

Smart Door Systems in the IoT Era

Sandeep Singh

Department of Information Technology
Greater Noida Institute of Technology, Greater Noida, U.P., India
Sandeepsingh26367@gmail.com

Rohit Ram

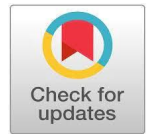
Department of Information Technology
Greater Noida Institute of Technology, Greater Noida, U.P., India
rohitram0569@gmail.com

Naim Akhtar

Department of Information Technology
Greater Noida Institute of Technology, Greater Noida, U.P., India
naimakhtar003@gmail.com

Prof.(Dr.) Vikas Singhal

Head, Department of Information Technology
Greater Noida Institute of Technology, Greater Noida, U.P., India
hodit@gniot.net.in



Publication History

Manuscript Reference No: IJIRAE/RS/Vol.11/Issue11/NVAE10081

Research Article | Open Access | Double-Blind Peer-Reviewed | Article ID: IJIRAE/RS/Vol.11/Issue11/NVAE10081

Received:03,November 2024,Revised: 11,November 2024,Accepted: 18, November 2024, Published Online: 28,November 2024. <https://www.ijirae.com/volumes/Vol11/iss-11/02.NVAE10081.pdf>

Article Citation: Sandeep,Rohit,Naim,Prof.(Dr.)Vikas(2024), Smart Door Systems in the IoT Era. IJIRAE:: International Journal of Innovative Research in Advanced Engineering,Volume 11, Issue 11 of 2024 pages 800-805

Doi:><https://doi.org/10.26562/ijirae.2024.v11i11.02>

BibTeX Key: Sandeep@2024Smart



Copyright: ©2024 This is an open access journal, and articles are distributed under the terms of the Creative Commons Attribution License; Which Permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Abstract: Security has grown in importance in recent years as a result of the increased number of security-related problems that people are facing globally and the fact that security is now everyone's top priority. The protection of our life and belongings is referred to as security. Ensuring the safety of individuals and their belongings is crucial in order to deter unlawful handling. Thus, concentrating on gate or door lock security is crucial to minimizing other problems in the area under observation. Designing an internet-connected locking system that could be readily put on a variety of doors, operated online, and depended upon for security was the project's goal. Wireless switches with centralized management systems are quickly replacing standard switches in contemporary houses. A home system controlled by a smart phone is a modern option. The three primary advantages of our proposed solution are the capacity to design and implement an open-source, cost-effective home automation system, enhance home security, and develop a smart door lock that can be accessed by a smart phone. Through improved security, convenience, and the capacity to lead a luxurious lifestyle, this initiative will make people's lives more adaptable and will ultimately make them far more straightforward, refined, accessible, and stable.

1. INTRODUCTION

In computer terminologies, "internet of things" refers to the idea of connecting commonplace physical objects to the internet. Connected to the internet and able to recognize and comprehend how other devices interact with stuff found online. The Internet of Things (IOT) is a technology framework for electrical device connectivity in the age of modern computers. In certain industries, such as consumer electronics and home security, wirelessly operated devices are becoming more and more dominant due to their adaptability and simplicity of use. We call this type of technology the "internet of things." New automation systems are being developed using this technology for application in homes, offices, and other environments. Enhancing living circumstances through the introduction of the network tools and equipment within the home is the main objective of smart home technology. Complete automation made possible by a smart home makes for comfortable living arrangements and further benefits for people with impairments. Currently in use, all door locking systems require a conventional key or some kind of Node MCU in order to be accessed. It can be accessed and controlled via webpage. Additional wireless connections to business places, such as money changers, ATMs, and so on, can be used to broaden this approach. The home is among the structures that have been inhabited for a considerable amount of time. Most homeowners spend most of their time away from home. In big cities, these kinds of situations are frequent. Because of this, the residence is frequently vacant for extended periods of time, especially around holidays like Eid, Christmas, and New Year's Eve. Living in such conditions might incite thieves to take anything. As technology advances, homes become increasingly sophisticated. In contemporary homes, centralized control systems with remote switches are rapidly replacing traditional switches. Most important our suggested method has the potential to be utilized to develop and implement an open-source, affordable smart home system, enhance home security, and construct mobile-accessible smart door locks. Through improved security, convenience, and the ability to live more sustainably, this initiative will make it simpler to save human lives and make our lives safer and easier to access.

