International Journal of Informatics, Information System and Computer Engineering

Design and Construction of a Smart Lock System using Internet of Things (IoT)

Muhammed Abudu Aniru, Enoma Victor Osasenaga, Osamwonyi Efosa Emmanuel, Matthew Onyeka Gerald, and Emede Oghenekome Melody*

Department of Electrical/Electronics, University of Benin, Benin City, Edo State, Nigeria.
*Corresponding Email: abudu.muhammed@uniben.edu

ABSTRACTS

This paper aims to design and construct a smart door lock system using the Internet of Things (IoT), WiFi module, relay module and other peripheral devices to provide people with an incomparable level of control and accessibility over their home's entry points. Traditional door lock systems are slow, insecure and with high vulnerability and they require human intervention to lock and unlock them. Thus, an IoT-based smart door lock system offers a proper lock protection mechanism with better performance. The system comprises a microcontroller (NodeMCU ESP8266), solenoid lock, DC battery(12V), 5V 3A buck converter (LM7805), WiFi module and a switching device (Relays). The setup of the system was tested with 3 independent devices for 10 trials. All of the trials accurately interpreted the received commands and transmitted the corresponding signals to the interfaced relay module. Subsequently, the relay module effectuated the lock/unlock operation on the integrated solenoid lock mechanism, thus accomplishing the intended objective of the study.

ARTICLE INFO

Article History:
Received 25 Sept 2024
Revised 19 Okt 2024
Accepted 23 Nov 2024
Available online 10 Dec 2024
Publication date 01 Jun 2025

Keywords:
NodeMCU
ESP8266.lock/unlock,
Soleniod, Smart, Integrated

DOI: https://doi.org/10.34010/injiiscom.v6i1.14127
p-ISSN 2810-0670 e-ISSN 2775-5584

1. INTRODUCTION

While keys have long served as the gatekeepers of our homes, the rise of smart technology has birthed a more convenient and adaptable alternative: the smart door lock. This innovative upgrade surpasses the limitations of its manual precursor, offering not just security but also enhanced accessibility through keyless entry and remote control. Smart door locks simplify everyday routines as it eliminates the need for physical keys and allowing seamless access management, as its usher in a new era of connected home security. In our today's world, home security has become an essential concern for individuals and families. Even as it provides basic level of security, traditional lock systems are often prone to various security threats, such as lock picking, key duplication, and forced entry. The emergence of smart home technology has flagged way for innovative solutions that address these security concerns while offering enhanced convenience and accessibility. One such solution is the smart lock system, which combines advanced electronic components, wireless communication technologies, and mobile applications to provide a secure and user-friendly access control system.

A multi-level security biometric door-locking system that can be controlled remotely (Anirudh et al., 2021). The primary objective of the research was to implement the door lock system utilizing a fingerprint sensor as the authentication mechanism. This objective was achieved through a Bluetooth-connected Arduino microcontroller, facilitating remote access and control. While their approach demonstrated a commendable effort, a notable limitation was observed concerning the proximity constraints. In scenarios where a user desires to access the door from a distance exceeding 10 meters, the system's functionality becomes diminished due to the inherent bandwidth limitations of Bluetooth technology, rendering the services of the application unsatisfactory.

A Radio-frequency identification (RFID) door lock was proposed for security and access control (Ting and Keane, 2014). While designed for convenience in unlocking doors without traditional keys, the system lacked important security features, prompting suggestions for enhancements such as adding a buzzer for alerting purposes, SMS alerts, and more. Ni Ni and San San, recommended incorporating a keypad in RFID door lock system (Ni Ni and San San, 2019). The addition of a password after scanning the RFID tag was proposed to enhance security and provide an extra layer of protection. In another work, Adole et al., introduced an RFID-based Security Access Control System with GSM Technology (Adole et al. (2016). While advanced and equipped with GSM technology for user alerts, the additional technology increased the overall system cost, limiting its cost-effectiveness compared to other systems. On creating a smart door lock that allows users to unlock the door using a smartphone, promoting easier interaction compared to other locking systems (Kamelia et al., 2014). The proposed door locks integrated various technologies, including Bluetooth module as a command agent, a smartphone as a task handler, Arduino Uno microprocessor serves as a controlling and data processing unit, and a solenoid as the output.

