CHAPTER 1

INTRODUCTION

The term Internet of Things generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention. There is, however, no single universal definition.

The Internet of things may be a hot topic in the industry but it's not a new concept. In the early 2000's, Kevin Ashton was laying the ground work for what would become the Internet of Things (IoT) at MIT's AutoID lab. Ashton was one of the pioneers who conceived this notation as he searched for ways that Proctor & Gamble could improve its business by linking RFID information to the Internet. The concept was simple but powerful. If all objects in daily life were equipped with identifiers and wireless connectivity, these objects could communicate with each other and be managed by computers.

In a 1999 article for the RFID Journal Ashton wrote: "If we had computers that knew everything there was to know about things—using data they gathered without any help from us—we would be able to track and count everything and gently reduce waste, loss and cost. We would know when things need replacing, repairing or recalling, weather they were fresh or past their best. We need to empower computers with our means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory. RFID and sensor technology enable computers to observe, identify and understand the world—without the limitations of human-entered data".

Today, the size and cost of wireless radios has dropped tremendously. IPv6 allows us to assign a communication address to billions of devices. Electronics companies are building Wi-Fi and cellular wireless connectivity into wide range of devices. ABI Research estimates over five billion wireless chips will ship in 2013. Mobile data coverage has improved significantly with many networks offering broadband speeds. While not perfect, battery technology has improved and solar recharging has been built into numerous devices. There will be billions of objects connecting to the network with the next several years. For example, Cisco's Internet of Things Group (IOTG) predicts there will be over 50 billion connected devices by 2020

IoT describes a system where items in the physical world, and sensors within or attached to these items, are connected to the Internet via wireless and wired Internet connection. These sensors can use various types of local area connections such as RFID, NFC, Wi-Fi, Bluetooth and Zigbee. Sensors can also have wide area connectivity such as GSM, GPRS, 3G and-LTE.

From a broad perspective, the confluence of several technology and market tends is making it possible to interconnect more and smaller devices cheaply and easily:

- **Ubiquitous connectivity** – Low cost, high-speed, pervasive network connectivity, especially through licensed and unlicensed wireless services and technologies, makes almost everything "connectable".
- **Widespread adoption of IP-based networking** – IP has become the dominant global standard for networking, providing a well-defined and widely implemented platform of software and tools that can be incorporated into a broad range of devices easily and inexpensively.
- **Miniaturization**- Manufacturing advance allow cutting edge computing and communication technology to be incorporate into very small objects. Coupled with greater computing economics, this has fuelled the advancement of small and inexpensive senor devices, which drive many IoT applications.
- **Advance in Data Analytics**- New algorithms and rapid increase in computing power, data storage, and cloud services enable the aggregation, correlation, and analysis of vast quantities of data; this large and dynamic dataset provide new opportunities for extracting information and knowledge.
- **Rise of Cloud Computing**- Cloud computing, which leverages remote, networked computing resources to process, manage, and store data, allows small and distributed devices to interact with powerful back-end analytics and control capabilities.

From this perspective, the IoT represents the convergence of variety of computing and connectivity trends that have been evolving for many decades. At present, a wide range of industry sectors- including automotive, healthcare, manufacturing, home and consumer electronics are well beyond- are considering the

potential for incorporating IoT technology into their products, services and operations. The basic idea of IoT is shown in the Figure 1.1 where it denotes connections at anytime, anywhere and anyplace.

Smart locks are now widely available, and allows users to open & close a door. Some locks are even connected to the cloud, and allows the user to open/close it remotely, and share the access to the door with other people.

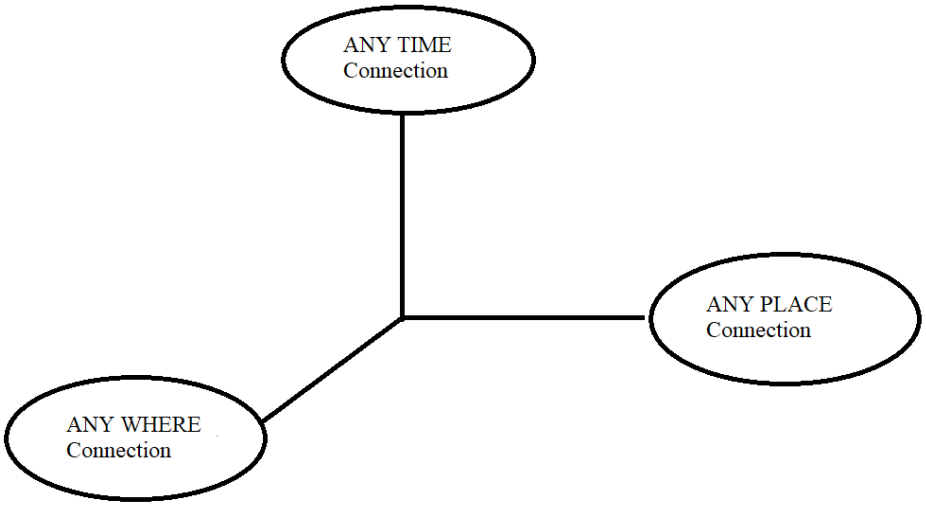

Figure 1.1: Internet of Things

Smart lock authentication system is to open and close the door automatically by using Wi-Fi protocol without manual keys to prevent the access from unauthorized access to enter the room in order to provide security and privacy to our confidential to our data and property.

CHAPTER 2

LITERATURE SURVEY

In the article entitled “Portable Smart Door Lock” written by Hussain F. Alsaif, Program in Electromechanical Engineering, College of Engineering Wentworth Institute of Technology, “Control of the lock for a door remains unsatisfactory for many people. The conflicting needs of security, convenience and retaining control, whether physically present or not, lead people to seek solutions beyond conventional methods. Certain available home security systems would meet the needs, but they are expensive, require professional installation, and are difficult to operate or maintain. Some of the more recently developed smart locks show promise as viable security systems, but lack some portability and control. The purpose of this project was to design and test modules for a smart lock system that can be monitored, controlled and moved within a building or between buildings. Components of the system included a wireless module, along with a motor and a gear mechanism as an actuator to function as the locking mechanism. A mobile app would be able to provide the user with control over the lock. The modules will be tested on a variety of key-lock assemblies to ensure compatibility with a wide range of doors. The state of the door will also be monitored and recorded.” [1].

In article titled “IoT based secure door locking system” written by Vedala Sharath Department of Research and Development, Robolab Technologies Private Limited, Pune Security is the main issue that must be addressed in the present society. With the latest developments in emerging technologies, IoT stands out to be the Cutting-Edge technology solving many security related problems. Here is a Home security solution based on IoT, in this system we will have a wireless module which connects to the Internet and communicates with the user through internet from anywhere in the world. User can lock his Home’s door by using a mobile phone with an app installed in it. The main objective of this paper is to embed a locking system in the door with two locking positions each individually controlled by the user using mobile phone and intruder alert system when someone tries to open the lock manually. An additional feature which gives better security option is, user can use this system in two modes. One is connecting to the internet and the other one is Hotspot mode, where user can connect to local hotspot created by the system and monitor the home in and around about a range of 30meter. [2].

