www.dergipark.gov.tr
ISSN:2148-3736

El-Cezerî Journal of Science and Engineering
Vol: 10, No: 2, 2023 (193-207)
DOI: 10.31202/ecjse.1099817

ECJSE

Research Paper

Smart Multi Verification Based Security System

Uma MAHESWARI K[1a], Kishore BALASUBRAMANIAN[2b*], Ishwarya NIRANJANA M[3c], Dhanu ARAVINTH K[4d], Karthik V[5e], Padmanaban V K[6f]

[1,2]Assistant Professor, EEE, Dr. Mahalingam College of Engineering and Technology, Pollachi, India
[3]Assistant Professor, ECE, Sri Eshwar College of Engineering, Coimbatore, India
[4.5.6]UG Students, EEE, Dr. Mahalingam College of Engineering and Technology, Pollachi, India
bkishore1979@gmail.com

Received: 07.04.2022 **Accepted:** 14.03.2023

Abstract: Security is crucial in this age of rapidly advancing technology for stopping various crimes and thefts. This contradiction gave rise to a creative concept for how to raise the level and address the issues already there. A clever idea for how to raise the bar and deal with the existing problems resulted from this paradox. This article suggests a suitable multilayer security system for use in homes, bank lockers, and other venues. In contrast to the widespread use of password and biometric double-layer security methods, this embedded solution sequentially identifies fingerprints, OTP, and RFID. A microcontroller with a GSM module connects and controls essential modules. The mobile application displays the status of each action, and the system pushes every action it does to the IoT cloud. The magnetic switch may only be opened with the proper authorization, and any unauthorized access sets off the alarm and sends the necessary message alerts. The multistage security of the proposed system makes it more dependable and efficient, and the combination of all three phases makes it difficult to break. The whole system's workings indicate by led flashes. This implementation has shown better results and a higher performance rate than existing methods.

Keywords: RFID, GSM module, Fingerprints, IoT, Multilevel Security

1. Introduction

Since ancient times, humans and powerful beasts have had to safeguard precious things. But in this modern century, human life depends on technology. It instils a strong belief in multi-level technological security. In a traditional security system, there are RFID, password, or biometric-based systems that are more likely to break such a one- or two-level security system. The main impact of this study is to offer multi-level protection which doesn't breach the security of the unknown person, and the term "multi-level" refers to the three-tiered security provided by RFID, fingerprint, and OTP. The microcontroller operates the consecutive layers of the system. Every incorrect and correct operation performed by the system is sent to the IoT cloud, and the mobile app displays the status of each action. To verify authorised or unauthorised persons, the system uses Radio Frequency Identification (RFID) technology as the first level of security. The active RFID uses a 13.56 MHz electromagnetic field that communicates with RFID tags. It communicates with a microcontroller using the Serial Peripheral Interface (SPI) communication protocol to send a unique identifier (UID) code. A notification is sent to the authorised individual if someone tries to open the door without authorization. Next to RFID, the system uses biometrics as the second-level verification, and the wrong attempt that happened in between will increment the count for alarm operation. In the second level of authentication, the system requires the user's fingerprint to identify the accurate identification of authorization. Optical fingerprint sensors capture high-resolution images at the fingertips and create rows of identifiers used uniquely to identify a particular fingerprint. It can store more than single-person data, so the system enables a more user-friendly option, and multi-access enhances

How to cite this article
Uma Maheswari K, Kishore Balasubramanian, Ishwarya Niranjana M, Dhanu Aravinth K, Karthik V, Padmanaban V K, "Smart Multi Verification Based Security System", *El-Cezerî Journal of Science and Engineering*, Vol. 10, No. 2, 2023, pp. 193-207.
ORCID: [a]0000-0001-6961-3401; [b]0000-0003-1918-9774; [c] 0000-0002-5242-7626; [d]0000-0002-4837-9166; [e] 0000-0002-0145-7892; [f]0000-0001-5607-8374

large-scale business. If the fingerprint is identical to the registered fingerprints, access is accepted, and the GSM module generates a random One-Time Password (OTP) for the user's mobile number. The greatest merit of the OTP-type system is that it is not necessary to remember any passwords. There is a possible reason to easily copy fingerprints to overcome this issue, as the third level of security provided by GSM generates random OTPs for the registered mobile numbers. If the user has successfully reached the third level of security, the system will give access to the user, which will be shown in the mobile application.

The paper is organised as follows: Section 2 outlines the literature survey related to the work proposed. The proposed methodology is elucidated in Section 3, and the results are reported in Section 4. Section 5 reports the conclusion.

