Highbrow Asylum For Hostel Using Internet Of Things (IoT)

[1]R.Sumathi , [2]N.Karthika, [3]K.Ramya, [4]B.Snegha, [5]S.Viji
[1, 2, 3, 4, 5] Department of Information Technology
[1] Professor,Saranathan College of Engineering, Trichy
[2, 3, 4, 5] Students, Saranathan College of Engineering, Trichy

Abstract-*In recent days security is the major issue faced in, almost every domain, particularly for personal and belongings security. Security is increasing day by day in lodging industries like college hostels, hotels and private lodging institutions. Due to the huge opportunities in software jobs many number of students prefer to pursue their higher education in cities hostel stay becomes mandatory for students as well as employees. Nowadays there is a gradual increase in student/employees migrant and 40-45% [1] of them are girls who take up lodging in private institutions and college hostels. The safety of the hostel inmates is the foremost preference of many hostel owners. The hostel does not allow any unauthorized person to enter the lodging premises; hence there is strict watch on the security to keep vigil on the inmates. This cannot be administered by a single care taker. Hence the security of the institution can be taken over by the Internet of Things (IoT)Technology and enforcing fingerprint biometric for the dual layer security in the proposed system. The IoT brings all the control to one fingertip from anywhere at any time. The IoT is the new emerging technology in all over the world for enforcing security to access the vital information. By using fingerprint biometric it is highly unique and confidential about one's data.OTP uses dynamic passwords which are not vulnerable to replay attack, it means an OTP that was already used to login will not be able to use it again. The entire system is maintained by the overseer of the hostel.*

Keywords-Fingerprint Biometric, Internet of Things (IoT) , GSM.

I. INTRODUCTION ABOUT INTERNET OF THINGS (IoT)

The Internet of things (IoT) is the internetworking of physical devices, vehicles also refer to connected devices and smart devices buildings, embedded with electronics, software, sensors, actuators, and network connectivity that enable the objects to collect and exchange the data(Fig .2).

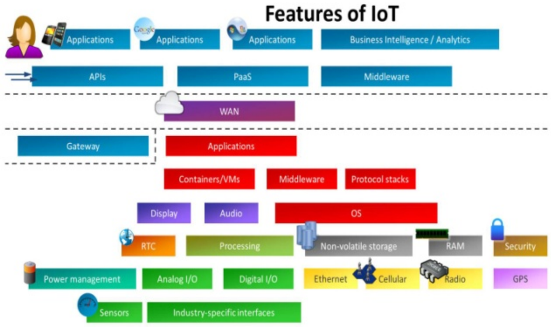


Fig 1. Features of IoT

Internet of Things (IoT) emphasis on enabling technologies, protocols and application issues. The IoT is the latest developments in RFID, smart sensors, communication technologies, and Internet protocols. The basic premise to have smart sensors collaborate directly without human involvement to deliver a new class of applications. The current revolution in Internet, mobile, and machine-to-machine (M2M) technologies (Fig.3) is the first phase of the IoT. In future, the IoT is expected to bridge diverse technologies to enable new applications by connecting physical objects together in support of intelligent decision-making. Session starts by providing a horizontal overview of the IoT, some technical details that pertain to the IoT enabling technologies, protocols, and applications.

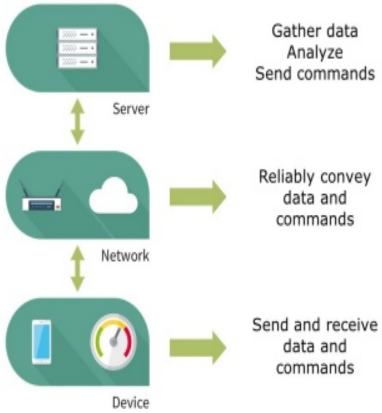


Fig 2. Iot with cloud environment

The IoT is built on many semiconductor technologies, including power management devices, sensors and microprocessors. Performance and security requirements vary considerably from one application to another. One thing is constant, however. And that is (omit) the success of smart homes, connected cars and Industries 4.0 factories hinges on user confidence in robust, easy-to-use, fail-safe security capabilities (Fig.1). The greater the volume of sensitive data we transfer over the IoT, the greater the risk of data and identity theft, device manipulation, data falsification, IP theft and even server/network manipulation.

