JES
Journal of Engineering Sciences

Vol 13, Issue 06, JUNE/2022

ISSN NO:0377-9254

SECURITY BASED BANK LOCKER SYSTEM USING RFID SYSTEM CONTROLLING

G.VEERANJANEYULU[1], D.LAXMI MURTHY[2]

[1]PG Scholar, Dept of ECE, St.Mary's Group of Institutions, Guntur, Ap, India.

[2]Assistant Professor, Dept of ECE, St.Mary's Group of Institutions, Guntur, Ap, India.

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 applying Android App, using keypad to generate OTP which check out the user. As compare to any other previous approaches our system uses the Android App which generates an OTP to registered mobile number which highlights the smart security. The designed system is highly proficient and consistent because of two security stages and not capable to break the combination of this three stages.

Key words: Internet of Things (IoT), Sensors, Security, Rfid, Keypad.

1. INTRODUCTION

Security is of primary concern and in this busy, competitive world, human cannot find ways to provide security to his confidential belongings manually. Instead, he finds an alternative which can provide a full fledged security as well as atomized. In the ubiquitous network society, where individuals can easily access their information anytime and anywhere, people are also faced with the risk that others can easily access the same information anytime and anywhere. Because of this risk, personal identification technology, which can distinguish between registered legitimate users and imposters, is now generating interest. Generally passwords, identification cards and PIN verification techniques are being used but the disadvantage is that the passwords could be hacked and a card may be stolen or lost.

In current scenario, bank and locker robberies are frequently happening; this means our locker is to theft since it has no ultimate protection rather than a lock and key. In the automated world of living, new technologies are evolved day by day and there is a need of peculiar attention on rendering security to lockers. Nowadays larceners are becoming too smart in larceny and opening the lockers brilliantly. To protect our possessions from them is highly challenging task to public. It is a painstaking job for the bank administration to track an account of the locker activity as there is no dedicated employee for tracing the locker activity. To get rid of these issues, bank security system like this one is needed which does not require any special invigilators for 24x7 monitoring of lockers. Lockers are used to safeguard the money, Jewelry, Important documents and licenses. Locker security system is most important for the safety of money, Jewelry, Important documents and licenses. Currently, most of the banks use two keys to open the lockers. One key is with the customer and another key is with the bank manager. In this case, the bank manager cannot open the locker without the acknowledgement of the

customer because those two keys must be inserted at the same time while the opening of the locker. This system is having the following drawbacks.

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 jeweler, or cash etc 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 huge 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 multi stage 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 biometric 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.

2. LITRATURE REVIEW

Approximately after 35 years the Internet went important, and today the world, its people, and devices are connected in ways that the Internet's importance could never have imagined For a common individual the bank infers a spot which addresses a best component of security. Reliably we are drawn in with banking trade. To confirm our exorbitant pearls, basic reports or cash, we use to use bank locker rooms. It has transformed into a basic bit of our life. To get by in this forceful world and for a predictable improvement, the budgetary business needs to give an abnormal state of security. Because of the open interest every day new branches are opening. The more number of branches required more noteworthy security. Current structures and organizations are ending up to a regularly expanding degree independent and the monetary region isn't unreasonably far from it. Video observation in moving domains has transformed into a present topic of energy for PC vision development. You can see all the branches are under the perception of CCTV cameras, alert systems, emergency gets, etc. The CCTV cameras are used to screen the unapproved activity. It ought to be watched reliably by an individual which is troublesome work; especially in nighttimes. The alert emergency get moreover needs to be pressed physically. This conventional structure requires some portion of work. A structure can be made which will customized recognize unapproved development and instruct to the security experts concerning the banks by different ways with no need of a person. The Microcontroller Based Bank Security System fulfills all these necessities. A model of this security structure has been arranged in the composition to extend the component of security in bank locker rooms enough. The development area will be done through camera itself and the hardware related with it will give unmistakable ways to deal with light up the security experts for instance using alert system a notice message and the image which has recognized the development will be normally exchanged on page which can be downloaded from wherever. For illuminating a GSM module will be utilized. The fundamental point of this examination is to structure a framework for alarming burglary and to auto capture the

criminal in bank or ATM itself from brought together checking unit. The motivation behind the framework is to plan a savvy and concentrated checking and control framework utilizing IOT advances. The basic objectives of bank security system are following the bank locker room locales, acknowledgment of development and making the principal control move. The further portions will depict that how these objectives have been practiced.

