Asian Journal of Applied Science and Technology (AJAST)
Volume 8, Issue 1, Pages 01-13, January-March 2024

Revolutionizing Home Security: A Comprehensive Overview of an Advanced RFID Door Lock System for Keyless Access and Smart Home Protection

Mohankumar A.[1*], Irfan Ahamath M.[2] & Gowtham R.[3]

[1-3]*UG Scholar, IFET College of Engineering, Villupuram, Tamilnadu, India. Email: mohankumar071104@gmail.com**

DOI: https://doi.org/10.38177/ajast.2024.8101

Article Received: 12 November 2023 *Article Accepted: 18 January 2024* *Article Published: 27 January 2024*

ABSTRACT

The abstract presents a cutting-edge RFID door lock system that does away with traditional physical keys to improve home security. The system uses state-of-the-art components, such as an RFID (Radio-Frequency Identification) reader and an Arduino microcontroller, to provide a safe, keyless access option for homes. This technology provides homes with more protection and convenience, which is a comfort in a world where theft and unwanted access are ongoing issues. Conventional keys are not the best option for home security because they can be stolen, lost, or duplicated. By using customized RFID cards or key fobs, the RFID door lock system, on the other hand, streamlines the entry procedure while significantly lowering the possibility of unwanted access. An RFID reader module, an Arduino microcontroller, and an electronic locking mechanism are the three most crucial parts of the system. Once the authenticity of the card has been confirmed by the RFID reader, the Arduino microcontroller will utilize the obtained data to initiate the lock. Additionally, the system can be improved with features like smartphone applications for remote access control, which let homeowners monitor and grant access from a distance. This RFID door lock system has many advantages for homeowners, including strong security features, user-friendliness, and the capacity to monitor access events. These features provide homeowners with convenience and peace of mind. RFID-based security systems are an important development in the rapidly developing field of smart home technology.

Keywords: Radio-Frequency Identification; Home Security; Arduino Microcontroller; Smartphone Applications.

1. Introduction

Using cutting-edge technologies into home security systems has become essential to bolstering our living areas' security in this constantly changing field. At the nexus of creativity and usefulness is the Radio Frequency Identification (RFID) door lock system, which is driven by the adaptability of Arduino [1]. By introducing a smooth, keyless access system that blends the accuracy of RFID technology with the versatility of Arduino microcontrollers, this system redefines conventional door locking systems.

Home security has historically depended on mechanical locks and keys, but the RFID door lock system changes this idea. This system provides a safe, contactless way to manage access by integrating RFID technology, which uses electromagnetic fields to identify and track tags attached to things [2]. The popular open-source Arduino microcontroller platform acts as the brains of the system, coordinating the physical door lock actuation and organizing the authentication procedure.

With the help of this revolutionary integration, homeowners may improve their security infrastructure with a cutting-edge, effective solution. The RFID door lock system makes sure that only people who are permitted and have RFID tags or cards can enter the building [3]. This enhances home security by doing away with the need for conventional keys and adding a level of complexity and flexibility. They combine security and accessibility to offer a complete answer to home security requirements. The RFID door lock system powered by Arduino is a shining example of innovation and dependability in a time when security is of the utmost importance. Driven by the demand for a smooth, high-tech solution for home security, this system gets rid of the weaknesses in conventional locks [4]. The promise of RFID authentication and keyless entry not only improves convenience but completely changes the way our homes are secured. Because of its open-source philosophy, Arduino encourages people to

take ownership of their security by offering an easily customizable and user-friendly platform that combines state-of-the-art RFID technology with a do-it-yourself attitude [5]. This reinforces the idea that comprehensive home security is not only possible but also affordable for everyone.

The goal of utilizing Arduino to implement an RFID door lock system for home security is to create a safe and sophisticated access control system that improves the general security of residential areas [6]. The system attempts to do away with traditional keys by combining RFID technology with Arduino microcontrollers, providing a reliable and easy- to-use keyless entry solution. The main objectives are to manage the authentication process with ease by using Arduino's capabilities, to provide customizable access control, and to guarantee that only authorized users with RFID card [7]. The system also intends to include features like security logging and possible integration with smart home systems, raising the bar for contemporary home security that places an emphasis on effectiveness, user- friendliness, and adaptability.

