Utilizing the Internet of Things, Monitoring and Protecting System for Automated Teller Machines

Mohammad Naveed Hossain
Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
naveedhossain99@gmail.com

Md. Shaba Sayeed
Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
shaba.sayeed@gmail.com

Sheikh Fahim Uz Zaman
Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
sheikh.fahim.zaman@gmail.com

***Abstract*—For the vast majority of people in modern society, ATMs are the preferred method of cash withdrawal. ATM robberies have happened even in locations where CCTV cameras are installed at the ATM facility. The security mechanism will need to be tweaked. To combat these types of robberies, we developed a theft protection system for ATMs that makes use of cutting-edge technology. This system also looks at various physical assaults using ATMs. The device we propose to utilize to take an image of the individual entering the system is a Face Recognizing Camera. Anomaly behavior at an ATM can be detected using sensors that measure tilt and vibration. Any strange conduct will be detected by the LED light and buzzer, which will alert security personnel, the ATM machine will act like money withdrawing. Our system's main goal is to send out a warning via email or other social media. IoT and GSM networks are used by both Facebook and Instagram. An alert will sent to the security force and a fake transaction process will be set to confuse the suspect. To avoid the unwanted incident after a certain time some anesthetic gas will be released, to make the suspect unconscious. Monitoring and control are now become easier because to this technology.**

***Index Terms*—component; ATM; IoT; GSM; Tilt sensor; Face Recognition;**

I. Introduction

Automated Teller Machine (ATM) security systems are intended to provide many levels of protection against ATM theft, both electronically and physically, as well as safety for ATMs when they are installed. The change is depicted by automated banking machines. This is known as a Medication-Assisted Treatment, and it enables customers of a financial institution to conduct their own financial transactions, including cash withdrawals. Customers may now utilize this technological and telecommunications technology as an alternative to interacting with a real person. Globally, almost 5 million ATMs are in operation (ATMs). In addition to the more common uses of automated teller machines (ATMs), cardholders in Bangladesh can transfer money instantaneously, pay bills, order food or products, and purchase mobile minute bundles via ATMs. Due to the fact that modern ATMs take both magnetic stripe and chip cards, which carry a unique card number and extra security data such as the expiration date or CVV (last three numbers on the back of the card), the machine can instantly authenticate the user's identification (CVV). [8] When a consumer inputs their personal identification number (PIN), it must match the PIN stored on the chip of their credit card or in the financial institution's database. Customers may, for instance, use ATMs to withdraw money from their bank accounts, check their account balances, or recharge their mobile phones. Because ATM terminals cannot be physically attacked and dispenser mechanisms are employed, conventional ATM security measures are viewed as being more effective than newer technology. [12] At least one heist is necessary to clear the neighborhood of those who would steal from that ATM. In the present day, ATM security is dependent on a variety of Intelligent Automated Systems. Due to the usage of these methods to determine whether or not the user is a thief, an ATM robber will be unable to withdraw cash. Our proposed solution for ATM networks includes the installation of various monitoring sensors, a GSM module, and the dissemination of current status information via social media. By employing this strategy, our likelihood of being robbed at an ATM is diminished.

II. Existing Model

A. Automated Teller Machine

By connecting the national identity number to our bank account while using an automated teller machine, we may eliminate contacts with bank workers and consumers (ATM). A number of financial operations, including cash deposits and withdrawals, fund transfers, and account information, can be completed via an automated teller machine.

A customer can do basic financial transactions using an automated teller machine (ATM) without the aid of a bank employee. Two types of automated teller machines can be distinguished (ATMs). [2] In the most fundamental form, customers can simply withdraw cash and get a statement of their account balance. A more complex gadget is also available, which not only accepts deposits but also accepts credit card payments and monitors account balances.

