International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (01), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

ATM Secure Monitoring Using IoT

Swetha B[1], Obulakshmi V[2], Vigneshwari R[3]

[1,2,3]UG Student, Department Of ECE

Sengunthar Engineering College, Tiruchengode

ABSTRACT

Automated Teller Machines (ATMs) security is provide multiple points of protection against physical and electronic theft from ATMs and protecting their installations. The Machine-to machine (M2M) communications technology is achieved. It provides real-time monitoring and control without the need for human intervention. anti-skimming defend system to silent indicate systems, integrated ATM video surveillance cameras and ATM monitoring options, security specialists are ready to help the people get more out of the ATM security and ATM loss prevention systems. The setup is proposed for ATM security, comprising of the modules namely, authentication of shutter lock, web enabled control, sensors and camera control.

key words- PIC Microcontroller, IR sensor, vibration sensor, temperature sensor or gas sensor detects, chloroform(5ml.)

I.INTRODUCTION

In recent years, the usage of ATM service is increased drastically as it offers more sophistication for the customers to withdraw their amount at 24*7 hours. The growth in electronics transaction has been adapted by banking sector. Yet ATM service suffers lots of security issues, which threatens the entire banking sector and customer. Due to the prevailing fraudulent act like card skimming, cash trapping etc., the secure financial transaction is not ensured. According to the recent survey, rate of robbery and theft is increasing in every year. The following statistical report shows the crime rate. The ATM crimes are happening at a frequent rate because of lack of security system in center. Mostly robberies are taken place during off-peak hours, such activities lead to 11% of transaction and 60% of crime on day to day routine. A statistics stated that, about 5500 crimes have been recorded in a year. The lack of security encourages these types of crimes which are increasing steadily. ATM centers play a vital role for money withdrawal. Other than the application it has many purposes like money transactions, cash deposits, registrations. Such wide usage of a card demonstrates as how it is indispensable for modern age. Instead of carrying money which is vulnerable for attacks in a society where the unemployment and inflation dominates so it is safer to carry thin flat card which is compactable in wallets. It holds the identity of a person which is unique and subjected to personal usage. This system we have a watchman and a camera to monitor the ATM system. The recent enhancement made in the security system for a few ATMs is that it is provided with security to the entrance doors itself such that to enter the ATM we need to use the card to unlock the door. System for a few ATMs is that it is provided with security to the entrance doors itself such that to enter the ATM we need to use the card to unlock the door. Thief can kill the watchman and to break the camera. It cannot be send the information.

II.RESEARCH BACKROUND

ATM center are now a day's increasing large in number, which will be comfortable for people to do easy transaction at any point of time. Though many procedures which are indispensable to be followed inside a centre people fail to do this paves way to crimes like ATM thefts, manhandling prevails inside the centre. There are several DO'S and DONT'S inside an ATM center which are captioned outside the center but people in their busy schedule even fail to have a notice at the boards. Small faults can lead to unpayable consequences. As stated in an English proverb "LOOK BEFORE YOU LEAP" precaution measures must be taken before you step in danger zone. The classic scenario which falls in this category is smoking which will lead to dangerous fire accidents causing damage both to life and property. So, smoking inside ATM is strictly prohibited shows in fig.1. The figure also depicts prohibition to the usage of cell phone, which makes use of electromagnetic waves for communication. It is observed from basic physics that two electromagnetic waves can undergo constructive or destructive interference which deteriorate the performance of a machine. ATM is also an electronic machine uses EM waves. For high degree of transaction and resolving EM interference usage of cell phone is forbidden. The CCTV camera are provided at the door step to identify the people entering the centre but then when the customer enters with the helmet there is no use in providing CCTV shows in Fig.1. When the crime occurs inside the centre, legal evidences can't be gathered criminal cannot be traced even if they are arrested they will escape from the hands of law.

Fig.2.1. Infringing the ATM center codes

III.EXISTING SYSTEM

In this system we heave a watchman and a camera to monitor the ATM system. The recent enhancement made in the security system for a few ATMs is that it is provided with security to the entrance doors itself such that to enter the ATM we need to use the card to unlock the door. System for a few ATMs is that it is provided with security to the entrance doors itself such that to enter the ATM we need to use the card to unlock the door.In this existing system, the person should enroll his or her finger print into the finger print reader, later the fingerprint database compares the live sample provided by the customer with the template in the database, for identification. On confirmation the information provided is factual and then the customer is granted access to

the ATM system. Likewise, it has also proposed customer's nominee concept for doing the transactions while actual customer is unable to do the transaction.Since the fingerprint can be easily forged, it becomes a major drawback to be used for biometric authentication[1].

