International Journal of Scientific Research & Engineering Trends
Volume 7, Issue 2, March-April-2021, ISSN (Online): 2395-566X

Bank Locker System Using IOT Concept

Saifali Shaikh, Rani Jawale, Rushikesh Kandalkar, Onkar Shinde,Prof. Ganesh Kakade, Prof.Shrikant Dhamdhere(HOD)
Department Of Computer Engineering
Parvatibai Genba Sopanrao Moze College Of Engineering Wagholi
Pune.
saif.shaikh914@gmail.com, rj.ranijawale03@gmail.com, hrishikandalkar@gmail.com, onkar.shinde2010@gmail.com

***Abstract*- The main aim of this project is to develop a device for the bank locker security purpose for alerting theft and to auto arrest the thief in bank itself from centralized monitoring unit and control system using IOT technologies. Even the latest technology such as fingerprint sensor lock can be unlocked with ease. So to overcome this problem , this project suggest the use of Internet of Things(IoT) to provide secure enter only to authorized person. For this we are using Raspberry Pi for capturing image, processing it and then sending it via mail to the user's email account. The Raspberry Pi captures the image when a person tries to enter the bank locker and then process it and sends it to the user's email account as picture message. The user can then provide authorization to the Raspberry Pi from his/her email account whether to open or remain it shut.**

***Keywords*- Convolutional Neural Network, Image processing, Feature extraction, Segmentation, Identification, Classification.**

I. INTRODUCTION

In this period of innovation we have seen a few advances which are even hard to envision. Be that as it may, best of best organizations or associations can't carry out the successful route for Bank storage security framework. To address every one of those security issues related with the banks, we need a successful swap for our conventional actual storage spaces. At the point when any Authorized individual needs to get to a bank storage then he expected to get his face checked by our face acknowledgment framework. In the event that the approved individual isn't visiting the area and somebody sake of him might want to get to the storage then they need to introduce the static secret phrase and OTP created upon demand as shared by approved individual.

The approved individual will likewise be given a static secret key already and he should change his static secret key opportunity to time. The OTP with Static secret key is an elective technique for getting to the storage. The movement locator what capacities in night helps in a guarding the storage region for any the moreover. Typically, when an individual visits a bank, there is a safety officer utilized by the bank to ensure that the individual entering the storage is authentic and is getting to his storage as it were. In any case, the current game plan has a couple of provisos and furthermore requires labor.

In the RFID innovation in the event that somebody attempts to open the storage it will be detected and sends the sign message to the client through GSM. In this finger print strategy, the storage in the bank will be opened just when the novel graphical security is drawn on the screen and furthermore the example can be effortlessly distinguished by obscure individual and that individual can undoubtedly open the storage with no special case from the client. The principle disadvantage is that it won't recognize who is opening the storage. In this system the strategy carried out was that the bank storage can be opened exclusively by the confirmed client with the assistance of his/her unique finger print. It is not difficult to follow the validated client unique finger print without his/her insight. With the assistance of finger print obscure individual can undoubtedly break the unique finger print security framework.

II. LITERATURE SURVEY

An Automated Safety Vault with Double Layered Defense Mechanism was planned [1]. The arrangement included an Electronic Lock driven by secret word confirmation and a Biometric verification for clients utilizing a Fingerprint filtering and detecting instrument. Both of these two layers guaranteed the credibility of the client by forestalling any unapproved enter to the Vault. The framework was then executed in a model degree for testing and approval of the recommendations. The carried out framework and testing information showed that the Automated Safety Vault with all its security highlights had effective activity. The detail of the entire framework just as the outcomes was noticed and confirmed.

Planned [2] and carry out a bank storage security framework dependent on Finger print and OTP innovation. This can be coordinated in bank, workplaces and homes. In this framework just the verify individual recuperate the records or cash from the storage spaces. In this security framework finger impression and OTP is utilized. In this framework first individual select client name and secret word and versatile number. In the event that client name

© 2021 IJSRET

and secret phrase matches, Finger of individual will recognize and store with ID. In the event that the ID gets matches. At that point four digit code will be sent on approved individual portable to open. So biometric and Bluetooth security is a bigger number of benefits than other framework. This framework can likewise make a log containing check in and checkout of every client alongside essential data.

The thought was to build up a Bank Locker Security framework [3] that allows the director to see the events from a confined territory and discover the edge contingent upon its benefit. This will be acclimatized by arranging site pages, associating them with the information base, picture getting by raspberry pi, face affirmation, face revelation, organizing of the application and allowing/ denying the customer section.