2. Literature Survey

The Arduino Uno board was used to develop a home automation system, and the AT Mega 328 microcontroller was used to manage the system. The system was designed to incorporate an automated door lock and password authentication. The first thing that is done is to compare the user's combination with a password that is stored in the memory of the system, which is a password that has been predetermined [8]. If a user's combination matches the password, then the user's door, light, and fan will all be able to be unlocked immediately. Additionally, the system was designed to be locked with a single key press. An Arduino UNO microcontroller board is used in this system to interface the various hardware peripherals, created a deadbolt-sensing electronic combination door lock [9]. The electronic combination door lock combines a manually actuated deadbolt on the door with an outer turning knob that can be used in conjunction with a push keyboard.

The keyboard's electronic circuitry compares an input code to a stored code; if the two codes are the same, the stored code is used to generate an enabling signal. When the door is locked, it is prohibited from manually turning the outer turning knob to release the deadbolt [10]. It is possible to manually retract the deadbolt once the low-energy enabling signal has released the restraint that was placed on the outer knob. It is possible to locate the clutch disk on the interior of the door as well. A hub drive and driver disk are responsible for returning the rotating motion of the clutch disk to the door, where it is able to reach the mortise latch hub that is located within the mortise housing of the door [11]. There are numerous instances in which the electrical components of the cardboard reader and clutch assembly are neatly housed inside the interior housing assembly. Additionally, the surface of the door on the inside is also contained within this configuration. Therefore, the clutch disk and assembly are frequently thrown out of the housing [12]. This is because of the reason stated above.

The usage of solenoid lock needs more power supply and it leads to power in availability while frequent usage. In this project they used multiple sensors and components to form their circuit and it leads to make more compliments in creating models [13]. Complicated circuits and need programming knowledge due to usages of several highly modified components. It became highly complicated is any damage or error occurs while importing program and functioning the system. GSM module is complicated to use in security system. It is hard to combine both RFID and

Finger print sensor both in same circuit. They find some difficulties in accessing both identifiers. It is stated in [14] that a biometric security system was developed to automatically unlock doors through the use of fingerprint recognition. The data was stored in Secure Digital (SD), and instructions for adding new fingerprints and removing old ones were written in C++. Through the utilization of the information that is stored in the Secure Digital (SD) drive, it is possible to maintain a record of the real-time clock-in hours of the employees [15]. The components that comprised the system were as follows: an electric plate, an Arduino, a biometric sensor, pushbuttons, a 16x2 LCD screen, a relay, a real-time clock, and internal memory of the device.

The development of a smart card system for the purpose of automatically unlocking doors was stated as the objective in [16]. The user is required to enter both a smart card number and a personal identification number (PIN) in order to gain access to this system. Whenever the microcontroller has completed its verification of the card that has been inserted into the reader, the user will be prompted to enter a pin code on the LCD unit [17]. Under those circumstances, the message "INVALID CARD" will be displayed. A message that reads "TIME OUT, PLEASE REMOVE YOUR CARD" will appear on the LCD screen in the event that the user does not enter the pin code within the allotted amount of time. Once the PIN has been validated, the system will display the message "ACCESS GRANTED" and activate the relay that controls the door [18]. The user will then be presented with a prompt to remove the card from their wallet. In the event that the timer goes off, the door will automatically close. The message "REMOVE YOUR CARD, INVALID PASSWORD" will be displayed on the LCD screen in the event that the pin code authentication technique is unsuccessful [19].

The study included a large number of significant elements [20]. These included two switching transistors, two 10A - 12VDC relays, a 12V DC motor, a rack and pin system, a 16x2 LCD screen, a keypad module, a power supply unit with three regulated units (12V, 5V, and 3.3V), and an ID credential and reader. In this process, a rack and pinion mechanism was also utilized.

