International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 11 | November - 2022 Impact Factor: 7.185 ISSN: 2582-3930

The RFID Enabled Cloud based Security System for Door Locks

Prof. Varsha Dange, Pranay Nannaware, Sahil Patil, Omkar Pawar
Department of Computer Engineering, Vishwakarma Institute of Technology, Pune - 411037

Abstract– The need for trustworthy, secure systems that are simple to access has been growing across businesses and industries. One of the most reliable and quick methods of identification is RFID (Radio Frequency Identification).Due to their low cost, ease of use, and effectiveness, RFID is quickly replacing the use of barcodes and biometric authentication.
Moreover, the project's capability is expanded through the usage of an application and Cloud-enabled features. This paper describes a prototype that uses RFID and a NodeMCU module to enable security access and addresses the aforementioned issues.

I. INTRODUCTION

One of the main reasons why individuals have tried to construct their own homes and flats is the desire for safety. There are one or more major entrances in every home. The major entrances are one of the most crucial components of safety. The installation of a security system in a room is essential for safeguarding priceless items and preventing unwanted entry. In order to prevent the loss of goods or sensitive data, security must be enhanced.
Different types of door locks, including mechanical and electrical ones, have been used to try to assure security. Because these locks have well-known weaknesses of their own, crimes do still occur even after utilising them. Some locks can be picked, while others can be partially or completely deactivated. Sadly, it is insufficient to detect illegal access. It is less dependable and more prone to theft attempts. As a result, new lock types that are challenging to break and even when they are will be more challenging than previous types of locks must be created.
It is crucial to develop a system that would provide individuals peace of mind regarding their home security. The system should be capable of the following:

1. Ease of Control: The system should be simple for home owners to operate.
2. Durability: The system should be durable enough.
3. Security: The system itself must be secure in order to provide security.

An electronic locking system is created to enhance security and authentication. The NodeMCU ESP8266, RFID, solenoid lock, relay, and many more IoT-related components are employed in this system.
The Google Firebase Realtime Database and Cloud Fire store, a set of application development tools backed by Google and used for creating, managing, and modifying data generated by Android and iOS applications, web services, IoT sensors, and hardware, among other sources, were used to help create this system. We will link the Dashboard Application with Google Firestore, which saves the data in the form of Documents and Collections, using the Firebase Host and Authentication Key, as well as the API Key.A Python script is used to move the data from the Cloud Firestore to the Firebase Realtime database. Through an Internet connection, the Google Firebase data is currently being transmitted to the NodeMCU Board, where the system will subsequently carry out the task. The solenoid lock, relay, and battery are interconnected so that when we scan our authorised card, the condition specified in the programming matches, and the command specified in that condition becomes active, the lock opens. However, when an unauthorised or unregistered card is scanned, the door lock will remain locked, and the system will sound an alarm.

II. Related work.

For the benefit of their institutions' security, several companies have begun utilising RFID-enabled locking systems. The technology known as RFID, or radio frequency identification, uses radio waves for the purpose of identification and authentication with the use of a tag and a reader.
A microcontroller is necessary to use RFID technology for authentication. C. Mayani et al. utilised an Arduino Uno to complete the task, although this limited the capability because the scope was confined.
In an additional effort to broaden the project's scope,

Umar Farooq et al. used GSM, however doing so limits real-time communication.Additionally, Peter Adole et al .'s use of embedded C-programmed Microcontrollers with the AT89S51 so that the microcontroller may be programmed using Assembly. After reading the works of Yordan Hasan et al. and KhaingMyatNwe et al , the use of Bluetooth for connectivity has also been considered, but it again has a lot of disadvantages and restrictions when compared to Wi-Fi enabled systems, which RFID enabled Cloud based Security System for Door Locks provide a direct way of communication to the server as suggested in other works studied as well.Additionally, Chukwunenye Okafor et al. and Jie-Ci Yang et al. explored the idea of a camera module, while Ni Ni San Hlaing et al. explored the idea of a keypad, Chukwunenye Okafor et al. explored the idea of speech recognition, and Ni Ni San Hlaing et al. investigated the idea of speech.

While the suggestion to integrate a database made by Gyanendra K Verma et al. was taken into account, a cloud-based database was incorporated to this project.

Given its Wi-Fi capabilities and low cost, NodeMCU was chosen as the circuit's controller based on these earlier studies and many others. Along with this, a cloud-based database will be kept using Google's Firebase services in conjunction with a Python script, and a Flutter-based application will be utilised to give the administrator access to a dashboard that may assist in doing the necessary tasks.