DOI: https://doi.org/10.34010/injiiscom.v6i1.14127
p-ISSN 2810-0670 e-ISSN 2775-5584

An access control system, leveraging One-Time Password (OTP) technology, with aims to address the limitations inherent in traditional user authentication methods such as digital and mechanical door locks (SeungSoo et al., 2013). Unlike these conventional systems, the proposed approach eliminates the need for administrator intervention when granting access to the facility. Instead, users are required to possess knowledge of the OTP and have a registered mobile phone. Upon user request, the OTP is promptly generated and transmitted to their mobile device, streamlining the access process. This innovative system not only mitigates the risk of loss or theft associated with conventional access control mechanisms but also enhances user authentication by incorporating a combination of card and number input methods based on the OTP value. Focused on the necessity of a low cost electronic home security system designed in coordination with other security measures to reduce the risk of home intrusion (Mishra et al., 2014). Keeping this problem in mind, they worked on a project on automatic password based door lock systems utilizing the electronic technology to build an integrated and fully customized home security system at a reasonable cost.

Paper delved into the design and development of a sophisticated home security system that leveraged human face recognition technology and remote monitoring capabilities to verify visitor identities and regulate door accessibility (Sahani et al., 2015). At the heart of their security system lies a combination of wireless control and accessibility features. A ZigBee-based wireless network technique, coupled with a Principal Component Analysis (PCA)-based image processing technique, formed the backbone of the system's operation. This integration ensures the system's responsiveness and reliability in addressing security concerns as they arise. The utilization of ZigBee modules in tandem with electromagnetic door lock modules facilitates seamless control over door accessibility, offering a robust barrier against unauthorized entry.

An innovative Android-based door-locking system that enabled remote control and monitoring capabilities through a user-friendly mobile application (Adarsh et al., 2018). Their system employed a microcontroller as the central processing unit, interfaced with various hardware components, including a solenoid lock, sensors, and a WiFi module. The Android application facilitated seamless communication with the system, allowing users to lock or unlock the door, receive real-time status updates, and configure access permissions remotely. Developed an Android-based door-locking system that leveraged the Internet of Things (IoT) paradigm (Agbo et al., 2017). Their approach integrated a Raspberry Pi single-board computer as the system's core, enabling robust computational capabilities and seamless integration with cloud services. The Android application served as the primary interface, enabling users to monitor and control the door lock status, while also providing additional features such as motion detection and user authentication through biometric recognition. Important contributions are made by integrating Android-based systems with automation and security features (Shafarana and Aridharshan, 2017). Their research endeavor aimed to leverage the

DOI: https://doi.org/10.34010/injiiscom.v6i1.14127
p-ISSN 2810-0670 e-ISSN 2775-5584

widespread adoption of Android devices to develop a comprehensive smart home solution that encompasses door locking mechanisms as well as other home automation components. The researchers recognized that the design and features of smart door lock systems are inherently influenced by the specific requirements and available resources within different regions and countries. Consequently, their approach focused on developing a flexible and adaptable framework that could be tailored to meet the diverse needs of various contexts. By harnessing the capabilities of Android devices and their seamless integration with wireless communication technologies. The user-friendly Android interface provided a centralized platform for managing these diverse functionalities, enhancing convenience and operational efficiency.

All research efforts highlighted the potential of Android-based solutions in addressing the evolving security needs of modern households. The integration of mobile applications with embedded systems and IoT technologies facilitated remote access, enhanced user convenience, and provided real-time monitoring capabilities. Furthermore, the adoption of secure communication protocols and user authentication mechanisms ensure the integrity and confidentiality of the systems.

The use of Bluetooth technology to establish communication between the Smartphone and controller board (Sravani and Kannappan, 2017). The system supports both microcontroller controlling and manual controlling to lock and unlock of the system. The system relies on the availability of the Bluetooth connectivity to provide remote access from smart phone or tablet.

