Advanced Home Security System Using IOT

Vinoth R[1], Nagaraj G[2], Vetri E[3]
[1]*Assistant Professor, Department of Information Technology, Agni College of Technology, Chennai*
[2,3]*UG Student, Department of Information Technology, Agni College of Technology, Chennai*

Abstract **- Human detection and recognition field is very significant and has undergone rapid changes with time. An important and very reliable human identification method is fingerprint identification. Fingerprint of every person is unique. Therefore, this helps in identifying a person or in improving security of a system. A special type of sensor reads fingerprint of a person. Fingerprint sensor can be interfaced with a microcontroller. Through keypad, we can add new user and delete the existing user, also identify the user by selecting corresponding option through keypad. In this project, we use a fingerprint sensor to read ones identity to automatically operate the door. Initially the fingerprint is authorized it will access and if not authorized person or un known user is try to access the system, the face of the person is snapped and send to the Admin mail. The time of Unavailability of Authorized person is complex process in current market products, here we provide OTP option also generated simultaneously and the OTP send to a mail of the authorized person as well as accessed persons image. If the OTP is shared, he can access the door. The PIR sensor also implemented here to take the snap of the person if anyone near to the door when it was enable and which is used for knew the person who is in front of the door by authorized person through the snap via mail. If we have a network problem, we can use Security Questions but here we store the person's image in local memory. So that we ensure the security in each level of verification.**

Index Terms **- Internet of Thing, Email, Fingerprint, Secured, Arduino, Micro Controller.**

I.INTRODUCTION

Increase in anti-social activities could be a reason behind concern as criminal considers the banks. Increasing incidence of crimes against banks has necessitated a significant re-look at the protection arrangements and pointers followed by the banks. The prevailing crime situation demands compatible, economical and reliable security and safety measures. So as to beat this sort of frauds, authentication of the one who desires to use the locker is incredibly vital. Within the omnipresent network society, wherever people will simply access their data anytime and anyplace, folks also are featured with the chance that others will simply access a similar data anytime and anyplace. Due to this risk, personal identification technology, which might distinguish between registered legitimate users and imposters, is currently generating interest. The projected system are developed on Associate in Nursing authentication system exploitation fingerprint and SMTP technology. Statistics deals with machine-controlled technique of distinguishing someone or supportive the identity of someone supported the physiological or behavioural characteristic, and then square measure used for authentication in several of the net transactions. The biometric that has been chosen for implementation is fingerprint since fingerprint biometric is well on the market and extremely reliable compared to several different statistics. Fingerprint of the users is keep in initial and therefore the verified at the time of use.

If fingerprint is matched to the trained prints, then access was accepted once more through SMTP OTP was generated mechanically so send to registered mobile variety. If it absolutely was written by data input device, then LCD displays approved person accessed. Fingerprint verification is one amongst the foremost reliable personal identification ways in statistics. If we are not available for certain days, we can enable the PIR sensor to monitor our house it will snap and store those are come near the door. The OTP also shared after getting persons information and verification of the Authorized person. In this project we are providing three level of Security. If we face any network issue during the OTP sharing, then we may use last level of security by our predefined Security questions. Here we ensure the security by store the person's image in local memory.

II. ARCHITECTURE

A. Literature Survey

Jayasree Baidya et al (2019), Security has always been a major concern for the households and the office environment, and for this concern various approaches are in place to address the problem. Most of the major door lock security systems have several loopholes which could be broken down to gain access to the desired places, and it creates a concern for a secure lifestyle and proper working environment. Additionally, terrorism and unauthorized access to places have become a major issue now-a-days, and there is a need for a secure system to prevent unauthorized access especially in shared access environment. With this consideration, a design and prototype of a biometric fingerprint-based door lock system has been presented in this paper. Biometric systems such as fingerprint provide tools to enforce reliable logs of system transactions and protect an individual's right to privacy. The RFID or password-based door lock mechanisms can easily be compromised when the RFID card or passwords are shared or stolen, thus for facilities with shared access require biometric-based secure system. In the proposed system, fingerprints of the authorized users are enrolled and verified to provide access to a facility that is used by multiple users. A user can also be removed, and a new user can be enrolled in the system. We have implemented a centralized control system from where we can control who can enter in which rooms and who cannot. This is an Arduino UNO device based flexible working device that provides physical security using the fingerprint sensor technology.