ATM card fraud is causing billions of dollars in losses for the card payment industry. In today's world the most accepted payment mode is Debit card for both online and also for regular purchasing; hence frauds related with it are also growing. To find the fraudulent transaction, we implement an Advanced Security Model for ATM payment using Hidden Markov Model (HMM), which detects the fraud by using customers spending behavior. This Security Model is primarily focusing on the normal spending behavior of a cardholder and some advanced securities such as Location, Amount, Time and Sequence of transactions. If the trained Security model identifies any misbehavior in upcoming transaction, then that transaction is permanently blocked until the user enter High Security Alert Password (HSAP). This paper provides an overview of frauds and begins with ATM card statistics and the definition of ATM card fraud. The main outcome of the paper is to find the fraudulent transaction and avoids the fraud before it happens.[2]

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 personal identification numbers (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. An embedded fingerprint biometric authentication scheme for automated teller machine (ATM) banking systems is proposed in this paper. In this scheme, a fingerprint biometric technique is fused with the ATM for person authentication to ameliorate the security level.[3]

Automated Teller Machines (ATMs) security is the field of study that aims at solutions that provide multiple points of protection against physical and electronic theft from ATMs and protecting their installations. From anti-skimming defend systems to silent indicate systems, integrated ATM video surveillance cameras and ATM monitoring options, security specialists are ready to help the people get more out of the ATM security and ATM loss prevention systems. The aim of the proposed work is to implement a low cost stand-alone Embedded Web Server (EWS) based on ARM11 processor and Linux operating system using Raspberry Pi. It offers a robust networking solution with wide range of application areas over internet. The Web server can be run on an embedded system having limited resources to serve embedded web page to a web browser. The setup is proposed for ATM security, comprising of the modules namely, authentication of shutter lock, web enabled control, sensors and camera control. This project consists of two sides, one is at the door side with AT89S52 microcontroller and another one is inside ATM with Raspberry Pi. Smoke and vibration sensors are used for protection purpose. Ethernet is used to upload the sensor values to the HTML web page. The alert messages will be sent to the authorized person if vibration or smoke is detected. The person's mobile number is stored in the system at the initial stage.[4]

Block diagram of module in ATM using ARM

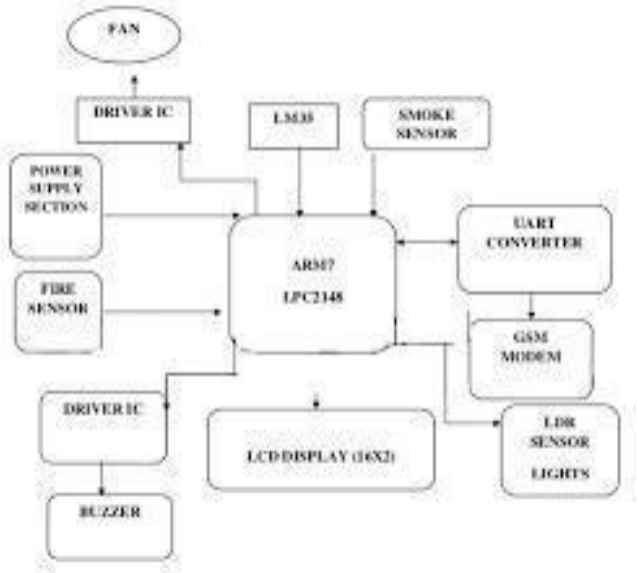

Figure 2. Block diagram of module in ATM

IV.PROPOSED SYSTEM

The proposed work is to implement a low cost stand-alone Web Server (EWS) based on Pic controller. It offers a robust networking solution with wide range of application areas over internet. The Web server can be run on an embedded system having limited resources to serve embedded web page to a web browser. It more securable system. Quickly send the information. In real time one can make an ATM better safe from intruder and thefts.