From the paper titled “Smart Door Security using Arduino and Bluetooth application” written by Ketan Rathod Department of Electronics Engineering, Vishwakarma Institute of Technology, Pune, India. As per survey there exists many such systems that could control door. Each system has its own unique feature. Following model describes the work performed in project. Arduino UNO itself act as a microcontroller. Design and implementation of low, smart and real-time monitoring and controlling of door security using Arduino. Arduino along with HC-05 and mobile Applications allows us to control door from anywhere in the home and constantly keep watch on it. Some system provides security alarm using low processor chip. R-Pi would exchange data or would communicate with the help of Bluetooth, Wi-Fi and Ethernet. These systems have their own disadvantages. For example, system implementing must requires Wi-Fi/Ethernet for the data communication. These systems also proficient for home automation [3].

From article titled “Key Authentication Based Door Lock Monitoring System using MQTT on ESP8266” written by Avinash Bagul Department of Computer Engineering NBN Sinhgad School of Engineering, India. An ESP 8266 is Wi-Fi enabled wireless microcontroller. It has been implemented in this scenario in a door mounted security system with the help of a sensor. The basic components that are used here are a reed switch, an alarm, an ESP 8266 module and a e power supply. 3 interfaces have been used. First an ESP 8266, which is connected to a buzzer and a reed switch. These three components have been mounted on the door frame. The second interface is an application which will run on either a stationary workstation or a mobile workstation. The third component is a server, which will handle traffic routing and synchronization tasks when a scenario with multiple doors is involved. These three interfaces will be connected and synchronization will be carried out with the help of the MQTT protocol. Two of these three interfaces i.e. the application and the door mounted system will serve as clients whereas the server will be the broker. The system will use a messaging mechanism to ensure two step verification either via email or via a text message. This system will be fault tolerant and scalable because it will be easy to facilitate addition of new devices [4].

CHAPTER 3

PROPOSED SYSTEM

As the writing study propose framework will execute a brilliant entryway framework by using Wi-Fi for its power and unwavering quality to make a savvy situation to unravel the approval solicitation to the opening and shutting of the entryways.

3.1 Motivation

The framework is anything but difficult to utilize and requires no extraordinary preparing or hardware, the Wi-Fi is easily available in every smartphone nowadays for the ease of access and high availability of the range of 30mts, QR code is globally used for payments requires no instructions to use as it requires no external training,

3.2 Problem statement

The inspiration to execute a keen entryway confirmation framework by utilizing Wi-Fi to make our grounds into a "Smart Campus" and along these lines explaining the security-related issues to opening and shutting of entryways which are gotten to by unapproved clients.

3.2.1 Problem description

Different control frameworks have been structured throughout the years to counteract access to an unapproved client. The fundamental point of giving locks to our home, school, office, and the structure is for the security of our lives and property. It is in this way imperative to have an advantageous method for accomplishing this objective.

Programmed entryway framework has turned into a standard component on a wide range of sorts of structures and homes. Furthermore, they are getting to be well known each day to build up a powerful electronic gadget which gives security. Home security has been a noteworthy issue as a result of the expansion in wrongdoing rate and everyone needs to make a legitimate move to avoid unapproved clients. There was a need to computerize home.

3.2.2 Problem analysis

The confirmation framework is basically a client id and password check framework that plays out approval from the entered client id and password the approved client accommodated get to depending on the application context, the authentication system

typically operates in one of two mode: verification and validation as shown in Figure 3.1.

In check mode, the framework confirms an individual's character by contrasting the entered client id and the customized client id, which is pre-put away. Character check is ordinarily utilized for constructive approval, where the point is to give various individuals from utilizing a similar client id.

In-approval mode, the framework perceives the password entered with the client id and contrasts it and the modified password which is pre-put away when both client id and password is legitimate to access is conceded to the approved individual.

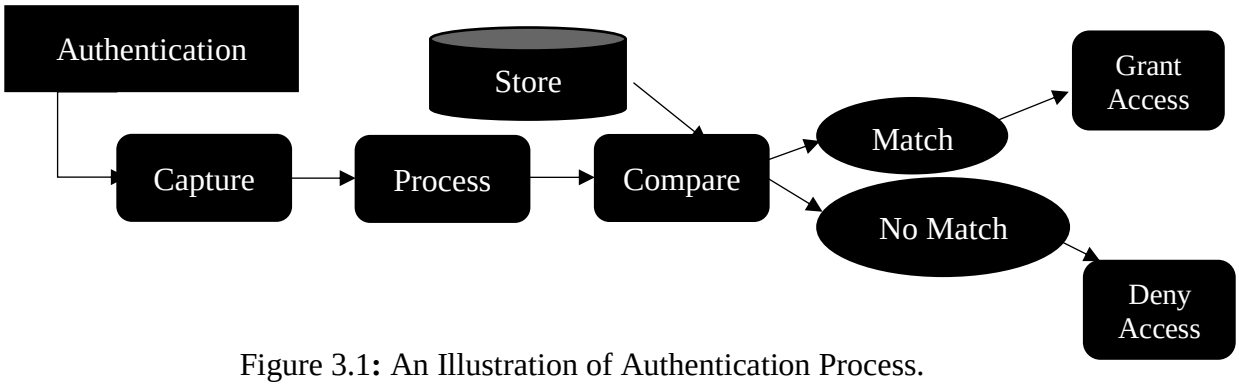

Figure 3.1**:** An Illustration of Authentication Process.

1. **Capture:** The user id and passcode are captured on the smartphone by web interface.
2. **Process:** The captured data is communicated through Wi-Fi to ESP module.
3. **Compare:** The user id and passcode are compared with the stored credentials.
4. **Match:** At the point when the certifications are legitimate, the entrance is allowed.
5. **No match:** At the point when the accreditations are not legitimate, the entrance isn't allowed.

CHAPTER 4

METHODOLOGY

4.1 Purpose & requirements specification

The first step in IoT system design methodology is to define the purpose and requirements of the system. In this step, the system purpose, behaviour and requirements (such as data collection requirements, data analysis requirements, system management requirements, data privacy and security requirements, user interface requirements,) are captured.

Applying it to the smart login system, the purpose and requirements for system may be described as follows:

- **Purpose:** A smart login system that allows only authenticated users to enter a room/class by using Wi-Fi.
- **System management requirement:** The framework ought to give remote observing and Control capacities.
- **Data analysis requirement:** The framework ought to perform nearby investigation of the information.
- **Application deployment requirement:** The application ought to be sent locally on the gadget.
- **Security requirement:** The system should have basic user authentication capability.