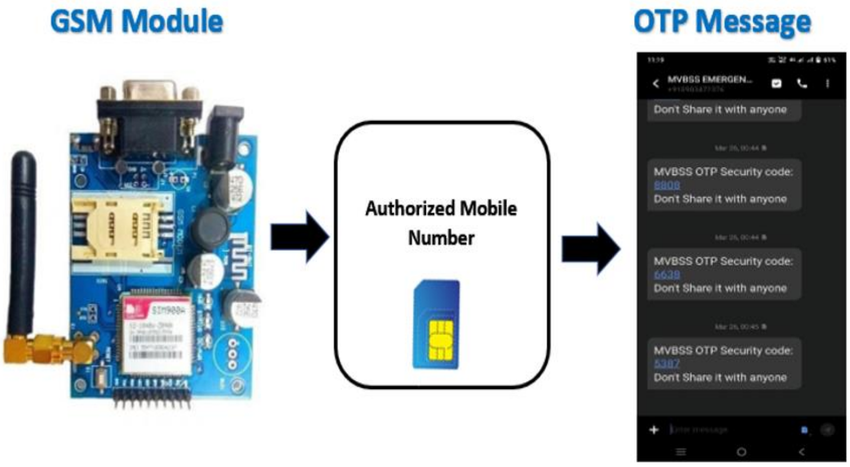
2. Related Work

Abdulwahid et al. [1] discussed how the network performance of the president building of the University of Medical Technology was explored based on the ap space in the target building. Wireless insight software was used to conduct this analysis, which was based on an estimate of path loss and the power measurements obtained. The results showed a significant difference in network performance and building-wide coverage. As a result, a major contribution to improving network performance was proposed by reducing the number of app devices used from 13 to 8. Abdulwahid et al. [2] introduced an RSS-based scaling-based localization technique for efficient app deployment. RSS measurements were taken on a variety of real-world sites. The optimal direction for each given point was determined using measurement results collected with special software. The algorithm was a two-step localization approach with a data collection phase and a localization phase. The investigation was seen as a silent verification of the results achieved using wireless intelligence software and access to 3D ray tracing. Anand et al. [3] explained how to control and manage home appliances and equipment and how to express a combination of hardware and software. In today's society, the basic goal of using the internet (IoT) to monitor electronic devices is to manage them according to their location. As technology advances, the need for effective monitoring increases as performance improves and more energy and resources are conserved. Doing so eliminates the need to turn on the lights during the day. Nodemcu is very popular for in-house automation. IoT development was a breeze thanks to its wi-fi capabilities and Arduino IDE support. Home appliances could be controlled with the blinking app on an Android processor. Bhatt et al. [4] described a bank security vault. It overcomes the issues in conventional systems. It used a two-door security system. The first door used biometric and keypad entry security levels. Finally, the second door required an OTP and was subject to detection entry. This proposed technology would aid in the high-level protection of bank vaults. Dioses et al. [5] explained how home automation had given life a whole new meaning. Home equipment such as televisions, air conditioning, lighting, and fans were all controlled by a controller. Instead of a remote-controlled computer, these devices could only be controlled by remote control. The method employed only the Arduino and smartphone with the existing Bluetooth transmission. The fan speed was automatically controlled from speed no. 1 to speed no. 2 using voice recognition in the Philippine language. The user utilises voiced instructions to carry out specific tasks. Fan speeds 1 and 2 obtained 50% accuracy in the test, while speeds 3 and 4 both reached 100% accuracy. Fan et al. [6] described RFID as a key technology in IoT. The usage of the RFID in the medical practise could effeciently resolve this issue of medical privacy. RFID tags on a computer could collect useful information and transfer it to the reader via a back-end server. The entire communication process was primarily carried out via text message. In the context of IoT, the article presented a lightweight RFID medical privacy protection plan. This programme guaranteed the privacy of data collected through secure authentication. The security analysis and evaluation of this programme indicate that the protocol could effectively prevent the risk of easy leakage of medical privacy data. Govindraj et al. [7] stated that today's contemporary world is a transition to a wireless world. This system focused on authentication time. This proposed solution was based on a one-of-akind smart door design that employs a biometric NFC band and OTP authentication procedures to provide secure and convenient entrance into our homes. Goyal et al. [8] created a high-security surveillance system. For high-level enterprises, the technique comprises primary and secondary security. A hex keypad, Bluetooth, and RFID were all part of this three-stage system. The secondary system consists of a fingerprint sensor, and the primary and secondary are independent. When the primary system was complete, it would be moved to the inner vault. The valuables in the inner vault were further protected by a fingerprint scanner, as the second structure was independent of the primary system. If anyone tries to reach most circles, three-level security authentication is required, which becomes the primary level of security. The Raspberry Pi computes the entire system. Once a security breach was discovered, the SMS shield would notify the appropriate authorities. The raspberry pi enables the additional feature of 24x7 surveillance monitoring. The vault was segregated from the core system to improve reliability, and the Raspberry Pi camera operation monitor has a fingerprint sensor. Gupta et al. [9] built a multi-layer security system. This methodology consists of RFID, passwords, and biometrics. A microcontroller controls all three stages. The multi-stage system was more efficient and reliable, and the combination of all three levels made it difficult to breach. The LCD shows the instructions and status of the system. If unauthorised attempts occur, a notification would be sent. Hersyah et al. [10] developed a dual authentication method known as "biometric authentication," which used fingerprints and passwords. The double authentication system in the laboratory room was meant to strengthen security and make admission to the laboratory room easier for the user. It took around 0.62 seconds for the system to change the condition of a closed door to “opened”, and 3.74 seconds to change the state of an opened door to “closed”. Imran et al. [11] developed an alert system with theft protection. The methodology consists of fingerprints, GSM, GPS, and solar panels to power the system. This advanced system is used in the surveillance area for valuable items. In this system, fingerprinting with a GPS module was enabled, and the system recognised the actual position of the event. Jacobsson et al. [12] described the risk analysis used for a smart home automation system developed in a research project involving leading industry actors, with 9 of the 32 risks classified as low and 4 classified as high. Most of the risks identified were considered moderate. Higher risks were related to human factors or software components of the system. The results indicate that by implementing standard safety features, new and current risks could be minimised to an acceptable level, although the most serious risks, those derived from the human factor, have been carefully considered. were inherently complex to handle. Jamal et al. [13] described multi-level home management, security, and safety systems based on the Arduino microcontroller board. The recommended system illustrates the reliability of the performance system in IoT-based applications. Furthermore, this system demonstrated independence at one point of failure. Moreover, such a system could be considered a low-cost technology used to achieve high security levels in various locations and protect against widespread disasters. Noman et al. [14] outlined how automobiles would start using RFID, fingerprint, or password technology. If an unauthorised person tries to open the door of the vehicle, they would be asked for the correct RFID, password, or fingerprint. The tilted sensor detects any breakage or movement of the vehicle's windows or doors and notifies the owner's phone via the GPS-GSM module. A warning was also triggered by the computer. Also, the connection to the car's fuel injector was disabled to prevent the vehicle from starting without permission. This improved the anti-theft mechanism. Shukla et al. [15] described the proposed smart ration card system that uses RFID and IoT to combat fraud and corruption in the current ration distribution system. An RFID tag would replace the traditional ration card. The user authentication of this RFID tag had been checked at the Fair Price store. A microcontroller linked to an Amazon Web Services (AWS) database verifies the user's identity. For added security, the user's registered mobile number would receive a one-time password (OTP), which must be entered into the system. The monthly ration quota available to the user would have been displayed if the user had been verified to be genuine. Taha et al. [16] described a fire extinguishing robot commonly used to extinguish a fire and treat fires in closed areas to protect personnel in the fire department from burning, exposing, or inhaling toxic gases. The basic idea of the fire detection and treatment robot was to detect the fire with a wireless camera, turn on the water pump, suppress the fire by sending a command from the mobile phone via Bluetooth connection, and then extinguish the fire. Tahmidul Kabir et al. [17] articulated the security system that is enabled with the RFID module, GPS, and gsm module. The system includes a memory module, an ultrasonic sensor, fingerprint security, an RFID module, GPS, and a GSM module, among other things. The security breach was solved using the proposed system. Tahmidul Kabir et al. [18] described a security system for transferring or owning items while preventing unwanted access. The system includes a memory module, PIR sensor, fingerprint protection, encoder-decoder, RF module, GPS module, and gsm module to give the highest leveled of security. The suggested security method would significantly enhance the transit of vital papers, money, or jewelry from one location to another, particularly for banks transporting valuables. Tshomo et al. [19] reported a dual-locked system that includes radio-frequency identification and fingerprint recognition. It was a secure and trustworthy locking system that may be utilised in homes, businesses, schools, and other organizations. Wang et al. [20] described the development of a wirelessly controlled module-based smart home management system. Mobile phones may be used to remotely operate and monitor household appliances through the internet in real-time, as well as handle crises in a timely manner. As a result, the quality of life at home, as well as security and comfort, may have been significantly enhanced.