Block diagram of module inside ATM:

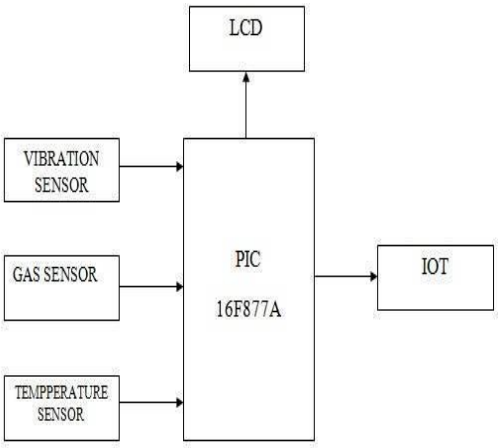

Figure 3. Block diagram of module inside the ATM

V. IMPLEMENTATION

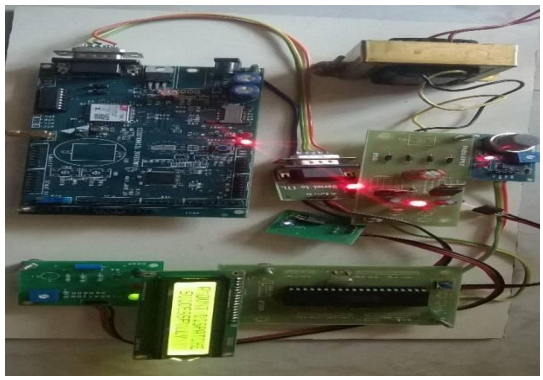

Figure 4. Circuit board of module at ATM

Fig4 shows the proposed work implementation in a secure way of accessing an ATM by authorized persons alone in terms of monitoring the ATM using IOT and the above said module is accomplished by using RFID tags, RFID reader, and PIC microcontroller. In the protection purpose, we are using the gas sensor, the vibration sensor, the temperature sensor and the IR sensor. If any of these four sensors detects, the alert message will send to the authorized person. If the IR sensor, vibration sensor, temperature sensor or gas sensor detects, the Microcontroller will soon send the information to the mobile or web server to the authorized person and stores in the cloud. The sensor values are uploaded to the web page using Internet of Things. of the project is very essential in order to make the design system more advanced. Then door lock in case thief tried to break the door. The chloroform gas is spread to the floor through the air conditioner. The chloroform level increase if the thief don't get unconditional stage. It continue until thief get unconditional stage.

Figure 5. LCD Display

In fig5 shows the LCD display which displays the vibration level, gas level, amount dispatch and temperature level. If vibration sensor, gas sensor, temperature sensor or IR sensor detects, then the information will be displayed on the LCD. If so there is no detection, then it will be displayed as normal condition.

VI. EXPERIMENTAL RESULT

The simulation helps to understand configurations and avoids time wasted on setup problems. The system program written in Embedded C

VII. CONCLUSION

With the wide use of internet this work is focused to implement the internet technology to establish a system which would communicate through internet for ATM secure monitoring system. Internet of things is expected to rule the world in various fields. Hence present work is done to design an IOT based on atm secure monitoring system using a PIC16F877A microcontroller. In this work is designed gas vibration and temperature sensor is used. The data is also sent to the LCD for display so ATM secure status. During any problem occurring in atm to send the information in control room. The Future work.

REFERENCES

[1] 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

[2] Ms. Priyanka. Rao is pursuing BE in Electronics and Communication at Jyothy Institute of Technology, Bengaluru, Karnataka, India.

[3] "Advanced Security Model for Detecting Frauds in ATM Transaction",Vivek. V. Jog, Assistant Professor Dept. of Comp. Engg. SKNCOE, Pune.Nilesh R. PardeshiPG Student University of Pune SKNCOE, Pune. International Journal of Computer Applications (0975 – 8887) Volume 95– No. 15,June 2014.

[4] Yang Yun and Mi Jia "ATM terminal design is based on fingerprint recognition" IEEE-2008

[5] Xihao Zhang, Lin Zhou, Tao

[6] Zhang,Jie Yang"ANovelefficient method for abnormal face detection in ATM"IEEE-2014

[7] Rozeha A. Rashid,Mohd Adib Sarijari,Ahmad Aizuddin Abdul Aziz "Design and implementation of voice recognition system (VRS)"IEEE2008

[8] Siva kumarT,GajjalaAskok, K.SaiVenuprathap,"Design and implementation of security based ATM theft monitoring system" Vol3,ISSUE(August 2013)pp:01-07