed advance software that could identify anomalies in transactional data that hint towards criminal activity.

In 2020, the state of Bihar in India had the maximum number of ATM fraud offences recorded, with more than 642 cases registered with the authorities. The country recorded over 2000 cases associated to ATM frauds that year. This class of crime came below the purview of Sections 420 of the Indian Penal Code.



Source: Statista 2022

Fig.2 Number of ATM fraud incidents reported across India in 2020

Banks in India have lost 2.35 billion of money within the last five years to incidents of burglary, robbery, dacoity and theft. The number has been intensifying since 2013-14 when 587 such cases were recorded, amounting to a loss of Rs 343 million. In 2017-18, 972 cases of theft and burglary were reported, a rise of 65 per cent, resulting in a loss of Rs 444 million. RBI has informed that it has suggested banks to review and strengthen the safety arrangement in their branches and ATMs to handle with instances of theft, etc. and for dealing with risk awareness emerging from such incidents. These include coverage of branch/ATM by CCTVs and establishing adequate guidance of security staff. Additionally, RBI has also been forwarding suggestions for advancement, received from police authorities in this regard to banks for review and adoption," said Minister of State for Finance Shiv Pratap Shukla in Parliament. Seven years ago, the Delhi police entered the Limca Book of Records for repairing one of the largest cash robbery cases in India. On 27 November 2015, they chased down the driver of a cash transport van who drove away with over Rs 2.2 million cash.

ATMs work on advanced network systems and a lot of information processing is involved during a transaction. They have an operating system to accomplish various functions, Windows OS being the most familiar one. However, criminals have found ways in which to use vulnerabilities of those systems, thus logical attacks on ATM technology are promptly increasing and posing a serious threat. Therefore, proper enhancements in the logical security of ATMs and their significance become vital. Some of the measures that can help enhance ATM security are mentioned below which are also suggested by high-level professionals from this domain.

- Ensure proper encryption.
- Regular Updating of the software.
- Install a firewall.
- Define roles for access.
- Establish password policy.
- Conduct regular security tests.
- Deploy proper anti-malware/protection software.

While most of us can use an ATM while not having something bad happen, some criminals prey upon ATM users. Here are six tips for keeping yourself protected at an ATM:

1. Use an ATM at a public place. Try to excort clear of ATMs in isolated, poorly lit spots. Rather, Utilize an ATM where there are other people around, such as a grocery store, or where there's plenty of light.
2. Concentrate to your surroundings, especially at night. If you see anyone or anything doubtful, use an ATM at a different location.
3. When you're at an ATM, don't calculate or show the money you've just withdrawn. This might cause you a major target for a thief.
4. Cover your PIN. Do what you can like using your hand or body as a shield to avoid someone standing close to you from seeing you enter your PIN.
5. Watch out at drive through ATMs. If you're using a drive-through ATM, confirm your car doors are secured and your car windows are rolled up, and keep the engine running.
6. Be careful for card skimmers. A card skimmer is a device which can be installed on an ATM to steal card numbers once cards are inserted into a card reader. It's challenging to see a card skimmer right away. However, a card skimmer could be attached to the ATM if the card reader position feels loose, the colour of the reader will not match the ATM's colour scheme or the keyboard doesn't feel right (such as the keyboard buttons' being difficult to press).

III. METHODS

The following are some methods that were used to protect the ATMs from thefts. Most of them are based on microprocessor.

3.1 Monitoring ATM using K-Band Doppler Radar

A Doppler radar is used to supervise human activities and with the aid of gas sensor we can identify the toxic gases like carbon monoxide, nitrogen oxides etc. Here RFID module is employed to enhance the security and more efficient than magnetic cards. The coverage area of Doppler radar is exceeding PIR sensor. Therefore, the coverage area of Doppler radar is 360 degrees. Vibration sensor is used to defend the machine from strangers. Arduino mega R3 board is utilized in this system since it is an open-source hardware and software. The advantage of using radar is that it will sense person movement behind the items also (i.e.) wall, doors etc. The entering of an authorized person using RFID reader is implanted on the outside of the shutter and is isolated from the main controller unit. The controller accepts the serial data from the reader and manage the door. The RFID tag is kept near the RFID reader it receives the data over electromagnetic induction. Then it matches this information with the program memory. The door opens for authorized person only. Vibration sensor sense the vibration from ATM machine and therefore warning alarm is activated using buzzer and SMS is delivered to authorized person.