3. Proposed System

The proposed system builds to develop high security with a multi-level security system. Compared to conventional approaches, the novel idea offers more advantages. The proposed solution is unique in that it provides three levels of security: RFID, fingerprint, and OTP verification. This system comes along with the multi-user feature. Every operation of the system has instantly reflected in the mobile application. It's always connected to the IoT cloud, which is more reliable. Authorized users can connect to the system from a distance using the mobile application. This method employs off-grid battery power to prevent problems such as power failures. To avoid the hacker's attack, a series of false attempts will activate the alarm and notification.

The first stage of the RFID module comprises a reader and a transponder UID tag. If an unauthorised person tries to access it, a notification is sent to the authorised person via the system's GSM module, as shown in Figure 1.



Don't Share it with anyone

MVBSS OTP Security code:
8808
Don't Share it with anyone

MVBSS OTP Security code:
6638
Don't Share it with anyone

MVBSS OTP Security code:
5387
Don't Share it with anyone

Figure 1. GSM Mobile OTP

All authorised users have that registered UID tag, and a UID contains a set of unique hexadecimal codes to show off. The reader then identifies it and sends it to the microcontroller for verification. The nodemcu sends every action to the cloud access point, which is used to update the mobile application shown in figure 2. This approach is helpful to determine the state of the security system. Remote users can monitor the operation status via the mobile application.

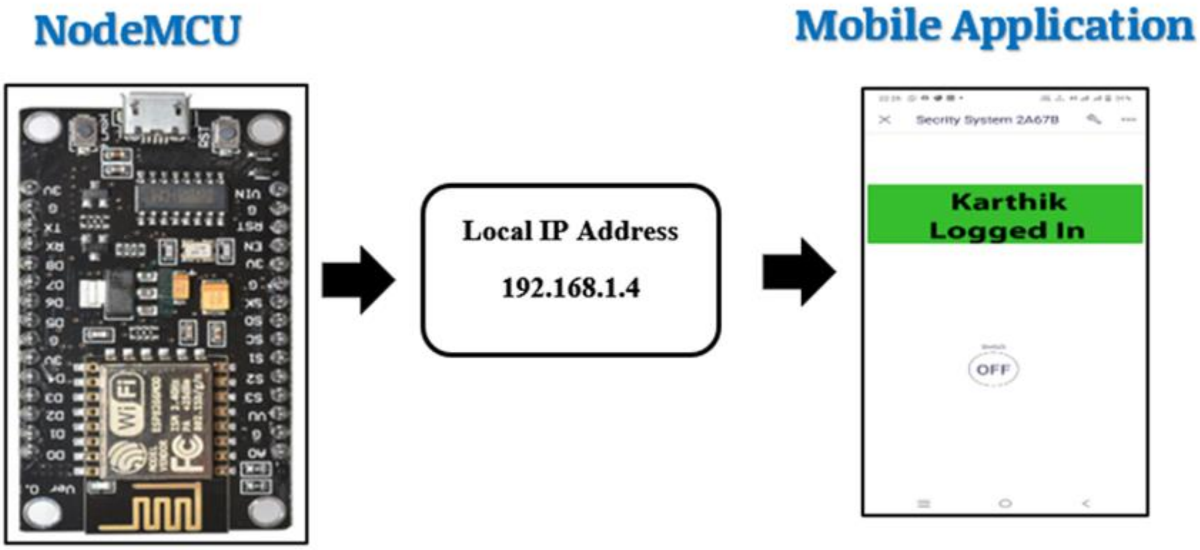


Figure 2. NodeMCU Mobile Application

The second layer contains fingerprint verification. So, fingerprint registration and fingerprint matching are two steps required. During the registration procedure, the user must place his finger twice. The user can save fingerprint data to the module and configure it in 1: 1 or 1: N mode to identify a person. This module can capture fingerprints at a resolution of up to 500 dpi. The user must then enter his password using the keypad. The GSM module sends a random OTP to the consecutive operating user. The system uses a 4x4 matrix-configured keyboard to enter a one-time password manually. When the following user enters the code into the matrix keypad, the microcontroller confirms the code. Its characters are made up of numerals 0–9, letters a, b, c, d, and special characters * and #. If the user continues to input the incorrect code, the associated buzzer will sound an alert, and the user will be unable to access the door. In addition, a notification is sent to authorised users. The GSM module can be used as a receiver, sending an alert to the authorised person to notify him of the entry. For the GSM module, AT instructions were used. The system employs the required cellphone number for this purpose.

