iJETRM
International Journal of Engineering Technology Research & Management

MULTILEVEL BANK SECURITY WITH MASTER AUTHENTICATION OVER INTERNET

S.Caroline [1]
Yohannes Bekuma [2]
J. Sam Alaric [2]
[1] Department of ECE St. Xavier's Catholic College of Engineering, Anna University, India.
[2] Department of ECE Wollega University, Ethiopia

ABSTRACT
The conventional locker system available in banks use key for opening and are not highly secure. Security becomes a major issue. To overcome this, a Multi-Layer Bank Security System is proposed. This system is used for managing the security of bank locker rooms. There are many banks which permits access control approach to prevent the locker room from unauthorized access. The main purpose of this project is to design and implement a high level locker security system based on RFID, PASSWORD and IoT technology which can be used in bank, secured offices and homes. In this system, only authentic person can be able to recover money from locker. It contains door lock system which can activate, confirm and validate the user and unlock the door in real time for locker secure access. The main advantage of using RFID, PASSWORD and IoT is more secure than other systems and also it provides the theft protection system. The system proposed is a highly secure system in terms of number of level of security.

KEYWORDS:
Multi Layer Bank Security System, RFID, PASSWORD, IoT, locker high security system

1. INTRODUCTION

RFID is a means of identifying a person or object using a radio frequency transmission. In other words RFID is an electronic method of exchanging data over radio frequency waves. We can identify, track, sort or detect a wide variety of objects using this system. Some people will try to steal the property which may endanger the safety of money in the bank, house and office. RFID based access – control system allows only authorized persons to open the locker with IoT technology. IoT technology is used to authenticate the user and gives the locker door information through the internet. Here we use the matrix keypad to enter the password for door locker. When the entered password matches the system password the locker will open. The sensor is used to find the status of door. If the door is open for more than certain period, the alarm system will be activated. If someone tries to tamper the locker the vibration sensor will detect the threat and activate the siren and send the information to the authority.

II LITERATURE REVIEW

A new approach towards the security of ATM (Automatic Teller Machine) systems is proposed. The objective of the paper is to know the Enhanced smart ATM security system which is developed using the Embedded system and advanced technologies. In this system, RFID card is used as ATM card, IR sensor in order to sense the presence of the card holders. SMS will be sent via GSM to the two main stations, if the ATM card is tampered. GPS is used to track the location in case the cash box is robbed. Finger print is used to identify and verify authorized bank personnel. Hence the proposed system is the highly secured system for ATMs [1].

There is a sudden exponential use of security systems in our day to day life. For example, security in a business space, organisation, or bank locker is important to every individual now. Later, security cameras are being utilized in order to build safe and secure places in organizations. However, this technology needs a person

iJETRM
International Journal of Engineering Technology Research & Management

regularly to detect any problem in the frame taken from the camera. The main aim of this paper is to enhance the traditional security system. The security system based on the IoT platform has the potential of interacting real-time with the device. The system consists of a camera, voice sensor/microphone, motion/activity sensor and an LTE/Wi-Fi module [2].

This paper mainly focuses on the control of home appliances from a remote place and provides security. The system is SMS based and uses wireless technology which is more adaptable and cost effective to revolutionize the standards of living. This system provides ideal solution to the problems faced by home owners in daily life. The HACS system provides security against intrusion as well as automates various home appliances using SMS. The system uses GSM technology thus providing ubiquitous access to the system for security and automated appliance control [3].

The banking process is a completely automatic system, which will increase security features and at the same time increase the efficiency in the working of the banks to a great extent. The entire transaction system will be completely automatic, which will make the banking process much faster, thus saving the time of the customers and also making the system error-free to a great extent. Aims have also been made to increase the security of these banks with the help of image processors, sensors and GSM. Various other features like aid for handicapped, speech recognition for senior citizens have also been implemented. Apart from these features, several other features like automatic fire extinguishing have also been introduced in the system. Hence, the main aim of the project is to make the banking process completely user-friendly, secure and automated, without the requirement of any kind of human intervention [4].