III. Methodlogy

The hardware (with NodeMCU, the sensor, the lock, etc.), the Flutter application, the Firebase Realtime Database, the Cloud Firestore, and the Python script can all be broken down into five main components.

The input phase, processing phase, and output phase are the three main processes that make up the functioning. The system will initially request input from the administrator via the application for each Level/Group of RFID tag permission.Then, for the Processing phase, the aforementioned saved data in the form of collections on the Cloud Firestore sent by the Flutter application will be exported to the Firebase Realtime Database in the form of JSON via a Python script running on Google Colaboratory because it gives us a constantly running server that helps its users run scripts or notebooks using Google Colaboratory's resources. The NodeMCU will retrieve the data from the Firebase Realtime Database for the output phase and determine which Level/Group of RFID tags to authorise and which to disallow. The RFID reader will then check for authorised tags, and if any are found, the relay will send a signal to the lock allowing entry.

A. Permission Hierarchy:

Prior to executing the project and preparing it to carry out tasks, it is necessary to establish our guidelines clearly. Whichever user will be given authorization to utilise the secure system. Although users and permissions can be changed later, certain decisions must be made now in order to get things going and establish a code of behaviour.

There will initially be five clearing groups.

If additional sets of RFID tags are needed, we can also have clearance levels, where the permissions are interlaced to provide access at a higher clearance level when a lower clearance level is granted.

B. Detection

The RFID MFRC522 Reader is an anomaly and nothing less than a lifesaver in this new era of pricey read and write detection devices. It was selected for the entire system because of how quickly it reads tags and how inexpensive it is. In the end, the job will be completed quickly and at a low cost. The RFID MFRC522 Reader is further wired to the NodeMCU for power and control. When a tag is scanned by a user, the RFID module transmits radio signals that activate the tag and cause it to produce radio signals with the data it has stored on it. After that, the reader transforms it into digital signals and sends them to the esp8266 module for processing.

C. Processing

The ESP8266 begins analysing and making decisions after receiving the data from the RFID module.TheNodeMCU's primary function is to format the receiving data and send out signals in accordance with that format. It then establishes a connection with the

Firebase Realtime Database to obtain the authorisation guidelines. Using the Python script, Firebase Realtime Database then retrieves the data from Cloud Firestore. This project's inclusion of this arrangement is justified by its affordability and usability. To aid transmit the administrator's directives, the Cloud Firestore is to be paired with a Flutter application.

The Realtime database in Firebase has the special quality of being a free service for developers to utilise. The information kept in this Realtime database serves as the foundation for the permission hierarchy. Once a specific user's data has been retrieved from the database, it is obvious whether to grant the user permission to enter through the door or refuse it depending on that permission or the outcome of any unknown input. The procedure then moves on to the output step.

In the end, the system uses a relay to determine whether to approve admission or not after verifying the user's clearance through the system.

D. Output

Now that it has been chosen whether to allow the user or not, the solenoid lock's next task is to be either unlocked or remain locked. The used solenoid lock is a 12V solenoid lock that is powered by the battery and receives commands from the NodeMCU module through a single channel 5V relay.

Clearance Levels for the system's authorisation can be set. In other words, higher levels automatically obtain access if a lower level is allowed to pass through. This aids the organisation in preserving the chain of levels' hierarchy of order.

IV.ANALYSIS AND RESULTS

The security of businesses with level-based clearance systems, such as those in the defence and intelligence sectors, can be greatly improved by using this circuit in conjunction with the features of the Flutter Application, Cloud Firestore, and Firebase Realtime Database. Analysis of the use of the mentioned technologies:

Flutter: A variety of languages, including Kotlin for Android devices, Swift for Apple devices, C++ and Java for native programmes, and JavaScript for web applications, are used today to construct applications for devices. In spite of the confusion around cross-platform connectivity and code reuse, there is one technology that outperforms all of these languages. Flutter, which was first presented in 2015 and then made available for development in 2017 by Google, is far superior to the other technologies. It can run on numerous platforms with the same code, including Linux-based operating systems like Ubuntu for both development and production, as well as Windows apps, Apple devices, Android devices, Web applications, and other platforms. Flutter is available as a software development kit that can be combined with IDEs, primarily Visual Studio Code and Android Studio. Flutter makes use of the Dart programming language, which includes more sophisticated facilities for developing and debugging code. It operates on the Dart Virtual Machine. It is an engine made for quick execution. The app we'll be utilising was developed with Flutter technology and will function as an admin app. The ability to modify data in the Firebase real-time database will be granted to it. Consequently, our duty is greatly simplified and is more user-friendly.