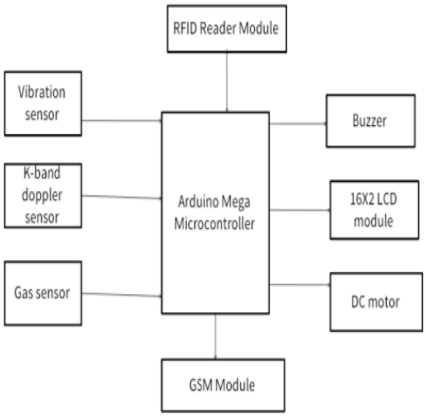


Fig.3 Block Diagram of monitoring ATM using K-Band Doppler Radar

3.2 Smart ATM using Arduino

The vibration sensors will provoke a signal whenever somebody tries to vigorously open or damage the ATM machine. Once the detection of such signal immediately, a message will be sent to the authorized person of the bank, making him/her conscious of the situation. Also, we are utilizing a wireless camera, so that in such cases, authorized person can watch the live footage of the ATM facility onto his/her mobile phone. Whenever somebody tries to cause destruction or want to lift the ATM machine from its place, consequently vibration sensor attached to the ATM machine will be activated and sends a signal to controller. When the controller obtains the signal, it locks the door of ATM by the rotation of motor, and will deliver a message to assigned authority about the theft occurring through GSM modem. After this the sprinkler (DC Pump) installed within the ATM will get activated and it will spray the chloroform chemical which causes the person unconscious and at the same time buzzer will be activated.

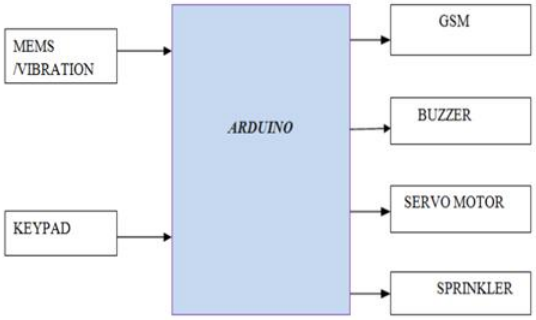


Fig.4 Block Diagram of Smart ATM using Arduino

When the incorrect pin entered for the first-time the buzzer will beep and message would be sent to the account holder. When the incorrect pin is entered for the second time, an intimation through voice module will be observed. When the incorrect pin is entered for every third time consequently doors will be closed by using servo motor. Additionally, message will be sent to the account holder; on the opposite hand, if any tilt is occurred in ATM machine, then spray instrument will be activated. It can also produce the status of ATM machine by presenting red and yellow signals.

3.3 ATM theft monitoring using Raspberry pi

The infrared sensor is employed while human efforts are made to unseal a money locker. Whenever a sensor moves an element, the door will be locked automatically. The IR sensor is installed at the money locker as the barrier passes over the IR sensor, then it transfers the data to Raspberry Pi through the GPIO pins. We tend to use the camera to recollect the face. Using the Servo motor to open and close the door. If all of these sensors are temperature-like, IR will turn on a buzzer to warn the sound, and therefore resulting alert message will

be transmitted to the authorized person. Additionally, if somebody manages to open the money locker, the gas is sprinkled on the thief to render him unconscious. Whenever a person enters the ATM centre to use ATM facilities within the ATM, the camera records the person's image and checks the stored information when the image fits, the door is either opened or closed. L293D is a typical 16 pin IC engine driver.

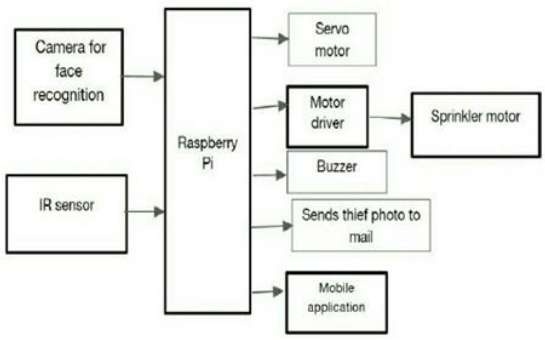


Fig.5 Block Diagram ATM monitoring using Raspberry Pi

As the name proposes, it is mainly used to drive the engines. We used DC motors to close and open the ATM door. The DC motor power supply is provided as 12VDC to manage it. An electrical mechanism which will drive or rotate the object very precisely is the servo motor. Use a servo motor if you prefer to rotate an object at a certain angle or size. The infrared sensor is an electronic instrument used to identify certain properties of its surroundings. It does this by here by transmitting or sensing infrared radiation. DHT 11 (Temperature Sensor) is an economical optical sensor for temperature and humidity sensing. Buzzer is a digital structure and raspberry pi in need of enough current to drive circuits like flag exchange circuits.

