Cloud-Lock: Private Locker with secure Cloud Verification

Pratheek Prakash Shet[1]
Mayur B[2]
Dr. D. Bhuvana Suganthi[3]*

[1] *Student, Department of ECE, BNMIT, Bengaluru.*

[2] *Student, Department of ECE, BNMIT, Bengaluru.*

[3] *Associate Professor, Department of ECE, BNMIT, Bengaluru.*

Abstract - *We live in a world where privacy is essential. There have been reports of security breaches in both residential and official places. A unique digital locking system is proposed that can work with various technologies like Cloud computing, Data Encryption, and Biometrics. Design is done to enhance security and also ensure user convenience. A few years back, lockers used in public locker facilities such as banks, malls, and corporate lockers required a physical digital signature key, like pen drives. Which when lost, would make it difficult for the user to access the contents of the locker. To overcome such problems, this new security protocol is proposed, which makes use of cloud computing for remote authentication of the user, and biometrics for added security benefits are used. Cloud computing not only makes the authentication more streamlined but also improves efficiency. This entire process takes place directly on the cloud [8]. As a result, the security module used in the private locker becomes cost-effective and is far superior in performance.*

Keywords: **Private Locker, Cloud-based encryption protocol, Security systems, Cloud Computing.**

1. INTRODUCTION

A locker is a storage compartment for storing valuables. The lockers available in the market have security loopholes because they have a single layer of security that is password protected or uses the old-school locking mechanisms. These have had various problems in the past. To make the security protocol better on the locker, a few new technologies like biometric and hex keypad are used. The use of cloud computing ensures increased safety, improves efficiency, and reduces the overall time taken to compute the security protocols [8]. Hosting software platforms remotely, the computing power of cloud servers increases and also clears the memory. Cloud benefits the users by providing advanced security features that ensure the safety of data [8]. In a few schemes that have come out in the past years, a user has to produce a private key to realize data auditing. With demands for private lockers increasing, the implementation of biometric and hex keypads along with password protection, the overall security grade of the lockers improved significantly [7].

2. OBJECTIVE AND MOTIVATION

Our project is designed to help people secure their valuables in a much effective manner. Previous techniques, such as the generic username–password system, the integrity of the data wasn't secure, and hence this project aims to solve that issue. Previously used techniques required USB tokens and Smart cards, which if lost would make it very difficult to access the contents inside the locker. In recent times, many people are shifting from public lockers to private lockers for their secure storage needs. That's another reason where this project could be helpful.

To overcome this problem, a new technique called data integrity auditing is used in order to restrict the usage of the hardware token. We need to develop a locker with a software key, test key excluding a Private key for cloud services [6]. This project, when complete, will be a great product in various industries. From banking sectors to tourism, this has many useful applications. There is great market value, and this project has many other benefits when technologies like cloud computing are added.

3. RELATED WORK

Literature surveys are summaries of research papers that are studied, analyzed, and implemented. Writing structure should seem logical. It must represent the development of the ideas according to the field. The length of the literature survey depends on the purpose. Research papers can be reviewed and it also gives a clear understanding of the work done.

3.1 "Security and Usability Improvement on a Digital Door Lock System based on Internet of Things", by Ilkyu Ha, Kyungil University, Republic of Korea.

This paper describes a unique prototype of a private locker security system with five potential levels of security in a single device. Efficiency, accuracy, and implementation are made simple. Machine learning is used along with Bluetooth to authenticate the password. If there is a password error, the controller detects it and uses a camera to capture a visitor's image. Then the user receives the image on the mobile. The controller database has access to records that can be queried using the mobile device of the user. If visitors lose their key, their image is captured and transferred to the user's mobile device by pressing a specific key; now the user can have full control of the door lock after verifying visitors. Automatic opening and closing of doors after verifying visitors. When users attempt to access the locker which contains the object, the lock becomes difficult to open, the controller then communicates with the user's mobile device using Bluetooth and it provides access to the contents present in the locker. Mobile devices obtain impact detection information and invalid visitor image information. If the user

has image information for a valid visitor, the opening and closing of the door lock are performed. Incoming and outgoing records can be questioned [1].

3.2 "Microcontroller Based Reprogrammable Digital Door Lock Security System by Using Keypad & GSM/CDMA Technology", By Mohammad Amanullah, International Islamic University Chittagong, Bangladesh.

