Int. Conf. on Signal, Image Processing Communication & Automation, ICSIPCA

IoT based ATM Security using Finger Print Module

Akshata R. Belure[1] and NatarajUrs H D[2]
[1]M. Tech Scholar
Akshatabelure1409@gmail.com
[2]Assistant Professor
natarajurs@revainstitution.org

***Abstract*— The IoT (internet of things) which will help us to connect with devices, systems and services for communication. The paper presents the surveillance of the ATM. ATM frauds are increasing day by day which is now became a very serious issue. ATM has became a target for robbery because of cash availability as the human is very greedy about money. To protect this smart system we use the embedded technology with various sensors for monitoring the surroundings such as physical attack and the theft. This paper presents how to secure the ATM from both the physical attack and Software attack. This system uses the Raspberry Pi, Fingerprint module, GSM and some sensors to protect the system. The present proposed system removes the drawback of manual controlling of door, it is cost effective and this system can stand alone.**

***Index Terms*— Raspberry Pi, Fingerprint module, PIR sensor, Accelerometer, GSM.**

I. INTRODUCTION

The self-banking system has became very popular due to its 24 hours service. To access the money at any time the ATM is helpful. This can be activated by placing the card, and after that we need to enter the pin number of that particular card. But this system is not safe because one can access the money if they have the card and the pin. Even the attack on ATM's are raising due to the availability of cash.

The GSM technology is used to secure the ATM transaction which will send the one time password to the registered number. This method is very secured one in which the OTP will not be known to anyone. To send this OTP the finger print of a person should match, only the OTP will be sent.

The finger print module uses two steps to identify the finger print those are by enrollment and the matching. The finger print of every person will differ that's the reason why we are using the finger print module. The biometric system is very efficient and the result will be accurate. The authority will collect the all personal details of the person during the account creation, at that time they will collect the finger print of a person. After that the authority will provide an login ID to the account holder. Whenever a person wants to access the amount from the ATM the person should enter his login ID and he must validate his finger print then both will sent to bank authority for validation. If this is validated than it will send OTP to the registered number through the GSM system. Once OTP received that person should enter that as pin than the transaction of money will takes place. Even if we lose ATM card than it is not an issue. The main advantage is that no need to carry the ATM card along with us.

This system is divided into two parts, the one part consist of finger print module that is place at the ATM machine which will check the authorized finger print. The second part consists of Raspberry Pi which is

Grenze ID: 02.ICSIPCA.2017.1.6

place inside the ATM for sensing the surroundings and controlling the attacks. The proposed system will prevent the physical attacks made on the ATM by using the sensors. The robbers can directly attack on to the machine itself due to readily available money.
The rest part of the paper is organized as follows: Section II discuss about the ATM attacks, Section III discus the protective measures, Section IV presents related work, Section V gives the proposed system, Section VI gives the flow chart of the system and lastly Section V is conclusion over this paper.

II. ATM ATTACKS

The ATM is a very attractive target for robbers therefore a continuous attacks are taking place everywhere. There are three basic types of attacks on ATM.

- Physical attack: The large force attack is done to gain the money from machine.
- ATM fraud: In this the card information can stolen.
- Software attack: In this a very sensitive information will be hacked.

III. PROTECTIVE MEASURES

The proposed system will protect the ATM machine and money transaction. To protect the physical attack we need to use the burglar circuit, audible alarm or buzzer is used to indicate the attacks on the machine. Even it can be protected by the barriers nothing but the bumpers around the ATM's.
To protect the software attacks we are using the finger print module. Due to which the transaction of money is secured. The biometric technology is used because of its high accuracy and they are efficient. By using the GSM and the alert system we can prevent the attacks and safe guard the machine.