They [4] gave two choices to an approved individual to have an enter to his storage. One is Face Recognition framework and other alternative is OTP alongside static secret phrase. Our definitive test would be the means by which adequately and precisely we will execute this approach. The framework has Object Detection sensor for distinguishing object inside the storage. At the point when someone goes into bank then the bell will be on. The framework incorporates the Object Detector, Wireless Motion Detector (WMD), microcontroller, LCD show, ringer and 5V force provided to work the framework.

III. HARDWARE SETUP

- Raspberry pi :- Acts as an controller to the system
- PIR Sensor
- LDR
- IR Sensor
- Lock
- GSM Module
- Camera
- Buzzer
- Light

IV. IMPLEMENTATION DETAILS OF MODULE

In this system, if a person tries to enter the locker the signal conditioning unit will be activating the complete circuit and it will be sending the picture to the authenticated user via email. The camera is kept next to the locker. The person who is trying to enter the locker will be captured by the camera and then it will be processed in Raspberry Pi and sends it to the user's email account as picture message. If the person in the image is known to the user, he/she can permit the locker to open, Else the locker to be in a closed state if the image is of unknown to the user.

Hence the locker can be highly secured from unknown person. LDR is used to sense intensity of light. If intensity of light is below a predefined limit then light will be turned on, on detection of person in night mode. For controlling light a relay will be used which will be controlled through raspberry pi.

Assume bank was locked and a thief enters at bank then this framework will give a caution through the burglary action. PIR sensor was fixed in various part of bank and IR sensor was fixed in the entrance of every room, all the doors are connected with magnetic locks controlled by relay and burglar alarm connected with the relay circuit. We utilize the IR Sensor for catching the present location of thief inside the bank. Thus IR and PIR sensor detect the motion and presence and offer back to the microcontroller.

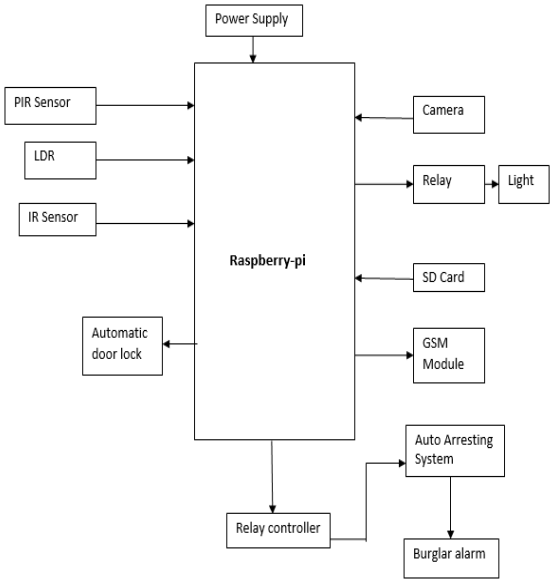

Fig 1. System Architecture.

While in central processing unit all the actions were monitored by the executives and information will be passed to the bank managers and local police stations. After that if the theft was confirmed by the executives by checking the values of several sensor inputs, executives activate the arresting system which locks all the doors inside the bank like manager room, locker room, etc.. And then the executive activate the burglar alarm. Also SMS will be sent to police through GSM module to take action.

Then the thief will be arrested with auto arrest system. We link all sensors in the IOT terminal. We set up web based application to monitor or control the movements in the bank.

V. CONCLUSION

In this project we presented a system that allows if a person tries to enter the locker the signal conditioning unit will be activating the complete circuit and it will be

© 2021 IJSRET

sending the SMS to the authenticated user via GSM. In addition, the camera is kept next to the locker.

The person who is trying to enter the locker will be captured by the camera and then it will be processed in Raspberry Pi and sends it to the user's email account as picture message. If the person in the image is known to the user, he/she can permit the locker to open. Else the locker to be in a closed state if the image is of unknown to the user. Hence the locker can be highly secured from unknown person.

REFERENCES

[1] J.S Vimali, Senduru Srinivasulu, Gowri. S, "IoT Based Bank Security System", International Journal of Recent Technology and Engineering (IJRTE), 2019.

[2] Lokesh M. Giripunje, Suchita Sudke, Pradnya Wadkar, Krishna Ambure "BASED SMART LOCKER SECURITY SYSTEM", International Journal of Advance Research in Science and Engineering, 2018.

[3] Bhupesh Mankar , Digvijay Raut , Akash Bobde , Ishant moon, "Performance Survey on IOT Based Security System for Social Safety", International Journal of Innovative Research in Computer and Communication Engineering, October 2018.

[4] Hiloni S. Detroja and Disha D. Kotadiya and Prutha J. Vasoya, "GSM Based Bank Locker Security System using RFID, Password and Fingerprint Technology", International Journal for Innovative Research in Science & Technology, April 2016.

© 2021 IJSRET