Smart Locking System

Sakina Dasorwala
Dept. of Computer Engineering
K.J. Somaiya College of Engineering,
Mumbai - 400077, India

Aniket Patil
Dept. of Computer Engineering
K.J. Somaiya College of Engineering,
Mumbai - 400077, India

Raj Vora
Dept. of Computer Engineering
K.J. Somaiya College of Engineering,
Mumbai - 400077, India

Prof. Mansi Kambli
Dept. of Computer Engineering
K.J. Somaiya College of Engineering,
Mumbai - 400077, India

***Abstract* — Currently, we are looking at the era of smart systems. For more than a couple of decades now, the internet has been a medium that connects people as well as devices to transfer static information. The internet is influencing the working of humans interaction and also has a huge impact on the everyday lives of the people. The concept of Internet of Things(IoT) came into existence by taking the capabilities of the internet one step ahead by enabling different devices to work dynamically and interact with other devices. We are making everything smart right from our mobile devices to our televisions. But when it comes to security and locking systems, we are still one step behind. This paper makes use of randomization, hashing and NSDT[1] (Near Sound Data Transfer) to create a Smart Locking System to replace the conventional lock & key mechanism locks.**

Keywords* — *IoT, Door locks, NSDT, RaspberryPi, Chirp, Flutter

I. INTRODUCTION

Internet of Things (IoT) is a recently developed concept of connecting all the real-world objects (which are defined as things) to the internet. IoT is a computing concept that paves the way for a future where everyday physical objects will be connected to the Internet and be able to identify themselves to other devices with least human intervention. IoT can be applied in various sectors of everyday life like offices, traffic lights, homes, petrol pumps, etc. Sensors play an important role in IoT as they are used to sense the state of the environment. There can be varied types of sensors depending on the type of information to be collected from the environment.

This technology was used to create a smart and secure locking system. The main aspects of this system are using revolutionary IoT technology by integrating them for the locking functionality to make the system smart, and the other using advanced encryption algorithms to make the system more secure.

The paper talks about a locking system which can be used in place of the traditional locks. This system makes use of randomization, hashing, emerging technology like Near Sound Data Transfer and IoT devices to make it as secure as possible.

The door does not have any physical point of interaction from outside, that is, no keyhole to tamper with. The occupant's smartphone sends a unique code to the microphone connected to the RaspberryPi. RaspberryPi decodes the unique code and opens the door after the occupant is authenticated, else the homeowner is alerted.

II. LITERATURE SURVEY

The smart security system is aimed at bringing in the concept of Internet of Things to provide security. This system should be very secure and at the same time, it should be smart enough to process the user inputs to authenticate the user. Incase of breaking in, the sensors should be able to sense the break in and alert the homeowner through various means. According to the FBI reports [4], home burglary accounts for 17.1% of the estimated number of property crimes in 2018. By subcategorization, 56.7% of burglaries involved forcible entry and the victims of burglary offenses suffered an estimated $3.4 billion in property losses in 2018. In the world that is advancing rapidly with technology where cars could drive on their own and drones could capture your food, burglary should not be of much concern but the above statistics just proves it wrong. This is a major problem and there is a need to overcome these personal property damages. The idea of linking security to the internet can be brought to practise. But it is difficult to achieve the security aspect of the system since there are many vulnerabilities while integrating devices with the internet. These challenges and open issues of constructing the system need to be recognised so that required steps and measures can be taken to overcome them. There can be a few alternatives for the safety and security of the system. These can be identified by reviewing the other works in the field of IoT and analyzing the challenges faced by those systems so as to be able to design a full proof system.

Door lock security has become very important in various sections of life. Electronic lock systems and IoT have revolutionized the history of door lock systems from mechanical door locks to the remotely controlled and highly secured locks. There are different techniques which categorize the door lock systems.

Password-based door lock contains a touchpad to enter the password and store it in EEPROM. For the radio-frequency identification (RFID) lock system you need to carry a card with you. The system uses electromagnetic fields for data transmission. RFID provides a low-cost system, but if the card is lost or stolen the system could be at risk. Multiple doors unlocking systems have also been developed by RFID. Biometric lock systems verify unique physical characteristics to grant access to the user, Such as voice recognition, face recognition, and thumb impression recognition. The major limitation on such systems is that we will have one password (ever) which could be vulnerable in case of physical damage.