N Meenakshi et al, Security is the serious issue looked by everybody when we are far from our family unit. In the present situation acceptable answer for the above issue isn't yet found. Introduced here is an electronic securing framework which Arduino assumes the job of the preparing unit. Arduino which is a microcontroller board has a place with at uber family. It is an open source straight forward instrument. It can detect, screen, store and control application. Access control for the entryway is accomplished utilizing Arduino Mega 2560 board. This task displays a keyless framework for locking and opening purposes utilizing a predefined PICTURE secret key and OTP. Unauthorized person access is ensured by sending OTP and PICTURE password to ADMIN to get OTP and PICTURE password where the person needs to contact the ADMIN to get OTP and PICTURE password. It is entered through the 2.8" TFT touch display, which display all the UI messages and takes inputs from user. In case of authorized user, the system allows fingerprint sensor to validate the person followed by sending either PICTURE password or OTP via SIM using GSM module to the user registered mobile number saved in database (local SD card) in order to access the door. If the entered password matches, door will be opened automatically otherwise a message showing incorrect password will be displayed on TFT display and a notification will be sent to the owner that the security was tried to be breached. This hardware project achieves 3 levels of security with commonly available component and also consumes less power. This system also has an option to unlock the door through SMS in case of emergency by the ADMIN.

In this paper we have ensure the uniqueness by literature survey and we have referenced by lots of IEEE papers.

B. Existing Methodology

The Existing system has few digital techniques for Door security locks. These modern smart locking systems replace the role of traditional locking system which has lock and keys. The drawback of these locks is they can be easily welded without any alert to the user. People want their home, office, shops to be secured. This need for people is the main reason for developing smart lock.

Finger print locking System

Fingerprint locking system is a locking system using the user fingerprint with the help of fingerprint sensor module. The fingerprint sensor module the works with the help of Arduino or raspberry pi. The Fingerprint module checks the given fingerprint authorized or unauthorized. The locking system uses the user fingerprint to unlock the system. But the Authorized person should available all the time.

Pin /Password locking System

In Existing smart door lock Pin or password authentication is used along with the fingerprint authentication. It is used to unlock the system directly or used in the case of fingerprint failure. Most of the smart lock system pin number using keypad. The Existing systems has pin authentication to make users

easy when fingerprint sensor is not working. And the main advice to the user is to not to share the pin number with the outsiders or typing pin number visible to unknown persons.

RFID card

The user can unlock the system by using RFID card stands for radio frequency identification. The radio frequency in scanned by the scanner and check whether the identity is authorized or unauthorized. The main drawback of this system is hackers can duplicate these cards. So the user has the handle it safely. The Existing systems in market had RFID card with other security types like fingerprint, pin authentication, IOT access, etc.

OTP using GSM

OTP stands for one time password with is used for randomly changing the password for security purpose. OTP should be given in a particular time period otherwise the system will not recognize the password then the user has to refresh the OTP. The OTP is sent as a message using GSM modem, which is, used the send message to the registered mobile number.

Prof. Benazir H.M (2017) the author has discussed that, in the present current world, security assumes an essential job. For that reason, we proposed development security frameworks for managing an account locker framework and the bank clients. In this task we structure and actualize locker high security framework dependent on fingerprint, secret word and GSM innovation which can be composed in banks, ensured office and homes. It diminishes wastage of time for both broker just as client and gives propelled security. In this bank will gather the biometric information of every individual for allocating the lockers just credible individual can be recouped cash, records from the locker.

