INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 4.295

(Volume 4, Issue 3)

Available online at: www.ijariit.com

Key to the future

Tanveer Pasha
pashatanveer95@gmail.com
School of Engineering and Technology Jain University (SET JU), Bengaluru, Karnataka

Mohammed Omar
reachomar.mukthar47@gmail.com
School of Engineering and Technology Jain University (SET JU), Bengaluru, Karnataka

Omar
omar.prodevans@gmail.com
School of Engineering and Technology Jain University (SET JU), Bengaluru, Karnataka

ABSTRACT

To solve the current drawbacks being experienced by the current Lock-and-Key system by implementing the IoT technology and thereby modeling a Key which can be implemented alongside all the lock systems we use daily, with the help of biometrics being the singularity for uniqueness. Also making appropriate changes to the Lock to work cooperatively with the Key being made, satisfying the ideology of IoT technology of Unique Identity, being able to be connected to the Internet and communicate over it, and has to be remotely accessible.

Keywords: *Internet of things, Biometric, Lock, and key, Unique identity*

1. INTRODUCTION

Internet of Things is the network connectivity of physical devices and other items embedded with electronics and software, whose connectivity enables to connect and exchange information by creating opportunities for more integration of the physical world into software-based systems, improving the efficiency, benefitting the economy and reducing human intervention. The internet of things (IoT) has discovered its application in areas such as industry, energy, car, home, agriculture, connected building campus, healthcare, logistics, and smart-city among other domains. Toward the beginning of this decade, there were an expected 12.5 billion IoT devices, nearly twice as much as the total population of 6.8 billion individual. The quantity of IoT devices is expected to develop quickly in coming years.

2. BACKGROUND WORK

Internet Of Things: Internet of things devices possess network capabilities and contain a minimum of an area of the appliance logic. They perform Transmission Control Protocol/Internet Protocol (TCP/IP) communications on their own and can execute some of the sensor data. IoT incorporates the physical world with the virtual world by utilizing the web as the medium to convey and exchange data.

The IoT in this manner refers to the system of physical items embedded with hardware, programming, sensors, and network to empower objects to exchange information with the administrator, manufacturer as well as with other associated devices. IoT is projected as a constrained computing environment like low in memory, data storing capacity, battery and processing which is connected with an ad-hoc feature of supporting networks, it insists on absolutely new security phenomenon which is appropriate to this ecosystem.

The future of the Internet of Things (IoT) may be an open network and non-deterministic in which intelligent entities such as Web services, Software Oriented Architecture components and virtual objects will interoperate and will act independently depending on the circumstances of the environment. An IoT Smart Home System can be designed in a way that it provides remote control to home through mobile, IR as well as with PC/Laptop. IOT can be named as the association among different sorts of simple and advanced devices like PC, telephones, and tablets to the web that makes approach amongst things and people and subsequently among things. Two parts of the general public are confronting genuine issues with the normal regular strategies for controlling the switches inside the home. In view of our review, we presumed that the general population who are keen on controlling their home machines remotely are as follows: 79% among the extraordinary needs individuals, 91% among the elderly individuals and 88% among the typical individuals. Subsequently, the information we gathered from the review demonstrates the significance of giving an answer which is practical, solid, cost-proficient, and basic being used and establishment. These days, the web is all over the place, each home has its own particular WiFi Network, everyone has an advanced mobile phone. Which this improvement accomplished to the humankind, opened the way to another wording called IoT (Internet of Things). To overcome the previously mentioned issues the IoT design of Smart Home System is used. This framework additionally gives remote controlling to individuals who can't utilize advanced mobile phone to

control their devices, for example, a portion of the specially-abled individuals and uneducated elderly individuals.

Home automation was first introduced in the 1970s when it had introduced, it had failed to improve the lifestyle of its customers due to many reasons.1) Home automation technologies were not easy to determine the benefits of the economy. 2) To justify the cost of installing smart home technology. Home automation technologies require to be user-friendly, easy installation, inexpensive and flexible with several network infrastructure and appliances. Internet Of Things using The Raspberry Pi with some programming platform can assists interaction between the humans and technology by collecting information from the sensors or takes in speech or gesture commands and interprets them to manage household devices like, light, geyser, main door, fan and curtains, when a person is not physically present at home it can automatically turn off the appliances. It understands the system and its every part dynamically and smart control of home lighting can be implemented properly.