RFID-tags are becoming very fashionable and attractive tools for banknotes authentication and identification. They have a tiny microchip embedded with other functionalities that can be utilized for security defense. This chip functionality makes it possible to detect and prevent money counterfeiting. RFID-enabled notes can be easily tracked and verified by an authorized party. In this paper, a novel money counterfeit detection algorithm using an RFID-enabled smart phone is presented. With this algorithm, the communication parties can be reduced into two parties (i.e., regular user and monetary agency) unlike other presented schemes which involve the law enforcement agency, the central bank, and the merchant. This system is based on a software application which users need to download to check counterfeit money through their smart phones. This proposed form of security and performance is compared with other related algorithms [5].

An improved SMS based metering system using SMS technology is proposed in [6]. Here an Arduino controller is connected to a GSM based wireless communication module. It monitors the electrical pulses, measures the unit consumed, calculates the cost and displays the results in s LCD screen.

The proposed system replaces the traditional meter reading by automatic meter reading (AMR). This automatically reads the electric, gas or water meter reading without the help of human from a remote place. A PC with a GSM receiver at the other end, contains the database acting as the billing point. This provides fast and accurate billing. Live meter reading from the GSM enabled energy meter is sent back to this billing point periodically and these details are updated in a central database. A new interactive, user friendly graphical user interface is developed using Microsoft visual studio .NET framework and C#. With proper authentication, users can access the developed web page details from anywhere in the world. The complete monthly usage and due bill is messaged back to the customer after processing these data [7].

Nowadays, security is a major issue and plays a major role in almost all organizations, industries and healthcare facilities. A survey on various automatic identification and access control mechanisms that are used over the years to prevent unauthorized access is presented. In the past, traditional lock systems or passwords were employed in high security areas like locker rooms in banks. This method was highly insecure. Due to the advancements in technology RFID cards were used. The drawback with RFID card is that the user has the probability of getting the card lost, forgotten or stolen. Later various door lock security systems based on biometrics, GSM, OTP, cryptography etc were developed [8].

iJETRM
International Journal of Engineering Technology Research & Management

III SYSTEM ANALYSIS

This system consists of microcontroller, RFID reader, Matrix keypad, Magnetic sensor, buzzer, IoT and LCD as shown in Figure 1. In this system the RFID reader reads the id number from passive tag and sends it to the microcontroller. It then sends the permission request to the authenticated person. The authenticated person enters the passwords in the keyboard which was already given by the user and received from the microcontroller. If both codes are not matched the microcontroller sends the warning message to the authenticated person and it will remain in locked position.