Akanksha singh (2015) the author has discussed, the way to control home machines, wellbeing and security framework utilizing GSM innovation by utilizing android application through android portable telephone. We will likewise demonstrate that we can control the machines even without an android telephone by sending an ordinary SMS. The benefit of utilizing GSM innovation is that we can control the home machines from remote places anyplace on the planet. This framework enables the proprietor to control the machines and to get a criticism status of the home machines by sending directions in type of SMS just as through an android application. For the home security framework, we are utilizing an antitheft detailing framework which will report the proprietor by ringing a caution and by sending a SMS. Additionally, for the wellbeing framework in the event that of flame or gas spillage it will report the proprietor by sending a SMS and furthermore by ringing an alert. In this manner by utilizing GSM innovation, it gives the remote access to the gadgets to be controlled.

Raqibull Hasan (2015) the author has discussed planning and execution of a microcontroller-based home security framework with GSM innovation have been exhibited and examined. Two microcontrollers with other fringe gadgets, which incorporate Light Emitting Diode (LED), Liquid Crystal Display (LCD), Buzzer and Global System for Mobile Communication (GSM) Module, are in charge of solid task of the proposed security framework. Furthermore, a cell phone is interfaced with microcontroller through a Bluetooth gadget so as to control the framework. Additionally, manual keypad is another approach to bolt or open the framework. A Compiler Code Vision AVR is utilized to plan a program that controls the framework alongside keeping up all security capacities. The planned program is connected in Proteus Software for recreation. Finally, the aftereffects of down to earth circuit demonstrate the best possible capacities and furthermore confirm the dependable security inside sensible expense.

Limitations of Existing System

- The Existing system some time fails to provide security by various attack by hacker or unknown persons.
- The Existing system has fingerprint authentication for door lock system which may be open by unknown person by duplicating the fingerprint impression of the user.
- Another way of opening the lock is pin or password authentication. Here the user has to keep his password secured. In some cases, the hackers may get the password using various attacks or by using the scanner to check the finger impression on the keys
- The main drawback of IOT device is, they can't work without internet, so in the case of failure of power supply IOT may not work. And if the IOT

server is overloaded or error in server may became a problem

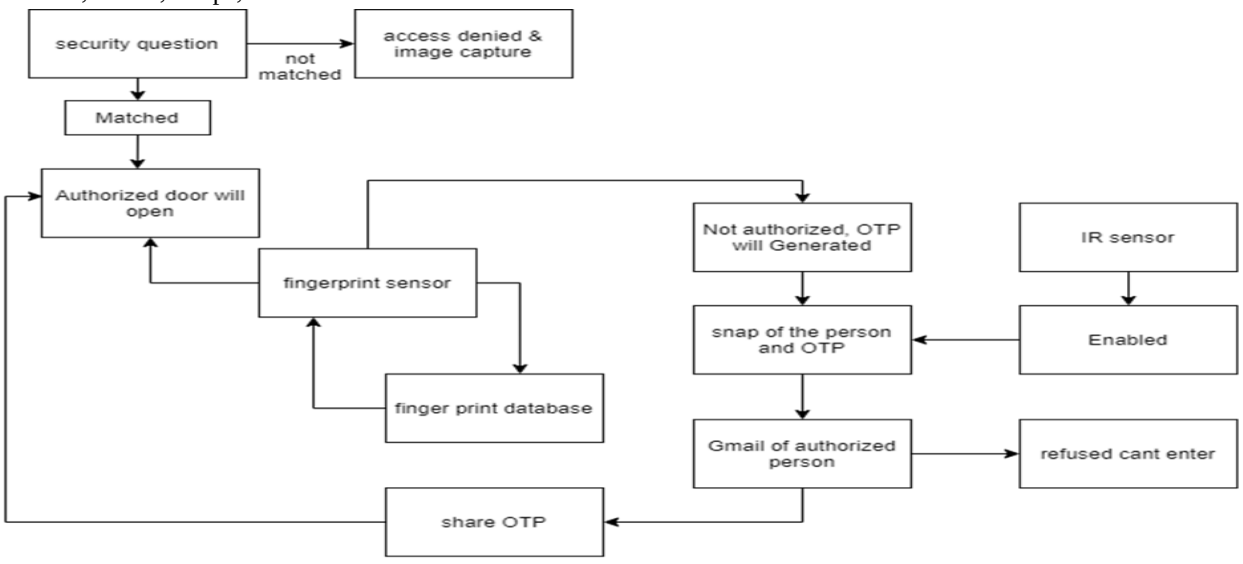
- Using RFID card to locking system is developed to make the user to easily lock or unlock the system. It is used in failure of pin and fingerprint, but these types of card can be duplicated.
- The drawback of the Existing system is, some system has more than one security in the same system but it requires any one authentication to unlock system
- Some system has two level authentications, but it can be easily hacked by hacker and guest can't be entered until the authorized user has to come and open the door.
- The process of changing the password and fingerprint is a difficult process in the Existing system.

