



AI Unlocking the Future: Intelligent IoT-Enabled Electronic Lock Control Systems for Next-Gen Door Security

Sweta Pareek¹, Shilpa Pareek^{2*}, Swati Sharma³, Deepa Chauhan⁴, Divya Sharma⁵
Neelam Sunda⁶,

University of Engineering and Management¹, Kanoria PG Mahila Mahavidyalaya,
Jaipur, Rajasthan, India²³⁴⁵⁶,
shilpapark@gmail.com*

Abstract. Establishing remote connections and monitoring the web enabled entities can easily be done with the help of IoT or Internet of Things as we popularly know. This concept can be used for implementing a robust home security system. This basically is the proposal of a door locking system for a smarter and safer abode using the IoT technology. The Arduino Nano controlled door lock system can be accessed from anywhere in the world using a simple application on mobile with a unique credential combination. In any kind of contingency like forceful entry, immediate alert message is sent to user on his phone. The proposed system consists of a microcontroller to control the electromagnetic valve of electrical lock, an onboard Wi-Fi module for accessing the internet and a power module to drive the entire system.

Keywords: IOT, Home Security Automation, Arduino, ESP01.

1 Introduction

The rise of IOT frameworks has impacted the domain of home automation systems. A smart home is an intelligent network of electronic devices which can control home appliances, lighting, and entertainment systems. Users can control these systems through tablets, mobile phone applications, web interfaces which are connected through the internet. Therefore, an intrusion detection system is required to restrict various unauthorized access as mentioned by [14]. The access for controlling the security related elements of smart homes with alarming systems should have very high priority.

The mechanical lock currently in use in most homes has certain disadvantages. The physical key has a high probability of going missing. The key must be shared with acquaintances who may need to access home in emergency situations and such sharing might not be possible all the time.

To overcome such issues, a digitized solution is proposed in this paper.

IoT architecture has 4 layers: Perception layer which has sensors used to measure physical quantities. Network layer is used to transfer sensor data for processing. The processing layer helps to store, analyze, and process the collected data by employing new technologies like Big Data. Application layer provides services to end

users.

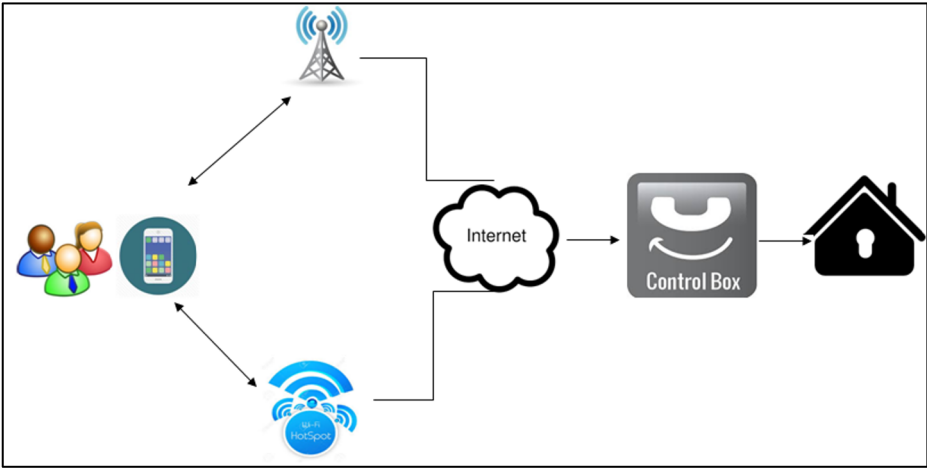


Fig. 1. Implemented Smart Lock System

Current home security systems use locks connected through Bluetooth which cannot be controlled from a distant location [1]. Zigbee technology has also been used to build home security systems due to its demand for low power consumption [3]. The

Proposed solution uses an existing IOT framework to provide a simple, cost effective and keyless solution for door locks [2]. This IOT based security system can provide information about any unauthorized access to property while the owner is away from home. Figure 1 describes the proposed system. An AWS server with an integrated database stores the information sent by door lock system. The hardware has SPDT relay controlled by Arduino Nano. An android application lets the user access the lock mechanism through unique user id and password which is already stored in database. It was also mentioned by [15], that one of the major challenges of smart devices is their security. The system is flexible enough to add multiple user accounts to access a single smart lock. Further, multiple smart lock devices for various sections of the house can also be accessed from a single user account.