4.2 Process specification

The second step in IoT structure strategy is to characterize process determination. In this progression, the utilization instances of the IoT framework are officially portrayed dependent on and got from the reason and prerequisite determinations. In a process diagram, the circle denotes the start of a process, diamond denotes a decision box ad rectangle denotes a state or attribute. Figure 4.1 shows the process diagram for the smart door authentication system. Each door has a solenoid lock.

4.3 Domain model specification

The third step in the IoT plan approach is to characterize the area model. The space model portrays the principle ideas, elements, and articles in the area.

Domain model characterizes the traits of the items and connections between articles. Domain model gives a unique portrayal of the ideas, articles, and substances in the IoT space, autonomous of a particular innovation or stage.

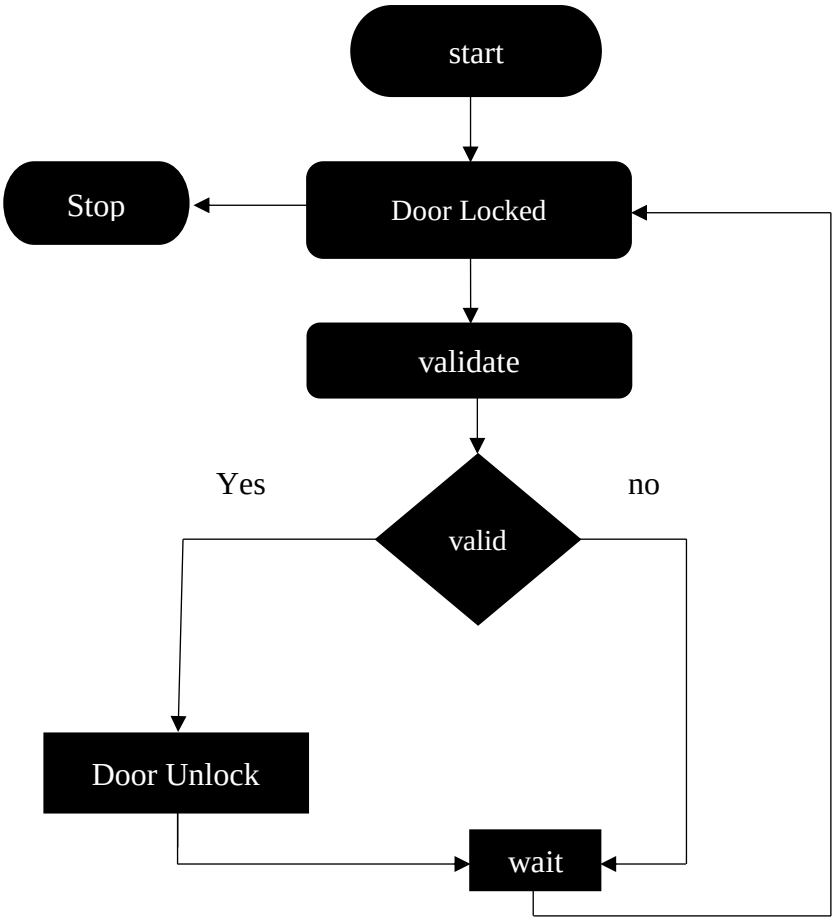

Figure 4.1: Process specification of smart door authentication system

With the domain model, the IoT framework originators can get a comprehension of the IoT area for which the framework is to be planned. The domain model for the smart door authentication system.

- **Physical entity:** Door
- **Virtual entity:** Door
- **Device:** on-device-resource
- **Resource:** On gadget is working framework which keeps running on single-board minicomputer.
- **Services:** A service that sets state to open or close and controller service that runs as a native service on the device.

4.4 Information model specialization

The fourth step in the IoT structure technique is to characterize the data model. The Figure 4.2 demonstrates the data model of the keen entryway verification framework, Information model characterizes the structure of all the data in the IoT framework, for instance, Attributes of virtual elements, relations, etc. Data model does not portray the points of interest of how the data is spoken to or put away. To characterize the data model, we first rundown the virtual elements characterized in the space model. Data model adds more subtleties to the virtual elements characterizing their characteristics and relations. In our smart door authentication system, we have one virtual entity for the door with attribute – door state.

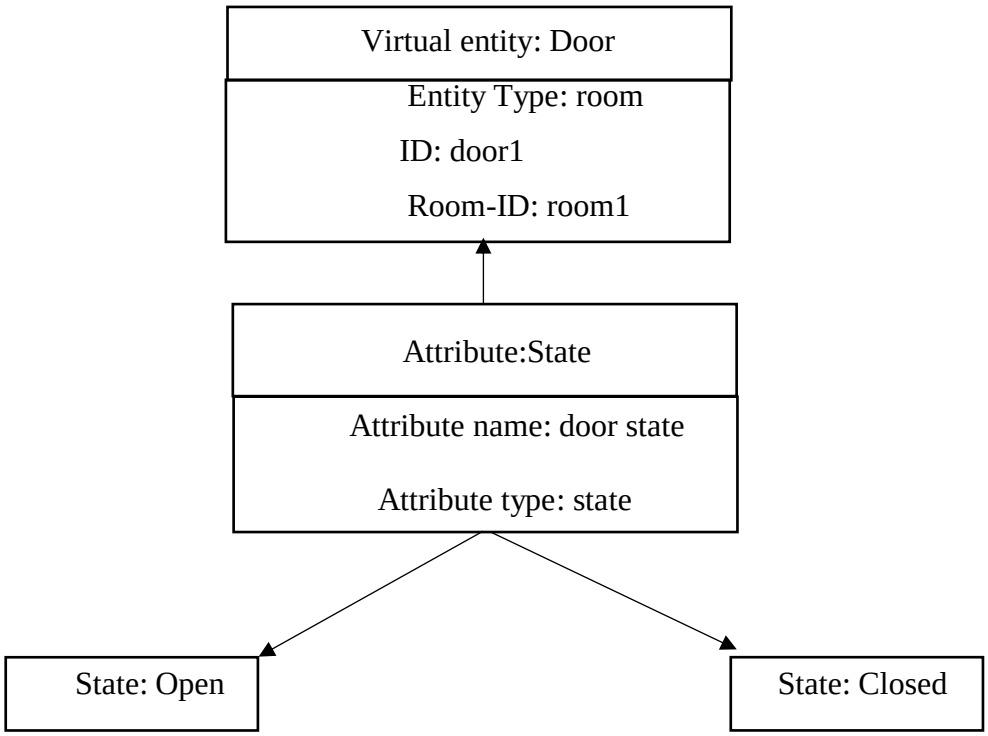

Figure 4.2: State information model of the door.

4.5 Service specifications

The fifth step in the IoT structure system is to characterize the administration particulars. Administration details characterize the administrations in the IoT framework, administrations types, administrations inputs/yield, administration endpoints, administration plans, administration preconditions and administration impacts.

Figure 4.3: Shows an example of deriving the services from the process specification and information model for the smart door authentication system. From the

process specification and information model, we identify the states and attributes. For each state and attribute, we define a service.