IV. RELATED WORKS

Fawaz A. Alsulaiman[4] have considered the three dimensional password for securing the information. The generation of graphical password using combination of alpha-numeric-Special characters, this is very strong password. But there is a possibility of tracing this password.
SungminEumhave used the concept of face recognition. This technology use Face Recognizability Evaluation for ATM applications with exceptional occlusion handling, the transaction proceeds only after the face of the card holder is recognized. This will help in tracking the suspects. But the disadvantage is that it will not authenticate the legal card holder.
Pennam Krishnamurthy [3] have considered the finger print and the GSM system for securing the ATM. When the figure print of a person is matched the OTP is send to the mobile this can be done by the GSM system. Witout the finger print and the OTP the amount transaction will not happen. This will secure the transaction. The disadvantage with respect to this system is that no back up plans are suggested for the failure of finger print or the OTP system.
K. LaxmiNarshimaRao[2] worked on the recognition of IRIS to protect the ATM. The IRIS recognition technology has the very high accuracy and secured. The main drawback of this system is that high installation and the maintenance cost.
M. R. Dinesh Kumar have considered the concept OTP to protect the cash withdrawal from the ATM. This one is secured but not feasible to everyone.
Lin Hong, Wan Yifei, Anil Jain have worked on the finger print image enhancement. In this they studied about the minutia extraction algorithm to get the high quality finger print image. In minutia they did complete study on the ridge ending and the ridge bifurcation. To get the enhanced image from the input image they provided the flow chart.
Arun Kumar Mistry, Suraj Kumar and Vicky Prasa have proposed their concept to secure the account transaction. Now a days the swipping of the card became a very popular and easy to access. But there may occur a malfunction, to prevent that on after swipping and entering the password it must send a alert message to the account holder after receiving that he must send a confirmation message than only the transaction will take place.

V. THE PROPOSED SYSTEM

- The system will monitor continuously by the sensors and that will help in detecting the attack.

- Whenever any attack happens it will inform to the controller and that will take a safety action.
- Buzzer will sound when the attack over the machine is done by the robbers.
- If the finger print is not verified then it will send a message that someone is trying to access the amount at the same time it will send the location and the time, based on that we can hold the robber.

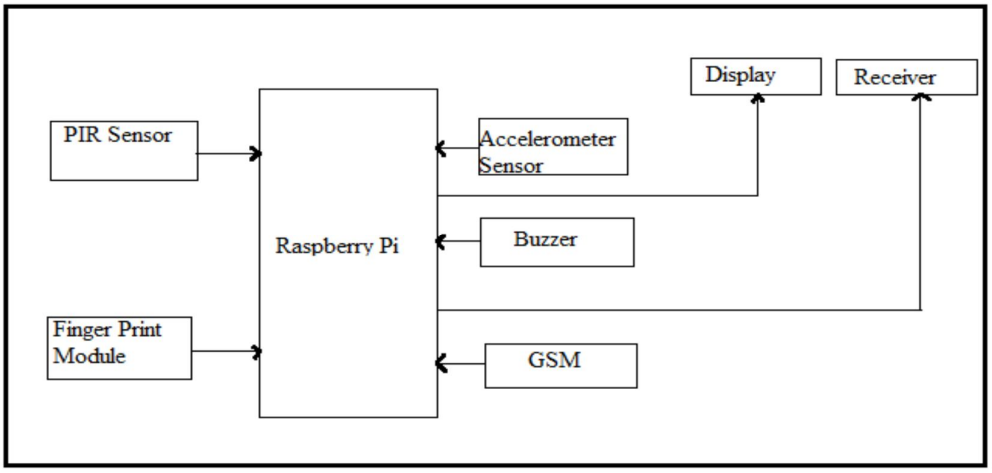

Figure 1. The basic block diagram of the Proposed system

VI. Flow Chart of the System

The flowchart of the proposed system[5] is shown in Figure 2. The ATM will be safe when the sensors are not triggered. When sensors triggered then the ATM is not safe. While relating to the finger print, the transaction will be done when the finger print matched. If finger print not matched it will send a location and time.