II. LITERATURE SURVEY

The authors suggest an IOT application for an automated home that combines cloud computing, wireless sensor nodes in it, and mobile devices to give users access to household appliances including door locks, lights, fans, and more. **Nikhil Agarwal et al.** created the innovative smart home security system. The door lock is secured by a password thanks to its LED-based resistive screen input panel, where a photo diode detects fluctuations in intensity of light generated by surrounding illuminated red LEDs and returns via finger. The paper describe a (FPGA)-based smart home automation and security system where FPGA stands for field programmable gate array. With an internet connection, users may remotely monitor and manage a variety of domestic products and more.

Using wireless communication networks and biometric technology, **Basma M. Mohammad et al.** [1] present a novel architecture for smart home automation that allows authorized users to enter more easily and enhances the security of existing homes by implementing biometric authentication at the home entrance.

Pavithra.D et al.[2] propose an IOT application for a home automation system that enables mobile phones with Raspberry Pi to control domestic appliances via Wi-Fi as a communication channel. Fans, lights, and door locks may all be easily operated and remotely monitored with the use of an internet website. Through the server that is physically connected to the various appliances via relays, the user may access them.

Using a Raspberry Pi, **Mohannad Ibrahim et al.**[3] offer a creative method for creating an affordable environmental tracking device. Seismic sensors are used to detect geological disturbances, such as natural catastrophes, and sensors collect environmental data, such as temperature, humidity, light intensity, and carbon monoxide concentration, which is then uploaded online for constant access.

Using networks of sensors, wireless nodes, and cloud servers, **Robert R. et al.** offer a novel approach to implementing internet of things applications in the Smart City idea. In their innovative home security setup, **Yan Wenbo et al.** propose the idea of an effective module and house proxy, both of which utilize the most of XMPP. The home proxy is connected to the distant server, which serves as a service provider and offers services for various homes and workspaces.

Ala Al-Fuqaha et al. list the main challenges with IoT and provide an overview of pertinent studies comparing IoT to other contemporary technologies including cloud computing, fog, and big data analysis. Future developments in RFID, smart sensors, Internet protocols, and Internet of Things nodes are covered in this article.

Jun Wei Chuah et al.'s examination of new perspectives in system design under IoT covers a number of important subjects, including IoT enablers, new and present IoT applications, and present IoT challenges. The IoT framework that might be the foundation for further research is described in the study.

Gerfried Cebrat et al. propose an Internet of Things application that uses a built-in flexible logic controller to control the temperature, and other aspects of the house. A security system for the home that safeguards the integrity of user data is also constructed.

Kai Zhao, Lina Ge, et al. analyze a number of security issues in the Internet of Things that arise in three layers and suggest potential fixes. The safety measures related to the perspective layer are thoroughly described, along with details on data fusion, security transit protocol, and key and algorithm management.

Andrea Zanella et al. suggest a smart city model that uses cutting-edge information technology to offer value-added services for both the city's residents and government. In partnership with the city municipality, this paper was carried out as part of the Padova Smart City initiative in Italy. Wu He, Li Da Xu, This article provides an overview of the latest IoT analysis, key enabling methods, key industrial applications, and a brief description of the IoT technologies presently in use in industries. The writers talk about significant discoveries, technical issues, and socioeconomic prospects in the age of smart cities. The Smart Sanander project, an EU initiative creating a city-scale test-bed for IoT and Future Internet experiments and offering an environment for the deployment of Smart City services, is where almost all of the data are gathered.