Building upon the insights gleaned from their work, a more robust and comprehensive approach was conceived. This enhanced solution encompassed the replacement of Bluetooth connectivity with a Wi-Fi module, thereby circumventing the range limitations imposed by the former. Furthermore, the Arduino Uno microcontroller board was replaced by the NodeMCU board, a platform that offers elevated functionality and seamlessly integrates a Wi-Fi module, addressing a critical deficiency encountered in the utilization of the Arduino Uno board. Through this strategic incorporation of advanced technologies and a meticulous design approach, the proposed system not only addresses the proximity constraints but also leverages the inherent advantages of Wi-Fi connectivity, such as extended range, improved data throughput, and enhanced scalability. By embracing the NodeMCU platform, the system benefits from a comprehensive suite of features and capabilities, enabling the development of a more robust, efficient, and versatile biometric door locking solution

2. METHOD

The system consists of 3 major parts: The power supply unit, the, the control unit and the display unit. Fig 1: represents the block diagram of the system. The block diagram shows the power flow and interconnections among the core components of the system. The NodeMCU microcontroller acts as the central processing unit. Key components depicted include the solenoid lock for door locking/unlocking, a voltage regulator, a relay module for controlling the solenoid, a user interface for system interaction, and a Wi-Fi module enabling wireless connectivity and remote access.

DOI: https://doi.org/10.34010/injiiscom.v6i1.14127
p-ISSN 2810-0670 e-ISSN 2775-5584

This diagram illustrates the integration and functional relationships between these crucial elements, providing a comprehensive overview of the system's architecture

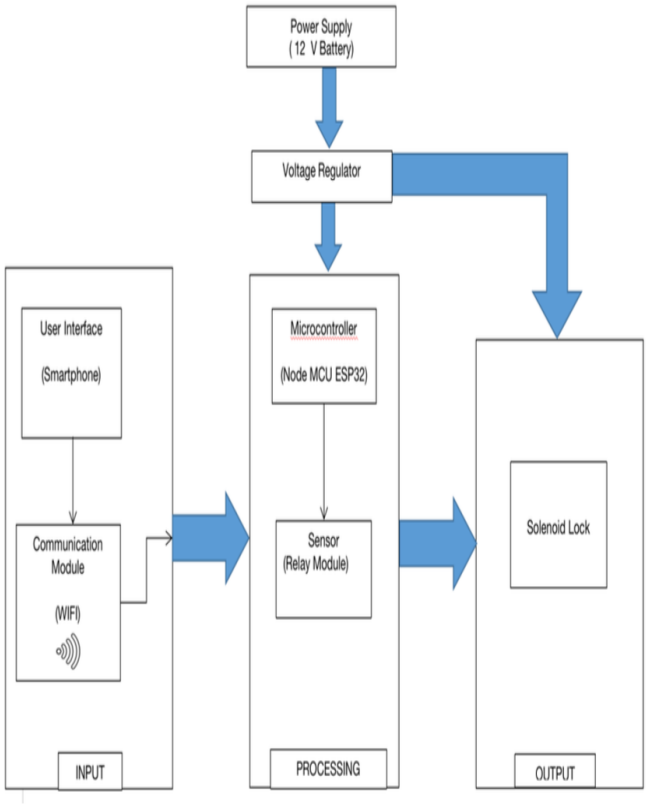


Fig. 1. Block diagram of the project operation.

2.1. Power supply unit

The system requires a 12V DC battery which supplies the necessary voltage to entire system. However, to ensure the compatibility with the different voltage requirements of the individual components, a voltage regulation mechanism was employed. Specifically, an LM7805 voltage regulator is utilized to step down the input voltage from the battery to a regulated 5V output.

This regulated 5V supply is then further conditioned and stabilized using two capacitors, a 0.22µF capacitor and a 0.1µF capacitor, (Fig 2) to ensure a smooth and consistent voltage supply.