1) ATM Networking: ATMs also rely heavily on Internet service providers (ISPs). Using this, ATM and host CPU data may be exchanged. The cardholder provides the necessary information during the transaction. The ATM sends this data to the host processor. An recognized financial institution confirms this information. The host processor provides a permission

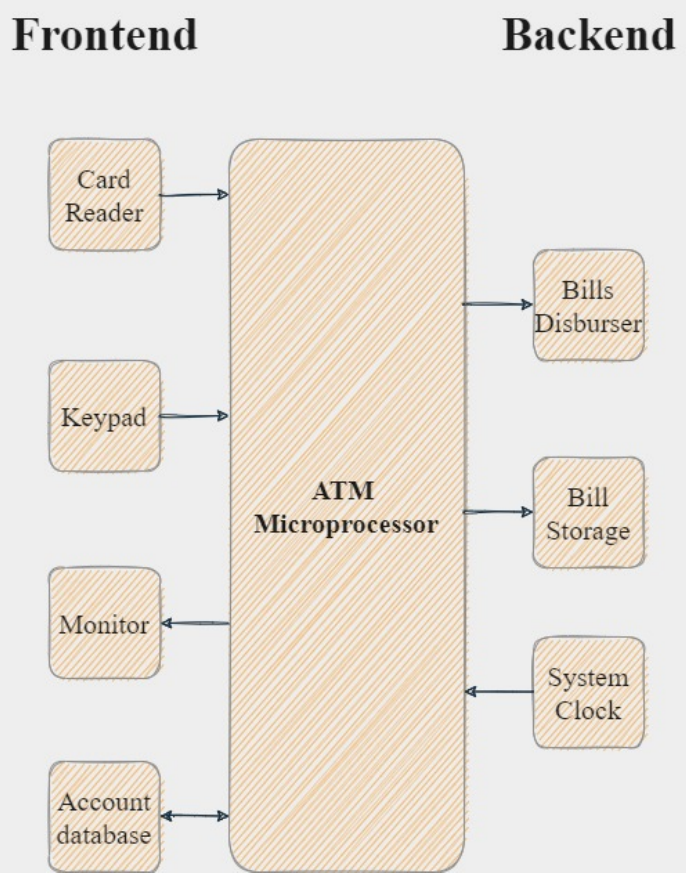

Fig. 1. Block Diagram of ATM

code to the machine if the information is accurate, allowing the transfer of funds to proceed.

2) ATM Working Principle: There are two inputs and four outputs on the automated teller machine. The CPU communicates with these devices. The ATM's beating heart is the CPU. There is a centralized database system that powers all ATMs across the world. The ATM must establish a connection with the host processor and exchange data with it (server).

The internet service provider and the host processor are in communication (ISP). [4] The cardholder may access any ATM in the world through this one point of entry. A cardholder uses a card reader and a keypad to enter the necessary information for an ATM transaction. [3] The host processor receives this information from the ATM. This is done by the host processor, who sends a request to the card holder's bank.

The host processor takes the cash from the card holder's account if the cardholder wants the cash. Cash is disbursed to an ATM or other approved machine after funds have been moved from a customer's account to a bank account at a host processor. This is how you withdraw cash from an ATM. Centralized databases underpin the ATM network in its entirety. Money and convenience will be gained as a result of this move.

To begin, go to a local ATM and insert the card into the machine. Choose the language that will be shown on the ATM monitor, such as native tongue or English. Various transactions like as money transfers, withdrawals, and deposits can be selected via a drop-down menu. Select a savings or current account type. To make a withdrawal, Need to provide your 4-digit ATM pin number and the desired withdrawal amount. To get your receipt, gather the money and do so. Selecting the option will allow you to carry out more transactions. [5] [6]

III. Proposed Model

Camera sensor- The camera sensor is utilized to identify the account holder by recognizing their face. A face recognition system can be either a computer program or a biometric approach that is used for automatically detecting individuals based on their faces.A person from within the confines of a picture or video frame. This could also be achieved by the application of a variety of methods such as movement of the individual, the skin tone, or the fuzzy human features and forms. The camera that is installed inside of the ATM can recognize individuals' faces. The automated teller machine will not function properly if either the person's face is not captured or the person's identity is incorrect. Another thing that we can do to make the system work more effectively is to create a local server that stores all of the information pertaining to the clients.

Card reader - The magnetic stripe on the back of an ATM/debit or credit card is scanned by the card reader, which then transmits the information to the appropriate database. This information is utilized by the host processor in order to direct the transaction to the bank associated with the cardholder.

Keypad: Customers use the keypad to enter information, such as their personal identification number (PIN), the type of transaction they want to do, and how much they want to do it for. With the keypad, the cardholder can tell the bank what kind of transaction is needed (cash withdrawal, checking balance, etc.) and how much money is needed. Also, the card holder's personal identification number (PIN) is needed for the bank to check. Federal law says that the PIN block must be sent in encrypted form to the host processor.