Stage 1: As shown in the block diagram (Fig 3), the first level of the authentication process starts with the RFID module. If the RFID UID tag matches, the loop advances to the next level of the fingerprint sensor; otherwise, the procedure is restarted. At this instant, with up to three false occurrences, the system allows the user to show the correct UID tag to pass this level. A series of wrong attempts beginning of security levels will eventually trigger an alarm and send an alert notification to authorized mobile phones by the GSM module. The system is coming along with the feature of multi-user customization. So, the system can store selective UID tags for the RFID reader. At the end of the first level of verification, the system will automatically scan the corresponding mobile number to send the OTP and ask for the corresponding user's fingerprint. A green LED blinks for RFID level verification, and a red LED indicates that the person needs to complete this stage. The progress of RFID operations is frequently updated in the IoT cloud, and remote users may monitor the status of the operation via the mobile application.

Stage 2: Continue with a biometric security level. Once the user has placed the fingerprint correctly, the system will move to the next stage of the OTP authentication level. Otherwise, the system will restart. Instantly, the system updates the operations in the IoT cloud. The multi-user feature enables the system to store multiple fingerprints. Due to consecutive verification, only RFID-confirmed users can place their fingerprints at this step. The green LED blinks for fingerprint level verification, and the red LED indicates that the person has not verified this stage.

Stage 3: At the OTP stage, the registered mobile number that has completed two levels will receive an OTP. When the user has finished all of the stages, the magnetic switch will open. Otherwise, the process needs to be restarted by the user. Finally, three green LEDs will blink to show the magnetic switch's open position, and the updated IoT Cloud and mobile app will show all three levels.

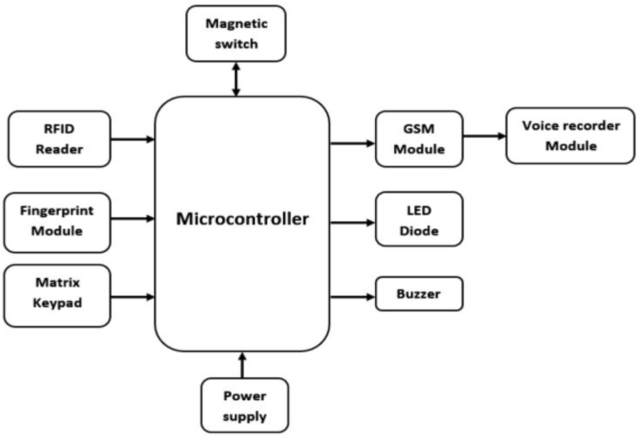


Figure 3. Block diagram of the approach

3.1. Design and Implementation

3.1.1. RFID Module

The primary level of security is the RC522 RFID tag system. The system has already defined the unique identification code for authorized users. Whenever the user brings the RFID tag closer to the reader, it will begin to signal to the controller if the tag code matches the pre-defined system code. Figure 4 shows the RC522 RFID module, and table 1 shows its specifications. When the system detects an unregistered tag, the code does not match, and the actuator does not transmit a signal to the microcontroller. The green LED shows the current level of the system, and the buzzer beeps for correct and incorrect operations. Nodemcu will update the data in the cloud when the RFID level is complete.

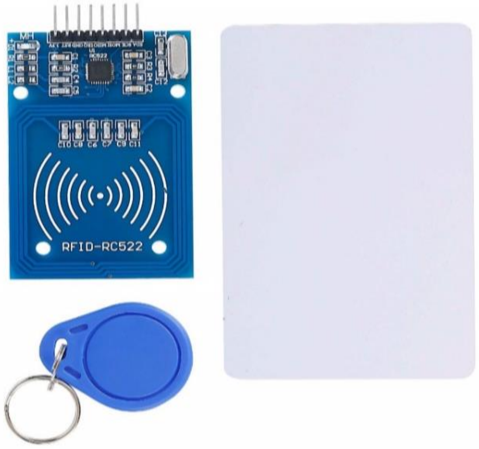


Fig. 4. RFID Module

Table 1. RFID Module Specification

Parameter	Specification
Operating Voltage	3.3V
Operating Current	26mA
Interface	SPI

3.1.2. Fingerprint Sensor

After passing the RFID level, the system's secondary security is an optical fingerprint scanner, R307. Figure 5 shows the R307 Fingerprint sensor, and Table 2 shows its specifications. It has an independent secondary processing unit and supplies power separately, and it stores data of authorized users' fingerprints. When a consecutive user tries the fingerprint level, it matches the stored fingerprint and moves the loop to OTP. The LED shows the current stage of the system. The buzzer sounds give the correct fingerprint identification.

Fig. 5. Fingerprint Sensor

Table 2. Fingerprint Sensor Specification

Parameter	Specification
Operating Voltage	5V
Operating Current	50mA
Interface	UART

3.1.3. Matrix Keypad

Fig. 6. Matrix Keypad

The Hex Keypad is the ultimate authentication level to go inside the premises in this multi-level security system. Figure 6 shows the 4x4 matric membrane keypad, and table 3 shows its specifications. Proper OTP allows the user to change the solenoid lock and open the door. Arduino activates the solenoid lock when the authorized user enters the correct OTP. The GSM module sends a random OTP to authorized mobile numbers. Finally, a double beep indicates the door's open status, and the mobile application shows the entry notification.

Table 3. Matrix Keypad Specification

Parameter	Specification
Operating Voltage	3.3V
Operating Current	30mA
Interface	UART

3.1.4. Matrix Keypad

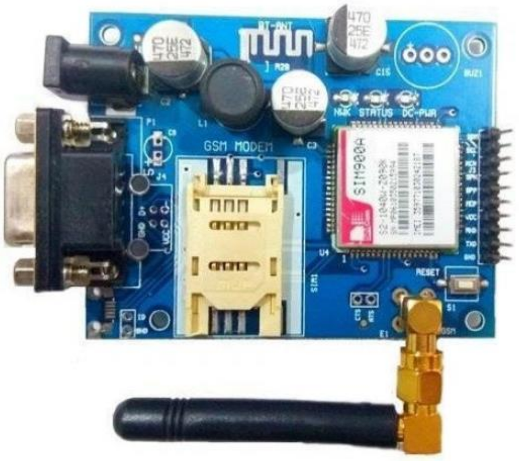


Figure 7. GSM Module

The GSM SIM900A module is employed to send messages and make emergency calls. The Arduino microcontroller connects to this module. Figure 7 shows the GSM Module SIM900A, and Table 4 shows its specifications. A 2G full-size SIM card will work properly in this GSM module. It is capable of making phone calls and sending text messages. A built-in microphone is used to record and convey voice messages. It has an external antenna; however, it should be placed in a signal-rich region, or errors may arise while it is functioning. The UART protocol uses all communication between the microcontroller and the GSM module.