Infinera[2] has developed a broad range of easy-to-deploy semiconductor technologies to counter growing security threats in the IoT. These solutions are enable the system and device manufacturers by service providers to capitalize on growth opportunities by integrating the right level of security without compromising on the user, complemented by software and supporting services, our hardware based products create an anchor of trust for security implementations, supporting device integrity checks, authentication and secure key management. The Internet of Things (IoT) is moving from a centralized structure to a complex network of decentralized smart devices. This paper elaborates IoT Technology in section I. The real time application of IoT is in section II. Existing system review about the hostel security is in section III and the proposed system is explained in section IV with the sample output.

II REAL TIME APPLICATIONS

2.1 Smart home

Smart home Smart Home clearly stands out, ranking as highest Internet of Things application on all measured channels. quite sixty,000 folks now rummage around for the term "Smart Home" every month. this is often not a surprise. The IoT Analytics company info for sensible Home includes 256 firms and startups. added firms square measure active in sensible home than the other application within the field of IoT. the overall measure of funding for sensible Home startups now exceeds $2.5bn. This list includes distinguished startup names like Nest or alert ME similarly as variety of transnational companies like Philips, Haier, or Belkin.

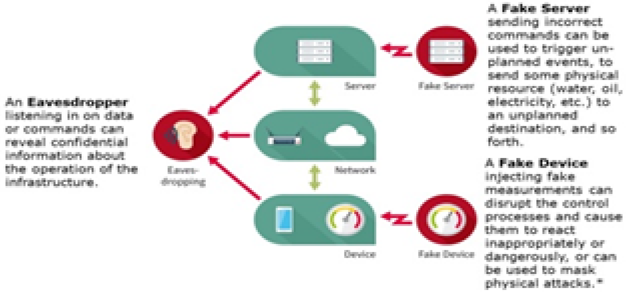

A Fake Server sending incorrect commands can be used to trigger un-planned events, to send some physical resource (water, oil, electricity, etc.) to an unplanned destination, and so forth.
Server
Fake Server
An Eavesdropper listening in on data or commands can reveal confidential information about the operation of the infrastructure.
Eaves-dropping
Network
A Fake Device injecting fake measurements can disrupt the control processes and cause them to react inappropriately or dangerously, or can be used to mask physical attacks.*
Device
Fake Device

Fig 3. Patterns of choice for IoT Security

2.2 Wearable

Wearable remains a hot topic too. As consumers await the release of Apple's new smart watch in April 2015, there are plenty of other wearable innovations to be excited about: like the Sony Smart B Trainer, the Myo gesture control, or looked bracelet. Of all the IoT startups, wearable maker Jawbone is probably the one with the biggest funding to date. It stands at more than half a billion dollars.

2.3 Smart City

Smart city spans a variety of use cases, from traffic management to water distribution, to waste management, urban security and environmental monitoring. Its popularity is fueled by the fact that many Smart City solutions promise to ease real pains of people living in cities these days. IoT solutions in Smart City solve traffic congestion problems, reduce noise and pollution and help make cities safer.

2.4 Smart grids

Smart grids sensible grids square measure a special one. A future sensible grid guarantees to use info about the behaviors of electricity suppliers and shoppers in an automatic fashion to boost the potency, dependability, and social science of electricity. 41,000 monthly Google searches highlights the concept's quality. However, the shortage of tweets (Just a hundred per month) shows that people don't have abundant to mention about it.

III LITERATURE SURVEY

The existing security management system of hostel manually maintained. It took a lot of time to do and require, lot of human resources and also for all inmates each and every one need separate keys and they too keep it carefully. By usage of keys anyone can forge it and have access of the room. The maintainer require student details like room number ,entries, fee details etc to keep record the inmates. When the student number are more they have to maintain a register to record the movement of hostel inmates like, when a student leaves or enters into the hostel. All these process will be time consuming .They must be kept securely , to avoid any theft of confidential information about a student. And also the information of each student is written in pen and if the paper is lost, the important details also is lost. Finally it is difficult to maintain the process by a single person.