Biometric locks: Biometrics verification is utilized as a part of software engineering as a type of recognizable proof and access control. It is additionally used to recognize people in groups that are under surveillance. Biometric locks use various techniques such as 1) Face recognition 2) Voice recognition and 3) Fingerprint recognition.

Face recognition has two types face verification and face identification. Face identification matches input identity with registered identity. Face verification authorizes proper access by verifying the individual. The system uses OKAO Vision algorithm when it captures the object. Face recognition isn't much secure.
Voice recognition is authenticated through voice. It can be easily hacked able by imitating or doing mimicry.

Fingerprint recognition may appear to be more secure since a unique finger impression would be difficult to copy or mimic. Vulnerabilities do exist in biometric security frameworks and the standard PIN or secret password security techniques. Fingerprint recognition is by all accounts a superior option contrasted with other biometric techniques for security. Reason being, voice and face recognition can undoubtedly be duplicated or faked utilizing a photograph or voice recording. Also, different strategies proposed. In addition, other methods proposed such as location tracking and user recognition can be too intrusive on human privacy. There are some circumstances which are extremely irritating like at the point when a man keeps himself out of his home or office or he leaves his key inside or some of the time when a criminal just breaks the bolt and takes everything.

These sorts of circumstances dependably inconvenience individuals who utilize manual entryway bolt with keys. In spite of the fact that in a few spots individuals utilize smart cards, there might emerge a circumstance when somebody loses the card or keeps the card inside. At that point in different situations, there are caretakers for locking houses or workplaces and protecting the keys. Be that as it may, on the other hand, there are times when a man accountable for the keys may not be accessible or has gone to some crisis schedule, which can cause undesirable postponement for individuals who require the key straightaway. These are a portion of the issues that individuals may confront when utilizing keys or smart cards.in this case, biometric fingerprint sensor comes in handy and solve the problems in the much easier way.

3. PROBLEM DEFINITION

To solve the current drawbacks being experienced by the current Lock-and-Key system by implementing the IoT technology and thereby modeling a Key which can be implemented alongside all the lock systems we use daily, with the help of biometrics being the singularity for uniqueness. Also making appropriate changes to the Lock to work co-operatively with the Key being made, satisfying the ideology of IoT technology of Unique Identity, being able to be connected to the Internet and communicate over it, and has to be remotely accessible.

To solve the current drawbacks being experienced by the current Lock-and-Key system by implementing the IoT technology and thereby modeling a Key which can be implemented alongside all the lock systems we use daily, with the help of biometrics being the singularity for uniqueness. Also making appropriate changes to the Lock to work co-operatively with the Key being made, satisfying the ideology of IoT technology of Unique Identity, being able to be connected to the Internet and communicate over it, and has to be remotely accessible.

On a daily basis we all, on an average, use 4 keys in our day to day lives. Be it to access out our homes, vehicles, personal lockers or drawers, office cabins and others. Interestingly we haven't ever noticed this daily routine of ours in the past years as we have been so accustomed to this lifestyle. The Key hasn't been reinvented due to this lifestyle of ours in a million years. We all have homes to which we all return to after dusk to rest and reside, and we all have some or the other personal or shared (in the family) means of transport for us to commute to our workplaces or for other reasons. Also even in our workplaces or places of education or recreational areas, we all have and will definitely be dealing with Keys and Locks.

But we haven't really been thinking about this scenario as we have just accepted these small actions of ours and been doing this since we have gathered our senses together. WE HAVEN'T REALLY RECOGNISED THE SINGULARITY IN THESE ACTIONS.
We are the ones who own the keys to our vehicles, our lockers, our homes, etc. so why have a key to every lock we use for our vehicles, drawers, lockers, homes, although we are the sole owners and will be using the keys.

Another question arises, WHAT IF WE HAVE TO SHARE THE KEYS WITH OUR FELLOW MATES AT WORK, FAMILY, AND FRIENDS???
The keys we use today don't really orient with the ownership property that is associated with it. In simple words, let's understand it through a scenario, I own a Lamborghini, and associated with this vehicle, I have a key to it. I use it on a daily basis and sometimes I share it with my younger brother. The key system doesn't really understand or care about the subdued ownership association. Putting the same scenario in different circumstances, instead of my younger brother, a stranger has access to the key, and indirectly access to my Lamborghini. No one would want

any sort of unauthorized access to something so highly priced and which is currently at a risk of misuse.

Similarly, your privacy is your fortune and no one would want to risk their privacy or their fortune, no matter how much both stand, to other hands leading to misuse.