The conditioned 5V output is then fed to the NodeMCU microcontroller, which serves as the central processing unit of the system. The NodeMCU further regulates the voltage to its operating requirement of 3.3V, enabling it to process and communicate with the software commands received from the smartphone interface

DOI: https://doi.org/10.34010/injiiscom.v6i1.14127
p-ISSN 2810-0670 e-ISSN 2775-5584

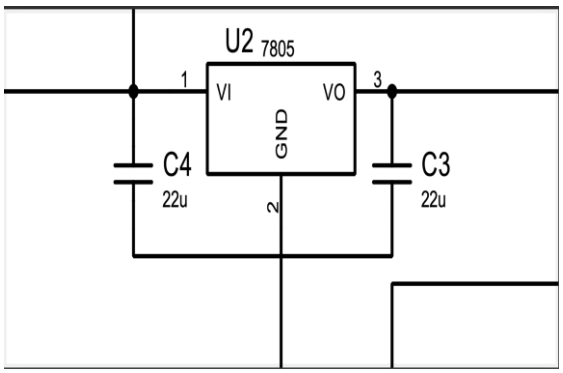


Fig. 2. Voltage regulator circuit

2.2. How the Voltage Regulator steps down the voltage input (Vin)

To calculate the output voltage for a voltage regulator, we use this formula:

$$\mathbf{V_{out} = V_{in} - (I_{load} \times R)}$$

Vout= ? , Vin = 12v and I_{load} = 1A (from component specifications) and R = ?.

But the voltage regulator undergoes some heating.

Heat generated = (Input voltage - 5) × Output current

Heat Generated = (12-5) × 1 = 7 watts

We know that; P = I2R

7 = 12 × R.

R = 7 Ω

Vout = 12 - (1 × 7)

Vout = 5v.

2.3. Control unit

The NodeMCU microcontroller serves as the control unit in the entire setup. It was programmed to receive a 5V input voltage which was further regulated internally by the NodeMCU to its operating requirement of 3.3V, enabling it to process and communicate with the software commands received from the smartphone interface. The NodeMCU was programmed to utilize the D0 pin as the output pin (Fig 3), facilitating the transmission of control signals based on the received commands. These commands, either 'ON' or 'OFF,' are interpreted as logical 'HIGH' or 'LOW' states, respectively, and are subsequently relayed to the input port of the relay module, which was connected to the NodeMCU's D0 pin.

Within the relay module, an additional voltage regulation mechanism was employed, consisting of a voltage regulator and accompanying capacitors. This mechanism steps down the 12V input from the battery to the required 5V operating voltage for the relay module itself.

The normally open port of the relay module was connected to the negative terminal of the solenoid lock, while the common port was connected to the negative terminal of the battery. Concurrently, the positive terminal of the solenoid lock was connected to the positive terminal of the battery, completing the circuit.

DOI: https://doi.org/10.34010/injiiscom.v6i1.14127
p-ISSN 2810-0670 e-ISSN 2775-5584

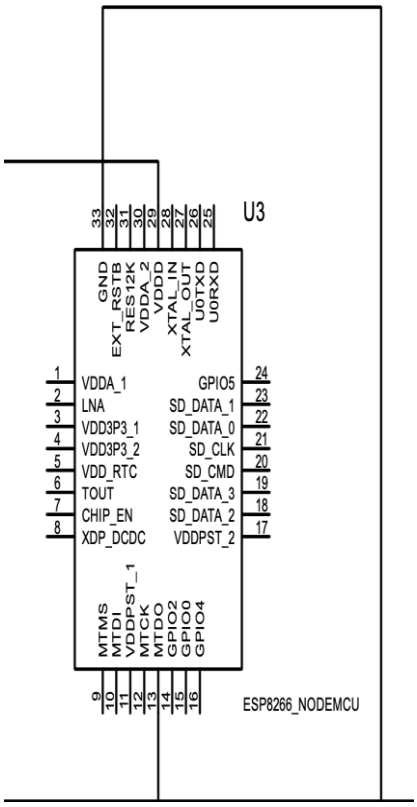


Fig. 3. The pins structure of the NodeMCU Microprocessor.

2.4. Control Flow

Fig. 4, represents the operational control flow of the system. The code written in C++ performs the operation of using the adafruit web interface to send the command from the app to the NodeMCU microcontroller. It starts by initializing the flow between the webapp and the NodeCU microcontroller. Then it ensures the device is connected to the same WiFi and the NodeMCU microcontroller WiFi module. When the user sends a command of open/close, the microcontroller receives that as High/Low signal and goes on to lock/unlock the solenoid lock.