Kosalendra Eethamakula and Dilip Prathapagiri proposed a smart door system design. We can use this system to check the device's status updates because we can forget to correctly lock the doors while we're in a rush. It takes a picture of the user and sends it to the owner when they touch a calling option. We may additionally keep an eye on whoever enters and exits our home by utilizing the Blynk app. The WiFi component is how the suggested system operates. The earlier suggested system would improve reliability and allow us to keep eye on it and determine its status, including if it is securely locked or not. Two machine learning algorithms that are utilized to operate home appliances are covered by the writers. The system is capable of machine learning, whereby a single processor learns user patterns by analyzing information received from household gadgets. The updated model is easier to use and fixes the smart home automation system lack of mobility and flexibility. PLC (Power Line Carrier) units are used by the nodes in this model to communicate with one another.

III. IOT - BASED SMART DOOR IN MODERN TIME

The features of a few chosen smart door lock systems that are currently in use and were created utilizing various technologies are covered below. The door would open as soon as they were identified.

A. Smart IoT-based Facial Recognition Door Lock System

One proactive approach that can react quickly to a security danger is an intelligent IoT-based facial recognition system. When someone is close to the entrance, the device detects their face and matches it to the identities that have been entered into the database. If an unauthorized individual arrives the building, one of the owners will receive a message and email with the picture of the outsider. This mechanism employs a Raspberry Pi camera to detect visitors, DC motors with relays to unlock the doors, LEDs for displaying accessibility, and a GSM module to send texts to a registered phone number.

B. Fingerprint Door Locking System

Because of their ease and uniqueness, fingerprints are the most widely used biometric identification method. They are safe and reliable to employ because of their distinctiveness and constancy. With the right small details identification techniques, fingerprint identification may be reliable, accurate, and reasonably priced (Fig.1). This thesis matches fingerprints using a precision recognition method. By considering the area and line structures between minutiae pairs, this method varies from conventional minutiae matching algorithms. More structural features about the fingerprint should be taken into account in order to increase the accuracy of matching details.



Fig.1.

C. Knock-pattern Door System

This technology employs a 'Secret Knocking Pattern,' using Arduino and GSM Communication acknowledged only to the keeper of the safe, suitcase, or any other item where the gadget is inserted. To unlock the lock, an individual must use a unique tapping pattern at a precise location. Changing an encrypted pattern requires unlocking the secret door. This approach does not allow for duplication due to the absence of a key.

D. Digital Door Locking System based on RFID

The Digital Door Locking System (Fig.2.) based on RFID captures a picture during operation. The photo is processed and compared to the database for matching. Accessibility is given or prohibited based on the card's Unified Information Devices (UID) and captured image, triggering an authentication warning. This type of device is a powerful both entry and exit tracking system that may be put at any entrance or exit. This technique can enhance protection in homes. This technique improves quickness by utilizing real-time visuals and the controllers' procedures.



Fig.2.

E. OTP BASED SYSTEMS

The recommended solution in most current work doesn't involve the administrator assistance to reach the office, as long as the client knows the OTP procedure and has an enrolled smart phone. When a visitor requests to visit the workplace, the owner generates and sends an OTP from their phone. For unlocking the door, input the OTP into the keypad. If the portable device is not accessible or turned off, you can open the door by answering the security question prompted by the system.

IV. METHODOLOGY

This paper proposes a technology that will increase the versatility of human lives by improving security, convenience, and the capacity to live an upper-class lifestyle, resulting in our lives becoming much simpler, nicer, more accessible, and consistent. It demonstrates ingenuity in home control by replacing manual keys with digital codes and knocks on a door lock, predicting future security trends, and replacing high-tech manual locks with Digital Smart Locks.

Also, the designed system's implementation costs have been kept to a minimal, making it affordable to anyone in search of home security. The Digital Smart Home is easier to manage and deploy than the other technologies covered in the literature review. It works with the free open-source Android operating system, cellular technologies, and the Internet of Things. In order to integrate Wi-Fi technology, an Android-based app for client access, and customer testimonials for dependability and verification, the suggested viewpoint registers together with the necessary architecture. Subsequently, the framework could be expanded to include more aspects of home renovation and stability. Furthermore, to support operating systems other than Android, these research paper projects are often expanded.