These services either change the state or attribute values or retrieve the current values. For example. In smart door authentication system, the state service sets the state to open or close.

Figure 4.3 and 4.4 show specifications of the state and controller services of the project.

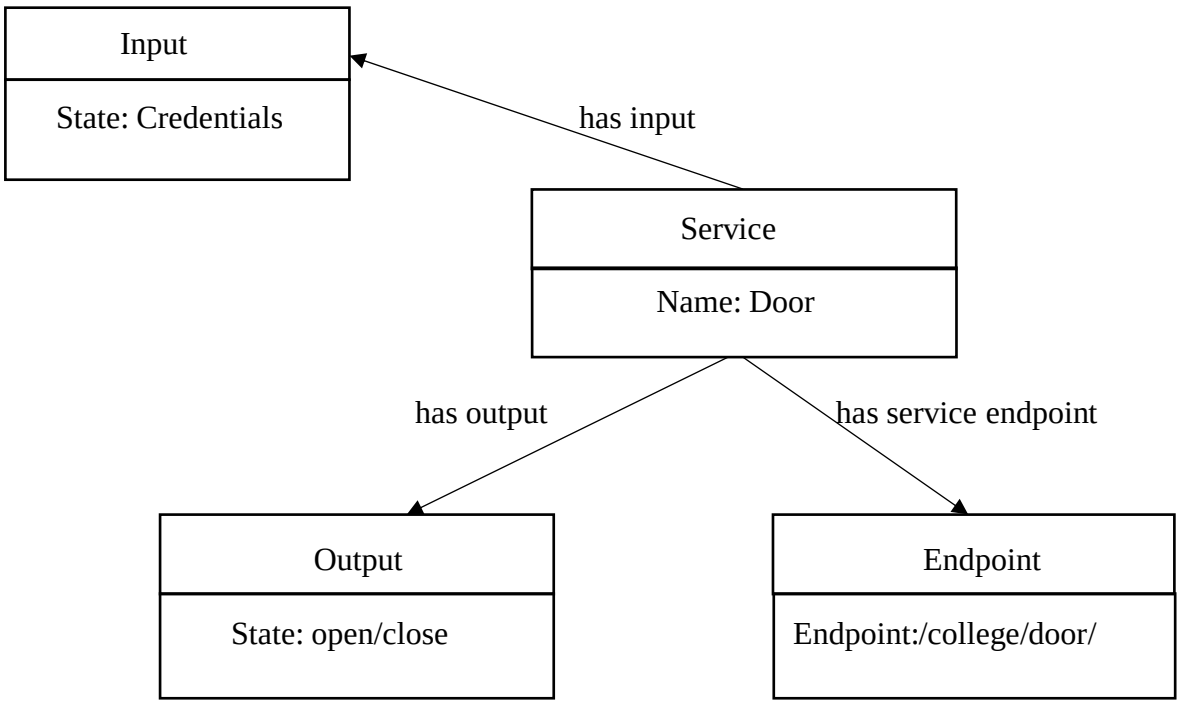

Figure 4.3 Service specification for smart door authentication system – State Service

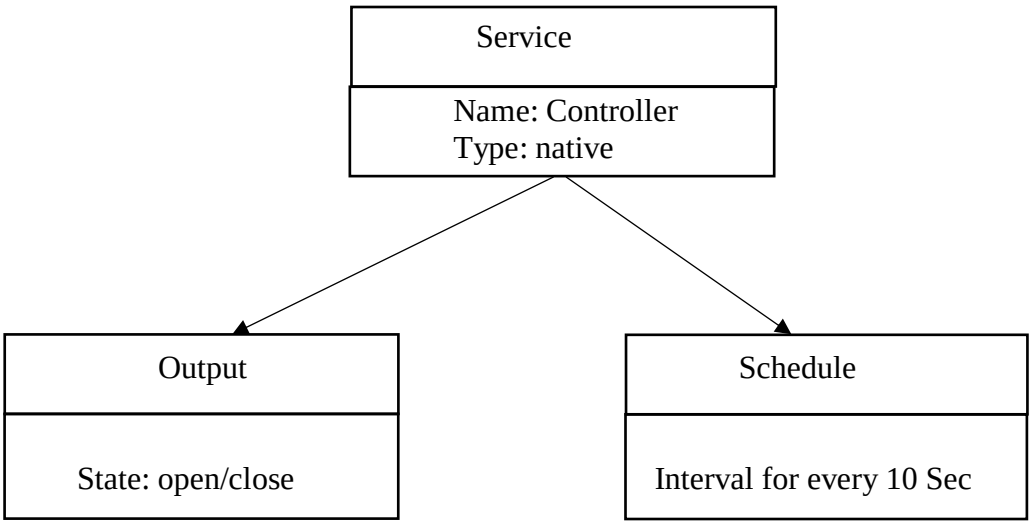

Figure 4.4 Controller specification for smart door authentication system.

4.6 IoT level specification

The sixth step in the IoT plan procedure is to characterize the IoT level for the framework.

4.7 Functional view specification

The useful view (UV) characterizes the elements of the IoT frameworks gathered into different utilitarian gatherings (UG). The functional groups (FG) included in a functional view include:

- **Device:** The gadget UG contains gadgets for checking and control. In smart door authentication system, the device UG includes a single minicomputer, a QR code and solenoid lock.
- **Management:** The administration UG incorporate all functionalities that are expected to design and deal with the IoT framework.
- **Security:** The security UG incorporates security instruments for the IoT framework, for example, verification, approval, information security and so on.

IoT device maps to the device UG (actuators devices, computing devices) and the management UG (device management). Resource map to the Device UG (on-device resource). Controller service maps to the services UG (native service).

4.8 Operational view specification

Different alternatives relating to the IoT framework sending and activity are characterized, for example, administration facilitating choices, stockpiling choices, gadget choices, application facilitating choices and so on.

Operational view particulars for the smart door validation framework are as per the following:

- **Devices:** Computing devices (ESP8266), Solenoid lock (Actuator).
- **Services:**
    1. Controller Service: Facilitated on gadget, actualized in installed C and keep running as a local administration.
    2. State Service: The door state weather is open or in closed state.
- **Application:** To lock and unlock a door using Wi-Fi protocol.
- **Security:** The passcode will be provided only for authorized personnel.
- **Authentication:** Passcode.

- **Authorization:** User ID.

4.9 Device & component integration

The device and components used in smart door authentication system are ESP8266 NodeMCU, minicomputer, Solenoid lock actuator.

4.10 Application development

The application has the controls for the state (Open and closed). In this state if the UserID and Passcode matches then it opens the door otherwise it remains in the closed State.