DOI: https://doi.org/10.34010/injiiscom.v6i1.14127
p-ISSN 2810-0670 e-ISSN 2775-5584

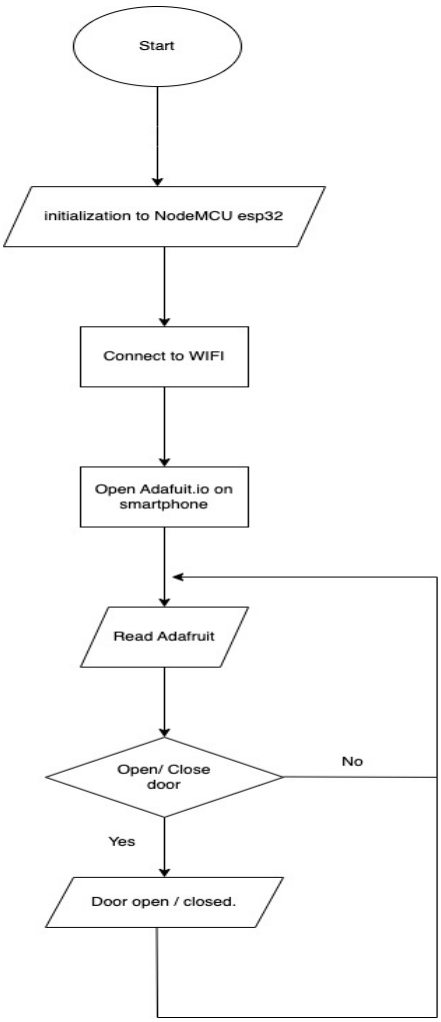
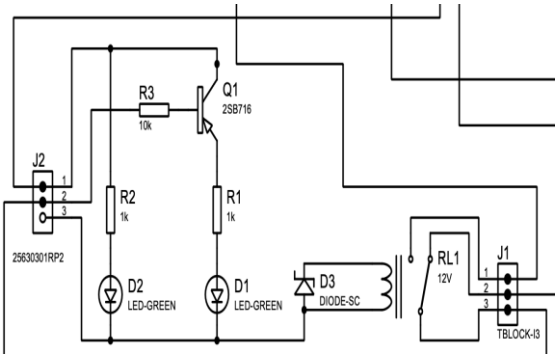


Fig. 4. Operational flowchart of the system.

2.5. Switching circuit

The switching circuit (Fig 5) is made of relay module that is responsible for completing or breaking the electrical connection between the solenoid lock and the power supply. When the control signal is sent from the microcontroller (e.g., ESP8266) to the relay module, the electromagnet energizes, and the movable contacts close, allowing electrical current to flow through the solenoid lock. This, in turn, causes the solenoid to engage or disengage the door locking mechanism, depending on the desired action (locking or unlocking).



DOI: https://doi.org/10.34010/injiiscom.v6i1.14127
p-ISSN 2810-0670 e-ISSN 2775-5584

Fig. 5. Switching circuit.

2.6. User Interface

The user interface for controlling the smart door lock system was developed on the Adafruit platform. Adafruit IO provides a cloud-based dashboard and tools for creating customized interfaces and integrating IoT devices. The interface allows remote monitoring and control of the door lock status through a user-friendly web application or mobile app.