Table 4. GSM Module Specification

Parameter	Specification
Operating Voltage	4.1V
Operating Current	2A
Interface	UART

3.1.5. Microcontrollers

The system uses an Arduino Mega 2560 and a node microcontroller, the ESP8266. Figures 8a and 8b show the Arduino Mega 2560 and NodeMCU ESP8266, and Table 5 shows their specifications. The

Arduino Mega handles all input and output peripherals, while the Node MCU handles all cloud work. The sensors use power sources from the Arduino Mega, which has 54 digital input and output pins that can be used to connect more sensors. The Arduino Mega provides the 3.3 volt power supply for the NodeMCU. The Arduino Mega and NodeMCU can communicate with each other through serial communication.

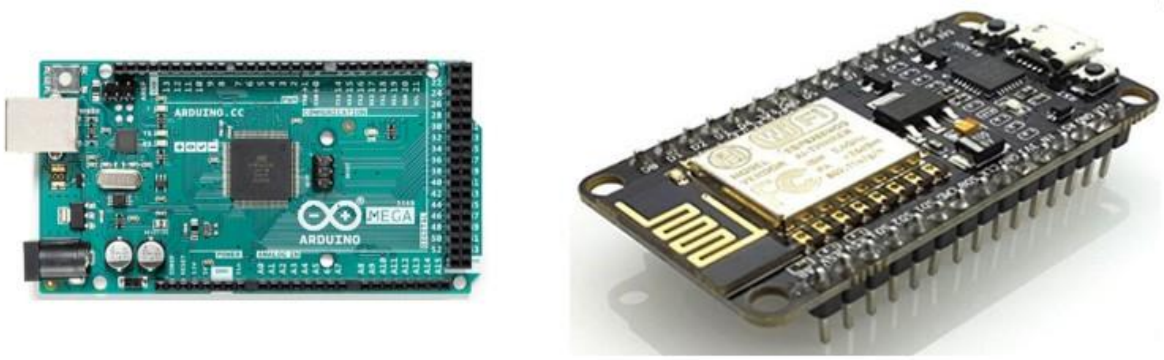


Figure 8. Arduino Mega 2560 (a) and NodeMCU ESP8266 (b)

Table 5. Microcontroller Specification

Specification	Development Boards	
	Arduino Mega 2560	**NodeMCU ESP8266**
Operating Voltage	5V	3.3V
Operating Current	40mA	600mA
Controller	ATmega2560	WiFi capability
Maximum Clock Speed	16 MHz	80 MHz

3.1.6. Magnetic Reed Switch

A magnetic door sensor MC-38 is an electrical switch that activates a magnetic field. Figure 9 shows the Magnetic Reed sensor, and Table 6 shows its specifications. It sends a signal to the microcontroller as it moves one another, instructing it to complete the necessary action. This sensor is appropriate for activating the pulse or functioning in tandem with the door. The sensor magnet induces this wire. Its high or low signal operation depends upon the magnet's distance from another one. The circuit will shut or open if the magnetism is too far away from the source.

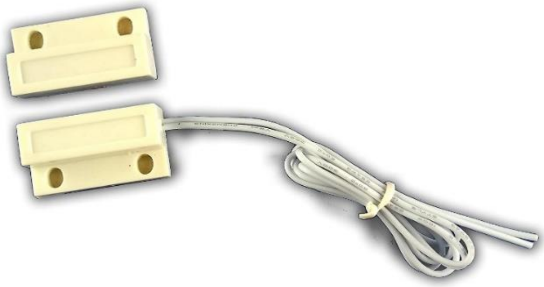


Figure 9. Magnetic Reed Switch

Table 6. Magnetic Reed Switch Specification

Parameter	Specification
Operating Voltage	5V
Operating Current	15mA

3.1.7. Solenoid Switch

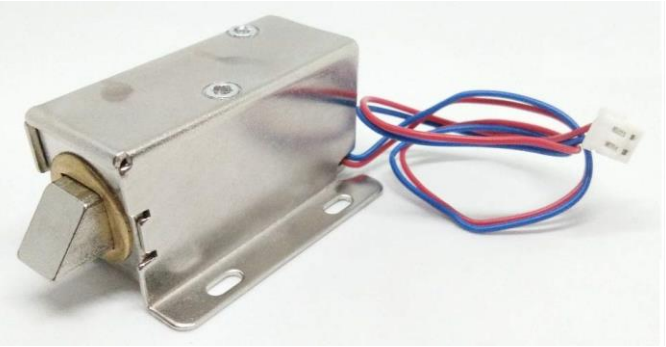


Figure 10. Solenoid Switch

The electrical opening and latch lock refer to a solenoid lock. The most common type of solenoids or electromagnets are electronic locks. Figure 10 shows the magnetic reed sensor, and Table 7 shows its specifications. When a user "opens" the lock, the current running through the wire coil generates a magnetic field that unlocks a metal plunger or lock pin.

Table 7. Solenoid Switch Specification

Parameter	Specification
Operating Voltage	12V
Operating Current	80mA
Power rating	9.6W

3.1.8. Flow Chart

The whole system consists of three primary loops, with the RFID acting as the first verification loop shown in Figure 11. It repeats the initial cycle three times until the proper RFID is recognized. Once verified, the correct UID code advances to the next fingerprint ring and sends the status to the mobile application. The second loop is the fingerprint verification loop.

If the user's fingerprint is the same as the saved fingerprint, it will move to the last ring. Finally, OTP verification is vital since it provides a person's unique authorization. It opens the magnetic door switch and allows entrance after third loop verification, and concurrent updates are available on the mobile app. Instantly, every incorrect status sends as a notification to the mobile app.