Introducing a new way of transferring data from one device to another, ultrasonic communication can be very useful [1]. The proposed study shows that ultrasonic communication is a robust and computationally efficient way of transmitting and receiving data on simulated as well as real time data. The perks of ultrasonic communication is that it can be used as an emerging technology for data transfer having an upper-hand over bluetooth and WiFi for many reasons. Unlike Bluetooth and Wi-Fi, high-frequency sound does not pass through walls, which is useful to limit the transmitter and receiver to approximately, within earshot. Also, establishing a WiFi or bluetooth connection can take a few seconds, whereas on the other hand, sound playback can take tens of milliseconds. The bluetooth, WiFi can usually be disabled which can be problematic. So, ultrasonic sound transfer can help increase speed and efficiency. Although having many benefits, the sound transmission has a couple backdrops; the frequencies around can interfere with the sound while data transmission. Since the sound is audible, the people around may find it distracting or offensive. This sound transfer can be used as keys for smart locking systems with the help of encryption/decryption algorithms.

Making these devices IoT based and securing the information over the network is still an issue. We need to encrypt our information while transmitting it over the network. Securing the information over the network is still an area of interest for many researchers. Encryption based lock systems are more secure where the confidential data is converted into another format, so even if a hacker tries to hack the data, he will not get the lock credentials.

Another study on smart surveillance systems shows that the concept of the internet and security to go hand in hand is very difficult. The proposed system [2] is used to capture movements of the environment by the camera sensors. The WiFi module in the Rpi is used to upload these images to the cloud. The display monitor displays the movements captured. As the system starts, the Raspberry Pi is initialised followed by the initialization of the WiFi module and the camera. The camera captures an ideal image and then as and when some motion is detected, the images are captured by the sensor. Incase of motion, an SMS is sent to the user notifying them of the unusual activity. This system is vulnerable to tampering as no solid authentication mechanisms have been provided. This may lead data integrity of the surveillance system to be at stake. Even though the working of the system is well organised, the few limitations cannot be overlooked.

The paper IoT based smart surveillance system [3] integrates different sensors that are used to keep a tab of the environment of the home. These sensors include, PIR sensor, gas sensor, fire sensor, light control sensors. Whenever the sensors detect any kind of input signals, the Raspberry pi alerts the owner using WIFI or GSM module and then the owner can take action accordingly. And the case when nothing abnormal is detected by the sensors then the Raspberry Pi does not perform any operations. Hence the owner would not need to continuously monitor his home manually. Instead, Raspberry Pi and the sensors do.The system architecture is divided into different layers; the perception layer, network layer and application layer. The paper also talks about the different attacks that can take place at these layers and how to tackle them. But one of the major limitations of the system is if the internet is down, then the system is unable to sense and operate. The alternative to this limitation is given in the paper by intimating the user of the house as soon as the WiFi is down by using the GSM module.

For the smart locking system that is proposed in this article, there should also be a door security alarm. To get a better idea of the door security alarm and its working, there has been a system implemented that activates/deactivates the door security alarm with the help of Google assistant [5]. After activating the system, if there is an intrusion then the owner is alerted with the help of an email.

III. OBJECTIVE

The aim of IoT is to make our day to day life safer and more efficient. Security and safety can be very vulnerable if the security system is not full-proof. While designing and implementing such a security system, there are a few key objectives that should be achieved in order to make a successful security system.

Home security should be the topmost priority while making smart security systems. The application should only be accessible to the homeowner and the registered family members. Secure login, registration and access mechanisms should be used to avoid masquerading. Since the system uses the internet and encryption algorithms, it should be ensured that the system is not vulnerable at any point in time.

It is essential that the system is efficient at all times for it to be consistent. The door should be unlocked any time the unlock button is pressed. 100% efficiency should be ensured in the project. This gives a satisfying user experience which helps the owner be more comfortable using this IoT based smart system with ease.