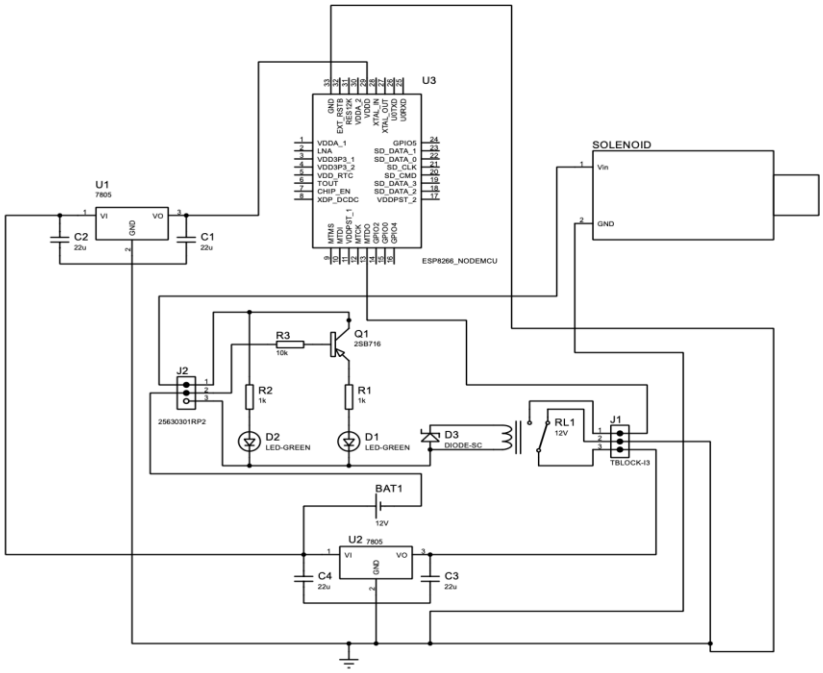


Fig. 6. Complete circuit diagram of the smart lock system.

The complete circuit diagram of the system (Fig 6), shows the connectivity and inter relationship of the various component of the smart lock system. The ESP8266 NodeMCU microcontroller D0 pin is the output pin, facilitating the transmission of control signals based on the received commands. These commands, either 'ON' or 'OFF,' are interpreted as logical 'HIGH' or 'LOW' states, respectively. This signal is subsequently relayed to the input port of the relay module, which is connected to the NodeMCU's D0 pin.

Within the relay module, an additional voltage regulation mechanism is employed, consisting of a voltage regulator and accompanying capacitors. This mechanism steps down the 12V input from the battery to the required 5V operating voltage of the relay module itself.

The solenoid lock, an electromechanical device, incorporates an internal mechanism that facilitates the retraction and protrusion of the locking component, effectively securing or granting access to the designated entryway.

Table 1 is the bill of engineering material used for this research showing

DOI: https://doi.org/10.34010/injiiscom.v6i1.14127
p-ISSN 2810-0670 e-ISSN 2775-5584

the components, number of units and the price of each unit. The total price of the project is also included.

Table 1: Bill of Engineering

3. RESULTS AND DISCUSSION

Testing was performed at various stages throughout the construction of this project to determine if the outcomes obtained at each phase met the desired standards. After the design and implementation phases, the developed system had to be tested for durability, efficiency, and effectiveness to establish if any adjustments to the system design were necessary.

Initially, a veroboard was utilized to assemble the system components. During this prototyping stage, various tests were conducted on the veroboard setup, where all the components were properly installed and interconnected. The microcontroller program of NodeMCU ESP8266 was developed in C++ language and the Arduino IDE was used to compiled program into executable file. This executable file was imported into the Proteus Design Suite for the circuit design and simulation. Upon successful software simulation, the implementation of the hardware was built on a Veroboard.

Table 1. Electrical Components.

S/n	Items description	Quantity	Cost per unit (₦)	Amount (₦)
1.	Microcontroller Board: NodeMCU ESP8266	1	12000	12000
2.	Veroboard	1	1000	1000
3.	Power supply (A 12V battery)	1	16000	16000
4.	Voltage regulator	2	500	1000
5.	Jumper wires	1 pack	750	1500
6.	Speaker wires	1 yard	250	250
7.	Capacitors	4	50	400
8.	1-channel relay module	1	3500	3500
9.	Solenoid Lock	1	10000	10000
10.	Male to Male connecting pins	1	240	240
11.	Female to Female connecting pins	1	240	240
12.	Crocodile clips	2	200	400
13	Plastic Box	1	2500	2500
14	Wood	1	3000	3000

DOI: https://doi.org/10.34010/injiiscom.v6i1.14127
p-ISSN 2810-0670 e-ISSN 2775-5584

S/n	Items description	Quantity	Cost per unit (₦)	Amount (₦)
15	Nut and screws	10	30	300
16	Transportation cost	1	800	800
17	Shipping Cost	1	10000	10000
	TOTAL		(₦)61060	(₦)63130

At different phases of the project's development, tests were carried out to assess the functionality and performance of the system. These tests aimed to identify any issues or deviations from the expected behavior, allowing for necessary modifications or improvements to be made to the system design.