4. Result and Discussion

The final results have been obtained in a similar manner to that of the flow chart. Figure 11 shows the approach of the whole prototype. The algorithm works with the sequential operations of RFID, fingerprint, and OTP verification. Firstly, RFID reads the UID tag; secondly, the fingerprint module scans the biometrics; and finally, the GSM module triggers the OTP typed on the matrix keypad. The mobile application frequently displays every operation and any required emergency switching performed by this user application.

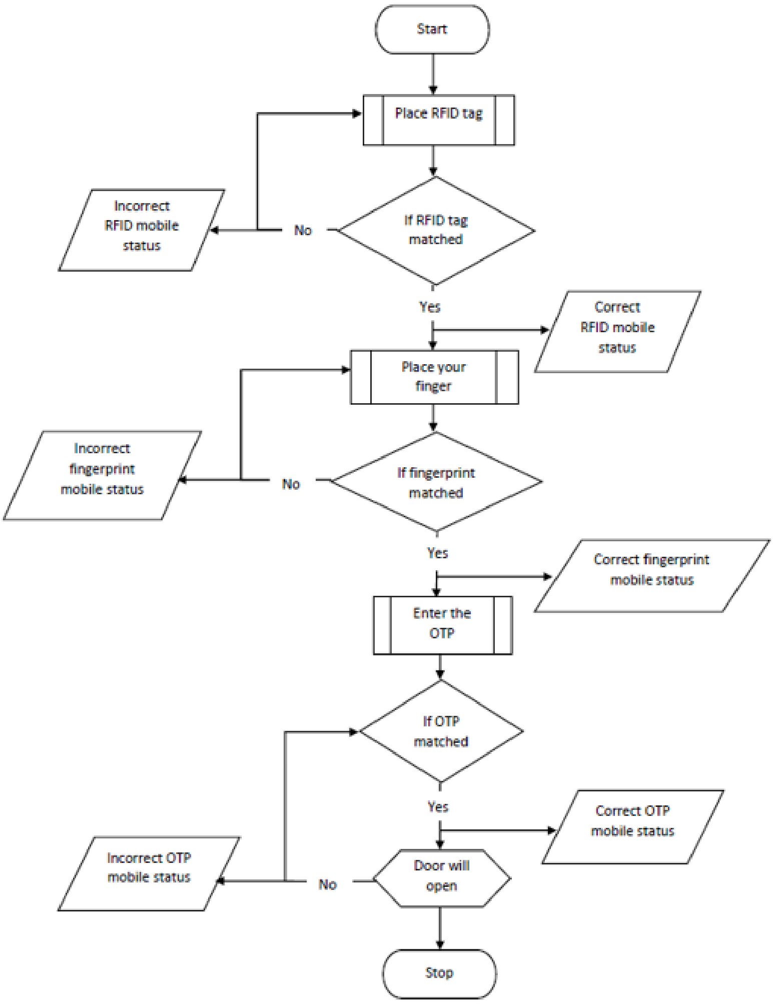

Start
Place RFID tag
If RFID tag matched
No
Incorrect RFID mobile status
Yes
Correct RFID mobile status
Place your finger
If fingerprint matched
No
Incorrect fingerprint mobile status
Yes
Correct fingerprint mobile status
Enter the OTP
If OTP matched
Yes
Correct OTP mobile status
No
Incorrect OTP mobile status
Door will open
Stop

Figure 11. Proposed Flow Chart

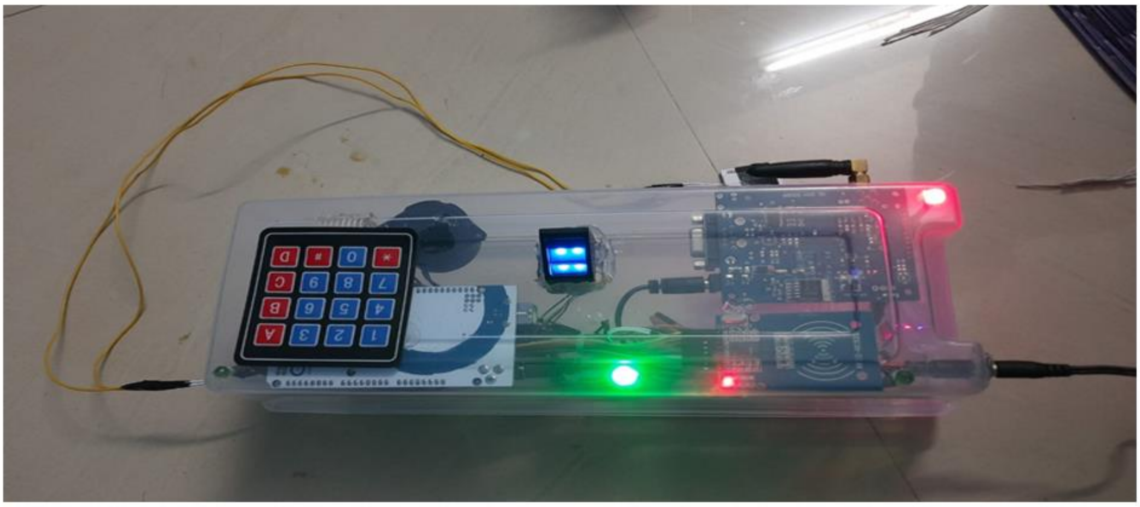


Figure 12. Proposed System Prototype

Mobile applications enable global access through the Node microcontroller. If all three levels are successfully confirmed, the magnetic switch will open and entrance will be allowed. The LEDs display the status of each stage, and the advantage of the sensor technology is that it offers a multi-user feature. Security breaches will result in a security alarm and notification to authorized users via the GSM module. Table 9 specifies the option of predicting the time a user can break the security system. The objective of the proposed system matched the obtained results, which are favorable for enhanced safety. Table 8 represents the comparative analysis with other security systems. Figure 12 shows the hardware implementation of the work and figure 13 its schematic sketch. Hardware wiring diagram is illustrated in Figure 14