The Internet of Things (IoT) was utilized by the researchers in [21], [22] in order to develop the model for the Smart Door System. This particular model is equipped with a dual authentication system that works with fingerprint modules, and it is designed for use in lodging establishments such as hotels and guesthouses. Comparatively, the proposed system architecture design provides a description of the individual modules, while the circuit diagram illustrates how the various modules are connected to one another [23]. The prototype of the software is initially implemented by employing the programming language known as C.

According to the findings of their research, the authors of [24] intended to create a door lock security system that was based on automated speech recognition. The task that was embarked upon had the objective of identifying particular users and granting authorization to certain individuals. The Mel-frequency Cepstrum Coefficients (MFCC) feature extraction method was utilized in order to train the system. The system was trained using the speech signals of five different individuals [25].

One of the subsets of technologies that are used in smart homes, the utilization of Bluetooth on mobile devices, was the focus of a study that was published in [26]. Furthermore, it makes use of open-source software platforms such as Android and Arduino, both of which are freely accessible to the public. A system that is capable of automating door

locks through the use of Android smartphones that are based on Bluetooth has been designed and prototyped [27]. Starting off, the text provides a description of the process of developing the software as well as the configuration of the hardware. The next section of the document provides an outline of the blueprints for a smartphone application that can lock or unlock the door using Bluetooth technology [28]. The hardware that makes up this system consists of a solenoid, an Arduino microcontroller, Bluetooth, an Android smartphone, and the system itself.

3. Proposed Methodology

3.1. Architecture Design

The integration of essential components is necessary for the circuit design of an Arduino- powered RFID door lock system in order to create smooth control and communication. As the central processing unit (CPU), the Arduino board serves as the circuit's beating heart. In order to enable power and data transmission, it is necessary to physically connect the RFID reader to the Arduino. This reader is responsible for reading data from RFID cards or tags. Connected to the digital pins of the Arduino are the RST, SDA, MOSI, MISO, and SCK interfaces. On the other hand, the power supply is connected to pins such as VCC and GND. All of the physical lock mechanisms, whether they are solenoid locks or servo motors, need to be connected to the Arduino simultaneously for power, ground, and control in order to achieve synchronization with the output of the RFID reader. Figure 1 provides a visual representation of the architecture of the system that is being proposed.

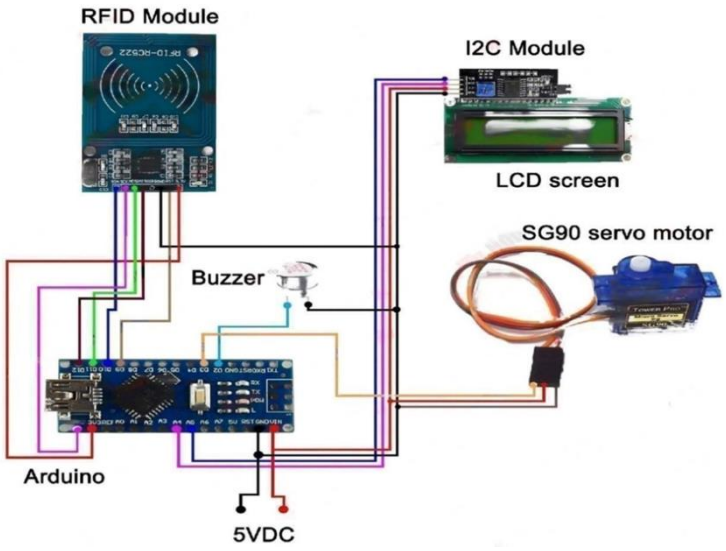

Figure 1. Hardware Design of Proposed Solution

It’s crucial to establish proper voltage levels throughout the circuit to prevent damage to components. The comprehensive design considerations encompass voltage compatibility, pin configurations, and the synchronization of RFID reader and lock control, culminating in a secure and efficient RFID door lock system with Arduino at its core.

