IOT based Smart Framework for ATM Security with Electricity Saver

Deepak Kumar Verma[1*], Karunesh Singh[2], Ayush Srivastav[3], Vartika Singh[4]

[1,2,3,4]Department of Computer Science, Dr. Rammanohar Lohia Avadh University, Ayodhya, India-224001

Corresponding Author: deepak.discrete@gmail.com, Tel.: +91-9452834077

Abstract - ATM machine is a great piece of technology used by millions of people around the world. It makes our daily transactions easier without loading up the banking systems. However, it is important to keep them secure from thefts and other malicious activities. This work deals with the prevention of ATM theft from robbery, so overcome the drawback found in existing technology in our society. Whenever robbery occurs, Vibration sensor is used here which senses vibration produced from ATM machine. Here DC Motor is used for closing the door of ATM when the vibration is sensed, also a buzzer is also used, once the vibration is sensed, beep sound will occur from buzzer. Furthermore, infrared sensor is also used to develop the automatic light switching system. The automatic light switching system will lead to energy saving and efficient energy usage which could benefit every single individual. This system is developed with safety environment, switching the light 'ON' or 'OFF' during entry and exit. In this paper we have proposed a model for smart security and electricity saver system developed with the help of Arduino uno kit and sensors.

Keywords— ATM security system, ATM anti-theft system, light control switching, Arduino uno, Infrared System.

I. INTRODUCTION

An automated teller machine (ATM) is a specialized computer that allows bank account holders to check their account balances, withdraw or deposit money, transfer money from one account to another, print a statement of account transactions, and even purchase stamps. The first ATM was set up in June 1967 on a street in Enfield, London at a branch of Barclays Bank, credited to a British inventor named John Shepherd-Barron. The idea of designing Anti-theft ATM security system project is introduced by observing our real-life incidents. In our project, IR sensors and vibration sensor are used. IR sensors detects the person entering and coming out of cabin and opens the door. Vibration sensor detects the suspicious movement like when someone tries to break ATM machine. The Arduino board is an open-source software and hardware development enrollment. It is used to store and implement the programs or codes written in different machine understandable programming languages. This system process real-time data collected using IR sensors and vibration sensor. Once the suspicious movement is detected, the buzzer starts producing buzzing sound, the servo motor that is used to open and close the door is closed permanently so, no one came out of ATM till officials arrives. This system allows only one person at a time to enter to ATM cabin, once a person enters to cabin, the entry sensor stop working till the person came out of cabin. In this system automatic lighting system is also embedded, when someone enters to cabin, light turns ON automatically and on exit it turns OFF automatically.

Through this we can easily prevent ATM theft and the criminals can also be caught. The overall objective of this project is to create a public friendly environment and decrease the rate of theft and robberies.

In recent years, physical attacks on ATMs have increased, due to both difficult economic circumstances and access to technology to break into the machines. ATMs will always be a high-profile target due to the volume of cash and the fact that they are often unattended. The combination of challenging economic times, along with easy access to technologies, have increased the levels of criminal activity. Few major security techniques that are most widely used in ATM security are following:

1.1 Face Recognition Technology: Face recognition is done by camera place at the door of ATM counter. The face detection is done by either biometric technique or computer application which recognizes the customer from image or video frame. The door will open only if the face is detected. The detection is accomplished by using techniques like blurred human shapes or skin tones. Face recognition is done by using Haar cascade classifier for face recognition to increase ATM security. The facial detector is applied on each frame of the captured image. Then a recognition model of the face is built from the frame using local binary pattern histogram (LBPH) and it is recognized.

1.2 Fingerprint Verification Technology: The fingerprint detected by the sensor is scanned for the biometric trait in the template database. In the decision module the similarities in the matcher module is checked and authorization is granted.

1.3 Global Positioning System (GPS) and Global System for Mobile Communication (GSM) Technology: ATM attacks can also be reduced by using GSM and GPS technology. If ATM is tampered an SMS will be send to the main controlling station through GSM. If cash box is robbed it can be tracked by using GPS.

1.4 OTP Verification: The transactions can also be authorized based on OTP verification. The transactions are authorized only after confirmation of the message by the user which may be a onetime password (OTP) or confirmation message. The OTP is send by using GSM technology.

