IOT BASED SMART LOCKER SECURITY SYSTEM

Lokesh M. Giripunje[1],Suchita Sudke[2],Pradnya Wadkar[3],Krishna Ambure[4]

1Assistant Professor, 2,3,4 Student ,

Department Of E&T C, DYPIEMR,Akurdi,Pune

ABSTRACT

This project will focused on effective recognizing and controlling system for Bank locker room which is fully self-determining. In cases of robberies, its commonly happen that the banned entrance in the locker room area which can be detected by our security system. If the robbery take place the banks are not be capable to recognize the robber due to absence of the proof by using the current human operated security system. The system will designed in effective way by recognizing and controlling illegal person to access the locker for the safety of bank locker room. In this, we proposed a three phase conformation of procedure for smart locker, by providing User Name and Password, using Fingerprints and OTP which check out the user. As compare to any other previous approaches our system uses the verification process which generates an OTP to registered mobile number which highlights the smart security. The designed system is highly proficient and consistent because of three security stages and not capable to break the combination of this three stages.

KEYWORDS – Bank Locker Security System, Fingerprint, GSM, Internet Of Things, Wi-Fi module.

I. INTRODUCTION

The Bank,which is a place that indicate very high level security. In day to day life every person are involved in banking transaction. Because of high level security, we uses bank lockers to secure our important documents, expensive jewellery, or cash ect in it. Hence it has become an very important part for every common human being. To suffer in this world and for a continuous development; the banking sector needs to accommodate a very hige rise security. As we know new branches are opening by considering the public interest. Hence more security for every sectors is required. Because of development current system and services becomes autonomous and banking service is not so far from that.

Various researches shows that there are accountability in devices and technologies in security system. The detection of motion will be done by the camera[2] itself and hardware connected with it which provides multisatge security[3] i.e. using PIR sensor and RFID system[4], warning message and the face recognition which identifies the user face[5], and also by using dual keys[6]. Occasionally the biometrice mechanism i.e. fingerprints[8] are used which gives high security. For messaging a GSM module[9], email alert[7] or getting an real time update IOT[10] will be utilized.

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.03, April 2018
www.ijarse.com

IJARSE
ISSN: 2319-8354

Objectives of our work:

Our project uses 2 methods:

Method 1-

- Successfully verify an User name and Password of user.
- verify a user accessing the locker by using fingerprinting.
- OTP which is generated by GSM and identify the user accessing the locker using his/her OTP No.

Method 2-

- By using Wi-Fi third party can Access the locker after authentication process.

II. LITERATURE REVIEW

Sr. no.	Name of paper	Year of publish	Methodology used	Result	Limitation
1	Improving Home Automation Security; Integrating Device Fingerprinting into Smart Home	2016	1)Device fingerrprint using JavaScript 2) Login Credentials 3)OTP generated by sever	To improve the Home Security it verifies the user and also device.	Malicious user tried to gain the access of locker more than one time.
2	Development of an Intelligent System for Bank Security	2014	1)Motion detection 2)messaging through GSM module	Unauthorized image detection signal sends to microcontroller and warring message will be generated	Uses of microcontroller not gives that much of reliable system
3	An Efficient Multistage Security System for User Authentication	2016	1)RFID system 2)Password 3)Biometric consecutively	By using matrix keypad, GSM technology,RFID tag the security system is successfully implemented	The password can be hacked by the unauthorized user
4	An Advanced	2017	1)PIR sensor	Motion is detected	The security

	Internet of Thing based Security Alert System For Smart Home		2)email alert	by PIR sensor then that will sends to owners email which gives the warrning of theft.	alert warrning is only given by the email.
5	Web-Based Online Embedded Door Access Control and Home Security System Based on Face Recognition	2015	1)Face recognition 2)GSM 3)zigbee	In this system monitoring and controling of equipment is based on web.	Face detection takes more complex algorithm
6	Authenticated Secure Bio-metric Based Access to the Bank Safety Lockers	2014	1)dual key safety lockers 2)bio-metrics	This system provides the dual key of an special characters and a biometric is only for staff id.	It can be easily hacked by any unathorized user.

TABLE NO.1 LITERATURE REVIEW

III. METHODOLOGY

This project provides a highly secure, valid and easy to operate for both the customer's who has a locker in a Bank and the head of the branch who responsible for all the operations connected to the safety lockers. Our project works on two methods :

Frist method is, by tripple verification process by user fingerprint, legitimate login credentials and OTP for authorized user. When a user wants to access the locker he/she enters the login credentials, if login credentials verification is passed then system request to give an fingerprint of user. Then the obtain fingerprint is analyzed and matched with original one.