IlkyuHa et al. [3] proposed the door lock security system using Internet of Things technology. In case of invalid user who are trying to use the room, the image will be captured and send to the owner. If/have in any physical damage in the alarm will be raised and information will be send to the owner as a message. This system is mainly based on machine to machine communication so we can use anywhere at any time. There are four main features. First physical force alarm which means when an intruder tries to do physical damage to door an alarm will be ringing. Second image will be captured for person who does not belong to that house and it will be sent to the owners mobile when they are trying to attempt with as many as wrong passwords and so many times. Third, the user queries about all the incoming and outgoing records are stored in the database. Finally the user can use the door elsewhere at anytime. They had the conclusion of saying that all things will be at fingertip control and it is easy with mobile that saves time and our effort. Digital door lock is an extra security in this one. During natural calamity time, if the house member are away from town ,they cannot like the Machine – Machine communication. So they cannot allow the neighbor/relatives to save their property.

Anubal et al. [4] proposed the fingerprint biometric door lock. Earlier of lock and key security and password authentication and RFID authentication system is overcome by fingerprint authentication because single lock and single key can be overcome by multiple key for single lock. Disadvantage of the system proposed by Anubala at anyone can break the database and read the passwords and constructing strong passwords and maintaining it not a secure one in password authentication. By using RFID, duplication of RFID cards occurs and unlock the key. By using fingerprint biometric the fingerprint of each person is unique and it is not easy to forge it. And this one is the boon to the security. For each and every person the ridges and valleys will be different. The fingerprint scanner is accurate and cost effective method. In this two levels of authorized and unauthorized. For authorized person they will give fingerprint and the system unlocks the lock. For unauthorized the audrino capture the image of the person and send to owners mobile through GSM modem. By this whole of their system we come to know that it is unique and no forgery occurs.

IV. PROPOSED SYSTEM

Our proposed system is digitalized version of the security system and all are automated. It will take only a second or few to know the details of each person in hostels and implement the security system. Complete details of every student will be stored in the database instead of using paper and pen, this proposed system easy to update, delete and edit the details of the student by using query. The user can just give a query to know the details of every student. By using IoT, it is easy to use it from anywhere at any time as many copies of student details without any damage to the original data. The proposed system is also to find out whether the unauthorized person is the authenticated person or unknown.

When coming to the security we will be having fingerprint of every student in database and it is unique for each students. Our proposed system uses biometric authenticate and also to allow authenticate person to access their hostel-mates room to use random number OTP passwords. So they both joined will be providing a dual layer security. If an unauthorized person tries to use it, an alert message will be sent to the authorized persons. That is all the inmates of the specific room to which the unauthorized person trying to access.

The proposed system provides a security by using OTP and biometric fingerprint by using Internet of Things (IoT). The architecture diagram for the proposed diagram is depicted in fig. 4.The benefit of using fingerprint is uniqueness and can’t be forged. By using OTP (One Time Password) random password numbers are generated so none can forge it. In the proposed system, the details of the hostlers access their room will be sent to the supervisors log and updated by the IoT. The flow diagram of the proposed system is given in Fig.5. The steps involved in the proposed system are: Step1: The entire hostel members’ fingerprints are stored in database. Step2: Suppose if the member of the same room want to access the room, their Fingerprint is enough. Step3: In case, another member of the same hostel belonging to another room trying to use it for some urgent purpose ,the OTP will be sent to all the members of the particular room. If any one of the inmates of the room authorize the hostel mate (belongs to another room) who wants to access the room will get an OTP to open the door. Step4: If any unauthorized person tries to access the room, a alert notification will be send to the room members.