And even when we are fixed in a situation where our privacy, belongings, and identity are already being misused, we don't really know about it and we can't control the misuse and lock the system out from any unauthorized access and thereby safeguard your belongings.

For better understanding, we again push to scenario through another set of circumstances wherein, the car key is misplaced or is stolen and in the hands of someone who could misuse the car. And the car has been stolen from me or my younger brother moments ago and in a normal life, I don't really can control the car or the outcome and the only real help I could get to is to the Police.

All of these pose as challenges in the current Key and Lock system we use today and need to be addressed immediately as no one would want their Lamborghini to be stolen, same with having their belongings and privacy at risk.

4. PROPOSED SYSTEM

4.1 Architecture

KEY

The KEY will be powered by a bigger and faster motherboard or microcontroller – Raspberry Pi 2 and will be accompanied with a biometric fingerprint sensor, for biometric sensing capabilities and coupled to an RFID identity and a Wi-Fi shield or Wi-Fi module ESP8266, for connectivity and communication alongside a transmitter and receiver. To keep the KEY locatable, a GPS module from U-blox will also be rigged up alongside, to the motherboard. The KEY will have a unique ID.

LOCK

The LOCK will be powered by an Arduino, enabled with an ESP8266 Wi-Fi shield or module, for internet connectivity from a network, accompanied with an RFID reader to read the KEY in terms of worst-case scenarios. The LOCK will only respond to the registered unique ID of a KEY linked to it.

SYSTEM

Under normal operating conditions, the KEY when near a LOCK, it will connect to the same network or different network as the LOCK is in and it will be enabled to engage the unlock process of the system. The KEY will be ready to read an input biometric fingerprint. If the input fingerprint matches with the registered fingerprint, the unlock process is initiated. Since the KEY and LOCK are in the same network or different network and both online, the key will send a signal to the lock over the transmitter and it will be received by the receiver on the lock, over a close proximity range. Also, both the KEY and LOCK have to be online on the Internet, to have the system to work under all conditions.

Under conditions of lending the key to someone else, the registered user with the registered fingerprint must authorize the secondary user with access, by registering a secondary user and pairing his/her phone to the KEY to access the Internet over the secondary user's mobile network. And henceforth the normal system operations take place.

Under conditions of poor availability of resources like poor connectivity, dead battery, etc. The LOCK will allow just one-time single access to the user. It will read the RFID associated with the KEY and if it matches with the registered ID of the KEY, it will provide a one-time unlock and the next unlock has to mandatorily require the KEY to be online.

Under conditions of theft or unauthorized access, the primary registered user has to send a lockdown message through the internet to your KEY through its IPv6 identity associated with it. The KEY to function has to be online and once this message is received, the KEY will lockdown all operations and turn void until it reads a registered fingerprint of the primary user.

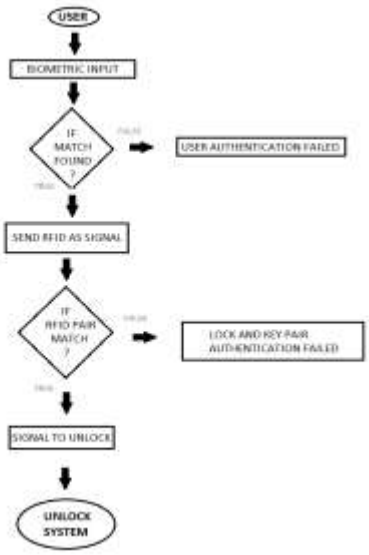

Fig. 4.1.1: Use case diagram of a system

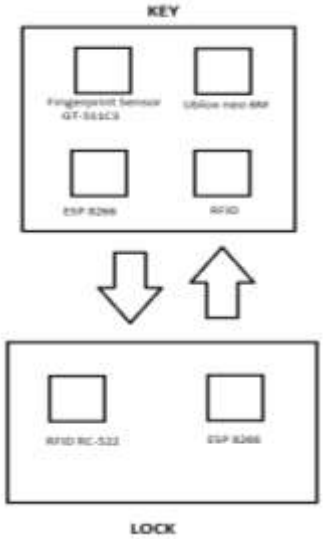

Fig. 4.1.2: System diagram

4.2. Methodology

Design and model an IoT device in terms of a KEY in the Lock-and-Key system.