By conducting thorough testing at multiple stages, it ensures that the final system met the desired specifications and requirements for durability, efficiency, and effectiveness. This iterative process of testing and refining the design played a crucial role in delivering a robust and reliable system that fulfilled its intended purpose. Fig 7. Shows the testing of the completed system with a 12v battery

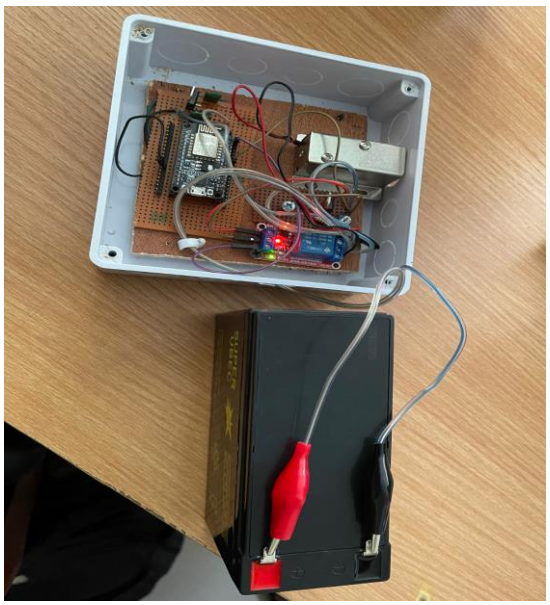


Fig. 7. Picture of system testing.

DOI: https://doi.org/10.34010/injiiscom.v6i1.14127
p-ISSN 2810-0670 e-ISSN 2775-5584

Fig. 8. Complete construction.

This study demonstrates a method to remotely monitor and control door locks. It offers a secure and convenient solution for smartphone users. Leveraging the free open-source software platforms of NodeMCU ESP8266 and smartphones, the implementation cost is kept inexpensive and accessible to the general public. The integration of WiFi connectivity into the microcontroller facilitates easier system installation. The prototype of the system to control the door's state using a WiFi-enabled smartphone and WiFi modules via the NodeMCU was successfully produced. The complete system is shown in Fig. 8 in a plastic enclosure.

4. CONCLUSION

After designing and testing the system, it was observed that the lock mechanism proved to be more versatile, reliable and easier to use compared to the traditional lock system. The utilization of NodeMCU ESP8266 serves as the brain of the system, providing necessary computational capabilities and connectivity options to interface with the solenoid lock and Adafruit platform. This thus enables remote control and monitoring of the door lock system via the internet. The implementation of a solenoid lock further enhances the security features of the system offering a robust physical protection against unauthorized entry. The solenoid lock's electromechanical design ensures reliable operation while minimizing power consumption, making it an ideal choice for battery-powered smart home applications. In all, the smart door lock system represents a culmination of innovation, efficiency, and practicality, providing homeowners with a sophisticated, yet user-friendly solution for enhancing home security.

REFERENCES

DOI: https://doi.org/10.34010/injiiscom.v6i1.14127
p-ISSN 2810-0670 e-ISSN 2775-5584

Adarsh V. P., Prakash S., Akshay S., Patgar C., Sharath Kumar A. J. and Mahadevaswamy P. (2018). Android based smart door locking system. *International Journal of Engineering Research & Technology (IJERT) 6(13), 2278-2281.*

Adole P., Joseph M. Môm, and Igwue G. A. (2016). "RFID based security access control system with GSM technology" *American Journal of Engineering Research 5(7), 236-242.*

Agbo D.O., Madukwe C., and Odinya J.O. (2017). Design and implementation of a door locking system using Android App. *Internationl Journal of Scientific and Technology Research 6(8) 198-203*

Anirudh R, Chandru V and Harish V. (2021). Multilevel Security Biometric Authentication Locking System Using Arduino UNO. *Advances in Parallel Computing Technologies and Applications 40:40-48*

Edozie E. and Vilaka K. (2020). "Design and Implementation of a Smart Sensor and RFID Door Lock Security System with Email Notification. *International Journal of Engineering and Information Systems (IJEAIS), 4(7), 25-28.*

Halliru U.M. (2020). Design and construction of smartdoor security system using arduino and bluetooth application. B.Eng. project, Electrical and Electronic Engineering department, Abubakar Tafawa Balewa University, Bauchi.