3.2. Circuit Operation

"Welcome, put your card" was shown on the LCD. Following that, the RFID reader scans the RFID tag when it gets closer to it. In that instance, the LCD shows it as "scanning." The door lock is then pulled back and the servo motor

starts if the RFID tag is valid. A buzzer will then sound. It reads "Door is Open" on the LCD. The servo motor will advance the lock when the RFID tag is brought closer to the RFID reader once more and it detects the correct tag. "Door is locked" is shown on the LCD. The program indicates "Wrong card" on the LCD and the device if the incorrect RFID tag is used alarm sound comes from buzzer. The RFID tag, RFID reader, and backend are the three fundamental parts of any RFID system, including the one described in this paper. The UUID of the RFID tag had to be added to the code. Rectangular in shape, matrix keypads, also known as thin membrane keypads, are constructed on a film membrane. We have utilized an Arduino RFID reader library that is available.

The door lock's behavior can be managed by the user by sending a message to the board. When a user sends the word "close" to the board, the lock will halt operating normally and wait for a confirmation message with the word "open" in it. Following the successful scanning of the appropriate tag, the homeowner will receive a message conveying confirmation that the door has been opened. The system can be stopped by the owner by sending an Arduino "close" message, and it won't resume its regular operation until an Arduino "open" message is received.

3.3. Component Description

3.3.1. Arduino UNO

When it comes to Arduino microcontroller boards, the Uno R3 is among the most popular options. 2011 saw the release of the third iteration of the Arduino board, which was the most recent version. The most important advantage of this board is that it has a microcontroller that can be replaced in the event that it experiences a malfunction. The most notable characteristics of this board are its detachable design, its availability in dual-inline-package (DIP) form, and its ATmega328 microcontroller. The ATmega328P serves as the basis for the Arduino Uno R3, which is an example of a microcontroller board that falls into this category. There are a number of components that are included in the device. These components include an ICSP header, a power connector, a USB port, six analogue inputs, fourteen digital input/output pins (six of which can function as PWM outputs), a sixteen MHz ceramic resonator, and a reset button.

3.3.2. Programming in Arduino Uno R3

Programming an Arduino Uno R3 can be accomplished through the use of the Arduino IDE software. The microcontroller of the board comes with a piece of software known as a boot loader already installed on it. A separate hardware programmer is no longer required in order to add new code to the microcontroller, as this capability has been made available. By transferring the code through the header and then utilizing the In-Circuit Serial Programming method, it is possible to program the microcontroller without the need for the boot loader to be utilized.

3.3.3. Servo Motor

Servo mechanisms, which are among the most fundamental types of electronic motors, make it possible to operate servo motors with a high degree of precision. When a direct current motor is coupled to a servomechanism, it is referred to as a DC servo motor. This type of motor functions as a controlled device. An alternating current (AC) servo motor is a type of servo motor that operates on alternating current only. Pulse width modulation, also known

as PWM, is a technique that involves an electrical pulse of varying width being transmitted over the control line in order to regulate the movement of servos. In addition to the repetition rate, there is also the pulse width and the pulse height. The majority of the time, servo motors is only capable of turning a maximum of ninety degrees in either direction, for a total of one hundred eighty degrees of movement. We refer to the motor as being in its neutral position when the potential for rotation of the servo is equal in both the clockwise and counterclockwise directions. A servo that is in a stationary state will resist the urge to move away from its current position when it is subjected to an external force by virtue of the presence of the force. The torque rating of a servo is a significant indicator of the maximum force that it is capable of producing. Servos are unable to maintain this position for an indefinite amount of time. To ensure that the servo remains in the same position, it is necessary to perform the position pulse multiple times. Using the pulse width modulation (PWM) signal, the timing of the pulses that are transmitted to the motor through the control wire is responsible for regulating the movement of the rotor to the desired position. The full range of motion for a servo motor is in the direction of ninety degrees, beginning with the neutral position. PWM, which stands for pulse width modulation, is one method that can be utilized to manage servo motors. That power comes from the wires that control the device. Every aspect of the pulse, including its width, height, and repetition rate, is present and can be accounted for. A pulse is anticipated by the servo motor at intervals of twenty milliseconds.