Firebase: The NodeMCU performs an excellent job of processing information and handling all the devices, but its built-in memory is very small or not designed to hold big amounts of data, such as the kind of database this entire project requires. We therefore use the real-time database provided by Google's very own Firebase to address this issue. It is allotted a small region in its cloud servers for the preservation of the data that we require, which will be adequate for our use for a very limited number of queries. No matter where the server is located, we can still reach it through the web from anywhere, and it has a huge amount of processing power to handle many requests at once—say, thousands at once. We can easily carry out our actions on the database by setting the read and write permissions in the JSON file of the permissions file. It gives us a confidential database key

and an API token. The private database key and API token enable our web-connected module to connect to the appropriate database server and IP address, respectively, over the internet.

V.CONCLUSION AND FUTURE SCOPE

This study has successfully created a real-time cloud-based door locking system that is quite efficient in terms of quality and technology. This research was successful in creating automatic home security that can be remotely controlled using a phone or tablet. The given application was created using the Flutter framework. The whole design was based on testing that was done regarding the design of prototype smart locks based on the internet of things with the ESP8266.

Each component performs admirably and in line with our prediction, according to the results of component testing that has been done. Large numbers of RFID tags can be enlisted for usage in this project's future scope. Additionally, complete system customization would expand the range between labels and locks. The Flutter app can also be expanded to run on a variety of different platforms. Additionally, in an emergency, fire control might be made available to open all the doors. Also, a whole database can be installed. With the help of intermediate nodes, we can extend range. Commercially available RFID locking systems are designed to control a single door, but if enough intermediate nodes are added and each entryway has distinct authorizations established, this system can be implemented to control even a multistory building. Additionally, it is a cheap system. However, if a transmitter broadcasts data within the system's operational range while using the same frequency as the system, the system is unable to function. The solution to this issue is to use a special frequency and baud rate. To avoid this issue, more work needs to be done to switch the full broadcast over to Wi-Fi transmission.

VI. REFRENCES

[1] Yordan Hasan, Abdurrahman, YudiWijanarko 2019 “The Automatic Door Lock to Enhance Security in RFID System”
[2] Peter Adole, Joseph M. Mom and Gabriel A. Igwue 2019 “RFID Based Security Access Control System with GSM Technology”
[3] “Enhanced Security Methods of Door Locking Based Fingerprint” - Hashem Alnabhi, YahyaAlnaamani, Mohammed Al-madhehagi, Mohammed Alhamzi [2020]
[4] “An Intelligent Automated Door Control System Based on a Smart Camera” – Jie-Ci Yang, Chin-Lun Lai, Hsin-TengSheu, and Jiann-Jone Chen [2020]
[5] C. Mayani, S. Pandya,2021 “RFID Based Security System Using Arduino”
[6] “RFID-Based Digital Door Locking System” ShubhamSoni, RajniSoni, Akhilesh A. [2018]
[7] KhaingMyatNwe, KaythiWutMhoneKhin, Zin May Win, ZarniSann. Year- 2019 “IOT based Smart Home Security System using RFID and Bluetooth”
[8] Cesar Munoz-Ascham, Juan Ruiz-Roserio and Gustavo Ramirez-Gonzalez. Years- 2021 “RFID Applications and Security Review”
[9] Sourabh Sarkar, Srijita in 2018 “Android based Home Security Systems using Internet of Things (IoT) and Firebase”
[10] Chukwunenye Ok 2022 a for, AlumonaTheophilus Leonard “Door Access Control Using RFID and Voice Recognition System”
[11] Harsh Kumar Singh1, SaurabhVerma 2020 “A step towards Home Automation using IOT”
[12]Gyanendra K Verma, Pawan Triatic in 2018 “A Digital Security System "with Door Lock System Using RFID Technology”
[13] “RFID based Door Lock System using Cloud Computing and Arduino Board” Dr.ShilpaAbhang [2018]
[14]Md.Kishwar Shafin1, KaziLutfulKabir in 2019 “Development of an RFID Based Access Control System in the Context of Bangladesh”
[15] Urvi Singh, M. A. Ansari, SMIEEE in 2018 “Smart Home Automation System Using Internet of Things”
[16]HartatiDeviana, M. Miftakul Amin, Roy Sandy, 2018 “Door Security Design using Radio Frequency Identification”