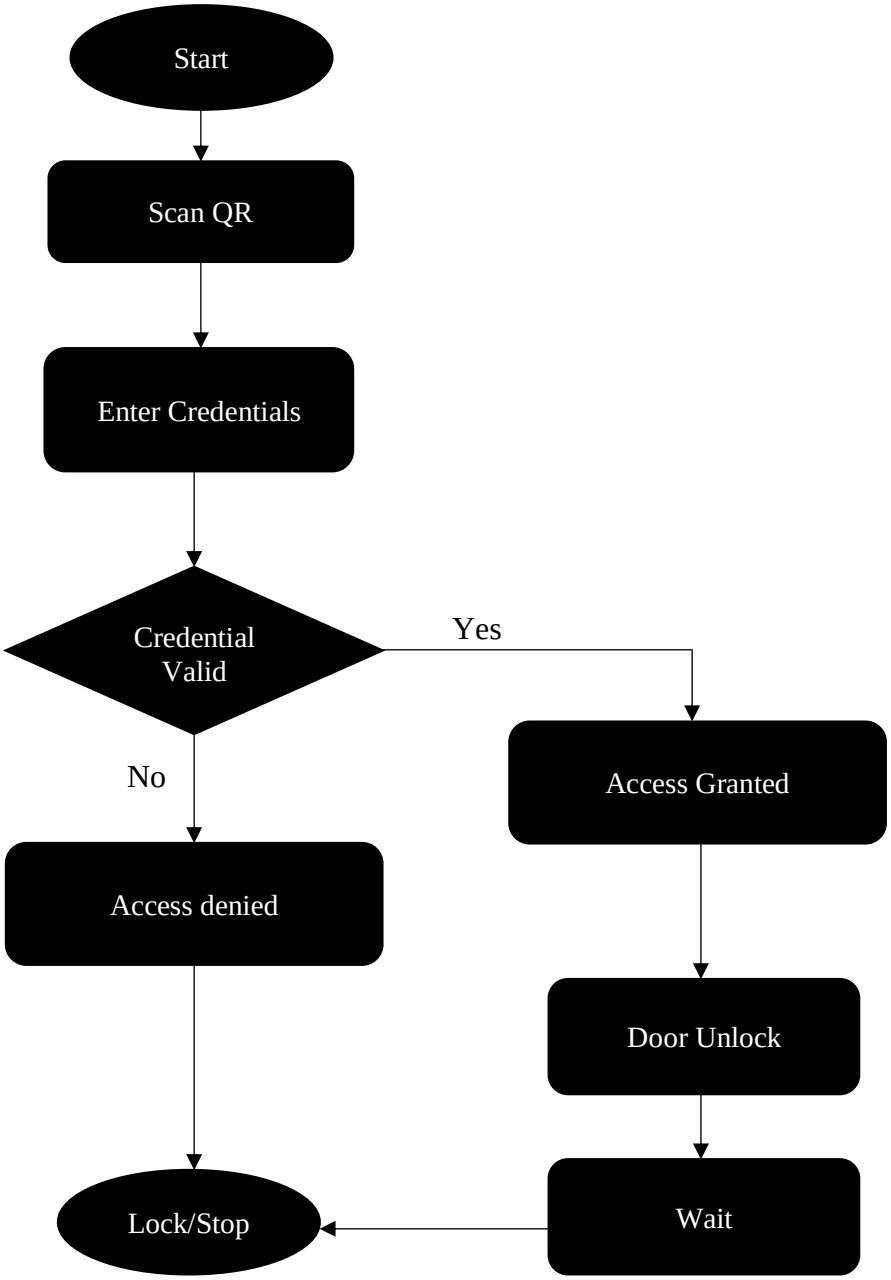

Figure 4.5: Flow chart for Smart door authentication system

There is a Wi-Fi network “SMART DOOR” the user has to connect their smartphone to the network and Sweep the QR code on the entryway which prompts the URL of the Authentication page of the savvy entryway. The Figure 4.5 shows the flow chart for Smart door authentication system.

The user has to enter their credentials in the provided UserID and passcode field. On entering the valid credentials, the user credentials are validated an alert is generated for the successful validation and the door is unlocked after a few second the door is automatically locked.

The Figure 4. demonstrates the square graph of the smart door authentication system where the user scan’s the QR code displayed on the site, on scanning the QR code the user is redirected to the Web page where person has to enter credentials, these credentials are validated, on successful validation an unlock event is called and a unlock signal is sent to the lock.

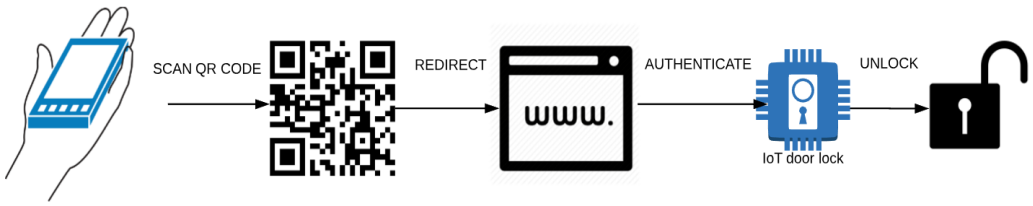

Figure 4.6: Block Illustration of Smart Door – Authentication System.

CHAPTER 5

SYSTEM REQUIREMENTS AND SPECIFICATION

5.1 Functional requirements

5.1.1 Solenoid lock

Solenoids are fundamentally electromagnets: they are made of a major loop of copper wire with an armature (a slug of metal) in the centre. At the point when the curl is empowered, the slug is maneuverer into the focal point of the loop. This makes the solenoid ready to pull from one end as shown in Figure 5.1.

This solenoid specifically is decent and solid, and has a slug with an inclined cut and a decent mounting section. It's essentially an electronic lock, intended for a fundamental bureau or safe or entryway. Typically, the lock is dynamic so you can't open the entryway in light of the fact that the solenoid slug is standing out. It doesn't utilize any power in this state. At the point when 9-12VDC is connected, the slug pulls in so it doesn't stand out any longer and the entryway can be opened.

Figure 5.1: Solenoid lock

5.1.2 ESP8266 NodeMCU

NodeMCU is an open-source firmware and advancement pack that causes you to model or construct IoT item. A picture of ESP88266 is shown in the Figure 5.2. It incorporates firmware which keeps running on the ESP8266 Wi-Fi SoC from Espressif Systems, and equipment which depends on the ESP-12 module. The firmware utilizes the Lua scripting language. It depends on the eLua venture, and based on the Espress if Non-OS SDK for ESP8266.

Figure 5.2: ESP8266 NodeMCU

5.1.3 QR code

A QR code (another way to say "quick response" code) is a kind of scanner tag that contains a network of specks. It tends to be examined utilizing a QR scanner or a cell phone with implicit camera. Once filtered, programming on the gadget changes over the specks inside the code into numbers or a series of characters. For instance, checking a QR code with your telephone may open a URL in your telephone's internet browser.

Figure 5.3: QR -code

5.2Non- functional requirements

- Performance.
- Efficiency.
- Security.
- Easy to use and expand.
- High adaption to smartphone.
- QR Code reader application.