1.5 Card less Transactions: ATM transactions are done without using ATM cards by combining IoT and computer vision for enhancing ATM security. Transactions are authorized on the basis of face recognition, fingerprint verification and OTP authentication without ATM card and PIN.

II. RELATED WORK

In paper "A smart home energy management system using IOT and big data analytics approach", the authors A.R. Al-Ali, M. Alikarar, R. Gupta, M. Rashid, I. A. Zualkernan, proposed an idea for implementing an Energy Management System (EMS) for smart homes. In this system, each home device is interfaced with a data acquisition module that is an IoT object with a unique IP address resulting in a large mesh wireless network of devices. The data acquisition System on Chip (SoC) module collects energy consumption data from each device of each smart home and transmits the data to a centralized server for further processing and analysis. This information from all residential areas accumulates in the utility's server as Big Data. The proposed EMS utilizes offthe-shelf Business Intelligence (BI) and Big Data analytics software packages to better manage energy consumption and to meet consumer demand. Some challenges of this system include: lifetime of a WSN network deteriorates with time due to the deployment of new sensors in the network, the data collected and aggregated solely by the home server in a system using zigbee as a communication protocol could lead to data loss in case of a system failure, the lack of standardized protocols and regulations were the main challenges in considering intelligent DC powered homes as suitable replacement to AC power systems and the device status and power consumption details transported to the web server through an extensible mark-up language (XML) interface would tend to be heavy weight for data delivery between browser and servers and the architecture will face significant bandwidth challenges in sending these large files across the network.

III. METHODOLOGY

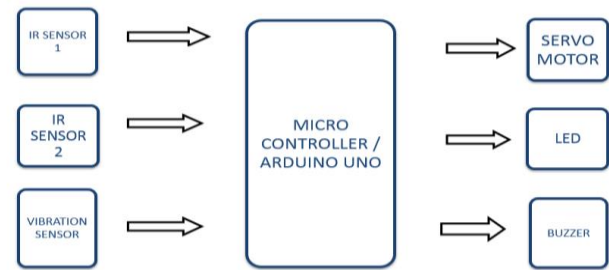The figure 1 shows the block diagram of proposed model for security and electricity saving purpose.

Fig 1: Block diagram of proposed model

The proposed model has six major components described below:

3.1 IR Sensor
This is the most fundamental type of sensor available in the market. The basic concept is simple. There is an emitter which emits infrared (IR) rays. These IR rays are detected by a detector. This concept is used to make proximity sensor (to check if something obstructs the path or not, etc), contrast sensors (used to detect contrast difference between black and white, like in line follower robots), etc.
The working of this sensor in the work is to detect the person to open the door and turn ON the light.

3.2 Vibration Sensor
Vibration sensors are sensors used to measure, display and analyze frequency, displacement, velocity or acceleration. There are various types but the most commonly used vibration sensor is accelerometer. It produces electrical signal proportional to acceleration of vibrating component. The working of this sensor in the work is to detect the vibration if any suspicious activity happen.

3.3. Arduino Uno R3 / Micro-controller
An Arduino is an open-source microcontroller development board. Arduino consists of both a physical programmable circuit board (often referred to as a microcontroller) and a piece of software, or IDE (Integrated Development Environment) that runs on computer, used to write and upload computer code to the physical board.

In the project we use it to communicate and provide interface between sensors and other end devices. It also stores program in which the project works.

3.4 Buzzer/Alarm
An audio signaling device like a beeper or buzzer may be electromechanical or piezoelectric or mechanical type. The main function of this is to convert the signal from audio to sound.
This device is used for alert purpose.

3.5 Servo Motor
Servo motor is basically a simple motor that works under the mechanism of servo mechanism. The main aim to use servo motor in the project is, it helps in closing and opening door. If the vibration sensor senses any suspicious activity, the door will automatically close.

3.6 LED Light

An LED is an electronic device that emits light when an electrical current is passed through it. It is used in this project for the purpose of light, inside the ATM cabin.