Monitor - It enables real-time analysis of the ATM health status, cash levels, and consumable levels, and it creates alerts, warnings, and information for proactive management of the ATMs based on the business rules that have been set. The interactive LCD display screen, also known as an LCD display monitor, is one of the essential components that may be found in automated teller machines, video teller machines, and other types of bank self-service kiosks. The screen display guides the cardholder through each stage of the transaction process with on-screen instructions. Displays known as cathode ray tubes (CRTs) may often be either monochrome or color on leased-line devices. LCD displays, either monochrome or color, are typically utilized in dial-up equipment. Account Database - Users of the ATM database system have the ability to perform cash transactions, see information about their accounts, and even change their passwords online. [10] To accomplish one's tasks at the bank, it is not necessary to be physically present at either location.

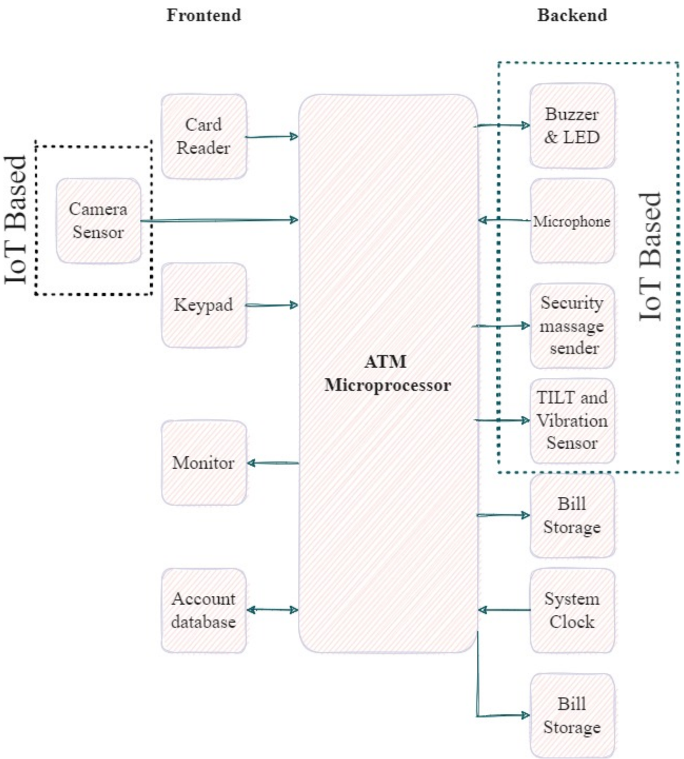

Fig. 2. Block Diagram of ATM

Bill Storage- Inside the ATM machine there is storage of the receipt we used for transaction.

Bill Distributor- The receipt printer provides the cardholder with a paper receipt of the transaction.

System clock- The clock speed, measured in gigahertz (GHz), is the number of cycles that your central processing unit (CPU) completes in one second (gigahertz). In computer science, a ”cycle” refers to a pulse that is synchronized by an internal oscillator. However, for our purposes, cycles are simply a fundamental unit that helps us comprehend the speed of a CPU. An architectural model for event timing, process duration manipulation, and system synchronization, the ATM system clock is a component of the architecture of the system.

Buzzer and LED - This system includes a buzzer that will sound when there is an alert for a false intersection. The LED will also light up. It is the authority at the main office that will be notified by the led and buzzer, not the attendant in the ATM booth.

Security message sensor- When there is even the slightest possibility of fraud, the security message sensor goes on. The security message sensor will send a message to the original account holder's cell carrier and social media account if it detects suspicious activity.

Microphone sensor – The sensors will give the cardholder auditory input that sounds like a fake, but it will actually be a fake.

Tilt Vibration Sensor - By utilizing tilt sensors, this system is able to provide additional information on the vibration that is occurring at the machine. If the vibration is increased to a level that is greater than the value, notifications will be issued to the authorities to wake them up by vibration sensor.