A. Hardware & Software Need

Classification	Component	Function
Hardware	Solenoid Lock	For Open & Close door
	One 5V relay	To control voltage
	Node MCU(ESP8266)	Data processor
Software	Arduino Uno	Write and Transmit code
	HTML	For Web Interface
	Proteus Circuit	For Simulation

B. Block Diagram

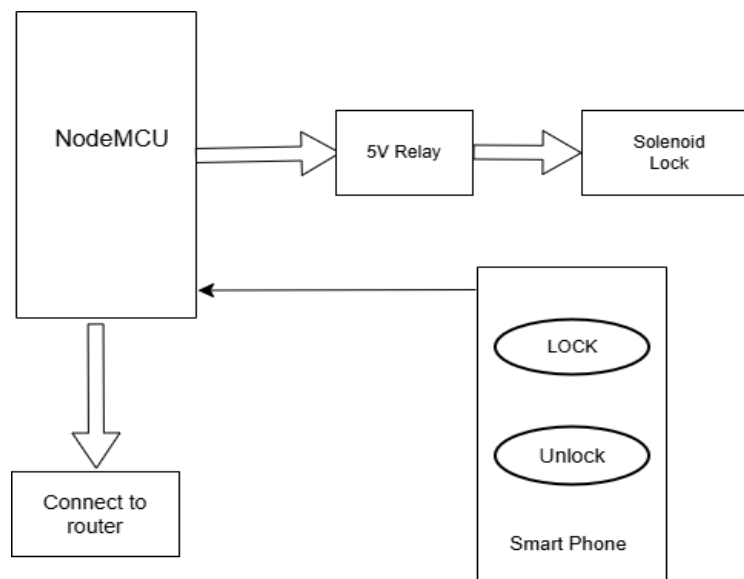
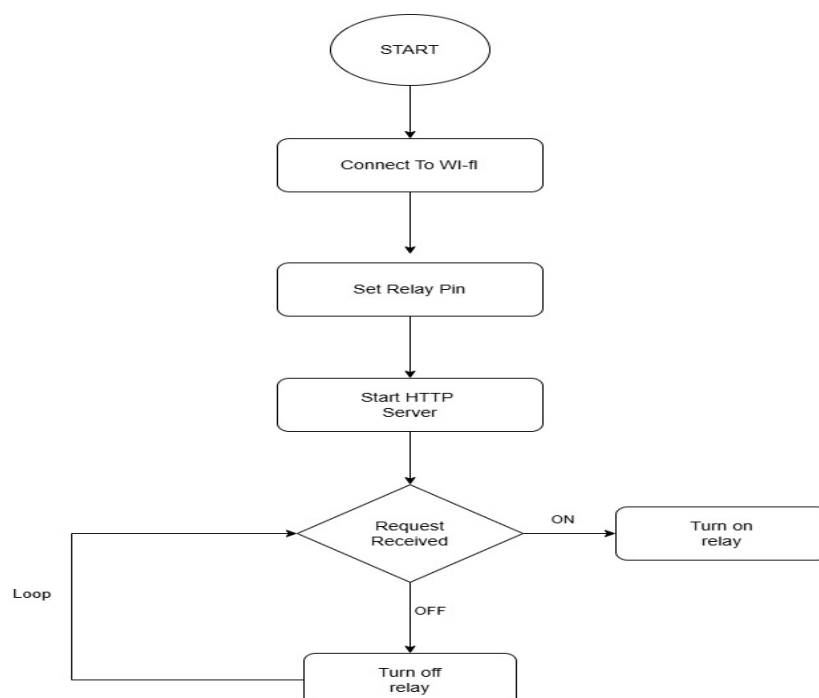


Fig. 3.2 C.Flow Chart



The flow chart for the proposed system is shown in fig3.3.