There are two lists in our database; the 'whitelist' is the list which consist of acceptable fingerprints of legitimate users and the 'blacklist' is a list of illegal fingerprints which for, who tried to approch the locker. The whitelisted user with their acceptable fingerprints can only access the locker after OTP No. verification. The blacklisted client along with their fingerprints are not permitted to use the locker although their User Name and Password are correct. The GSM simply generates an One Time Password(OTP) which consist of an random code and send it to the correct

users registered mobile number through message, That code is entered by the user into the webpage and thus authorized person is verified.

If the user is not able to verify any of this stages then that user is added in blacklist and he is not capable to access the locker at all. Then that blacklisted users information is given to that of authorized person. The authorized user can add the users in blacklist if he wants and trusted third party device can access the locker after verification by legitimate user.

Second method is by using Wi-Fi module(ESP8266). Wi-Fi module is used for when any third party wants to access locker. At that time authontication process is carried out by authorized user of that locker using Wi-Fi. If all the verification process is successful then that third party can access the locker.
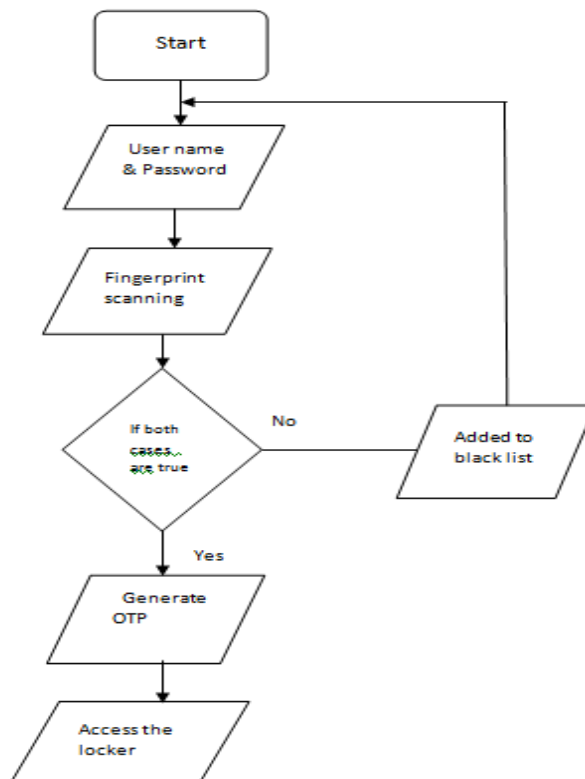
Flow Chart:

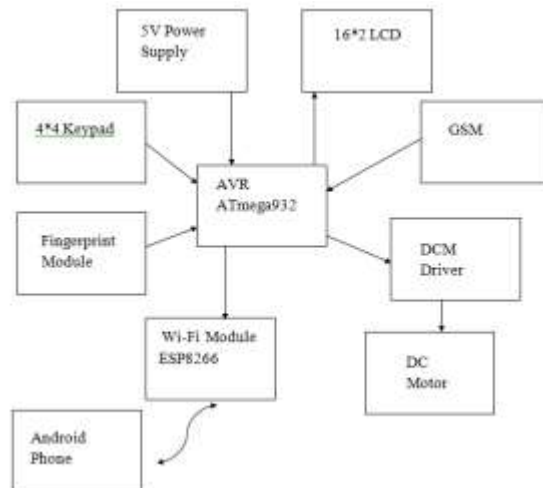**Fig.No.1 FLOW CHART FOR IOT BASED SMART LOCKER SECURITY SYSTEM**

Block Diagram:

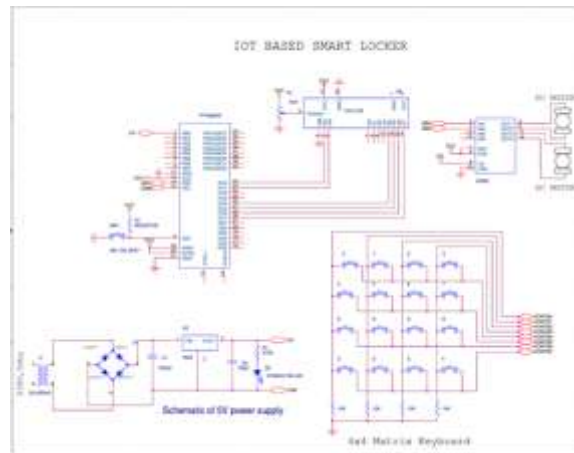**Fig.No.2 BLOCK DIAGRAM OF IOT BASED SMART LOCKER SECURITY SYSTEM**

IV. WORKING AND CIRCUIT DIAGRAM

Power Supply: Our project uses 5V,300mA Variable power supply.It uses stepdown Transformer which has input of 230V,50Hz in primary side that converts into 12V output at secondary side. Then the bridge rectifier circuit which takes input in AC from and Convert it into equivalent DC. That output is passes to filter circuit which gives pure DC. After that regulator LM7805 is used. It helps to regulate the DC and gives the 5V supply at output.