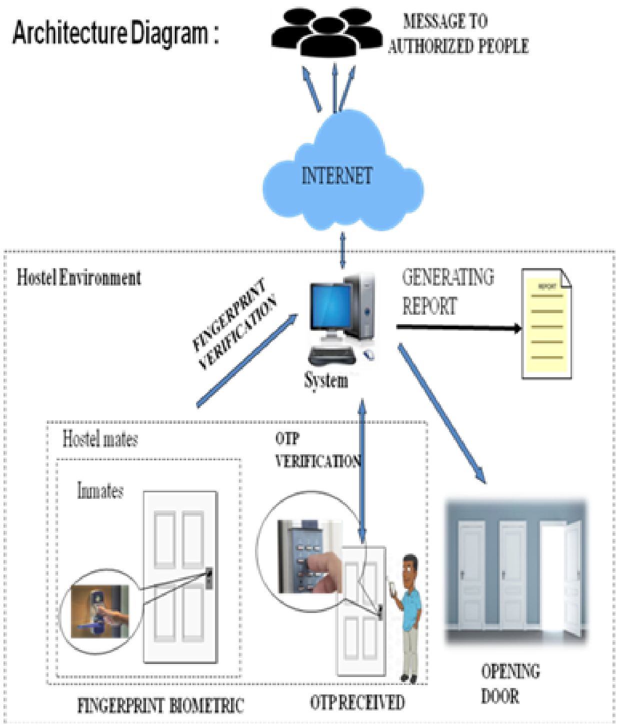


Fig.4 Architecture Diagram

Inmates :

If anyone of the inmate with affix their fingerprint, it will be verified by the system and report will be generated based on that the particular door of the room of the inmates get opened .

Hostel mates:

If anyone of their hostel mates wants to get into the room of inmates with their concern, they should affix their fingerprint. Based on their fingerprint a report will be generated and message notification will go to the inmates. If they give an option by saying “YES”,OTP will come to the hostel mates. If they enter the OTP, the door of the inmate room will get opened an the message notification will be sent to all the inmates.

The sample output taken in various stages of the proposed system implementation is presented (from fig. 6 to fig. 10) in the last part of the proposed system section.

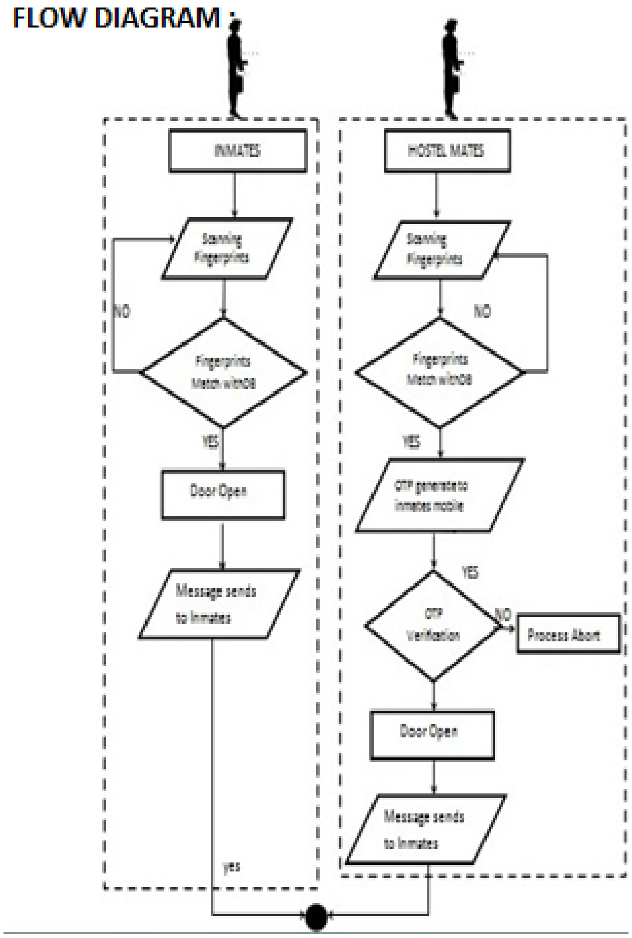
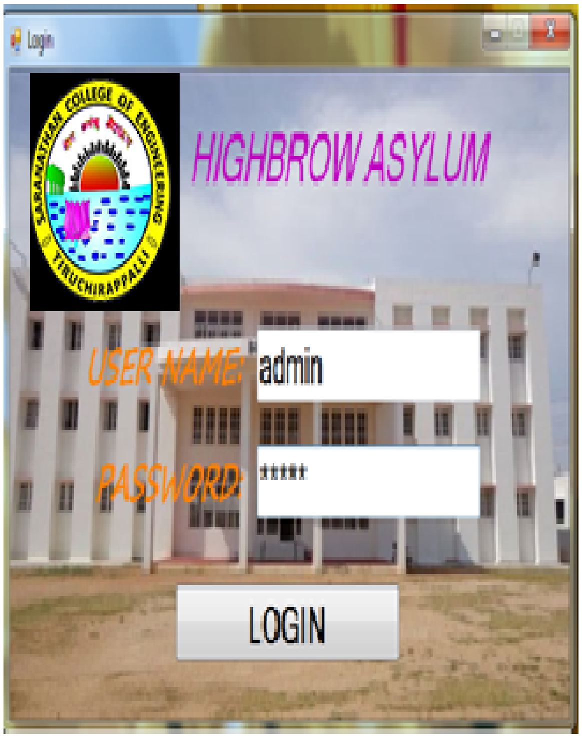