CHAPTER 6

IMPLEMENTATION

ESP8266 NodeMCU miniaturized scale controller controls every one of the gadgets associated with it, into ESP8266 board and associated with power supply. The gadgets are activated by the progression of the code. Right off the bat, the entrance qualifications must be put away in the microcontroller unit. After entering the right certifications, the entryway either bolted or opened. For opening the entryway clients' accreditations needs to coordinate with the put-away certifications.

i. **For authorized user:**

On the off chance that the client is approved and the qualifications is approved effectively by the module. The reaction will be the begin and underwear the solenoid lock to open the entryway.

ii. **For unauthorized user:**

In the event that the individual attempts to enter invalid qualifications to get to the entryway, is found as unapproved and if the approval fizzles, the ESP8266 will begin and intimates the solenoid lock to stay in lock state.

- **To display alert on the web-page:**

  First, connect the system and make sure it is functioning properly without any errors. With the help of SPIFFS protocol upload the code in the ESP file system using ArduinoIDE.

  To display alert on the web page.

```
function grantAccess(){
    var userid = document.getElementById("userid").value;
    var passcode = document.getElementById("passcode").value;
    var xhttp = new XMLHttpRequest();
        if( userid ===" || passcode ==="){
            alert("Please fill all fields...!!!!!!");
            return false;
        }//end if
    else if ( userid ==='lab' && passcode ==='lab001'){
            alert("Access Granted");
        xhttp.onreadystatechange = function() {
        if (this.readyState == 4 && this.status == 200) {
```

```
            document.getElementById("login").innerHTML=this.responseText;
            } };
            xhttp.open("POST", "/doorUnlock", true);
            xhttp.send();
        }//end else if
        else if ( userid ==='labuid01'&& passcode ==='bmslab001'){
            alert("Access Granted");
            xhttp.onreadystatechange = function() {
                if (this.readyState == 4 && this.status == 200) {
            document.getElementById("login").innerHTML = this.responseText;
                } };
            xhttp.open("POST", "/doorUnlock", true);
            xhttp.send();
        }//end else if
        else if ( userid ==='labuid02' && passcode ==='bmslab002'){
            alert("Access Granted");
            xhttp.onreadystatechange = function() {
                if (this.readyState == 4 && this.status == 200) {
            document.getElementById("login").innerHTML = this.responseText;
                } };
            xhttp.open("POST", "/doorUnlock", true);
            xhttp.send();
        }//end else if
        else if ( userid ==='labuid03' && passcode ==='bmslab003'){
            alert("Access Granted");
            xhttp.onreadystatechange = function() {
                if (this.readyState == 4 && this.status == 200) {
            document.getElementById("login").innerHTML = this.responseText;
                } };
            xhttp.open("POST", "/doorUnlock", true);
            xhttp.send();
        }//end else if
        else {
            alert ("Check ID and Password");
            return false;
          }}//end grant function
```

6.1 Circuit diagram of the system:

The circuit diagram denotes the endpoints to be connected in the system, the Figure 6.1 denotes the circuit diagram of the smart door authentication system.

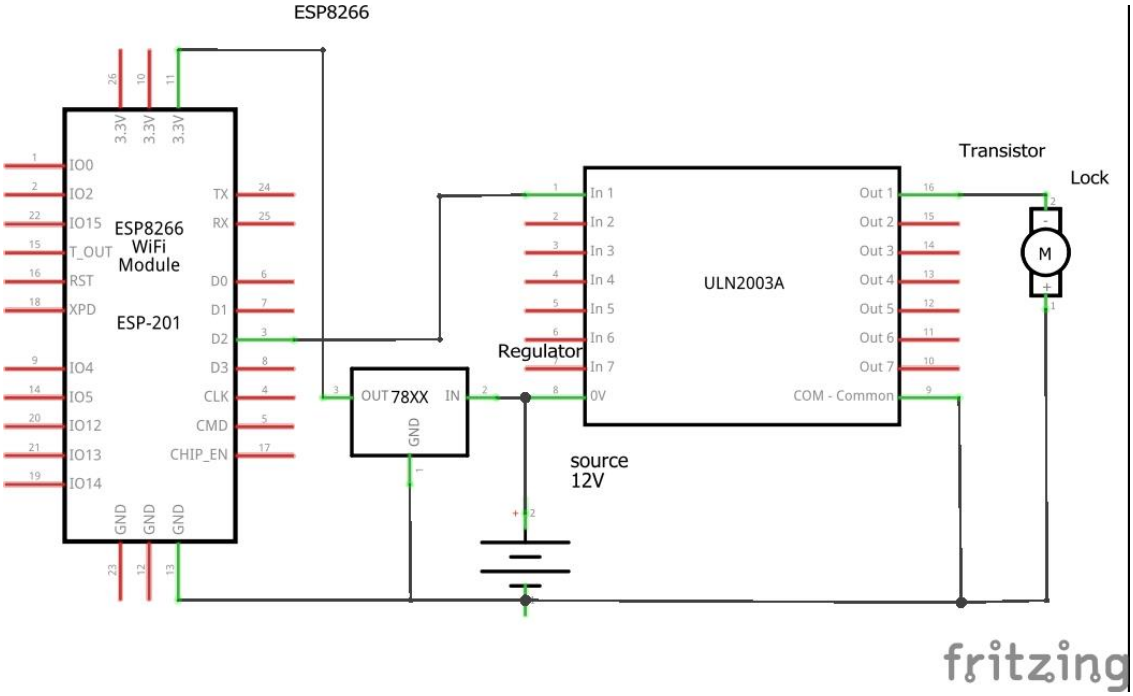

Figure 6.1: Circuit diagram of Smart Door System

CHAPTER 7

TESTING AND VALIDATION

Testing is the major quality control measure employed during software development; its major function is to detect errors in the software. Software testing is an investigation conducted to provide stakeholders with information about the quality of the product or service under test. Software testing can also provide an objective, independent view of the software to allow the business to appreciate and understand the risks of software implementation. Test techniques include but are not limited to the process of executing a program or application with the intent of finding software bugs (errors or other defects).

Software testing can be stated as the process of validating and verifying that a computer program/application/product:

- Meets the requirements that guided its design and development,
- Works as expected,
- Can be implemented with the same characteristics,
- Satisfies the need of stakeholders.

Software testing, depending on the testing method employed, can be implemented at any time in the software development process. Traditionally most of the test effort occurs after the requirements have been defined and the coding process has been completed, but in the Agile approached most of the test effort is on-going. As such, the methodology of the test is governed by the chosen software development methodology.

7.1 Testing fundamentals

During testing the product to be tried is executed with the arrangement of experiments and the yield of the program for the experiments is assessed to decide whether the program is executing as it is relied upon to do.

The achievement of testing depends significantly on the determination of experiments. The primary objective of check and approval exercises is to make the product won't experience a disappointment for a predetermined time under determined condition.

