IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

WIFI Controlled Door Locking System

Lakshmi.S
Department of ECE
SNS college of technology
Coimbatore, India

Surya Teja Kamma
Department of ECE
SNS college of technology
Coimbatore, India

Deepak.V
Department of ECE
SNS college of technology
Coimbatore,India

Karthik.M
Department of ECE
SNS college of technology
Coimbatore, India

Monika.R
Department of ECE
SNS college of technology
Coimbatore,India

Dhanush.S.M
Department of ECE
SNS college of technology

Karthik.M
Department of ECE
SNS college of technology
Coimbatore,India

***Abstract*—Protection of property is a matter of concern nowadays. The door provides entry- level security which is encrypted by a lock. By providing a better solution for the locking method, it hikes up protection. The implementation of wireless locking procedure provides better security by escaping hacking. The usual method of locking a door is by using exposed locks which can be unlocked by either a key or password. The matter of concern is -the lock is exposed outside, which paves the easiest way for hacking. The keys can be hacked by its duplicate or breaking the lock. The password locks are also prone to damage. Hiding the lock inside the door confuses the intruders so that they can't mess up with it without finding a way to unlock it. Hence this WIFI based locking system provides a three-layer authentication mechanism to communicate with the lock.**

Keywords*—WIFI network - Three step verification - indirect access - improved security - Low power consumption - multi device support - remote access - lock mechanism is confidential.

I. INTRODUCTION

The world has now become very cosy with technology advancements and increased civilization. Our resources and earnings are becoming expensive when compared to that of the times in the past. Hence there is a need to protect those from robbery and theft.

Nowadays the locks that are commonly used are easier to decrypt, since the mechanism is directly exposed. No matter how complex the mechanism is, it is viable outside. This proposes the risk of hacking it with modern tools.

But what if the mechanism is hidden and not exposed outside directly? What if there're steps of protocols to access the lock with our handheld device with enhanced protection?

That's when our WiFi based door lock comes into the pictures. Firstly, it totally hides the internal architecture thereby providing a contactless security mechanism.

Secondly, there is a need to monitor the people who are getting access. The system also provides an efficient way to achieve this by logging the data as a database in its own flash memory. Then additional security measures needs to be taken into matter. This system allows the integration of various sensors and notices the external conditions and work as per as the requirements.

Hence this system provides a efficient way to tackle the security process and ensures a low powered but highly secured encryption system.

II. LITERATURE REVIEW

The existing methods of safety includes usage of primitive locks and password related systems. They provide primary security, but still there are some controversies that exist. The mechanisms used are directly exposed and it is can be easily tackled by the intruders.

The locks can be opened by duplication of keys and password-based systems can be hacked mechanically. Hence irrespective of the technology that's used, it needs to be concealed from outside.

WiFi technology provides a primary encryption and it is followed by an IP and a password based protection. It replaces the conventional physical keypad with the most secured, three step verified, contactless security access.

It provides remote accessible operation. It also logs the timing and entry each and every time a call for entry is carried out. This system uses Internal Electronically Programable Erasable Memory (EEPROM).

The system creates an relative database inside the memory with the help of HTML and JavaScript to render the data as a webpage to provide the details whenever it is needed.

It is equipped with a vibration sensor and a passive infrared sensor to analyse the external criteria and provides an warning system .

III. PREVIOUS WORKS OF THE PAPER

The proposed system in the previously referred paper described an improvement of a security system that is integrated with an Android mobile phone device using Bluetooth as a wireless connection protocol.

It allows a user to lock or unlock a door for short ranges from the door. One author has designed a system by using a UTP cable. Hence it needs to be wired.

Another referral uses the Wifi-based network encryption but it relies upon the internet and the external server.

This causes problems while the internet or the server is down. All of the above-mentioned difficulties caused by the previous referrals can be solved by our prototype.

The prototype proposed by us relies on the primary access point but it does not use the internet. On the contrary, it establishes its server using its access point and it can also use the existing broadband network. Hence Network outage is not a concern here. The power outage can also be managed by providing an additional backup. The main power source of the proposed system is a rechargeable battery. Another advantage of our prototype is that the cabling will be decreased as there is no SLS connection, which promises a contactless transmission via WiFi.

The older system has less security whereas our proposed system has a 3-step verification process which includes SSID, IP address, and many more verification processes and is also long ranged.

IV. PROPOSED SYSTEM

The proposed prototype is a more secure and less cabled system in which there is no need for an SLS connection. In our proposed system, we are including a Node MCU ESP 8266 microcontroller module which is used to control the motor and acts as a server.

The ESP module is a microcontroller with inbuilt WiFi. It serves the purpose of providing network authentication and remote control. The module can create its own access point and can also connect to an already existing access point depending upon the purpose.

Every module has its own IP address and it also can be modified using this IP we can add another layer of security as it is used to access the rendered webpage. It can work on almost any device.

Hence it provides multi-device support. The web page is rendered by the Node MCU which is stored on its own internal flash memory and it solves the memory complications while running the program in RAM.

In addition, the web page is equipped with JavaScript with a dynamic user interface which is the source of control. It gathers the login credentials and also verifies them. It integrates an API based on JQuery to export the given data to an excel sheet.

A) Steps for getting access to the lock

The steps for connecting to the lock includes :

1) Connecting to the WiFi network.

2) Entering the IP address with a specific device port to any browser.

3) Entering the login credentials to the rendered webpage.