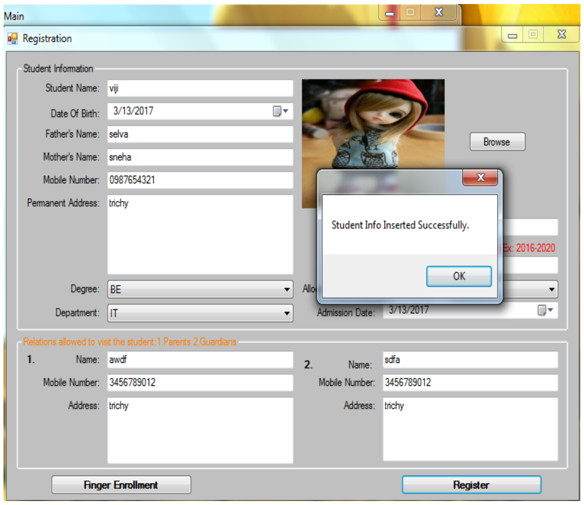
Fig.5 Flow Diagram



USER NAME: admin

PASSWORD: *****

Fig.6 Admin Login



Student Information

Student Name: viji
Date Of Birth: 3/13/2017
Father's Name: selva
Mother's Name: sneha
Mobile Number: 0987654321
Permanent Address: trichy
Degree: BE
Department: IT
Admission Date: 3/13/2017
Ex: 2016-2020

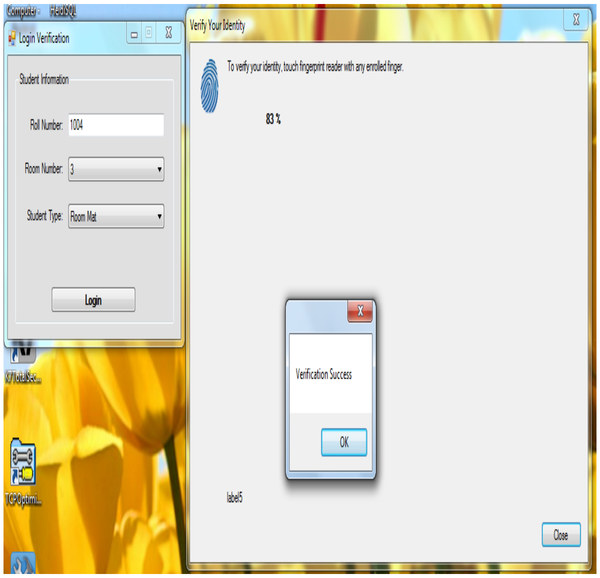
Student Info Inserted Successfully.