IV. Workflow

The process starts with the a camera verification the user's face will be verified by the camera sensor. If the user's face is not clearly detected in the first step then the second step face verification will occur if the face is detected proper in stage one or in stage two the user can do the transition properly. If the user can not be detected in the second stage then he/she will be considered as the suspect. The system will send the notification to the real user's contact number and social media. If the real user acknowledges that it was a known person of the user and a safe person for transaction than the system will permit the user to do transaction. On the other hand if the real user acknowledges the suspect as unknown then the system will send a buzzer and LED signal to the security person near the ATM. To keep the suspect busy till the security arrive the ATM machine will generate a fake sound of transaction via microphone. After a few minutes if the suspect understands is a trap and do any types of serious activity like harassing or threat-hing the other user or employee. The chloroform gas will be diffused and make the suspects and other victim unconscious. The process is only for the safety of the victims cause if the suspect has any type of weapons then it might lead to a serious situation. The safety ratio of the chloroform will be maintained. When the suspect will become unconscious the

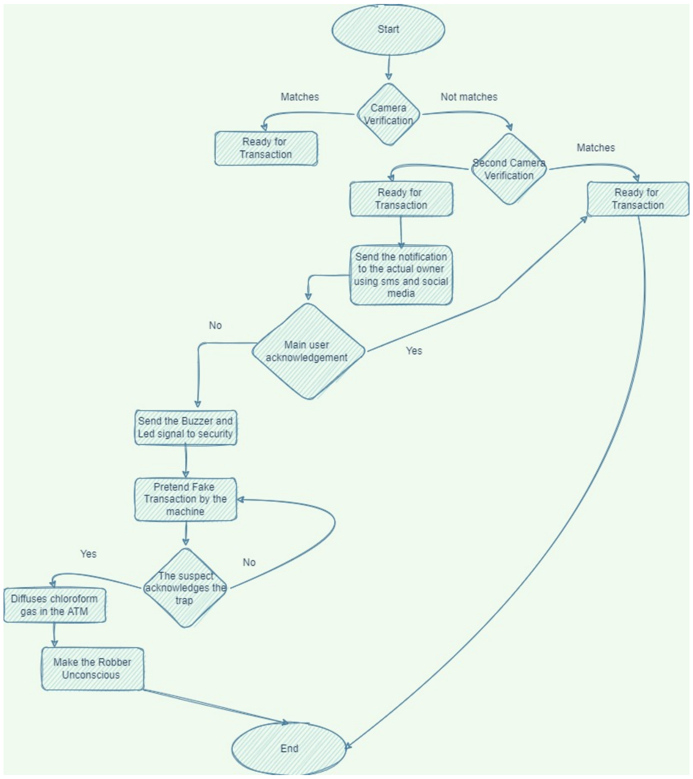
Start
Matches
Camera Verification
Not matches
Ready for Transaction
Second Camera Verification
Matches
Ready for Transaction
Ready for Transaction
Send the notification to the actual owner using sms and social media
No
Main user acknowledgement
Yes
Send the Buzzer and Led signal to security
Pretend Fake Transaction by the machine
Yes
No
The suspect acknowledges the trap
Diffuses chloroform gas in the ATM
Make the Robber Unconscious
End

Fig. 3. Workflow of the proposed model

police or the security service will take the necessary steps and victims should be sent for appropriate treatment.

V. Result and Analysis

In the first stage the face recognition process will take check the result in four steps. They camera sensor will capture the image of the user. It will extract the points of the face and compare those points with the database. If those point matrix's are same then the system will allow to go to the next step. Within 150ms this process will be completed. Only a few years ago, facial recognition was not nearly as accurate as it is now. According to tests conducted by the National Institute of Standards and Technology, the top face identification algorithm in 2014 had an error rate of 4.1 percent, but the best face identification algorithm as of April 2020 had an error rate of just 0.08 percent (NIST). [?] In our system the face recognition will occur twice so the possibility of error will be less. If the process is unsuccessful then the first work is to send a notification to the real user according to source it takes 1 second to send a notification to social media. The buzzer and LED signal will sent the notification with in 300ms. The sound of dummy transaction will continue till five minutes which will be enough for the security to take the necessary action. According to references we can consider the fact that the entire situation will take place with five minutes which is much quick for the suspect for taking any other illegal actions. If the suspect use any weapons or tries to threat any victims the chloroform gas will be spread using IoT. It will take two to five minutes to unconscious the suspect and the victim. If the chloroform is less than 50 ppm (244.43 mg/m^3) [15] will not do any serious impact in the health. Within 10 minutes all the process will be ended and compare to other methods its quick and simple.