This paper explains a user-friendly, minor complexity, power-efficient, and in-expensive remote door lock solution. The given model is based on GSM/CDMA and matrix keypad technology. Incoming number verification systems have been incorporated for both protection and control [2]. The door lock can only open when there is permission after successful verification. Few technologies are available commercially, this has helped in monitoring home appliances. Mobile telephony is accurate, efficient, and reliable. The model can also be addressed on potential development requirements with the integration of AI-based door lock system design The device can be used in security checking, hospitals, parks, etc.

3.3 "Remote Control Locker" by John D. Enderle, Greg Mierzejewski, University of Connecticut, Connecticut.

This paper explains the working of Remote-Control Lockers. The proposed locker is composed of a transmitter-receiver device along with mechanical components for access [3]. Transmission of radio waves occurs after the input button is pressed. The resultant signal activates the circuitry within the locker. Whenever signal interception is performed, processing of received output is done by the device. Now a voltage signal is passed into an electric strike. The lever opens the locker. Circuit failure is prevented by low power indicators at both the transmitter and receiver sides.

Usage of this locker ensures easy accessibility to the locker [3]. The mechanism adopted provides flexibility for both the opening and propping of the door. The Linx device transmits and receives radio signals. This signal goes through encoding and decoding to ensure accuracy in transmission. When the input key is triggered, a pulse signal is sent to the device. This signal then activates the mechanical circuit to successfully open the locker. Circuit chooses stand-by mode when it is not working. Low power conditions are notified by low power indicators.

3.4 "Smart Locker: IoT based Intelligent Locker with Password Protection and Face Detection Approach", by Ratna R Sarkar, Niaz Mostakim, Md. Anowar Hossain, University of Science and Technology, Uttara Dhaka, Bangladesh.

This paper suggested an IoT-adapted smart locker to ensure the protection of user valuables. OTP ensures security [4]. To begin with, a request has been sent by the user. Now OTP is provided at the server end, which is performed by sending a feedback email to the user. The server will provide this OTP by sending the user a feedback email. The equipment uses Face detection methods which count the number of total users present. If more than one face is identified at the same time by the device, then the user receives the message. This particular user-friendly smart locker is more efficient than a conventional locker.

3.5 "Octave-spanning supercontinuum generation from a NALM mode-locked YB-fiber laser system", by Song Yang, Tingting Liu, Zheng Guo, Heping Zeng, Hong Hu.

This paper explains the implementation of a phase-biased NALM mode YB-fiber system, whose function is to deliver output pulses with a pulse duration of 140-fs, pulses energy of 137-nJ [5]. Usage of an integrated phase shifter helps in the reduction of the mode-locking threshold. Stability can be brought to single pulse operations. SC ranging 600 nm to 1300 nm segments of nonlinear PCF and F-CEO signals which are greater than 30 dB SNR. This model used fiber components that were hybrid and multifunctional. A PM fiber with Bragg grating was used, and also a highly doped YB-fiber, whose purpose is to speed up the repetition rate of the laser system.

3.6 "Security and Usability Improvement on a Digital Door Lock System based on Internet of Things", by Ilkyu Ha.

This paper explains digital door lockers with improved security protocols were proposed that can implement IoT. Physical impacts of an invalid security breach are sensed by a given locker system and notifications are sent to mobile device applications. If there are repeated mistakes in entering passcodes, the locker captures images of the invalid users and passes them to mobiles, and thereby security function is strengthened.

4. HARDWARE AND SOFTWARE DESCRIPTION

4.1. Hardware Details:

1. Node MCU: It is a low-cost open-source IoT platform. It has firmware that runs on the ESP8266 Wi-Fi SoC. Its hardware originated from the ESP-12 module.

2.Fingerprint Sensor: They are unique and durable over the person's lifetime, and also difficult to alter. They provide an output based on match conditions.

3.Husky Lens: Husky Lenses are used for providing security using a feature called face recognition.

4.OLED: Organic Light-Emitting Diodes works as a flat light emitting technology, produced by the serial arrangement of organic thin films placed between two conductors. When an electrical current is supplied to the OLED, bright light is emitted. They are emissive displays that do not require a backlight. They are more efficient than LCDs to upload this source code to the cloud database

5. Relay: It is an electrically operated switch, consists of input terminals for control signals and a set of terminals that act as contact operators.

6. 12V DC Solenoid: It works similar to an electromagnet, which generates magnetism by electricity.

4.2 Software Details:

1. 000WEBHOST Database: It is a free and open-source platform used for scripting, managing, organizing database services.