V. PROBLEM STATEMENT

The rise of the Internet of Things (IoT) has opened new possibilities for enhancing home security, but traditional door locks often remain vulnerable to unauthorized access. This creates significant safety concerns for homeowners. The goal of this research is to develop an IoT-based smart door that not only improves security but also offers greater convenience for users. Many existing smart door solutions have limitations, such as connectivity issues, complex user interfaces, and a lack of integration with other smart home devices. Additionally, there are important concerns about data privacy and cyber security threats associated with IoT technology. By addressing these challenges, this research aims to create a smart door that meets user needs for security and usability while ensuring robust protection against online threats. Ultimately, this project seeks to contribute to the evolution of smart home technology, making homes safer and more connected.

VI. DEVELOPMENT OF THE SUGGESTED SYSTEM

We installed a door locking and unlocking system in our project that can be operated from a distance using a smart phone app. A 12v dc converter, a Node MCU ESP8266, a solenoid lock, and a single-channel 12v relay were used. Putting voltage to a solenoid lock will cause it to activate automatically. In a solenoid lock, a low-voltage solenoid pulls the latch back into the door when an interrupt is triggered. Until the interrupt is triggered, the latch will stay in position. The solenoid lock requires 12-15V operate. A smart door lock uses the Node MCU to connect a relay module and a solenoid lock. Below is a thorough description of the hardware and software utilized in this methodology.

A. Node MCU

The IOT platform Node MCU is open source and free The ESP8266 or ESP32 microcontroller, which offers Wi-Fi connection, is its foundation. Although support for other programming languages, such as Python, is also available, the firmware is designed to operate on the Espressif SoC (System-on-Chip) and comes with an integrated Lua interpreter for scripting.



B. Solenoid lock

A solenoid is a cylindrical coil of wire that generates a magnetic field. Conversely, the Solenoid Key, a combination of a key and a solenoid, is frequently used to electrify gadgets such as automatic locks and other like devices. French scientist Andre Marie Ampere made the discovery of the solenoid principle. This term is used in engineering to describe a machine that transforms energy into linear motion. When a coil is ignited with an electric current, an electromagnetic force is created that pulls the iron at the coil's core in a linear fashion.



C. Relay

A small amount of current applied to the signal pin causes an electromagnet to activate a relay. An Arduino, AVR, PIC, or ARM microcontroller may control the 5-volt, one-channel relay module, which is an interface board with screw terminals. The board has a high-quality relay that can manage up to 10 amps at 240-250 volts and 15 amps at 120-125 volts. The relay is easy to connect and disengage since its common-C, usually open-NO, and normally closed-NC connections are all connected to three-pin screw terminals. To facilitate troubleshooting, the board has a relay status LED and a power indicator.



ADVANTAGES

- Ease of use.

- Programmable Security Clearances.
- Automatic Door Lock/Unlock.
- Centralized Management.
- Easy maintenance and Updating.
- To increase data security.
- Smart locks increase accessibility.

CONCLUSION

Using a smart door lock is not something that is new for the scientific community; in fact, it has been around for many years. As technology develops, the home security system market is expanding quickly. In today's societal structure, safety is more desired if it can be improved and solidified through technological means. One of society's necessities, security, is substantially met by smart door lock technology. Our lives will become much more straightforward, refined, accessible, and steady as a result of this project, which will also increase security, convenience, and the capacity to lead an affluent lifestyle. The planned system is inexpensive since the implementation costs have been kept minimal. Security in the house is something that everyone wants. The IoT-based door lock system is easy to set up and maintain, unlike to most of the innovations discussed in the literature review. It is compatible with mobile communications, the Internet of Things, and an open-sourced, non-proprietary Android operating system. By incorporating various creative solutions recommended by some linked publications, the suggested approach seeks to enhance the existing one while improving its weaknesses.