The homeowners cannot be expected to wait for a long time for the system to process and authenticate the user before

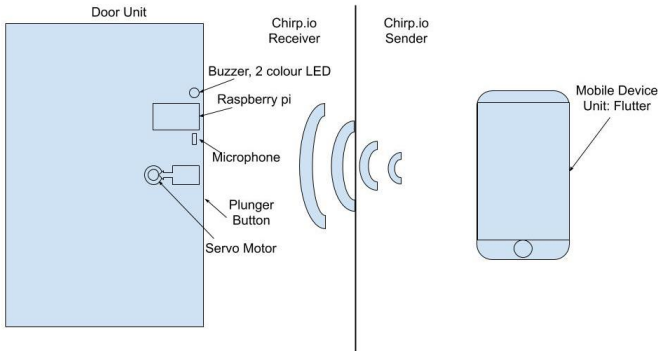

Fig. 1. System Architecture

the door unlocks. The whole process should take place in an acceptable time limit. The objective should be to make a fast processing system which requires the least amount of work from the user.

Understandability of the system plays an important role. The application and interface should be versatile for all kinds of users with no technical knowledge as well as others. No occupant will be the same, hence the UI should be self-explanatory and easy to use.

IV. SYSTEM ARCHITECTURE

A. *Door unit (Fig. 1):*

RaspberryPi:

Computes the incoming data from NSDT[1] and authorizes the user and accordingly executes the further steps.

Microphone:

Captures the incoming data from the mobile device via NSDT[1].

Servo Motor:

Used to operate the lock.

Buzzer:

Notifies about an attempted intrusion.

Plunger Button:

Informs the RaspberryPi that the door is shut and should be locked.

Chirp.io Receiver:

This software module is used to interpret the sound clip captured by the microphone and sends the data to other python functions for authorization.

B. *Mobile device unit:*

Flutter:

Used for development of a cross-platform application for Android and iOS.

Chirp.io Sender:

This software module is used to send the encoded message via mobile phone speaker.

V. IMPLEMENTATION

Randomization:

Whenever a new user is registered, the 15-character userid is randomly generated and uploaded to the cloud database. Also when a user registers for a new house, the secret key between the user and locking device is a 16-character randomly generated string.

Hashing:

Whenever the secret key is to be sent via NSDT it is first hashed via HMAC using the timestamp as secret and SHA256 encryption.

A. *Registration Phase (Fig. 2):*

1) User clicks on the “Add Home” button.
2) Mobile devices generate a random 16-character secret key and upload it to the cloud database..
3) This random secret key is hashed with the timestamp.
4) While the data is being uploaded, a message is generated <r><UID><hashed secret key>.
5) The message is sent to the RaspberryPi via mobile’s chirp sender software.
6) The RaspberryPi’s chirp receiver receives the message and decodes it.
7) The RaspberryPi retrieves the secret key using the UID received.
8) The secret key is hashed with the timestamp and checked for a match with the received hashed secret key.
9) If they are the same, the user is registered for that house, else the homeowner is alerted.
10) Once the registered user is verified, the IMEI of the user device is captured for security purposes.

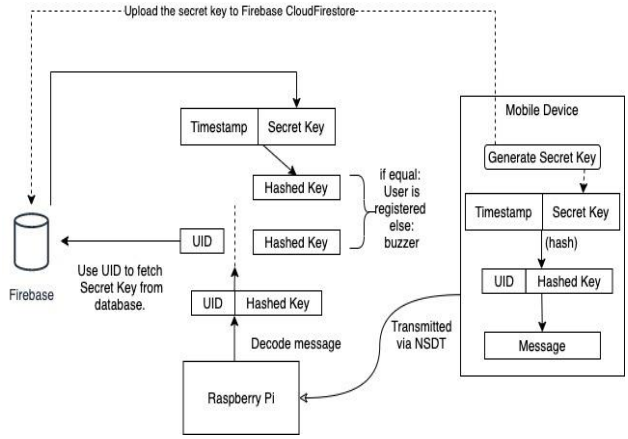

Fig. 2. User Registration Phase

B. *Unlocking Phase (Fig. 3):*

1) The user selects the door to unlock from the drop-down menu.
2) The mobile device retrieves the secret key from the firebase for the house selected.
3) The secret key is hashed with the timestamp.
4) A message is generated, <n><UID><hashed secret key>

5) The message is sent to the RaspberryPi via mobile's Chirp sender software.
6) The RaspberryPi's Chirp receiver receives the message and decodes it.
7) Using the UID in the message, RaspberryPi retrieves the secret key for that house.
8) The retrieved secret key is hashed with the timestamp.
9) The generated hashed secret key is matched with the received hash key.
10) If they match, the door is unlocked, else door remains locked and the owner is alerted.