2.PHP: PHP is implemented in web development and also as a scripting language for scripting applications.

3.HTML: It is abbreviated as Hypertext Markup Language which is primarily used for displaying web browser applications.

4.MYSQL: Database service used to deploy cloud-related applications. It helps in storing and managing resources efficiently.

5. WORK DONE

There are two major aspects to this project. The first part is software development. This part includes the cloud database setup and integration and uploading the developed code to the file manager of the cloud database. Then, the other part is the hardware setup.

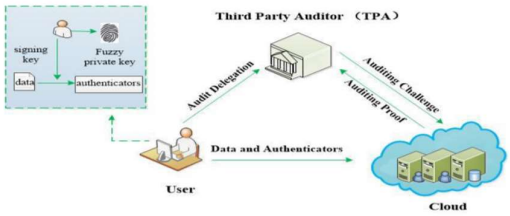

Figure 1. Working process

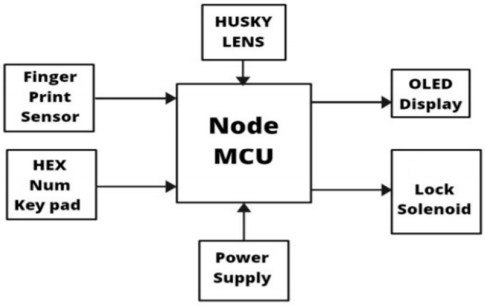

Figure 2. Block Diagram

This includes configuring the microcontroller and setting up other components and peripherals Now, we get into further details below:

1. Setting up the Cloud Database: There are many cloud service providers to choose from. For To The mechanism of this project, the 000WEBHOST online cloud database service was chosen. There are many benefits of choosing this service provider, firstly they have a fully custom control panel. This helps setting up the platform very easily. Then, they offer easy integration to query languages such as PHP and MySQL.

   We now create an account on 000WEBHOST. We do this by registering using an email ID and password. Attributes such as Database Name, username for each party, and password are given.

   The next step in the process is to configure the website settings that are suitable for our project. Once this is completed, our database can now be accessed.

   The 000WEBHOST supports PHP, MySQL, and HTML for the transaction of queries. For this particular project, we have made use of PHP and MySQL. The 000WEBHOST is equipped with PHPMYADMIN for the implementation of PHP. We have used PHP version 5.2, and hence, the PHPMYADMIN has to be configured for the same.

In order to make the authentication process work, a separate source code is written in MySQL. The query inputs are updated. photo a File Manager tool in the 000WEBHOST control panel is used.

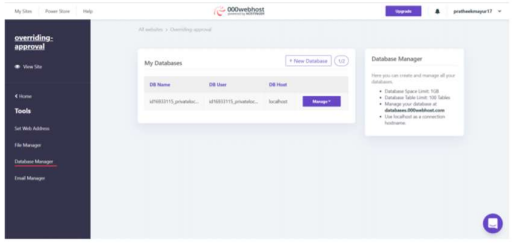

Figure 3. Created Database in 000Webhost

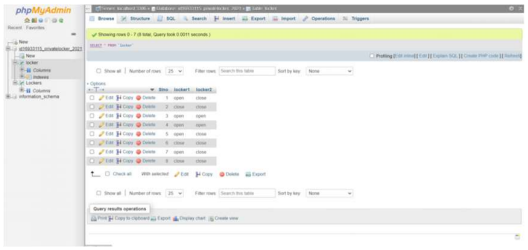

Figure 4. Table section of PHPMYADMIN

2. Creating the app interface: This step is very important as it gives a Graphical User Interface to the user. This app is created using the HTML language. Any commands given by the user on the front end using the app will be reflected on the PHPMYADMIN panel and the changes will be uploaded on the Cloud Database.

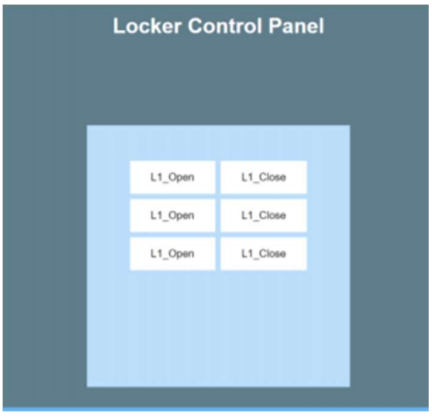

Figure 5. App Interface

3. Setting up NodeMCU: Now, we are going to set up NodeMCU and the control locker, which are connected to the HTML webpage. We can control the locker from the same network where the NodeMCU is connected. Then, connect the lock solenoid to Pins of NodeMCU, such that the positive terminal is connected to Pin 1 and the negative terminal of LED is connected to GND. Then, the other components such as the fingerprint sensor, the Hex Keypad, and the Husky lens are connected to the NodeMCU using similar techniques of configuration.