The controller is used in our project is ATmega32 which oprates in 5V supply which is generated by power supply. Keypad is connected to port B that is PB0-PB7. It is 16 key configuration which has 4 rows and 4 column. Rows are made open and columns are connected to VCC i.e to registers of 10k each. The configuration can work when all columns are made high on permenant basis and rows are changes as per requirement. If any key is pressed the potential of row key changes and that particular character will be displed at LCD. That data will be the user Id and password, this will be varified by controller by comparing with stored data which is already in memory.

If that will be varified then contoller activates the Fingerprint module connected at port PB0. This will be acts as input to the contoller. The data required for varification is stored in memory. At that stage the users fingerprint is matched with stored one at authentication process is carried out. After verification of fingerprint the OTP will generated sends to user's registered mobile number via GSM module i.e SIM 800 which is controlled by AT commands and oprates in 3.4~4.4V. As OTP is entered, the controller signals the motor dirver L293D which is used to drive DC motor. As all verification process is successful then door will be accessed.

Another mode is using Wi-Fi mode which is used for give the access to third person. The user must be connected to the access point and after that the password will be entered. If password is correct then access is given to third party.

Fig No.3. CIRCUIT DIAGRAM FOR IOT BASED SMART BANK LOCKER SECURITY SYSTEM.

V.   MODEL OF IOT BASED SMART BANK LOCKER SECURITY SYSTEM

VI.   ADVANTAGES

- It provides three stage security in two modes.
- High accuracy in terms of security.
- No one can hack or crack the system because of using the Android App.
- It is easy to use and required no special training and equipment.

VII. DISADVATAGES

- The unauthorized person cannot recognized clearly.

VIII. APPLICATIONS

- Bank security system
- Home security system
- It is use for protection and safety purpose
- Industrial security system

IX. CONCLUSION

This paper solution is for highly secured reliable smart locker system. The system will effectively detect and control unauthorized access by considering safety of the bank locker rooms. It will convince the bank customers to use system and hence defend their valuable things from robber and also any harm. This system is used where top level security is needed. The future enhancement to this work could be done by adding some more aspect such as face recognition. Therefore it improved the reliability of bank locker and unauthorized access will be minimized. The enhancement could be further applied to identify the illegal entrance.

REFERENCES

[1] Arun Cyril Jose, Reza Malekian, Member, *IEEE,* Ning Ye "Improving Home Automation Security; Integrating Device Fingerprinting into Smart Home"DOI 10.1109/ACCESS.2016.2606478,IEEE Access.

[2] Neeraj Khera, Amit Verma "Development of an Intelligent System for Bank Securiety"2014 5th International Conference-Confluence The Next Generation Information Technology Summit(Confluence).

[3] Ashutosh Gupta, Prerna Medhi, Sujata Pandey, Pradeep Kumar, Saket Kumar, H.P.Singh "An Efficient Multistage Security System for User Authentication" International Conference on Electrical, Electronics and Optimization Techniques (ICEEOT)-2016.

[4] S.Tanwar, P.Patel, K.Patel, S.Tyagi, N.Kumar, M.S.Obaidat "An Advanced Internet of Thing Based Security Alert System for Smart Home"fellow of IEEE and Fellow of SCS.

[5] Mrutyunjaya Sahani, Chiranjiv Nanda, Abhijeet Kumar Sahu and Biswajeet Pattnaik "Web-Based Online HEmbedded Door Access Control and Home Security System Based on Face Recognition" 2015 International Conference on Circuit, Power and Computing Technologies [ICCPCIT].

[6] Srivatsan Sridharan "Authenticated Secure Bio-metric Based Access to the Bank Safety Lockers"ICICES2014-S.A.Engineering college, Chennai, Tamil Nadu, India, ISBN No.978-1-4799-3834-6/14.

[7] K.Balasubramanian, A.Cellatoglu "Analysis of Remote Control Techniques Employed in Home Automation and Security System".

[8] Salil Prabhakar, Sharath Pankanti, Anil K. Jain "Biometric Recognition: Security and Privacy Concerns"

[9] S.V.Tejesvi, P.Sravani, M.L.Mythili, K.Jayanthi, P.Nagesh Kumar, K.Balavani "Intellectual Bank Locker Security System "Int. Journal of Engineering Research and Application ISSN:2248-9622, vol.6, Issue 2(Part-2) February 2016,pp.31-34.

[10] Safa.H, Sakthi Priyanka.N, Vikkashini Gokul Priya.S, Vishnupriya.S, Boobalan.T "IOT based Theft Premption and Security System"DOI;10.15680/IJIRSET.2016.0503229.