Verification and validation activities are classified as-

- **Static -** Static methods are the methods in which the behaviour of the system is observed without executing the system.
- **Dynamic –** In dynamic methods, the behaviour of the system is observed by executing the system. Testing comes under the dynamic category.

7.2 Levels of testing

The basic levels are:

- Unit Testing.
- Integration Testing.
- Validation.

Unit testing- unit testing focuses verification effort on the smallest unit of the software. Using the detailed design and the process specification, testing is done to uncover the errors within the boundary of the module. All modules must be successful in the unit testing before the starting of the integration testing begins.

Integration testing- Integration testing is a systematic technique for constructing the program structure while conducting tests, at the same time to uncover errors associating with the interfacing.

Validation- At the culmination of the integration testing, the software is complete as a package and the interfacing errors have been uncovered and fixed, final tests validation testing may begin. Validation test is succeeded when the software performs exactly in the same manner as expected with the requirements. Alpha and beta testing fall in this category.

7.3 Approached to testing

It is very difficult to test the entire system. Hence, different parts of the system should be tested independently. So, we assume the system has a hierarchy of modules. The common ways in which modules can be combines are-

- **Top down strategy**- In top-down strategy, we start by testing the top of the hierarchy and incrementally add modules, which it calls, and then test the new combined system.
- **Bottom up strategy**- The bottom up strategy starts from the bottom of the hierarchy. First, the modules at the very bottom, which have no sub-ordinates, are tested. Then, these modules are combined further with the higher-level modules for testing. If the system is developed in the down manner, top-down

testing should be used and if the system is tested in the bottom-up manner, bottom-up testing is used.

7.4 Test cases

SL.NO	TEST CASES	EXPECTED RESULTS	OBTAINED RESULTS
1	Scan QR	Encoded to redirect to the URL of the Authentication page	Successful
2	Login	Responsive HTML page to enter access credentials	Successful
3	Form Validation	Response from HTML page when invalid Credentials are entered.	Successful
4	Form Validation	Response form HTML page when no Credentials are entered.	Successful
5	Forgot Passcode	Responsive HTML page to get information when passcode is forgotten	Successful
6	Access Alert	An HTML Pop-Up when the correct access credentials are provided.	Successful

Table 7.1: Test cases table

CHAPTER 8

RESULT AND DISCUSSION

This part will give the outline of results observed on system. In this project the Smart Door authentication system will give access to authorized users of the room or a closet after validation through a Web interface where the user has to enter their credentials to enter the below snapshots shows the work flow of the project.

The Figure 8.1 QR-code will be displayed at the entrance of the door for the user to authenticate before entering the door. The user has to connect to the SMART DOOR Wi-Fi and scan the QR code to get redirected to the login page.

Figure 8.1: Snapshot of QR code for display

The Figure 8.2 is the authentication page for the smart door system where the user has to enter the credentials to gain access and unlock the door.

On entering the valid credentials as in Figure 8.3, the web interface will pop-up an alert confirming user that the access is granted and the door will be unlocked as shown in Figure 8.4, the Figure 8.5 and 8.6 shows the form validation fields when wrong passcode or no credentials are entered.

In case the user has forgotten the passcode and needs to contact admin. A get access details page is directed on clinking Get One Link on the access page as shown in Figure 8.7.