4. Controlling NodeMCU through the Cloud Database: In this step, we configure the NodeMCU to the previously created Cloud Database on the 000WEBHOST Platform. In order to provide visual feedback on the working of the locker, a separate App I is configured. Upon the working conditions provided by the server, the HTML page displays the Locker Lock-Unlock condition.

6. RESULTS AND DISCUSSION

With the completion of the software implementation, the next step is to simulate the working conditions. This step is very crucial as it helps in analyzing the code and checking for any limitations in the work that is being done so far.

In this case, we first launch the app interface that was previously designed. For any locker system, there are two possible conditions, which are LOCKER-OPEN or LOCKER-CLOSE. We test this by clicking on the L1_Open button when the locker is in a closed state. If the condition on the back-end, that is the PHPMYADMIN panel, changes to LOCKER-OPEN state, the command is executed successfully.

Similarly, to test the L1_Close condition, we ensure the locker is in the open state, and after clicking the L1_Close button, the locker condition should change to LOCKER-CLOSE. This, when completed successfully, ensures that our code is running without any errors and it is safe to move to the next phase, which is the hardware implementation part.

7. SOFTWARE AND HARDWARE INTEGRATION

The first step of the integration process is to connect the Wi-Fi module ESP8266 between the client and server. For implementing the Arduino Microcontroller, we import the “Arduinojson. h” header file. We are using servo motors to drive the locks, and hence we need to call them in our program, to successfully do the same.

Now, we need to configure the Wi-Fi module by giving it a suitable SSID and Password. The next step is to configure the previously developed website to integrate the Microcontroller. This is done by calling out the website credentials in the code.

There are three important things to consider - Gateway, Netmask, and IP. The Gateway monitors and helps control the Wi-Fi operations. The Netmask behaves as the interconnecting link between the client and the server. The IP is used for hardware configuration. The entire program is processed using JSON.

7.1 CONTROLLING SERVO MOTOR WITH NODEMCU OVER WIFI:

The NodeMCU serves a web page that contains the servo motor controls. The web page can be accessed by connecting to the NodeMCU ESP8266. The user must type the HTTP address of the server delivering the web page into the browser to open it.

Only 180 degrees can be rotated with RC servos. Their goal is to offer a precise location in an angle field ranging from 0 to 180 degrees. Tower pro micro servo SG90 is the RC servo motor used in this project. The servo motor SG90 is powered by 4.8 volts. The frequency and duty cycle of the PWM signal determine the spinning of the SG90 servo motor shaft. Most RC servo motors require a PWM frequency of 50 Hz. On a PWM signal duty cycle of 1 millisecond to 2 milliseconds, they can spin from 0 to 180 degrees. The servo shaft is moved to a 0-degree angle after a 1-millisecond duty cycle at 50 Hz frequency. 1.5 milliseconds equals 90 degrees, and 2 milliseconds equals 180 degrees. We can figure out the duty cycles for different angles on our own. For example, the duty cycle for a 45 degree shaft rotation is 45/180= 0.25, therefore 1(0 degree) + 0.25= 1.25ms.

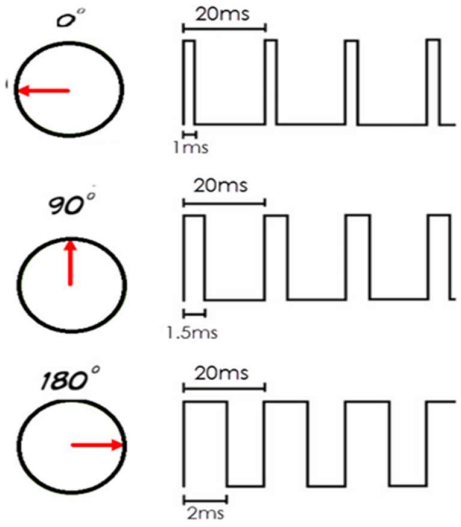

Figure 6. Duty cycle of SG90 Servo Motor

The NodeMCU is powered via the computer's USB connection, while the servo is supplied by a separate 5-volt adapter. The output voltage of the NodeMCU ESP8266 12V GPIO-2 or D4 pin is a PWM signal for servo motor operation. The PWM signal generated by the NodeMCU is also 3.3V TTL.