2 A Network's Architecture

Servers, hardware, and clients are all parts of the proposed network architecture. The entire home security system is managed on the server side. The node for controlling smart locks is part of the hardware. The user details can be added, edited, or deleted

from the client side. The sections that follow give a thorough understanding of network architecture.

2.1 Server Side

The server side has an AWS server with an integrated database which contains information about users and their credentials, access details and node information. Person info, node info, and node data are the three tables that make up the designed database [2]. Each registered user of the home security system has a user ID and password stored in the Person info database.

Each node and the door lock it regulates are listed in the table node info. Each sensor attached to each node is represented in the table of node data by a log entry. The server side manages access control to operate the home security system.

2.2 The Hardware

The hardware is an integral part of home security automation. It contains a solenoid valve based mechanical lock controlled by Arduino Nano circuit through an SRD-05VDC-SL-C SPDT relay. An EB2209A acts as the buzzer source to indicate error and lock states. The entire system is connected to the internet and all the data collected by magnetic sensor inside door lock is stored in cloud. The data exchange between hardware and server takes place with support from ESP8266 WiFi module with TCP/IP protocol built in. Network traffic can also exist during exchange of data and should be classified in a proper way with various techniques mentioned by [17].

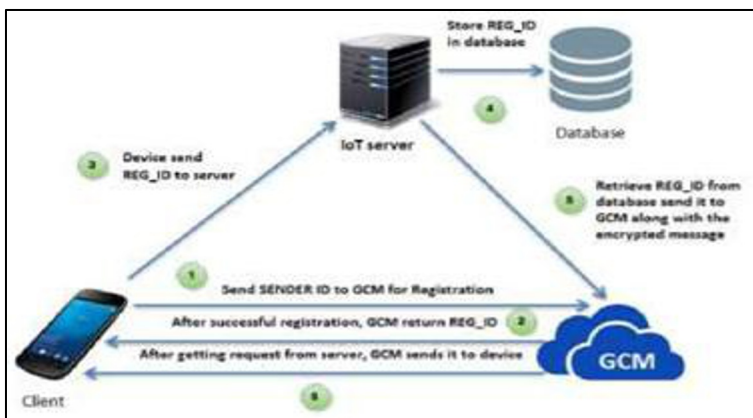


Fig. 2. An IoT server and an Android application's functional block diagram.

2.3 Client End

On the client side, there is an Android application that provides access to the nodes that control the mechanical door lock for users who have registered with the service. Network gateway then plays an important role for communication with cloud [16] and

Hence, A one-of-a-kind identifier (ID) will be sent to the GoogleCloud Messaging system viaan android application that the user has installed on their smart device. After the GCM has received the unique ID from the smart device, it will then send a handshaking signal to the device.

Once successful communication has been established between smart device and GCM, the device will send a registered user ID to the server which is stored in table of person info. This user ID is transmitted to GCM by the server. Any request that is sent by the server will have its response transmitted to the smart device through GCM. When a different browser is used instead of the smart device, the exact same process is carried out. The system at client-end is described in Figure 2.

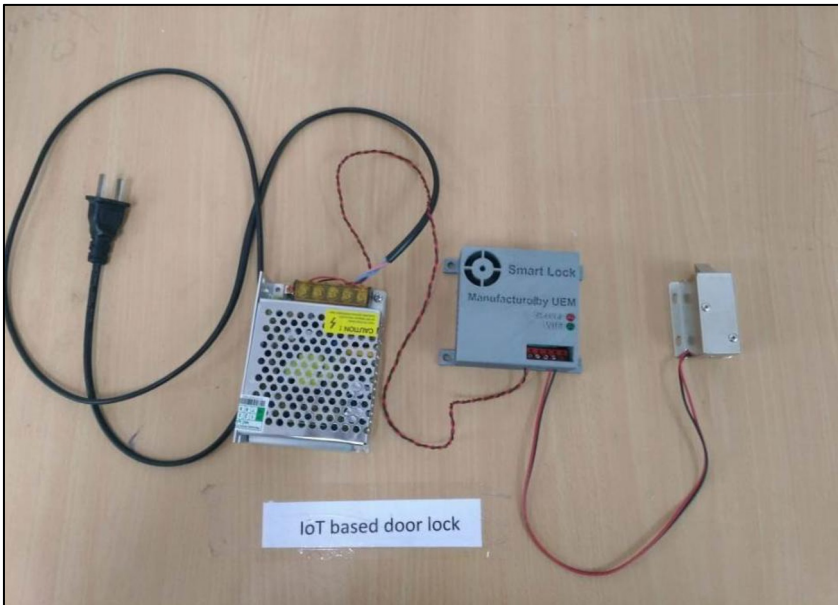


Fig. 3.Door lock node prototype.