C. Proposed Methodology

Our Proposed system overcomes all the security problems in the existing system and provides high security and efficiency. This is a perfect and optimal solution for saving one from the hassle of stolen or an unauthorized entry. The main advantage of our project is no can enter into the home without the knowledge of authorized person. If any unauthorized person can enter into the home without the knowledge of authorizer, our project helps to know the peoples who want to enter into the home without the permission of authorized one. This process overcome the problems faced by the Existing systems.

The Proposed system is used to provide high security to home, office, shops, etc. because as mentioned in above the Existing system can be hacked by cracking any one password, which is produced in the system. In our project, we have implemented four advanced features that is fingerprint, OTP generator, IR Motion detector and Security questions. In finger print sensor, we have to sense the fingerprint of authorized persons, if the fingerprints are matched to the authorizer the door will be opened or else the door cannot be open at the same time the snap of the unauthorized person is send to the authorizer one through the mail. In OTP generator, we have to use unauthorized person, if they are relations or friends want to open the door when the authorized persons are not available in home at the time. That situation we have to use OTP Generator. It helps to generate the OTP and snap of the person by webcam is send to the mail of authorized person. When the authorizer verified the persons of the snap then only, he shares the OTP as a password to the unauthorized person. if the OTP is matched, the unauthorized person can enter into the home or else the door cannot be opened.

IR senor is used for detecting the any unwanted motion when the authorizer was not available in the home. At the situation the webcam took the snap of the motions and send to the authorized person through the mail. Finally, we have to implement the Security questions, which is used for the persons who's want to enter into the home in poor network connections. At the time, the authorized person can share the answer to security question. if the answer is correct the door will be opened or else the door cannot be opened. So, the Proposed system is mainly used for overcome the security issues.



Arduino Mega 2560

Arduino Mega 2560 is a microcontroller board dependent on the ATmega2560. It has 54 advanced info/yield pins (of which 14 can be utilized as PWM yields), 16 simple sources of info, 4 UARTs (equipment sequential ports), a 16 MHz precious stone oscillator, a USB association, a power jack, an ICSP header, and a reset catch. It contains everything expected to help the microcontroller; just associate it to a PC with a USB link or power it with an AC-to-DC connector or battery to begin. The Arduino Mega can be controlled by means of the USB association or with an outer power supply. The power supply for the board ought to be 6 to 20 volts. Arduino Mega can be customized utilizing Arduino programming.

Fingerprint Sensor

Unique finger impression sensor is utilized for client ID. This is utilized for record distinguishing proof which give security to singular records. Unique mark handling incorporates two sections: finger impression enlistment and unique finger impression coordinating. While selecting client needs to enter the finger multiple times. The framework will process the two-time finger picture, create a format of the finger dependent on handling results and store the layout. While coordinating, client enters the finger through optical sensor and framework will produce a format of the finger and contrast it and layouts of the finger. Framework will contrast the live finger and explicit layout assigned in the module. In the event that the live unique mark is coordinated the framework continue effectively, else it is disappointment.