VI. RESULTS

Using NSDT[1] for data transmission is a fairly new and efficient method without the use of a key/card or any other biometric options. It also provides speed and efficiency. Along with developing a smart locking system, this paper also ensures that the system maintains utmost security at every step. Inorder to verify the homeowner, each registered owner has his/her own secret key. Also, to make the Chirp non reusable, the secret key is hashed with the time stamp. Incase of multiple failed attempts (more than 3), the occupants will be notified.

The mobile application has also been made as secure as possible. If the user credentials fall in the wrong hands and an impostor tries to login, they will not be able to access the application on another device since the IMEI has been captured when the user registers for the first time. Fingerprint authentication or face lock, based on the OS of use has also been implemented in the application. Hence, all these measures ensure that the system is secure.

VII. CONCLUSION

Thus a smart locking system has been made using randomization, hashing, encryption and revolutionary technologies like Near Sound Data Transfer and Flutter. The failsafe for this system is biometric authentication to be used mainly for children.

Currently, the whole system requires a consistent internet connection to work effortlessly. In the future, work can be done towards making the system work even with a periodic internet connection, with the use of hidden local databases.

The prototype is made to work with a normal latch door lock, but in reality, more complex and tougher locks are used to secure the door. A much powerful motor and a robust open & shut mechanism to use this system on modern-day locks can be used in the future.

The system can be improved so that it can be operated remotely over the internet to provide ease of use.

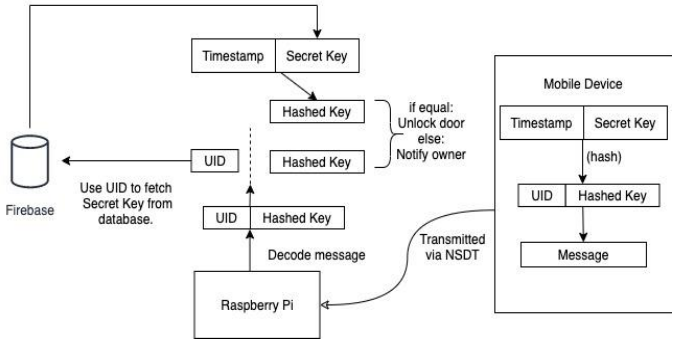

Fig. 3. Normal Operation Phase

REFERENCES

[1] P. Getreuer, C. Gnegy, R. F. Lyon and R. A. Saurous, "Ultrasonic Communication Using Consumer Hardware," in IEEE Transactions on Multimedia, vol. 20, no. 6, pp. 1277-1290, June 2018.

[2] N. Patil, S. Ambatkar and S. Kakde, "IoT based smart surveillance security system using raspberry Pi," 2017 International Conference on Communication and Signal Processing (ICCSP), Chennai, 2017, pp. 0344-0348.

[3] Leela Krishna Gunnemeda, Subhash Chowdary Gadde, Harshith Guduru, Moses Babu Devarapalli, Santhosh Kumar Peketi. "IOT Based Smart Surveillance System", International Journal of Advance Research, Ideas and Innovations in Technology

[4] "Burglary", Fall 2019, Accessed on: March 3, 2020. [Online]. Available :https://ucr.fbi.gov/crime-in-the-u.s/2018/crime-in-the-u.s.-2018/topic-pages/burglary

[5] A. Raj, IoT based Door Security Alarm controlled by Google Assistant, Nov 22, 2018, Accessed on: March 3, 2020. [Online]. Available: https://circuitdigest.com/microcontroller-projects/iot-based-door-security-alarm-controlled-by-google-assistant