3 Implemented Framework

The implemented framework is controlled by the user to monitor the complete home security system. The client end uses an android application and the cloud server can provide update about the condition of nodes.

An internet-connected device node controls four door locks using a static IP. The device node receives a signal from the android application and unlocks the particular door lock after verifying the user credentials.

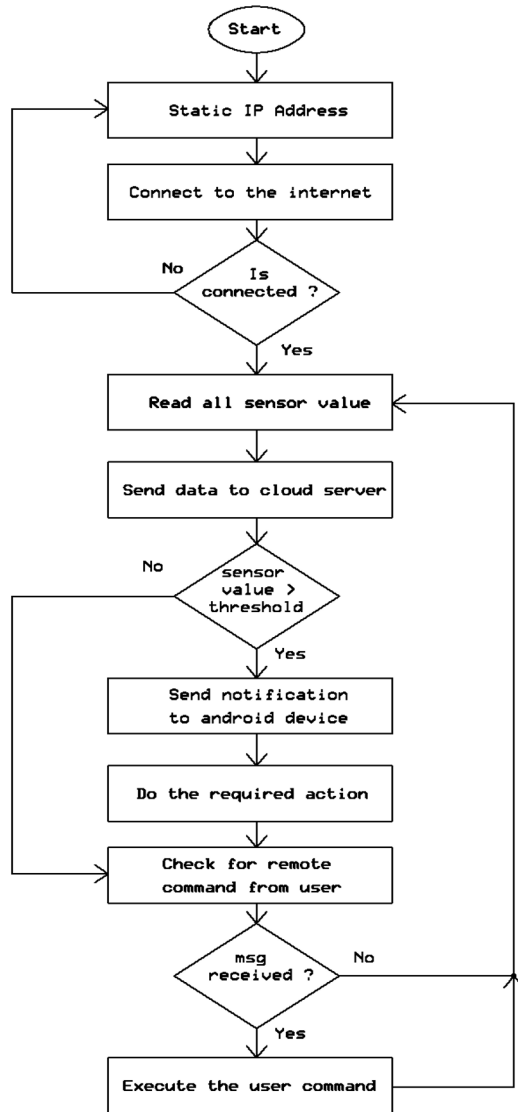


Fig. 4.The recommended framework flowchart

4 Configuration Of System

At the outset of the project, an Amazon Web Services (AWS) server is established, and within that server, a Linux instance is initiated. The instance that is now being run will bring the system online.

MySQL is utilized in order to establish a database instance.

This database has three different tables. The person info table contains user credentials of all registered users i.e., their person name and password. Information about each digital node and the door locks it controls is stored in a table known as the node info table.

The node data table has log information of the sensors connected to each node. Once the database is created, hardware is implemented as shown in figure 3. The smart lock control circuit consists of Arduino Nano which uses Arduino IDE for programming purpose. The operating voltage for Nano is 5 volts in DC and a clock with 16 Megahertz speed. The Nano board is attached to an SPDT relay which controls the mechanical lock. The internet connectivity for the full door lock system is provided by a Wi-Fi module with the model number SP8266 that employs the TCP/IP protocol.

A logic level controller works as an intermediary in communication between ESP8266 and Arduino Nano. The entire circuit consisting of Arduino Nano, Wi-Fi module, SPDT relay and EB2209A buzzer source is integrated in a package which is connected to a power supply. The other end of the package is connected to the mechanical lock. Each node can control four mechanical door locks. Arduino Nano will receive the user credentials through android application and after verification with help of Google Cloud Messaging service, it will unlock the specific door lock.

5 Result and Discussion

An existing framework is utilized for the home security system, and an android application is used for the system's implementation. The app is installed on smart devices owned by users who have been given access to the property which has smart door lock installed. When a user first launches the Android application, a home screen appears that prompts them to log in with their credentials, as illustrated in figure 5. After the credentials of the user are checked and found to be valid, they will be taken to a new page where they will be able to alter the settings of any door locks that are connected to nodes that they control. The current status of the door lock is depicted in Figure 5, along with the logged time.