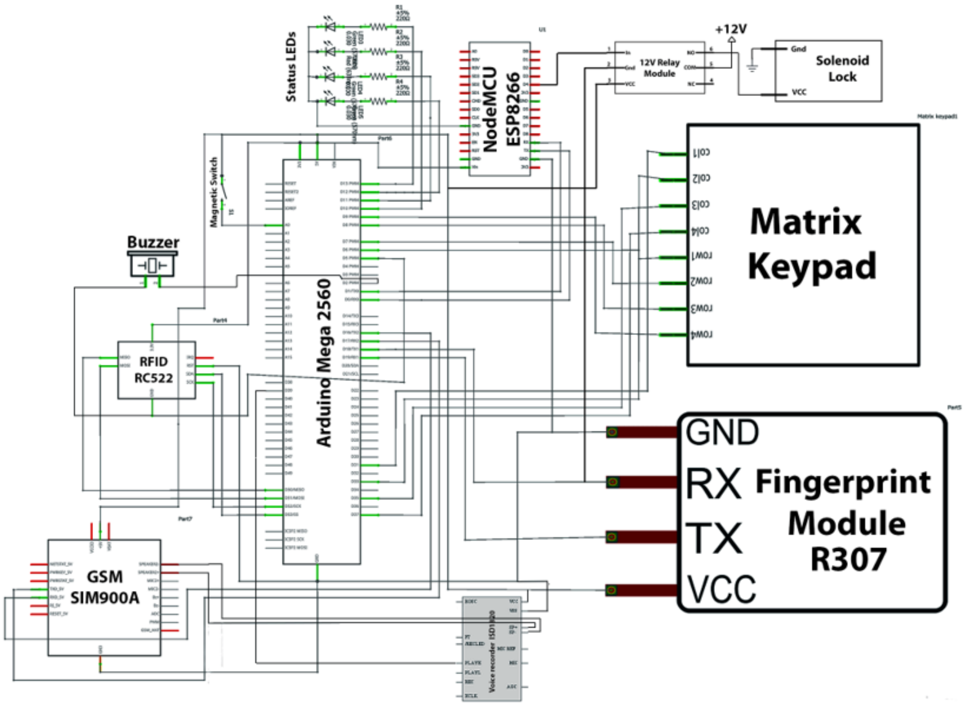


Figure 13. Proposed Schematic Diagram

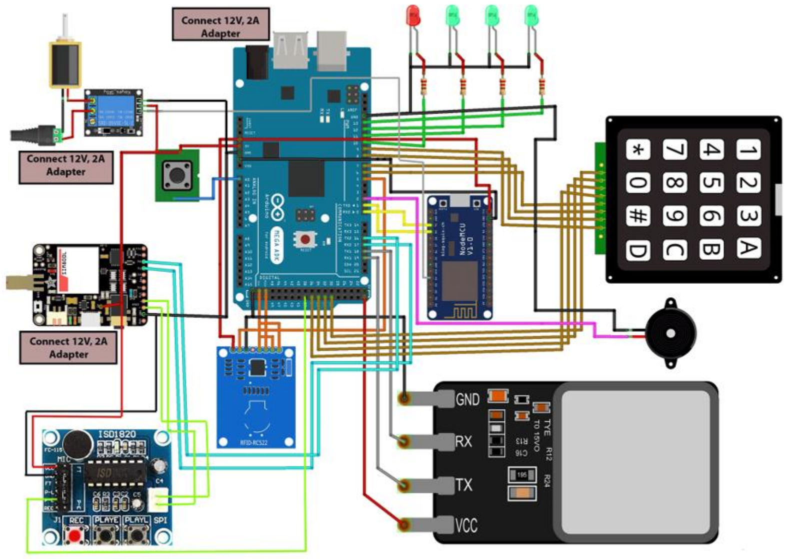
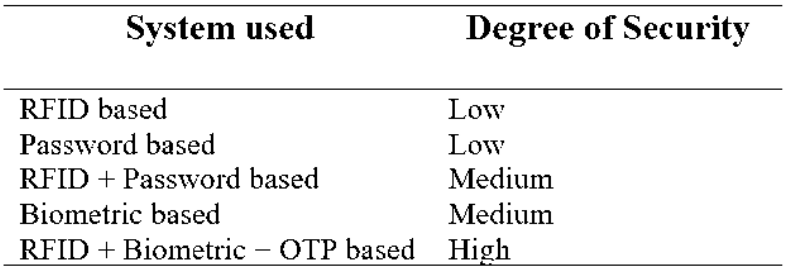


Figure 14. Hardware Wiring diagram

Further the security system with parameters like security level, RFID etc have been estimated with two different approaches. It can be seen that the estimated time required to hack the System is very low. The security breaching is also very low. The system is also tested with passwords of various combinations as seen from table 9. A high level of security is ensured when RFID, Biometric and OTP are combined.

Table 8. Degree of secrutiy



System used	Degree of Security
RFID based	Low
Password based	Low
RFID + Password based	Medium
Biometric based	Medium
RFID + Biometric − OTP based	High

Table 9. Security Level Estimation

S. No	Security System	Estimated Time Requied To Hack The System	System Breaching
1.	Security level	Low	Low
2.	RFID	Few Minutes	Could be Breached
3.	Password contains 0-9 &Aa-Zz	Within 1 minute	Could be Breached
4.	Password contains 0-9 &Aa-Zz and Special Characters *@#$%	More than 3 minutes	Could be Breached

5. Conclusions

The suggested system provides features for owner alert, theft prevention, and maintaining the safety of businesses, residences, etc. The anti-theft security system can be solved with multi-level protection, which offers a very safe and dependable solution.

The provided security system satisfies all relevant requirements. The technical advantages of this security system are improved. The upgraded multi-level system was researched and made to incorporate the technologies of the RFID tag, matrix keypad, biometrics, and GSM. This technology gives improved advantages in internet of things connectivity devices, making it suitable for usage in locations requiring extraordinary security. This security technology has the potential to reduce costs even more.

Authors’ Contributions

Conceptual design: Kishore Balasubramanian and Umamaheswari. Methodology: Ishwarya Niranjana M. Data Curation and original writing: Dhanu Aravinth K. Implementation and validation: Karthik V. Reviewing and Editing: Padmanabhan V K. All authors read and approved the final manuscript.

Competing Interests

The authors declare that they have no competing interests.