Software and Programming

The following software is used to build the proposed system:

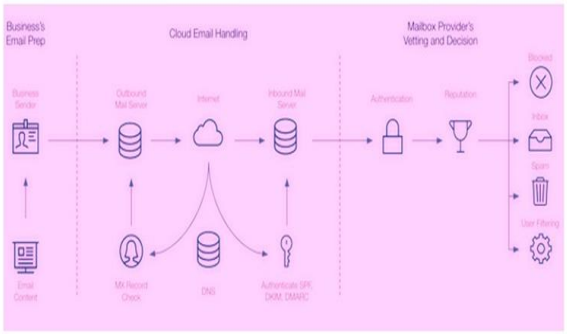
- Arduino software.
- Language used in 'python' program. The system uses Arduino mega 2560 as the microcontroller which is used to connect the other parts and process the working of these parts. So we use Arduino software to give instruction in a form of program (python language) to the board.

Email Delivery

An SMTP (Simple Mail Transfer Protocol) server is an application that's primary purpose is to send, receive, and/or relay outgoing mail between email senders and receivers. An SMTP server will have an address (or addresses) that can be set by the mail client or application that you are using and is generally formatted as smtp.serveraddress.com. (For example, Gmail's SMTP server address is smtp.gmail.com, and Twilio SendGrid's is smtp.sendgrid.com. You can generally find your SMTP server address in the account or settings section of your mail client.)

When you send an email, the SMTP server processes your email, decides which server to send the message to, and relays the message to that server. The recipient's inbox service provider, such as Gmail or AOL then downloads the message and places it in the recipient's inbox. Without an SMTP server, your email would not make it to its destination. Once you hit "send," your email transforms into a string of code that is then sent to the SMTP server. The SMTP server is able to process that code and pass on the message. If the SMTP server weren't there to process the message, it would be lost in translation.

Additionally, the SMTP server verifies that the outgoing email is from an active account, acting as the first safeguard in protecting your inbox from illegitimate email. It also will send the email back to the sender if it can't be delivered. This informs the sender that they have the wrong email address or that their email is being blocked by the receiving server. Twilio SendGrid offers free accounts that don't even require a credit card to enable. With a Twilio SendGrid free account, we give you access to the Twilio SendGrid SMTP server and allow you to send up to 100 emails/day. Active free account customers can use their account to send test messages and test their email deliverability before upgrading and sending larger amounts of email.



D. Authorized Person

The Authorized person can use fingerprint to open the door and the authorized person have three different

options to open the door. The Authorized person only have power to admit other known users and the proposed system have three different levels of security to ensure the security of the house.

E. Unauthorized Person

The Unauthorized person in our proposed system have two different options to open the door either they can use OTP option or Security question. To use of OTP option he should available in front of camera for snap a picture. After the verification of the Authorized person then only the unauthorized person can open the door.

F. Advantages of Proposed System

- Image with OTP password as a third security level
- Highly accuracy in term of security
- Relatively low cost so that everyone can use at their home, offices, shops, etc.
- Fingerprint enrolment is easier.
- Unlocking the system using any two security levels out of three security levels
- It helps to keep the place secure then other devices
- Alert message is sent when the first level is wrong, hence the user is alerted soon.
- No false intrusion
- No manual errors
- Maintenance of time

G. Application of Proposed System

- Security for homes
- Security for shops
- Secured offices, industries, server room
- Secures locker, gun box, bank lockers, etc.

III.CONCLUSION & FUTURE STUDY

In present situation, there are possibilities to hack and unlock the smart locks. The proposed system can overcome the security issues faced in the present situation. The 3-level security in the system can help the user for accurate security. The main reason for the proposed system is to secure the user living place, working place or to keep their valuable things, documents in a protected way. Hence this project can be understood by peoples and future work can be done. Various technology and update can be performed is the project. This project can be rebuilt by various microcontroller and various methods, and we can improve by face verification and can reduce the inconveniences in proposed system.