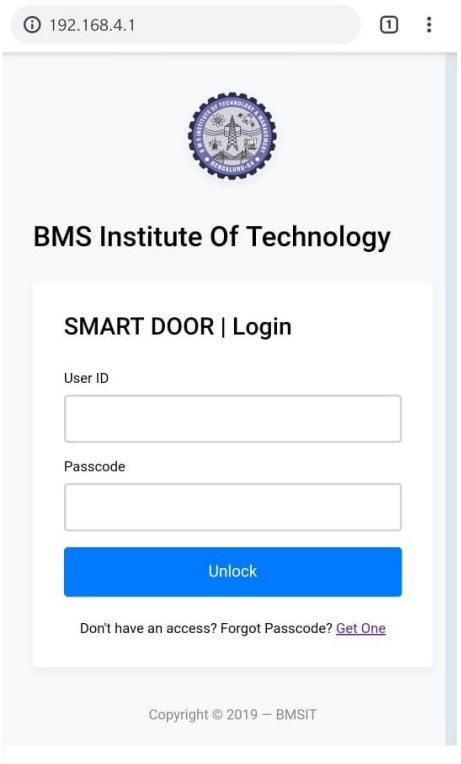

Figure 8.2: Web Login page

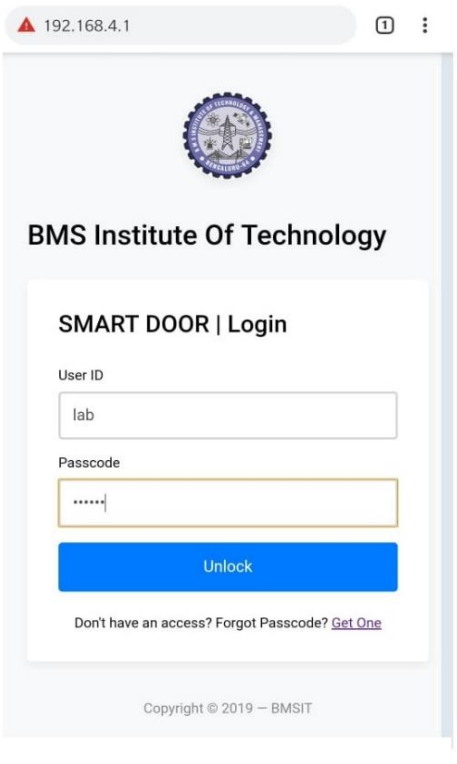

Figure 8.3: Credentials Fields

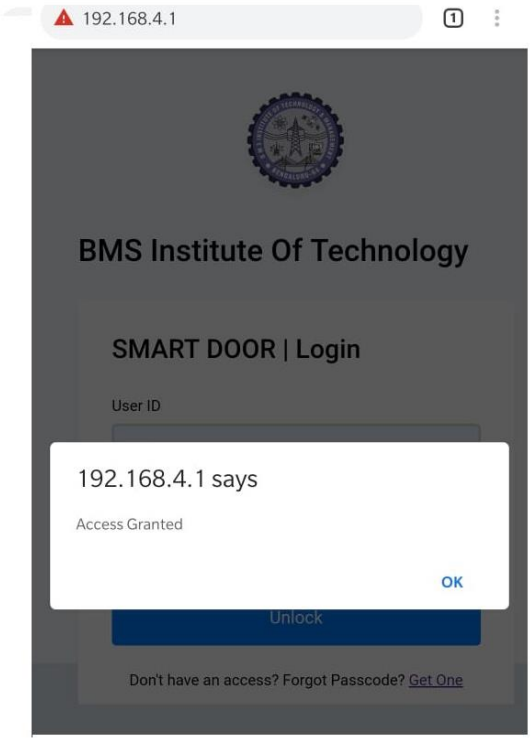

Figure 8.4: Access granted Alert

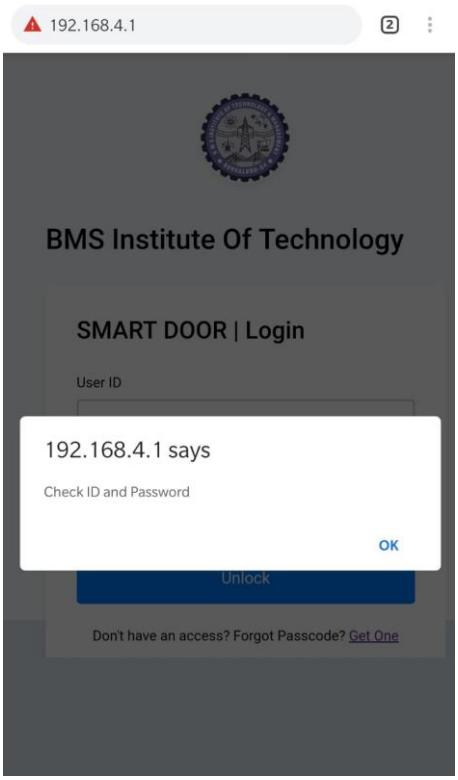

Figure 8.5: Incorrect Form validation

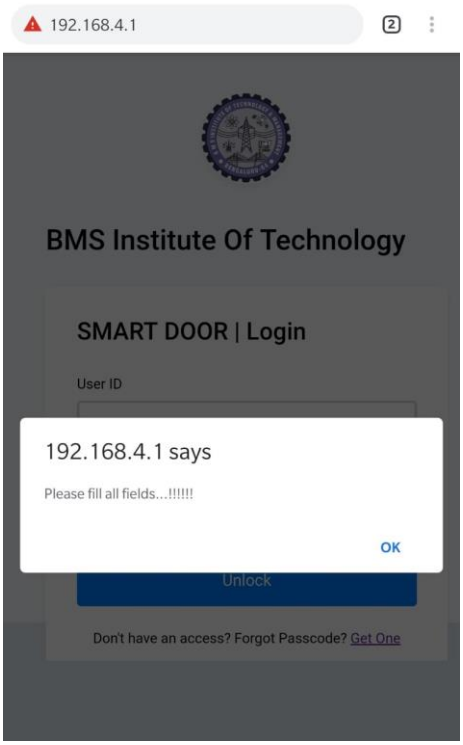

Figure 8.6: Check fields alert

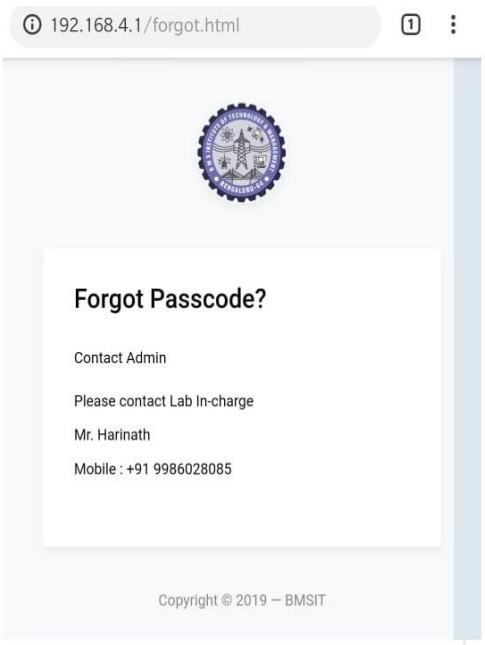

Figure 8.7: Forgot passcode page

CONCLUSION

Smart locks don’t always guarantee that they will be safer locks but they definitely provide more convenient way of locking and unlocking your doors. You will appreciate this purpose if you have ever walked up to your front door with your arms loaded down with grocery bags and forgot to grab you key first. With a smart lock all need to do is punch in an access code and you are in. This project describes the smartphones control the unlocking system and the way to develop this system, simply install on the door and configure it to communicate with the wireless network. The data transmission for this project is using Wi-Fi technology. In our opinion, Smart Lock System has great potential. It will allow users to forget about their traditional key and to use only their mobile device to get access to the needed area. To reduce the risks, all the possible security measures were taken, including the authorization to the mobile application. In case of loss of the mobile device, there will be option for the legacy key system, and thus giving access to the area.

FUTURE WORK

In this project we designed a lock module in which there are few components which are carrying all the operation. But our major aim to provide the both self-implemented software and hardware components. Here in this project we used web application which has its own private web server so that we don’t have to develop our own server. Our idea is to develop a lock module which can be access only through our smartphones MAC addresses. In future we will use a standard lock which operate via our whole module. For this we have to develop our own server which can saves our MAC address in its database. So that the Wi-Fi module can identify these addresses via its interface. For that we have to build a code using Arduino IDE to burn the code in the Wi-Fi module. We also have to develop a android application to control and monitor all operation instead of using web application. All these are our future plans to make this project major and more efficient to use in home automation and to provide increasing security to the houses.

BIBLIOGRAPHY

[1] Hussain F. Alsaif, Mohammed A. Almaghrabi and Douglas E. Dow Program in Electromechanical Engineering, College of Engineering Wentworth Institute of Technology “Portable Smart Door Lock”.

[2] Vedala Sharath Department of Research and Development, Robolab Technologies Private Limited, Pune International conference on emerging trends in engineering, science and management (2017) “IOT BASED SECURE DOOR LOCKING SYSTEM”.

[3] Ketan Rathod Prof.Rambabu vatti Mandar Nandre Sanket Yenare, Department Of Electronics Engineering, Vishwakarma Institute Of Technology, Pune, India. “SMART DOOR SECURITY USING ARDUINO AND BLUETOOTH APPLICATION”.

[4] Avinash Bagul, Chinmay Kulkarni, Gaurav Kayandepatil, Pranamya Korde, Shubham Amilkanthwar Assistant Professor, BE Student Department of Computer Engineering NBN Sinhgad School of Engineering, India “Key Authentication Based Door Lock Monitoring System using MQTT on ESP8266”.

[5] Y.Choi, Y.Park, W.Back, D.Lee and J.Byun, “Development of Home Automation System Using Digital Door Lock based on Wireless Sensor Network,” in Proceedings of KIIT Summer Conference, Vol.2011, No.5, pp.189-193, 2011.

[6] Ohsung Doh1, Ilkyu Ha, “A Digital Door Lock System for Internet of Things with improved security and usability”, Kyungil University, Gyeongsan, Gamasil-gil50, 712-701, Republic of Korea. Advanced Science and Technology Letters Vol.109 (Security, Reliability and Safety 2015), pp.33- 38 http://dx.doi.org/10.14257/astl.2015.109.08.

[7] https://www.hackster.io/electropeak/smart-door-lock-using-wifi-login-page-by-arduino-esp8266-e13825

[8] https://www.youtube.com/watch?v=PTSYfaWngTU