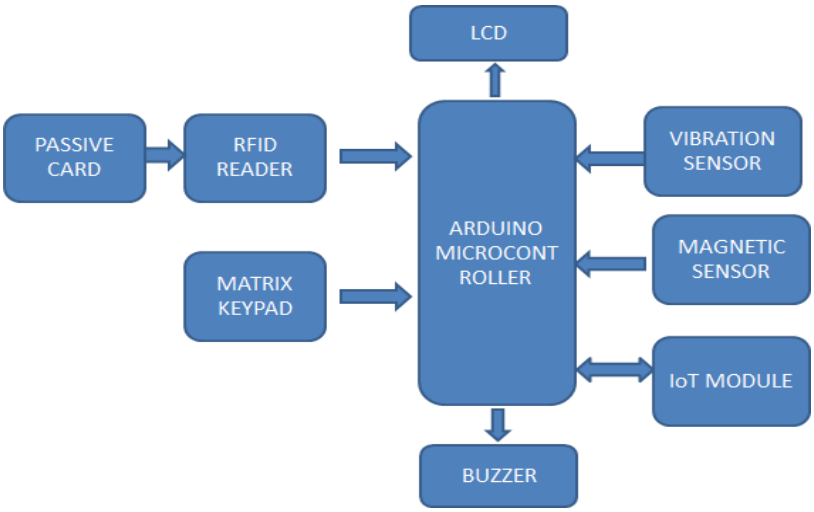

Fig.1: Block diagram of security system

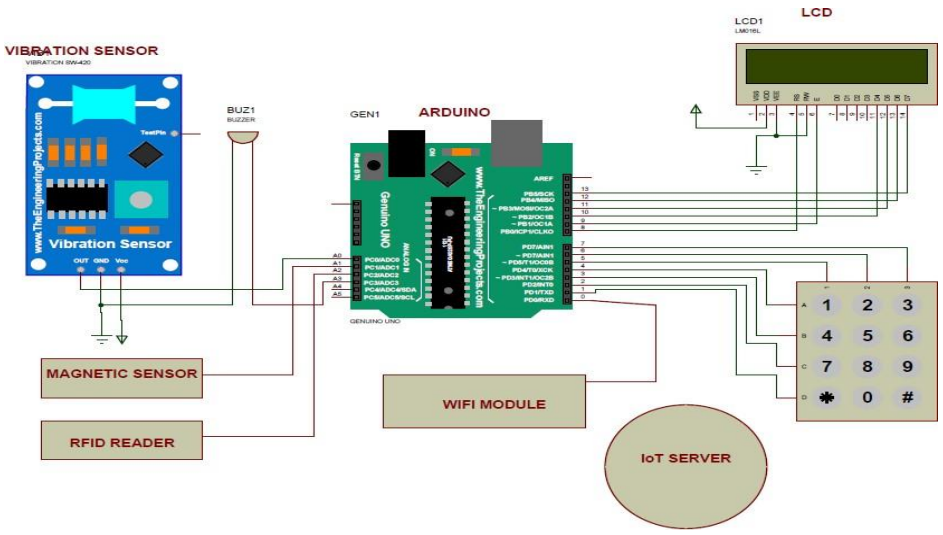

Fig. 2: Circuit Diagram

iJETRM
International Journal of Engineering Technology Research & Management

Fig. 2 shows the circuit diagram of the proposed system. Microcontroller controls and monitors the whole system by getting signals from sensors. RFID reader will read the RFID card details and provides to the microcontroller. If the valid details is presented microcontroller generates and sends the request to the server using WiFi module. The application in the mobile receives the request and when the application user accept the request the first locker door will open. Then the user need to type the password using matrix keypad, if matched the door will open. The magnetic read switch will sense the position of door and provides the data to the microcontroller, if door is open for above certain time period the microcontroller activates the buzzer alarm. A complete flowchart for the proposed system is shown in Fig. 3.