Relations allowed to visit the student:1.Parents 2.Guardians

1. Name: awdf
Mobile Number: 3456789012
Address: trichy

2. Name: sdfa
Mobile Number: 3456789012
Address: trichy

Fig.7 Registration



Student Information

Roll Number: 1004
Room Number: 3
Student Type: Room Mat

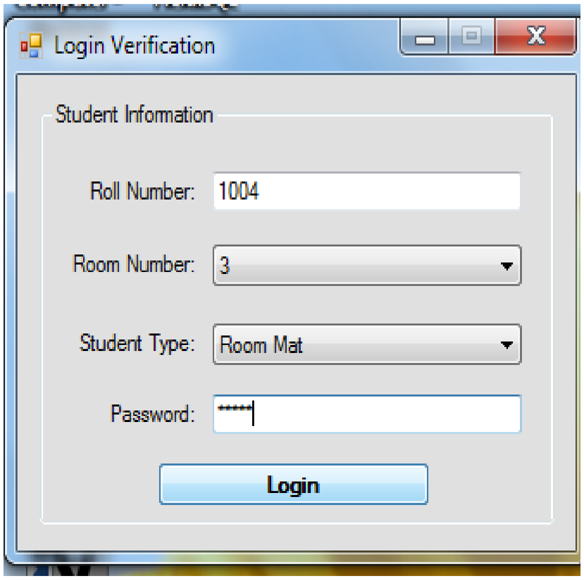
To verify your identity, touch fingerprint reader with any enrolled finger.

83 %

Verification Success

label5

Fig.8 Verification



Student Information

Roll Number: 1004
Room Number: 3
Student Type: Room Mat
Password: *****

Fig.9 OTP received by mobile

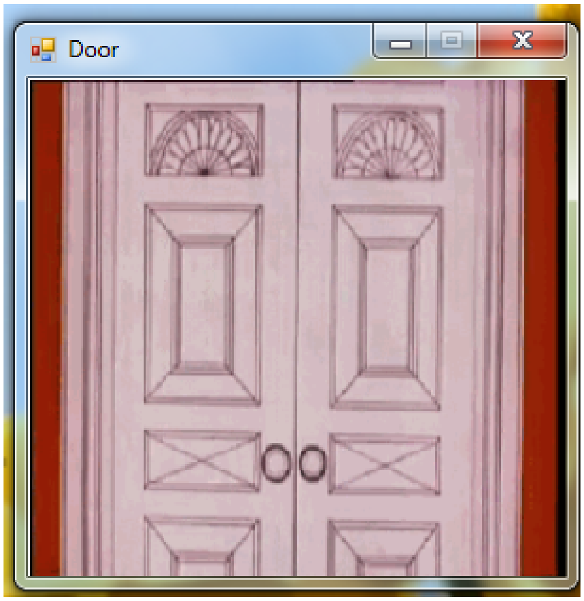


Fig.10 Door Opens

V. CONCLUSION

Thus Internet of Things (IoT) is an environment in which objects, animals or people are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. The aim of the proposed system is to give dual layered security for hostlers using IoT Technologies, hostel owners also can check the information about their hostel inmates in a single system. Proposed system provides high security to the hostlers using IoT technologies, biometric fingerprint verification system and OTP. The well know fingerprint biometric system along with OTP technique is utilized and is used for the purpose of allowing the other hostel mates to access the room of their friends in a genuine cases. IoT fulfill all security related needs in a fingertip with a strong security in easy way.

REFERENCES

[1] Anubala.B, Rahini.M, Bavithra.T, “Intelligent Door Locking System”, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 International Conference on `

[2] IlkyuHa, “Security and Usability Improvement on a Digital Door Lock System based on Internet of Things”, International Journal of Security and Its Applications Vol.9, No.8 (2015).

[3] Lee.S, Park.J, Woo.B and Choi.H, “Video Digital Doorlock System for Recognition and Transmission of

Approaching Objects," KIPS Transaction: Software and Data Engineering, vol. 3, no. 6, (2014), pp. 237-242.

[4] Mary Lourde R and Dushyant Khosla, "Fingerprint Identification in Biometric Security Systems", International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010.

[5] Seo.D, Ko.H and Noh.Y, "Design and Implementation of Digital Door Lock by IoT," KIISE Transactions on Computing Practices (KTCP), vol. 21, no. 3, (2015), pp. 215-222.

[6] Vijay LaxmiKalyani, Kavitapatidar, Harshita Sharma, "RFID Based Hostel Security System With Real Hardware Implementation", Journal of Management Engineering and Information Technology (JMEIT) Volume -3, Issue- 3, Jun. 2016.

[7] Infineon – www.infineon.com