The primary focus of our endeavor is to build and innovate an IoT based device ascertaining all the properties and characteristics of a regular key like Identity, Uniqueness and Simplicity in terms of use, while inhibiting basic IoT

ideologies of sensing and being connected to the Internet on the go, and also being remotely accessible.

To put forth such a feat to create a device from ideology to reality in terms of a prototype is quite overwhelming and also challenging although it holds a lot of Learning in the process.

The Key, based on the IoT platform will have the capability to sense its users through a biometric sensor and will also have a unique identity just like a regular key we use daily. Along with that, the key will be traceable with the help of GPS integrated into the device and it will also be dynamically synchronized with the User's mobile phone in order to access the Internet network on the go. Also when the device is inside the vicinity or range of an already registered network it will use the network to communicate through the Internet.

If operation conditions are to be really weak in terms of a Power outage, or a dead battery or poor Internet Connectivity, the prototype will hopefully adapt to such situations with an RFID identity linked to it providing a possible timed access to the Vehicle, or Home.

This worst case scenario will be handled securely by the device as the Key will allow only a single timed access before a temporary lockdown.

In terms of unauthorized access, or failed attempt to recognize the User, the owner only can terminate the temporary lockdown. In conditions of misuse or theft, the key when under-connectivity of the Internet, could be remotely accessed through its IPv6 identity and could be controlled to temporary lockdown. This temporary lockdown can be terminated by the owner only.

4.3 HARDWARE REQUIREMENTS

ARDUINO UNO
RASPBERRY PI 2

RFID - Radio-frequency identification

ESP8266 - Wi-Fi module

GPS module U-blox neo 6m

Fingerprint Sensor - (GT-511C3)

5. CONCLUSION

All in all, with the help of the IoT technology of today's world we enhance our lives and secure our essentials by putting this system into action. The User can secure his home or car through the KEY as easily and securely through his own biometric signature which stands unique. This unique signature coupled with another level of scrutiny which being the correct Wi-Fi client and server pair between the lock and the key stand as the primary parameters for unlocking. Once both the parameters hold true, only then will the lock open up for access. Else the door won't open in normality. Also, the lock stands remotely controllable through its unique IP address again pulling in advantages of locking it down and unlocking from afar through our own comfort with this, the KEY also stands discoverable all the time with its Location tracking capabilities with the GPS integrated within its build.

6. REFERENCES

[1] Smart IoT Devices in the Home: Security and Privacy Implications, Vijay Sivaraman and Hassan Habibi Gharakheili are with the School of Electrical Engineering and Telecommunications, University of New South Wales (UNSW), Australia.Digital Object Identifier 10.1109/MTS.2018.2826079 Date of publication: 31 May 2018

[2] Design of It smart home system. Akram Khan Department of Electrical Engineering, Umm Al Qura University, Makkah, Saudi Arabia akram.khan@outlook.sa 978-1-5386-4817-9/18/$31.00 ©2018 IEEE

[3] IOT BASED HOME AUTOMATION BY USING PERSONAL ASSISTANT DR v CHAYAPATHY Asso. Professor, EEE Dept, RVCE, Bengaluru 978-1-5386-0569-1$31.00 c 2017 IEEE

[4] MULTI-OPERATIONAL HOME AUTOMATION SYSTEM USING IOT, AN APPROACH, Abhishek Kumar Verma Dept. of C.S.E UEM Jaipur, India vermaabhishekkumar49@gmail.com 978-1-5386-3371-7/17/$31.00 ©2017 IEEE

[5] Preventing Cell Phone Intrusion and Theft using Biometrics, Donny Jacob Ohana, Sam Houston State University Huntsville, TX, USA djo007@shsu.edu © 2013, Donny Jacob Ohana. Under license to IEEE. DOI 10.1109/SPW.2013.19

[6] Design and Implementation of a Fingerprint Based Lock System for Shared Access, Jayasree Baidya, Trina Saha, Ryad Moyashir, Rajesh Palit, Department of Electrical and Computer Engineering, North South University, Dhaka - 1229{jayasree.baidya, trina.saha, read.moyashir, rajesh.palit} @northsouth.edu 978-1-5090-4228-9/17/$31.00 ©2017 IEEE

[7] Super Secure Door Lock System For Critical Zone Meera Mathew Divya R S, Dept. Of Computer Science Assistant Professor, Thiruvananthapuram, Kerala, India Mar Baselios College of Engineering, meeramathew777@gmail.com, 2017 International Conference on Networks & Advances in Computational Technologies (NetACT) |20-22 July 2017| Trivandrum