IV.   EXPERIMENTAL SETUP & WORKING

Figure 2 shows the actual experimental setup of proposed work carried out to achieve the security and power saving objectives.
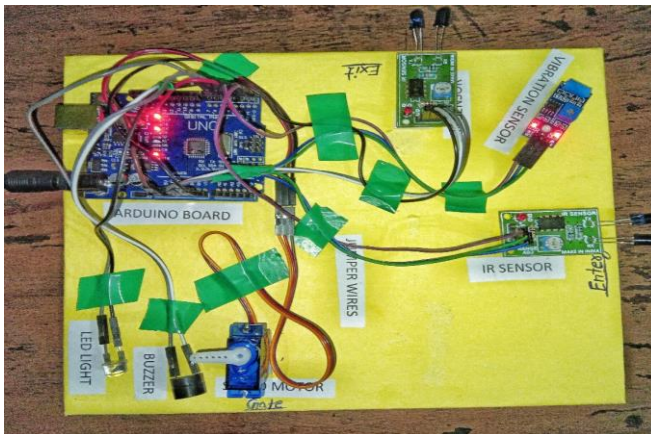

Fig 2: Actual Experimental Setup of proposed model

• There are three sensors (two IR sensor and one vibration sensor), one Arduino uno, one servo motor, one LED and one buzzer are used in the model.
• First IR sensor at entry, senses the person, sends signal to open gate and to turn ON gate.
• First sensor become inactive after entry, till the person inside the ATM cabin came out of it.
• Second IR sensor, senses the person on exit to open the gate and to turn OFF the light.
• Third sensor i.e. vibration sensor senses the vibration if any suspicious activity happens (like if someone tries to break the ATM).
• Vibration sensor sends signal to buzzer, to beep and to servo motor, to close the door till officials arrives.
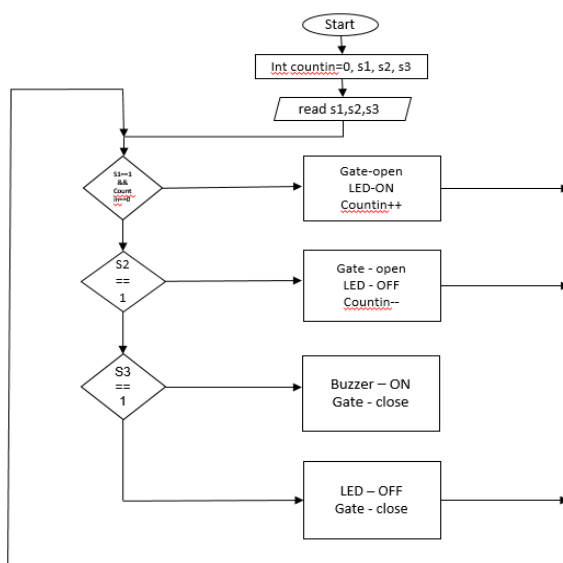

Fig 3: Flow chart of proposed work

V.   RESULTS AND CONCLUSION

Based on the result, the main objective of implementing IOT Based ATM security system using Arduino uno, IR sensors and vibration sensor has been achieved. The purpose of model is to provide security to ATM. Whenever someone tries to tamper the ATM, the sensor which senses the motion, sends the signal to the microcontroller. Once the controller receives signal, it locks door of ATM by sending signal to DC motor. At same time, the buzzer also gets activated which alert the officials.

Here, also the objective of saving electricity is achieved. When someone enters to ATM, sensor sends signal to microcontroller and it sends to LED light, that turns ON. When the person comes out of cabin, LED automatically turn OFF.

In this work both objectives, security to the ATM and electricity saving have been achieved through this IoT inspired proposed model.

REFERENCES

[1] Murugesan M., Santhosh M., Sasi Kumat T., Sasiwarman M., Valanarasu I. "Securing Atm Transactions Using Face Recognition", International Journal Of Advanced Trends In Computer Science And Engineering **Volume 9, No.2, Pp. 1295–1299, March-April 2020.**

[2] Frimpong Twum, Kofi Nti, Michael Asante, "Improving Security Levels in Automatic Teller Machines (ATM) Using Multifactor Authentication", International Journal of Science and Engineering Applications, Volume 5, Issue 3, pp. 126–134, 2016.