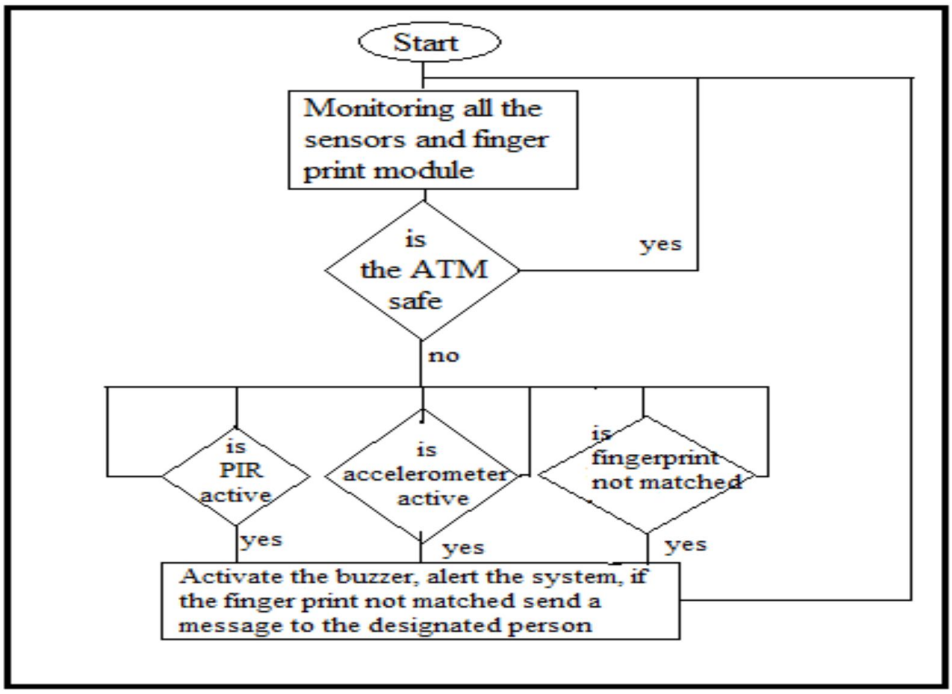

Figure 2. The flow chart of the proposed system

VII. CONCLUSION

The implementation of the ATM surveillance system using smart sensors has stability and reliability. This whole system is based on embedded technology which will provide more security to the system. Nowadays, most of the ATM has attacked by the robbers, in this paper to avoid these attacks we use the real time monitoring system by using sensors, finger print module. The proposed system concludes by the following points:

- Amount transfer from the ATM is secured due to fingerprint module.
- It avoids the manual controlling.
- This system is low cost and efficient one.
- The system it is able to prevent the physical attack and it sends a alert message to the necessary people, they can take an action and they can save the ATM attacks.

REFERENCES

[1] Arjun Kumar Mistry, Suraj Kumar And Vicky Prasa, "Secured Atm Transaction Using Gsm", International Journal Electrical and Electronic Engineering & Telecommunication, Vol. 2, No. 3, July 2013.

[2] Lin Hong, Wan Yifei, Anil Jain, "Fingerprint Image Enhancement: Algorithm And Performance Evaluation", IEEE Transactions on Pattern Analysis and Machine Intelligence, 20(8): 777-789, 1998.

[3] Pennam Krishnamurthy (2012), "ATM Security Using Fingerprint Recognition and GSM", International Journal of Electronics Communication and Computer Engineering Volume 3, Issue (1) NCRTCST, ISSN 2249 –071X.

[4] Fawaz A. Alsulaiman (2008), "Three Dimensional Password for More Secure Information", International Journal on Recent and Innovation Trends in Computing and Communication Volume: 4, Issue:6

[5] S.Shriram, Swastik B. Shetty, Vishnuprasad P. Hegde,KCRNisha, Dharmambal. V, "Smart ATM Surveillance System", 2016 International Conference on Circuit, Power and Computing Technologies [ICCPCT].

[6] Best Practice for ATM Security, GRPBanking Equipment (HK) Co..Ltd,

[7] Mrs. NitashaSoni, Mrs. Jyoti, "AT< Security By Using Fingerprint Recognition", International Journal of Applied Engineering Research,ISSN 0973-4562,Vol.7, No.11,2012.