Ho G., Leung D., Mishra P., Hosseini A., Song D. and Wagner D. (2016). Smart locks: Lessons for securing commodity internet of things devices. *In Proceedings of the 11th ACM on Asia conference on computer and communications security (pp. 461-472).*

Jeong Ji. (2016). A study on the IoT based smart door lock system. In : Kim, ., Joukov, N (eds) *Information Science and Applications (ICISA) (pp. 1307-1318).*

Ilkyu Ha (2015). Security and usability improvement on a digital door lock system based on internet of things. *International journal of security and its applications, 9(8),45-54.* Gupta K., Jiwani, N.J.,

Kamelia L., Alfin Noorhassan, Mada Sanjaya W.S., and Mulyana W.S. (2014). Door-automation system using bluetooth-based andriold for mobile phone. *ARPN Journal of Engineering and Applied Sciences.* 9(10), 1759-1762.

Lucas de C. S., Samaniego M. and Deters R. (2019). IoT and blockchain for smart locks. *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (pp. 0262-0269). IEEE.*

Md Haris U., Sharif M.A. M.and Afreen N. (2022). Smart door locking system using IoT. *In 2022 International Conference on Advances in Computing, Communication and Materials (ICACCM) (pp. 1-4). IEEE.*

Mishra A., Sharma S., Dubey S. and Dubey S.K. (2014). Password based security lock system. *International Journal of Advanced Technology in Engineering and Science, 2(5), 100-103.*

DOI: https://doi.org/10.34010/injiiscom.v6i1.14127
p-ISSN 2810-0670 e-ISSN 2775-5584

Ni Ni San H. and San San L. (2019). "Electronic Door Lock using RFID and Password Based on Arduino", *International Journal of Trend in Scientific Research and Development, 3(3), 799-802.*

Parushi M., Yashwant S., Pooja A., Deep K. B., Pradeep K. S. and Hong WC. (2021). *Internet of things: Evolution, concerns and security challenges.". Sensors, 21(1809), 1-35.*

Rajiwade, B., Thakar, S., Pokharkar, P. & Malbhare, S. (2016). Design and Implementation of Smart Door Lock Control System using Bluetooth Controller of Smart Phone. International Research Journal of Engineering and Technology (IRJET), 3(11), 482-484

Sahani,M. Nanda C., Sahu A. K. and Pattnaik B. (2015). Web-based online embedded door access control and home security system based on face recognition, *International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015]*, (pp. 1-6). Nagercoil, India, IEEE

Sravani P. and Kannappan S. (2017). High Security Door Lock System by Using Android Mobile with Bluetooth. *International journal of innovative technology and research (IJITR), 5(6), 7644-7648.*

Satyam M., Omkar M., and Kharat S. (2022). Smart Door Lock System Using Arduino *International Research Journal of Modernization in Engineering Technology and Science 4(4),1503-1507.*

SeungSoo S., Kun-Hee H. and Kwang-Yoon J. (2013). Digital Door Lock on the Access Control System using OTP-based User Authentication. International Journal of Digital Content Technology and its Applications. 7(11), 436-442.

Shafana A.R.F. and Aridharshan A. (2017). Android based Automation and Security System for Smart Homes. *International Journal of Computer Science and Information Technology Research*. 5(3),26-30.

Ting R and M. Keane (2014). RFID Door Lock. B.Sc Project, Electrical Engineering Department, California Polytechnic State University. San Luis Obispo. pp 1-34.

DOI: https://doi.org/10.34010/injiiscom.v6i1.14127
p-ISSN 2810-0670 e-ISSN 2775-5584