B) Response for unauthorized access

If any one of the above criteria is not met with, then the system will not decrypt. The password is embedded with the source code and hence it cannot be modified further. The JavaScript acts as a validator that verifies the credentials and sends the data to the server. Anyhow the data is not shared outside even with the browser development tools.

C) Tools Required for implementation

1. NODE MCU.
2. SERVO MOTOR.
3. 9V RECHARGABLE BATTERY
4. ARDUINO IDE 2.0.
5. VIBRATOR SENSOR
6. PIR SENSOR

D) About the controller

It is a 32 bit microcontroller which includes 8 digital pins, one analog pin and an integrated WiFi .

It supports 3 modes of operation on WiFi:

I) Access point mode

II) Access point and station mode

II) Station mode

Its firmware supports server side hosting which enables it to host any kind of webpage by acting as a server. It has internal memory of 32 MB EEPROM . It has a flash memory

of 16 MB. It possesses a total of 16 GPIO's which are multiplexed for different usages.

E) Additional security provided

- It is interfaced with a vibration sensor to detect the door vibrations and alerts on unauthorized entry.
- It has a Passive Infrared sensor to sense the person who are in front of it . If no person is detected, it won't decrypt the lock.
- It is not affected by power cuts as it has a secondary source for power.
- The power supply unit is also enhanced with high voltage protection and ensures continuous power supply is maintained.

F) Future improvements

This system can further be automated to messaging or email-ing the owner about the existence of causalities in front of it.

V) DESIGN IMPLEMENTATIONS

A) Empathy

This step basically focuses on understanding the customer or end user requirements and designing a prototype in accordance to it. Here the problem is about the security concerns that are being faced while exposing the mechanism of locking revealable. The prototype is designed in such a way that it overcomes this issue. The lock's functionality is almost hidden and its equipped with 3 layers of authentication which is hardware and software based. Hence this prototype is mainly made with the intention of attending the needs of the clients.

B) Defining the problem

The Defining part consolidates the previous issues encountered during the past developments and provides a solution that counters the same. The previous developments of the wireless door locking system makes use of Bluetooth, RFID, WiFi and wired protocols. But each of them have their own drawbacks . This system uses a protocol that uses WiFi but in an efficient way. It solves the glitch that causes the system to not be linear. It also solves the power issues that makes the system inoperable in the absence of external power . It makes the entire mechanism not exposable that in turn confuses the intruders on how to access it.

C) Ideating the solution

The Ideating stage prepares our mind to think how to tackle the problem with an apt solution. The development of blueprint for the prototype is the base part of it . It also includes the protocols on how the system should operate. The WiFi accessible door lock uses the ESP 8266 module as its heart. It can be programmed with Arduino IDE to assign the desirable task which is designed using C language. The core of the system establishes a server with HTTP protocol. The end user device which is connected to the corresponding WiFi network can communicate with it with the help of a unique IP address assigned to the module. This ensures a three-layered verification protocol for accessing the lock in a contactless manner.

D) Prototyping the Ideated solution

The development of the resultant prototype is the most essential task in providing the end users a real usable experience. The prototype can either be hardware or software but it must be customized to provide users a real time experience. Our idea is also modelled as a device that is updatable and not hardcoded, hence it is ready for the future improvements. By providing spatial improvements, this system can be made free of glitches and ready to handle real time situations. As the controller used is programmable, it can be modified to tackle different external difficulties by altering it without any physical changes. This a hardware-cum-software based development and it utilizes both for its operation. It also uses the sensors as its external inducers to analyse the conditions.

D) Testing the prototype

The testing of the model is the final phase before deployment. The system must be validated with different inputs to check if it responds the same to all the inputs. It also includes the end users who provide feedback based on the usage. By evaluating the system depending upon the feedback is the crucial updates that are need to be performed spontaneously.

V. CONCLUSION

Hence our proposed model will overcome the difficulties by providing enhanced security and contactless access. This methodology fulfils the need for supporting autonomous locking devices and easy key distribution while compared to a physical key. This system allows to log the data in real time thereby providing the data of causalities accessing the lock. Thus, this system is an updated version of the previous proceedings.

References

- Lv and L. Xu, "AES encryption algorithm keyless entry system", Consumer Electronics Communications and Networks (CECNet) 2012 2nd International Conference, pp. 3090-3093, 2012.
- On Android Mobile Devices for Home Security Application.In: Proceedings of IEEE Southeast con.. Potts J. and Sukittanon S. 2012. Exploiting Bluetooth
- Neelam Majgaonkar, Ruhina Hodekar, Priyanka Bandagale, Automatic Door Locking System, International Journal of Engineering Development and Research, Volume 4, Issue 1,2013 ISSN: 2321-9939.
- Bhalekar Pandurang, Jamgaonkar Dhanesh, Prof. Mrs. Shailaja Pede, Ghangale Akshay, Garge Rahul, Smart Lock: A Locking System Using Bluetooth Technology & Camera Verification, International Journal of Technical Research, 2013.
- Azmi, Smartphone activated door lock using WiFi. University Teknikal, Malaysia Melaka, 2015.

- Y.W Prakash, V.Biradar, S.Vincent, M.Martin, and A.Jadhav, smart bluetooth low energy security system, in 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), March 2017,

- Ribeiro, L. D. Oliveira, D. A. Nascimento, D. B. Alencar, and J. D. Júnior, "Application of the Internet of Things in the Development of a "Smart" Door," International Journal of Advanced Engineering Research and Science, vol. 6, no. 5, pp. 345-349, 2019, 10.22161/ijaers.6.5.46.