References

[1]. M. M. Abdulwahid, M. S. Al-Hakeem, M. F. Mosleh, R. A. Abd-alhmeed, “Investigation and Optimization Method for wireless AP Deployment Based Indoor Network,” *IOP Conference Series: Materials Science and Engineering*, vol. 745, no. 1, pp. 012031, 2020. https://doi.org/10.1088/1757-899x/745/1/012031

[2]. M. M. Abdulwahid, M. S. Al-Hakeem, M. F. Mosleh, R. A. Abd-alhmeed, “Optimal Access Point location algorithm based real measurement for indoor communication,” *Proceedings of the International Conference on Information and Communication Technology*, 2019. https://doi.org/10.1145/3321289.3321300.

[3]. S. Anand, S. R. Shenoy, “Efficient model for Automated Home Management System,” *2020 International Conference on Emerging Trends in Information Technology and Engineering*. https://doi.org/10.1109/ic-etite47903.2020.489.

[4]. R. Bhatt, K. Thakkar, H. Kanzariya and S. Iyer, “3 Tier Bank Vault Security,” *2018 International Conference on Smart City and Emerging Technology (ICSCET)*, Mumbai, India, 2018. pp. 1-4, https://doi.org/10.1109/ICSCET.2018.8537311.

[5]. L. Jesusimo, Dioses Jr, “AndroiDuino-Fan: A speech recognition fan-speed control system utilizing Filipino voice commands,” *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 3, pp. 3042-3047, 2020. https://doi.org/10.30534/ijatcse/2020/84932020.

[6]. K. Fan, W. Jiang, H. Li, and Y. Yang, “Lightweight RFID protocol for medical privacy protection in IoT,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 4, pp. 1656-1665, 2019. https://doi.org/10.1109/tii.2018.2794996.

[7]. V. J. Govindraj, P. V. Yashwanth, S. V. Bhat, and T. K. Ramesh, “Smart Door Using Biometric NFC Band and OTP Based Methods,” *2020 International Conference for Emerging Technology (INCET)*, https://doi.org/10.1109/incet49848.2020.9153970.

[8]. S. Goyal, P. Desai, and V. Swaminathan, “Multi-level security embedded with Surveillance System,” *IEEE Sensors Journal*, vol. 17, no. 22, pp. 7497-7501, 2017. https://doi.org/10.1109/jsen.2017.2756876.

[9]. A. Gupta, P. Medhi, S. Pandey, P. Kumar, S. Kumar, H. P. Singh, “An efficient multistage security system for user authentication,” *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, 2016. https://doi.org/10.1109/iceeot.2016.7755291.

[10]. M. H. Hersyah, D. Yolanda, and H. Sitohang, “Multiple Laboratory Authentication System Design Using Fingerprints Sensor and Keypad Based on Microcontroller,” *2020 International Conference on Information Technology Systems and Innovation (ICITSI)*, 2020. https://doi.org/10.1109/icitsi50517.2020.9264969.

[11]. M. Imran, A. Uddin, F. Rafath, M. Osman, A. Sultana, and K. Srikanth, “Real Time Application of Advanced Exam Paper Leakage Detection and Alert System with Theft Protection,” *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)*, pp. 421-427, 2020. https://doi.org/10.1109/icoei48184.2020.9142950.

[12]. A. Jacobsson, M. Boldt, and B. Carlsson, “A risk analysis of a smart home automation system,” *Future Generation Computer Systems*, vol. 56, pp. 719-733, 2016. https://doi.org/10.1016/j.future.2015.09.003.

[13]. S. A. Jamal, A. A. Ibrahim, M. M. Abdulwahid, and N. B. Mohamad wasel, “Design and implementation of Multilevel Security Based Home Management System,” *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 4, pp. 5716-5720, 2020. https://doi.org/10.30534/ijatcse/2020/224942020.

[14]. A. T. Noman, S. Hossain, S. Islam, M. E. Islam, N. Ahmed, and M. A. Chowdhury, “Design and Implementation of Microcontroller Based Anti-Theft Vehicle Security System Using GPS, GSM and RFID,” *2018 4th International Conference on Electrical Engineering and*

Information & Communication Technology (ICEEiCT), pp. 97-101. https://doi.org/10.1109/ceeict.2018.8628051.

[15]. S. Shukla, A. Patil, and B. Selvin, "A Step Towards Smart Ration Card System Using RFID & IoT," *2018 International Conference on Smart City and Emerging Technology (ICSCET)*, pp. 1-5, 2018. https://doi.org/10.1109/icscet.2018.8537337.

[16]. I. A. Taha and H. M. Marhoon, "Implementation of controlled robot for fire detection and extinguish to closed areas based on Arduino," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 16, no. 2, pp. 654-664, 2018. https://doi.org/10.12928/telkomnika.v16i3.8197.

[17]. A. Z. Tahmidul Kabir, M. Jubaer Islam Khan, A. M. Mizan, N. Debnath, M. H. Rahman, M. Tanvir Sadik, N. Zinnurayen, and A. J. Ta-sin, "Smart system integration of Question Paper Security System," *2020 17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, 2020. https://doi.org/10.1109/ecti-con49241.2020.9158284

[18]. A. Z. Tahmidul Kabir, N. Deb Nath, U. R. Akther, F. Hasan, and T. I. Alam, "Six tier multipurpose security locker system based on Arduino," *2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT)*, 2019. https://doi.org/10.1109/icasert.2019.8934615.

[19]. K. Tshomo, K. Tshering, D. Gyeltshen, J, Yeshi, and K. Muramatsu, "Dual Door Lock System Using Radio-Frequency Identification and Fingerprint Recognition," *2019 IEEE 5th International Conference for Convergence in Technology (I2CT)*. pp. 1-5, 2019. https://doi.org/10.1109/i2ct45611.2019.9033636.

[20]. N. Wang, A. Pan, and L. Wei, "Design and implementation of Intelligent Home Management System based on Wireless Control Module," *Journal of Physics: Conference Series*, vol. 1237, no. 4, pp. 042059, 2019. https://doi.org/10.1088/1742-6596/1237/4/042059.