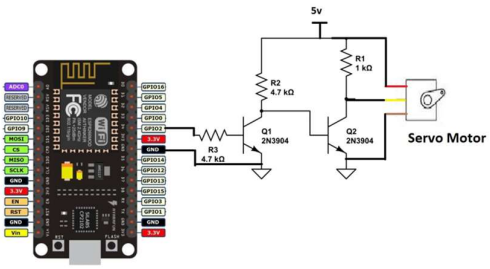

Figure 7. Node MCU-Servo Motor Connection circuit diagram

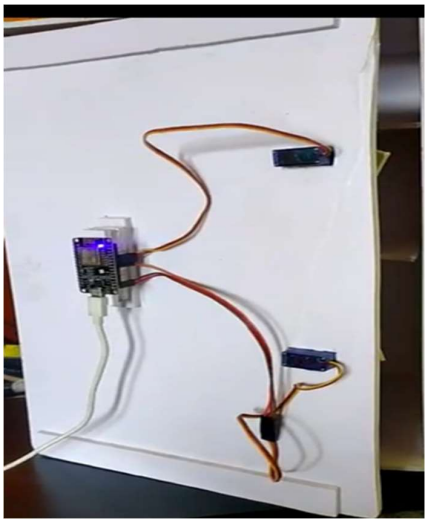

Figure 8. Connection of the Hardware Interface of the Locker

8. CONCLUSION

The intention behind this project was to improve the conventional lockers setup that was available in the market, so as to add safety and thereby ensure user convenience by utilizing recent technologies as explained.

The mechanism of the proposed locker comprises three levels of strict security which enhances portability, accuracy. Robustness can be improved in the future and its efficiency can be increased further. With good internet connectivity, our locker uses very little power for operation. The single microcontroller is sufficient for operations. Reduction of a security breach as there is a requirement of clearance at various different levels. Vulnerability towards malfunctions and theft is reduced significantly. Hence, the applications of this locker are numerous, like banking sectors, medical, IT, Government sectors, corporate sectors, etc.

REFERENCES

[1]. *Ilkyu Ha, "Security and Usability Improvement on a Digital Door Lock System based on Internet of Things", International Journal of Security and its Applications, Citation information : DOI: 10.14257/ijsia.2015.9.8.05, August 2015*

[2] *Mohammad Amanullah, "Microcontroller Based Reprogrammable Digital Door Lock Security System by Using Keypad & GSM/CDMA Technology", IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) - Volume 4, Issue 6, 2013.*

[3]. *Greg Mierzejewski, John D. Enderle, "Remote Control Locker", Citation Information : DOI :0-7803-6341-8/00/$10.00, IEEE, 2000.*

[4]. *Niaz Mostakima , Ratna R Sarkarb , Md. Anowar Hossain, "Smart Locker: IoT based Intelligent Locker with Password Protection and Face Detection Approach", I.J. Wireless and Microwave Technologies, 2019, 3, 1-10. Published Online May 2019 in MECS (http://www.mecs-press.net). DOI: 10.5815/ijwmt.2019.03.01 ,2019.*

[5]. *Zhengru Guo, Qiang Hao, Song Yang, Tingting Liu, Hong Hu, Heping Zeng," Octave Spanning supercontinuum generation from a NALM mode-locked YB-fiber laser system", Citation information: DOI 10.1109/JPHOT.2017.2655003, IEEE Photonics Journal, 2017.*

[6]. *Dr. D. Bhuvana Suganthi, et.al, "The Defense Against Jamming Attack in Cognitive Radio Networks: Energy Efficiency Management Perspective", Microprocessor and Microsystems, Elsevier, December 2020.*

[7]. *Dr. D. Bhuvana Suganthi, et.al, "Data imputation in Wireless Sensor Networks using Regression Models", International Journal of Advanced Trends in Computer Science and Engineering, Volume-9, Issue-5, October 2020. Page no. 8661-8665.*

[8]. *Dr. D. Bhuvana Suganthi, et.al "Reliable Security Policy in Mobile Distributed Network", IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology (RTEICT), IEEE Transaction on Communication Society, May 2016.*

[9]. *Dr. D. Bhuvana Suganthi, et.al, "Fault Tolerance Communication in Mobile Distributed Networks", International Conference on Data Engineering and Communication Technology, March 2016.*