3. THEORATICAL CONSIDERATION

Cortex is the major modules used in the project whose detailed information is discussed in this chapter. Along with all the individual modules and their explanation is provided in this chapter. Block diagram gives the brief idea about the overall modules used which is the explained prior to all other information.

4. BLOCK DIAGRAM

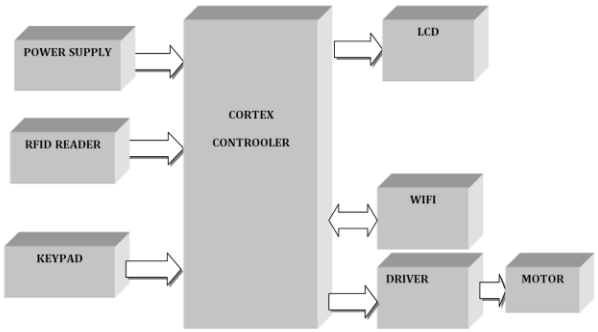

Fig 4.1 Block diagram

5 FLOW CHART

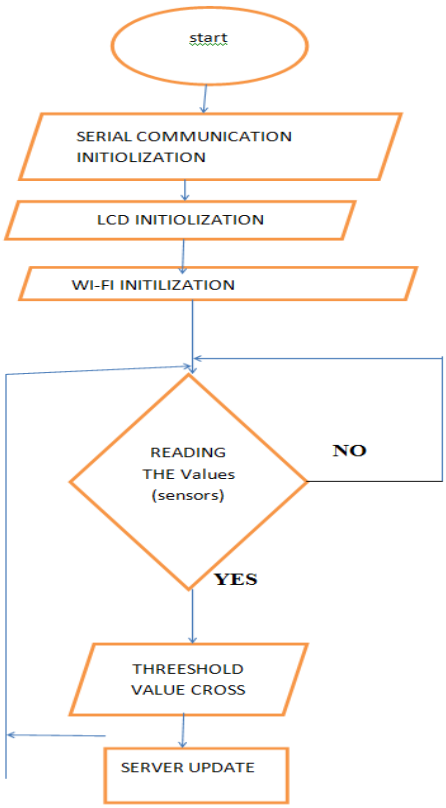

Fig 4.2 Flow chart

6. DESIGN ASPETS

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 : First method is, by two verification process by user RFID reader, 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 rfid of user. Then the obtain rfid card is analyzed and matched with original one. There are two lists in our database; the 'white list' is the list which consist of acceptable fingerprints of legitimate users and the 'blacklist' is a list of illegal card person which for, who tried to approach the locker. The white listed user with their acceptable rfid 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 keypad simply generates an One Time Password(OTP) which consist of an random code and send it to the correct 887 | P a g e 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 authentication 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. The configuration can work when all columns are made high on permanent 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 display at LCD. That data will be the user Id and password, this will be verified by controller by comparing with stored data which is already in memory. If that will be verified then controller activates the Fingerprint module connected at port PB0. This will be acts as input to the controller. The data required for verification is stored in memory. At that stage the users fingerprint is matched with stored one at authentication process is carried out. After verification of RFID the OTP will generated sends to user's registered mobile number via keypad module. As OTP is entered, the controller signals the motor driver L293D which is used to drive DC motor. As all verification process is successful then door will be accessed.

7. RESULTS

This is part of my "sensors using ARM7" tutorial series, explaining how you can create kite using In this article we will see how we can we measure the values of sensors cortex.