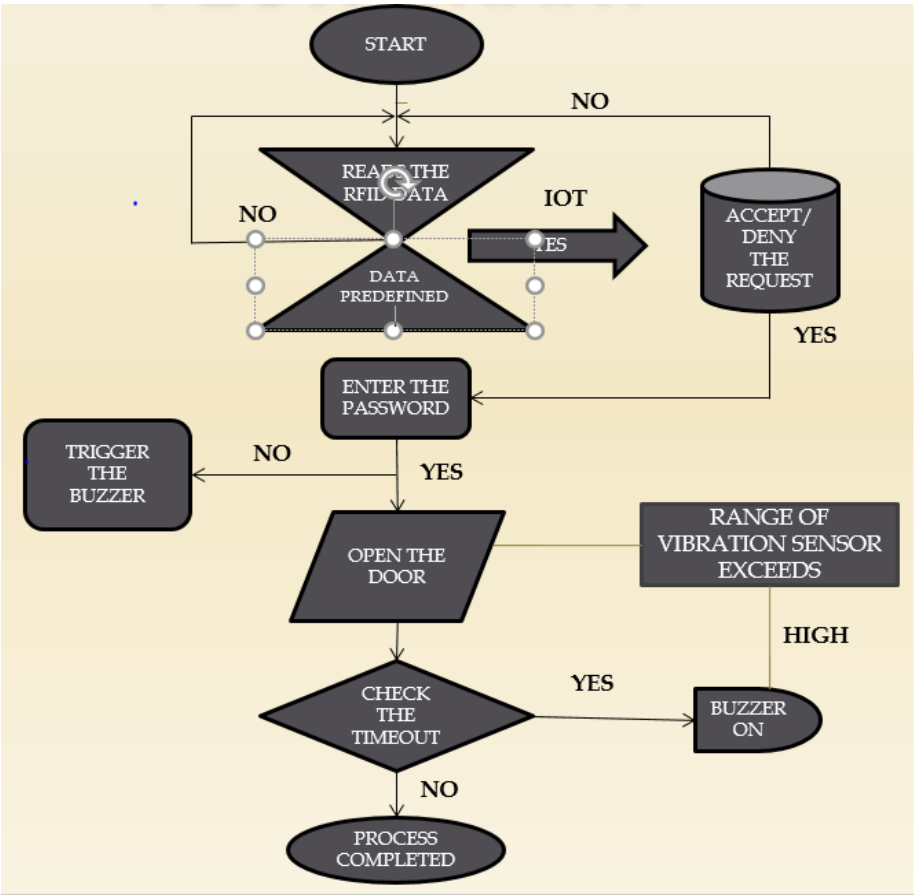

Fig. 3 Flowchart for the proposed system

iJETRM
International Journal of Engineering Technology Research & Management

IV RESULT AND DISCUSSION

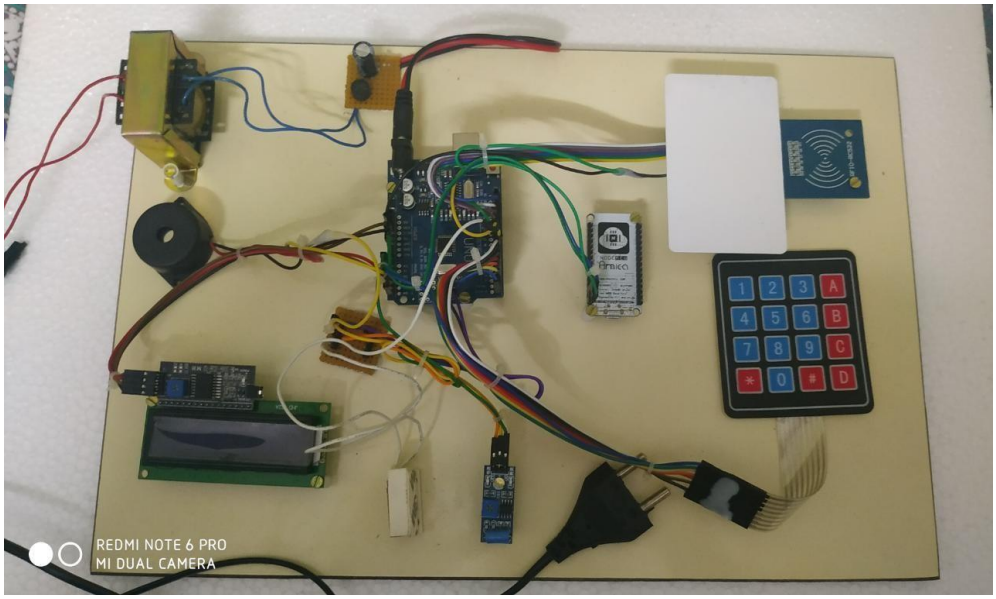

Fig. 4: Hardware setup

Figure 4 shows the overall hardware of the multilevel bank security system with master authentication over internet.

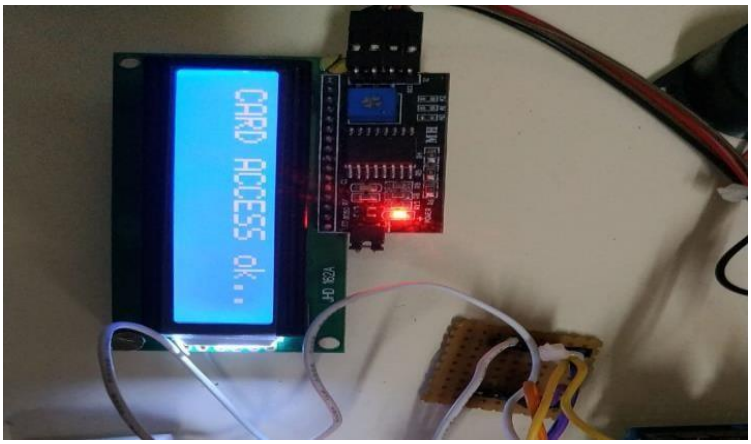

Fig. 5: Unauthorized User output

Figure 5 shows the output or message displayed in the LCD display. It shows the output for an unauthorized user output .Link 1: https://api.thingspeak.com/update?api_key=O6PM3R8UREC6TM8Z&fiel d1=0