3.4 Anti-theft ATM using Embedded system

We were compiling the SD card interfaced to the microcontroller within which the data of the sensor values are stored including time and date. Here, we are using the Gas sensor, Vibration sensor, PIR sensor. If any of the sensors switches on, then buzzer will alert sound and automatically an alert message will be sent to the authorized person. Likewise, we are using the SD card to store the sensor values in that for every specific time period. If the Gas was leaked within the ATM, then the gas sensor activates and triggers the relay to spray to disable the gas. Like that if remaining sensor activates, the alert message will be sent to authorized person. The LPC2148 microcontrollers are based on a 16-bit/32-bit ARM7TDMI-SCPU including real-time emulation and embedded trace support, that incorporate the microcontroller with embedded high-speed flash memory ranging within 32 kb to 512 kb. A 128-bit wide memory interface and specific accelerator architecture implement 32-bit code execution at the maximum clock rate.

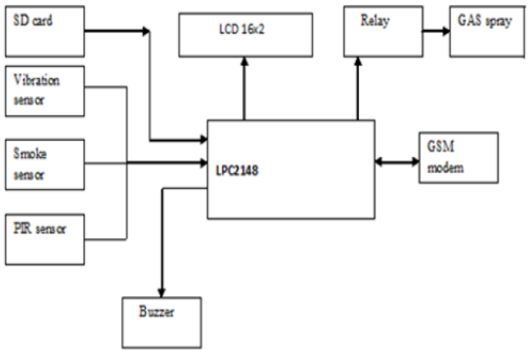


Fig.6 Block Diagram Anti-theft ATM using LPC2148

Serial communications interfaces starting from a USB 2.0 Full-pace material, numerous UARTs, SPI, SSP to I2C-bus and on-chip SRAM of 8 kb up to 40 kb, causes these devices very well suitable for communication portals and protocol converters, soft modems, voice recognition and low-end images, implementing both large buffer size and huge processing power. Numerous 32-bit timers, mono or dual 10-bit ADC(s), 10-bit DAC, PWM channels and 45 speed GPIO lines with up to 9 sensitive external interrupt pins causing these microcontrollers suitable for industrial control and medical systems.

IV. CONCLUSION

As we all know, these days utmost of the ATM has been invaded by the robbers. Also, gradual increases the theft of ATM after the year by year. In this research paper, we have given brief summary about the implementation of security system for Automated Teller Machine by different authors. Here the security has been enhanced by using some sensors and microprocessor, the information of the intruder will be collected using different methods.

REFERENCES

[1] R. Sathya, C. Pavithra, T. Santhiya, Ms. L. Revathi, "Design and Implementation of ATM Theft Monitoring System using K-Band Doppler Radar", *International Journal of Advanced Research in Computer and Communication Engineering [IJARCCE]*, Vol. 8, Issue 2, February 2019.

[2] PNB Swamy, A. Sathi Babu, S. Sravanthi, P. Sasidhar, MD. Mobin ul haq, P. Narendra,

"Smart ATM Security Using Iot", *IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)*, Volume 15, Issue 3, June 2020

[3] Kanchan P. Borade, Shewale Pooja J, Tayade Dipika P, "ATM Theft Monitoring and Security System using Raspberry Pi2", *International Journal of Engineering and Advanced Technology (IJEAT)*, Volume 6, Issue 3, February 2017

[4] K. Hema Sai Sivaprasad, Mr. B. Kanna Vijay, "Design and Implementation of Anti-Theft ATM Machine Using Embedded Systems", *International Journal and Magazine of Engineering, Technology, Management and Research [IJMETMR]*, Volume 3, Issue 11, November 2016

[5] Ajaykumar M (2013), "Anti-Theft ATM Machine Using Vibration Detection Sensor" *International Journal of Advanced Research in Computer Science and Software Engineering*, pp: 23-28.

[6] Raj, M. M. E., Anitha Julian, "Design and implementation of anti-theft ATM machine using embedded systems", *International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015]*, pp. 1-5, 2015.

[7] Narmada, D., and J. V. Priyadarsini, "Design and implementation of security-based ATM using ARM11", *International Conference on Inventive Computation Technologies (ICICT)*, Volume 3, pp. 1-4, 2016.

[8] Ravichandran, S, "Cloud connected smart gas cylinder platform senses LPG gas leakage using IOT application" *International Journal of MC Square Scientific Research*, Volume 9, Issue 1, pp. 324-330, 2017.

[9] https://en.wikipedia.org/wiki/Security_of_automated_teller_machines

Suganthi.S. "A Literature Survey on Automated Teller Machine [ATM] Theft Security Systems." *International Journal of Engineering Research and Applications (IJERA)*, vol.12 (05), 2022, pp 19-24.