Fig. 5. Android application screenshot showing (a) the Person login screen, (b) the node list screen, and (c) the node management screen

6 Result and Discussion

The smart lock system proposed in this paper for home security can be used through mobile applications which are connected to the internet. A single user account can control multiple smart lock devices. Any unauthorized access of door lock can send notification to the mobile application of registered user. The proposed home security system is economical and easy to use since the IOT based controller of the door lock can be installed and removed easily by a person with no technical ability. The future scope of the proposed system can include an enhanced encryption system as well as integrating other biometric parameters.

References

1. Shiu Kumar, Seong Ro Lee " Android based smart home system with control via Bluetooth and internet connectivity " pp.1-11, May 2014
2. Shopan Dey et al. "An IoT Framework for Smart Power Management System" IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), May 2017
3. Yong Tae Park, Pranesh Sthapit, Jae-Young Pyun " Smart Digital Door Lock for the Home Automation" IEEE Region 10 Conference, Jan 2009
4. Hajoon Ko, Jiong Jin, Sye Loong Keoh, "Secure Service Virtualization in IoT by Dynamic Service Dependency Verification," IEEE Internet of Things Journal, Vol. 3, no. 6, pp. 1006-1014, 2016.
5. Dongsik Jo, Gerard Jounghyun Kim, "ARIoT: Scalable Augmented Reality Framework for Interacting with Internet of Things Appliances Everywhere", IEEE Transactions on Consumer Electronics, vol. 62, no. 3, pp. 334-340, 2016.
6. Romano Fantacci, Tommaso Pecorella, Roberto Viti, Camillo Carlini, "A network architecture solution for efficient IOT WSN backhauling: challenges and opportunities," IEEE Wireless Communications, vol. 21, no. 4, pp. 113 - 119, 2014.
7. Jaime Lloret, Jesus Tomas, Alejandro Canovas, Lorena Parra, "An Integrated IoT Architecture for Smart Metering," IEEE Communications Magazine, vol. 54, no. 12, pp. 50-57, 2016.
8. Luca Catarinucci, Danilo De Donno, Luca Mainetti, Luca Palano, Luigi Patrono, Maria Laura Stefanizzi, and Luciano Tarricone, "An IoT-Aware Architecture for Smart Healthcare Systems," IEEE Internet of Things Journal, pp. 1-12, 2015.
9. Paolo Bellavista, Giuseppe Cardone, Antonio Corradi, Luca Foschini, "Convergence of MANET and WSN in IoT Urban Scenarios," IEEE Sensors Journal, vol. 13, no. 10, pp. 3558-3567, 2013.
10. Elias Kougianos, Saraju P. Mohanty, Gavin Coelho, Umar Albalawi, Prabha Sundaravadivel, "Design of a High-Performance System for Secure Image Communication in the Internet of Things," IEEE Access, 2016.
11. Fagen Li, Pan Xiong, "Practical Secure Communication for Integrating Wireless Sensor Networks Into the Internet of Things," IEEE Sensors Journal, vol. 13, no. 10, 2013.
12. Hairong Yan, Yan Zhang, Zhibo Pang, Li Da Xu, "Superframe Planning and Access Latency of Slotted MAC for Industrial WSN in IoT Environment," IEEE Transactions on Industrial Informatics, vol. 10, no. 2, 2014.

13. Shohan Dey, Ayon Roy, Sandip Das, "Home automation using Internet of Thing," Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), IEEE Annual, 20-22 Oct. 2016.
14. Prajapati, Gitesh, Pooja Singh, Rahul, "Anomaly Based Network Intrusion Detection System for IoT," International Conference on Data Science and Applications (ICDSA), Singapore: Springer Nature Singapore, Volume 2, pp. 693-706, 2022.
15. Rahul, Rauniyar Kritesh, Monika, Javed Ahmad Khan, "Application of IoT and AI in the Development of Smart Cities." In Smart Cities, pp. 181-196. CRC Press, 2022.
16. Rahul, Sahithi Bommareddy, Monika, Javed Ahmad Khan, Digvijay Pandey, "IoT implementation and challenges in healthcare industries." In Networking Technologies in Smart Healthcare, pp. 211-230. CRC Press, 2022.
17. Rahul, Amit Gupta, Anupam Raj, Mayank Arora, "IP traffic classification of 4G network using machine learning techniques." In 2021 5th International conference on computing methodologies and communication (ICCMC), pp. 127-132. IEEE, 2021.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