[3] Udhaya kumar N., Sri Vasu R., Subash S., Sharmila Rani D., "ATM-Security using Machine Learning techniques in IOT", International Journal of Advance Research, Ideas and Innovations in Technology, **Volume 5, Issue 2, pp. 150–153, 2019.**

[4] Siva kumar T., Gajjala Askok, Sai Venu, "Design and Implementation of Security Based ATM theft Monitoring system", International Journal of Engineering Inventions **Volume 3, Issue 1, pp. 01–07, August 2013.**

[5] Prashant Kumar Yadav, Akhtar Husain, Surjeet Kumar, "Enhanced ATM Security with OTP Based Authentication", International Journal of Advanced Science and Technology, **Volume. 29, Issue. 3, pp. 7987–7993, 2020.**

[6] Pavan S. Rane, Prashant P. Sawat, Sourabh B. Shinde, Prof. Nitin A. Dawande, "ATM SECURITY", International Journal of Advance Engineering and Research Development, **Volume 5, Issue 06, June -2018.**

[7] Ajay Kumar Bharti, Rashmi Negi, Deepak Kumar Verma, "A Review on Performance Analysis and Improvement of Internet of Things Application", International Journal of Computer Sciences and Engineering, **Vol.7, Issue.2, pp.367-371, 2019.**

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

[9] Rubea Othman Rubea, Xue Wen Ding, "ATM Security System on IRIS Recognition with GSM Module", International Journal of Science and Research, **Volume 7, Issue 3, March 2018.**

[10] Soneria Hardik Champaklal, Siba Ram Raut, "Enhanced Security for ATM Machine with Biometric Technology", International Journal for Research in Applied Science & Engineering Technology, **Volume 7, Issue 3, Mar 2019.**

[11] Jufishan Boksha, Romita Mondal, Soumi Mitra, Asoke Nath, "A Proposed Model of Advanced Security System in ATM: Implementation of Face Recognition and Finger Print Recognition", International Journal of Computer Sciences and Engineering, **Vol.7, Issue.10, pp.15-20, 2019.**

[12] K. Hema Sai Sivaprasad, A.P. 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 **Volume no-3, Issue No.11, 2016.**

[13] Kamaljit Kaur, Ramanjot Kaur, "A Literature Survey on Security & Privacy Issues in IoT", International Journal of Computer Sciences and Engineering, **Vol.9, Issue.4, pp.60-64, 2021.**

[14] R.Senthil Kumar, K. R. Sugavanam, D. Gajalakshmi, "Novel vigilant real time monitoring and security system for ATM", Journal of Theoretical and Applied Information Technology, **Volume. 67, Issue. 1, September 2014.**

[15] Ajay Kumar Bharti, Rashmi Negi, Deepak Kumar Verma, "A Framework for Performance Optimization of IoT Applications", - International Journal of Research and Analytical Reviews, **Volume 6, Issue 2, April – June 2019.**

AUTHORS PROFILE

Dr. Deepak Kumar Verma have done MCA from University of Lucknow, India in year 2011. Dr Verma has completed his Doctrate in Computer Science in the year 2016 and currently working as an Assistant Professor of Computer Science in Dr Ram Manohar Lohia Awadh University, Ayodhya, India. His research interests are Artificial intellegence, data security and Cyber Security. Dr Verma has published ore than twenty research papers in various refreed/reputed National and International journals and also presented several research papers in IEEE Conferences. He has 10 years of teaching experience and 07 years of Research Experience.

Mr. Karunesh Singh is scholar of final year of graduation with computer science from Dr Rammanohar Lohia Avadh University, Ayodhya, India. He has developed several mini projects based on arduino uno kit and sensors during his graduation. His research interests are Internet of Things, Smart technologies, sensors and Robotics.

Mr. Ayush Srivastav is scholar of final year of graduation with computer science from Dr Rammanohar Lohia Avadh University, Ayodhya, India. He has developed several mini projects based on arduino uno kit and sensors. His research interests are IoT, Big data technologies.

Ms. Vartika Singh is scholar of final year of graduation with computer science from Dr Rammanohar Lohia Avadh University, Ayodhya. Her research interests are Internet of Things, Big Data and Cloud Computing.