REFERENCES

1. Professor Nimesh Aote¹, Tejas Belsare², Shridhar Giri³, Shivam Giradkar⁴, Shubham Mohekar, Smart Digital Door Lock System, International Journal of Recent Engineering Research and Development (IJRERD) ISSN: 2455-8761 www.ijrer.com || April 2018 || PP. 41-45 || Volume 03 – Issue 04
2. Arpita Mishra, Siddharth Sharma, Sachin Dubey, S.K. Dubey, "PASSWORD BASED SECURITY LOCK SYSTEM" International Journal of Advanced Technology in Engineering and Science www.ijates.com Volume No.02, Issue No. 05, May 2014 ISSN (online): 2348 – 7550.
3. K.Srinivasa Ravi, G.H.Varun, T.Vamsi, P.Pratyusha, "RFID BASED SECURITY SYSTEM" International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-2, Issue-5, April 2013. <https://www.hackster.io/adarsh-bhola/iot-based-door-lock-system-4a40f0>
4. D. Parker, "An Overview of IoT Protocols and Their Applications," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp.23-45, 2020.
5. Pusiknas Bareskrim Polri, "Crime data (in Indonesian: Data kejahatan)," Polri. 2021, Accessed: Aug. 18, 2023. [Online]. Available: https://pusiknas.polri.go.id/data_kejahatan
6. I. Ha, "Security and usability improvement on a digital door lock system based on internet of things," Int. J. Secur. its Appl., vol. 9, no. 8, pp. 45–54, 2015, <https://doi.org/10.14257/ijasia.2015.9.8.05>.
7. G. Sowmya, G. Divya Jyothi, N. Shirisha, K. Navya, and B. Padmaja, "IoT based smart door lock system," Int. J. Eng. Technol., vol. 7, no. 3.6 Special Issue 6, pp. 223–225, 2018, <https://doi.org/10.22214/ijraset.2023.49470>.
8. M. J. Mahammad, Y. Al Mashhadany, and A. M. Eyada, "Real time model of a lock gate system upon fingerprint with microcontroller," Indones. J. Electr. Eng. Comput. Sci., vol. 21, no. 1, pp. 37 – 43, 2021, <https://doi.org/10.11591/ijeecs.v21.i1.pp37-43>
9. J. K. Abed, "Smart monitoring system of DC to DC converter for photovoltaic application," Int. J. Power Electron. Drive Syst., vol. 9, no. 2, pp. 722 – 729, 2018, <https://doi.org/10.11591/ijpeds.v9.i2.pp722-729>.
10. Jayant Dabhade, Amirush Javare, Tushar Ghayal, Ankur Shelar, "Smart Door Lock System: Improving Home Security using Bluetooth Technology", International Journal of Computer Applications (0975 – 8887) Volume 160 –No 8, February 2017.
11. ARDUINO Based industrial security system using piezo electric sensor", Rupinder Singh Brar.
12. Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, " AN ADVANCED DOOR LOCK SECURITY SYSTEM USING PALM TOP RECOGNITION SYSTEM", International Journal of Computer Applications (0975 – 8887), Volume 56– No.17, October 2012.
13. Gyanendra K Verma, Pawan Tripathi "A DIGITAL SECURITY SYSTEM WITH DOOR LOCK SYSTEM USING RFID TECHNOLOGY" International Journal of Computer Applications (0975 – 8887), Volume 5– No.11, August 2010.
14. Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. Internet of Things Journal, IEEE, 4(5):1125–1142, October 2017.
15. D. Surie, O. Laguionie, T. Pederson, "Wireless sensor networking of everyday objects in a smart home environment", Proceedings of the International Conference on Intelligent Sensors, Sensor Networks and Information Processing - ISSNIP - 2008, pp. 189 – 194.
16. "Sensor based home automation and security system," Instrumentation and Measurement Technology Conference (I2MTC), 2012 IEEE International, Graz, 2012, pp. 722-727. <https://doi.org/10.1109/I2MTC.2012.6229153>
17. YAN Wenbo, WANG Quanyu, GAO Zhenwei, "Smart Home Implementation Based on Internet and WiFi Technology" Proceedings of the 34th Chinese Control Conference July 28-30, 2015, Hangzhou, China pg 9072-9077.
18. E. Theodoridis, G. Mylonas and I. Chatzigiannakis, "Developing an IoT Smart City framework," Information, Intelligence, Systems and Applications (IISA), 2013 Fourth International Conference on, Piraeus, 2013, pp. 1-6.