iJETRM
International Journal of Engineering Technology Research & Management

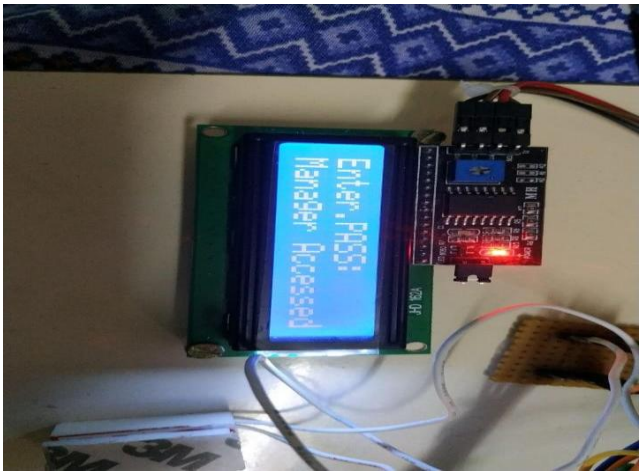

Fig. 6: Authorized User output

Link 2: https://api.thingspeak.com/update?api_key=O6PM3R8UREC6TM8Z&fiel d1=1

Figure 6 shows the output or message displayed in the LCD display. It shows the output for an authorized user output.

The above mentioned link 2 gives the permission to access the security system and the link 1 is to deny the access of security system

V CONCLUSION

Bank locker room security is an emerging need throughout the world. In this project we have designed the systems that allow unlocking a protected door. The security can be used in other highly restricted areas like private offices, laboratories etc. This study proposes an approach towards providing a more reliable and complete solution of implementing multilevel user authentication in a banking environment to maintain its maximum security. This proposed architecture can be easily tested and implemented by any of the bank with their existing security architecture, with introduction of little modification to avoid high level attacks from third parties at any level. The order of authentication level can be rearranged, according to the situation of bank security. In this project, we are using Arduino which is easy to use operate ,low cost ,lower in power consumption and smaller in size where high degree of security is maintained. In near future, more number of security levels can be added for monitoring as well as control such as dual Iris scanner which can improve the security system performance. Increase in number security levels could be more effective for security system.

VII REFERENCES

[1] Al-Ali, A.R. Rousan, M.A. Mohandes, M (2004), “GSM-Based Wireless Home Appliances Monitoring & Control System”, Proceedings of International Conference on Information and Communication Technologies: From Theory to Applications, Vol. 3, pp. 237-238.

[2] Bharati M Nelligani , N V Uma Reddy , NithinAwasti (2016),"Smart ATM security system using FPR, GSM, GPS" International Conference on Inventive Computation Technologies (ICICT) Vol.19, pp.27-36.

[3] Malik Sikandar Hayat Khiyal, Aihab Khan, and ErumShehzadi (2009),“ SMS Based Wireless Home Appliance Control System (HACS) for Automating Appliances and Security”,Issues in Informing Science and Information Technology, Vol. 9, pp. 887 – 894.

[4] Mayukh Roy , Md. Minhazuddin , ShreyasiGhosh , KuntalSarkar ; Tapan Kumar Rana

iJETRM
International Journal of Engineering Technology Research & Management

(2017),"Smart transaction and automation system for banks"; 1st International Conference on Electronics, Materials Engineering and Nano- Technology (IEMENTech) Vol.2, pp.473-480.

[5] Mohamed Hamdy Eldefrawy and Muhammad Khurram Khan (2016), "Detecting counter feit-money using RFID-enabled mobile devices" International Conference for Internet Technology and Secured Transactions Vol.9, pp.45-57.

[6] MohdHelmy Abd Wahab, Azhar Ismail, AyobJohari and Herdawatie Abdul Kadir (2009),"SMS-Based Electrical Meter Reading".In Proceeding of International Conference on Rural Information and Communication Technology (r-ICT), Bandung, Indonesia Vol.3, pp.71-79.

[7] Md. Wasi-ur-Rahman, Mohammad TanvirRahman, TareqHasan Khan and S.M. LutfulKabir (2009), "Design of an Intelligent SMS based Remote Metering System", Proceedings of the IEEE International Conference on Information and Automation, Vol.15, pp.1040-1043

[8] R.S.Divya , Meera Mathew (2017), "Survey on various door lock access control mechanisms";International Conference on Circuit ,Power and Computing Technologies (ICCPCT) Vol.34, pp.8-14.

[9] Santosh Mahendra , Mithileysh Sathiyanarayanan , Rajesh BabuVasu (2018), Smart Security System for Businesses using Internet of Things (IoT);Second International Conference on Green Computing and Internet of Things (ICGCIoT) Vol.10, pp.43-50.

[10] SreevidyaKhatravath,Sumanta Laha (2016),"Advanced Security Analytics"; 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT) Vol.3, pp.65-73.