IV. ACKNOWLEDGMENT

We would like to express our special thanks of gratitude to our project guide Mr.Vinoth R Sir who gave us the golden opportunity to do this wonderful project on this topic (Advanced Home Security System using IOT), which also helped us in doing a lot of research and we came to know about so many new things.

REFERANCE

[1] Meenakshi N, Monish M, Dikshit K J, Bharath S, International Journal of Engineering and Computer Science (IJECS) “Arduino Based Smart Fingerprint Authentication System” vol.4, issue03, december2015 (Reference).

[2] Manish Aggarwal, Department of Electronics and Communication Engineering, Elins International Journal of Science Engineering and Management ”Secure Electronic Lock Based on Bluetooth Based OTP System” vol.2, Issue1, January 2017.

[3] Pavithra.B.C, Myna.B.C, kavyashree.M Fingerprint Based Bank Locker System Using Microcontroller Proceeding of IRF International Conference, 5 April -2014, Pondicherry, India, ISBN: 978-93-82702-71-9.

[4] Akanksha singh, arijit pal, bijay rai, “GSM Based Home Automation, Safety and Security Using Android Mobile Phone”, International Journal of Engineering Research & Technology (IJERT), vol.4, Issue 5, May 2015.

[5] Raqibull Hasan, Mohammad Monirujjaman Khan, Asaduzzaman Ashek, Isarat Jahan Rumpa, “Microcontroller Based Home Security System with GSM Technology” open Journal of Safety Science and Technology, 2015,5,55-62 Published online June 2015 in sciRes

[6] Vini Madan, S.R.N Reddy, “GSM-Bluetooth based remote monitoring and control system with automatic light controller “, International Journal of Computer Applications, vol 46-No.1, may 2012.

[7] Prof.Benazir.H.M Dept. of ECE, Nisha S. Kalpathri, Chandralekha Sunagar, Shaikh Collage of Engineering and Technology, Belagavi, India

"Fingerprint Authentication Smart Locking System Using OTP", International Journal of Advance Research in Engineering, Science & Technology, vol 4, Issue 6, June-2017.

[8] Mr.Patil Bhushan S, Mr.Mahajan Vishal A, Mr.Suryawanshi Sagar A, Mr.Pawar Mayur B, Prof.Mr.U.R.Patole, " Automatic Door Lock System using PIN on Android Phone", International Research Journal of Engineering and Technology, vol 05, Issue 11, November 2018.

[9] Sri Prakash N, Venkatram N. "Establishing efficient Security scheme in home IOT device through biometric fingerprint technique". Indian Journal of Science and Technology, 2016 May.

[10] Jason Johnson and Christopher Dow, "Intelligent door lock system with encryption", US patent Application Publication Johnson et al., pp. 1-92, June 2016.

[11] Mustafijur Rahman, A. H. M. Zadildul Karim, Sultanur Nyeem, Faisal Khan, and Golam Matin; "Microcontroller Based Home Security and Load Controlling Using GSM Technology"; I. J. Computer Network and Information Security, 2015.

[12] Rohit Kadam, Pranav Mahmauni, and Yash Parikh; "Smart Home System"; International Journal of Innovative research in Advanced Engineering (IJIRAE), Vol. 2, Issue 1, 2015.

[13] Nazrul¬ Anuar¬ Nayan, Ili A. M. Ikhsan, and Yasuhiro Takahashi; "Using ZigBee Communication Technology in a Smart Home Wireless Sensor Network"; Proceedings of Second International Conference on Modern Trends in Science, Engineering and Technology, 2014.

[14] Rajeev Piyare and Seong Ro Lee; "Smart Home Control and Monitoring System Using Smart Phone"; ICCA 2013, ASTL Vol. 24, pp. 83 - 86, 2013. [15] Jayashri B. Angali and Arvind Shaligram; "Design and Implementation of Security Systems for Smart Home based on GSM Technology"; International Journal of Smart Home, Vol. 7, No. 6, pp. 201-208, 2013.