VI. Conclusion

The ATM system is the most sophisticated networking system we've ever seen. Keeping such a complex system secure is the most difficult task. People are only now beginning to raise concerns about ATM security. Experts in the field of security are available to assist individuals with issues relating to ATM security and loss prevention systems. We'll need some time to find out how to achieve all of our security objectives. ATM's purpose is to create a platform for networking and communication. ATM security must be more adaptable and compatible with other solutions. This will help to ensure the safety of ATMs. Our technique, as previously said, is controlled by Arduino. It protects goods from theft and human intervention with the use of sensors that detect things like temperature, vibration, and tilt. As a result, our system does not require constant monitoring, does not keep a large amount of undesired video footage, and only sends out information when anything goes wrong. If the system detects a danger, for example, it can swiftly shut down the ATM.

References

[1] Sharma, N., Panwar, D. (2021). Advance Security and Challenges with Intelligent IoT Devices. In Proceedings of Second International Conference on Smart Energy and Communication (pp. 177-189). Springer, Singapore.

[2] Parab, A., Nikam, A., Mogaveera, P., Save, A. (2020, March). A new approach to detect anomalous behaviour in ATMs. In 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS) (pp. 774-777). IEEE.

[3] Ullah, W., Ullah, A., Hussain, T., Khan, Z. A., Baik, S. W. (2021). An Efficient Anomaly Recognition Framework Using an Attention Residual LSTM in Surveillance Videos. Sensors, 21(8), 2811.

[4] Divya, U. H., Kumar, J. P. Detection of Abnormal Human Activities in Surveillance Video-A Survey. Journal of Interdisciplinary Cycle Research, 12, 929-935.

[5] Sharma, A. S. H. I. S. H., Varshney, N. E. E. R. A. J. (2020). Identification and detection of abnormal human activities using deep learning techniques. European Journal of Molecular Clinical Medicine, 7(4), 408-417.

[6] Murugan, K. S., Sudharsanam, V., Padmavathi, B., Simon, J., Jacintha, V., Sumathi, K. (2020, November). BER analysis of 40 Gbps Ro-FSO Communication System for 5 G applications under Fog Weather Conditions. In 2020 IEEE 7th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON) (pp. 1-6). IEEE.

[7] K H Shakthi Murugan, Sudharsanam V, Padmavathi B, Judy Simon, Jacintha V, Sumathi K, ”BER analysis of 40 Gbps Ro-FSO Communication System for 5 G applications under Fog Weather Conditions”, 2020 IEEE 7th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), pp.1-6, 2020.

[8] K. Gavaskar, U. S. Ragupathy, S. Elango, M. Ramyadevi, S. Preethi, ”A novel design and implementation of IoT based real-time ATM surveillance and security system”, Advances in Computational Intelligence, vol.2, no.1, 2022.

[9] Neha Sharma, Deepak Panwar, ”Advance Security and Challenges with Intelligent IoT Devices”, Proceedings of Second International Conference on Smart Energy and Communication, pp.177, 2021.

[10] Comparing rank-1 FNIR at N=1.6M FVRT 2018 mugshot photos for 2020 Yitu-004 algorithm (0.0008) and 2014 NEC-30 algorithm (0.041). Source: Patrick Grother, Mei Ngan, and Kayee Hanaoka, “FRVT Part 2: Identification,” March 27, 2020, https://github.com/usnistgov/frvt/blob/nist-pages/reports/1N

[11] Joy, A. Design and Implementation of Multilayer Security for ATM Machines.

[12] Jacintha, V., Nagarajan, J., Yogesh, K. T., Tamilarasu, S., Yuvaraj, S. (2017, December). An IOT based ATM surveillance system. In 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC) (pp. 1-6). IEEE.

[13] Dutta, M., Psyche, K. K., Khatun, T., Islam, M. A., Islam, M. A. (2018, August). ATM card security using bio-metric and message authentication technology. In 2018 IEEE International Conference on Computer and Communication Engineering Technology (CCET) (pp. 280-285). IEEE.

[14] Hazra, S. (2019, March). Smart ATM Service. In 2019 Devices for Integrated Circuit (DevIC) (pp. 226-230). IEEE.

[15] Agency for Toxic Substances and Disease Registry (ATSDR). Toxicological Profile for Chloroform. Public Health Service, U.S. Department of Health and Human Services, Atlanta, GA. 1997.