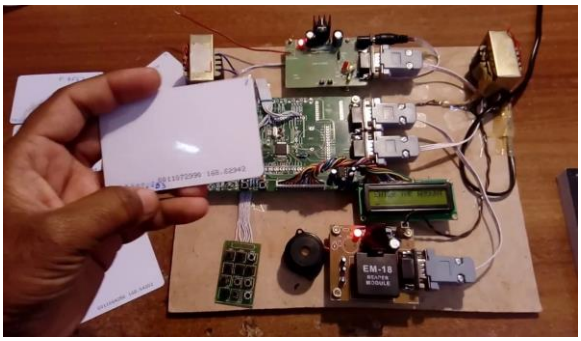

Fig 7.1 Hard ware implementation

8. CONCLUSION

We have implemented a Bank locker security system using IoT. In this project we presented a system that allows if a person tries to access the locker the signal conditioning unit will be activating the complete circuit and it will be scan rfid card. If the person is known to the user, he/she can permit the locker to open. Else if the person is of unknown to the user,he/she can make the locker to be in a closed state. Thus the bank locker will be of highly secured from unknown person.

9. FUTURE SCOPE

The developed system is very much flexible. The system we have created operates on only one lock, but in our current state, we can add more electronic locks, where each lock can be unlocked with specified print IDs. All it will need is more electronic locks and code modifications. There can be some other implementations to this system as well, some of them are given below.

Multi-lock/ Decoder network system:

As mentioned earlier, this system currently has one lock connected to, and we can add up to 5 more. In fact, by using a network of decoders, we can connect as many locks as we want and provide access to up to 126 different individuals. As shown in Fig. 7 a decoder network can be used with this system. Additionally, 6 different locks can be added. Instead of using those output pins from the no for locks, we can create a system using 7: 128 decoders. In that way, all the memory space of the fingerprint sensor (126 capacity), connect them to individual doorway or doorways with just one system.

REFERENCES

[1] JuhaHyyppa, et al "Map updating and change detection using vehicle-based laser scanning", Urban Remote Sensing Event, 22 May 2009.

[2] Tessa Tielert, Moritz Killat, Hannes Hartenstein, Raphael Luz, Stefan Hausberger, Thomas Benz, "The impact of traffic-light-to-vehicle communication on fuel consumption and emissions", Internet of Things (IOT), 29 Nov.-1 Dec. 2010.

[3] Chi-Man Vong, et al "Framework of vehicle emission inspection and control through RFID and traffic lights", System Science and Engineering (ICSSE), 2011 International Conference, 8-10 June 2011.

[4] Yuxiang Sun, Nan Wu, et al"Development of driving support system for electric vehicle by using image processing technology", Control, Automation and Systems (ICCAS), 2012 12th International Conference, 17-21 Oct 2012.

[5] N. P. Jain, P. N. Jain, T. P. Agarkar, "An embedded, GSM based, multiparameter, realtime patient monitoring system and control — An implementation for ICU patients", Information and Communication Technologies (WICT), 2012 World Congress on 30 Oct.-2 Nov 2012

[6] Mehaseb Ahmed Mehaseb et al"WSN Application Traffic Characterization for Integration within the Internet of Things", Mobile Ad-hoc and Sensor Networks (MSN), 2013 IEEE Ninth International Conference, 11-13 Dec 2013.

[7] Chi-Man Vong, Pak-Kin Wong, Zi-Qian Ma, Ka-In Wong,"Application of RFID technology and the maximum spanning tree algorithm for solving vehicle emissions in cities on Internet of Things", Internet of Things (WF-IoT), 2014 IEEE World Forum, 6-8 March 2014.

[8] Bill Montgomery, "IoT benefits beyond traffic and lighting energy optimization", IEEE Consumer Electronics Magazine, Volume: 4, Issue: 4, Oct. 2015

[9] M. Surya Deekshith Gupta, VamsikrishnaPatchava, Virginia Menezes, "Healthcare Based On Iot Using Raspberry Pi", Green Computing And Internet Of Things (Icgciot), 2015 International Conference On 8-10 Oct 2015.