3.3.4. LCD Display with I2C Module

When it comes to solid-state liquid crystal display devices, the modulation of light is controlled by liquid crystals. It is possible to make use of a screen or a visual interface. Unlike traditional computer displays, liquid crystal displays (LCDs) do not generate light, so they are able to display any image. In this particular design, a "16 x 2" LCD is being utilized. Input ports D0, D1, D2, D3, D4, D5, D6, and D7, anode "A," cathode "K," allow "E," reset "R/S," read and write "R/W," and ground Vss are all included. Additionally, the voltage supply pin Vdd is also included. The LCD pins have the functions as shown in table 1. The connection involves several pins for power, ground, data, and control signals.

Table 1. Pin Configuration of LCD

Parameter	**Representation**	**Corresponding Pins**
Power Supply	Vss & Vdd	Pin 1 & Pin 2
Ground	GND	Pin
Instructions	A4 & A5	Pin SCL & Pin SDA

A cell that is integrated into another cell is referred to as an inter-integrated cell. Indeed, it is a type of bus as well-known. All of this was developed by Philips Semiconductors. I2C, which stands for Inter-Integrated Circuits, is a synchronous, single-ended packet switched bus that is capable of supporting a large number of masters and slaves. The Serial Clock Line (SCL) and the Serial Data Line (SDA) is the two bidirectional open collector or open drain lines that are utilized by the I2C protocol. Both of these lines are connected to resistors with the same purpose. It is acceptable for a system to use any voltage that it is capable of using, even though the most common voltages are

+5 V and +3.3 V. There are a total of twenty male pins, sixteen of which are oriented vertically, and four of which are oriented horizontally. Two of the four pins, also known as SDA and SCL, are utilized in order to establish a connection between the 16x2 LCD and the 16 pins. The clock pin is designated SCL, and the serial data pin is SDA, the remaining two power supply pins (ground and Vcc). By turning this POT, we can adjust the LCD display's contrast. Moreover, a fixed number is present on the module. The LCD display will turn off its backlight when the jumper is removed.

3.3.5. RFID Reader and TAG

Whether it's permanently installed or easily transportable, an RFID reader is a network-connected device. These signals are sent to the Arduino Uno, which manages the locking mechanism's operation. As seen in the figure below, an RFID label or transponder (tag) is a device that reads and stores information electronically for up to a few meters. A transponder is used in radio frequency identification (RFID) to capture and store long- distance data. An RFID card or label is something that can be applied to a product, animal, or even a person in order to identify them through the use of radio frequency transmission at 125 kHz, 13.65 MHz, or 800-900 MHz. It transmits signals that activate the tag using radio waves.

RFID readers can automatically collect data from RFID tags without requiring line-of-sight or manual intervention. This automation improves efficiency and reduces the need for human involvement in data collection processes. RFID readers can quickly read multiple tags simultaneously, enabling rapid data transfer. This is particularly useful in scenarios where quick and accurate data collection is essential, such as in inventory manage mentor supply chain logistics. RFID tags come in various forms, including ruggedized and durable options suitable for harsh environments. This durability ensures that the tags can withstand challenging conditions, making them suitable for use in industries such as manufacturing, logistics, and agriculture.

3.3.6. Buzzer

By connecting the buzzer to an NPN transistor (BC547), the audio signal is amplified. This is accomplished by using the buzzer. Following the connection of a resistor with a value of 220k ohms to the base of the BC547 transistor, the microcontroller is then connected to the transistor through its analog input/port. The primary purpose of this buzzer is to generate an alarm whenever an RFID card does not meet the criteria that we have established. Whenever the tag does not correspond to the tags that have been programmed, the buzzer will continue to beep, and the LCD screen will display the message "Access Denied".

3.3.7. Jumper Wire

A wire is considered to be a jumper wire when it has a pair of pins attached to either end of it. A jumper wire is also known as a jumper, jumper cable, cable, DuPont, and jumper. These are just some of the common names for this type of wire. Connecting electronic components or a testing circuit can be accomplished with the help of jumper wires in situations where soldering is not an option. There is no difference between two jumper wires that belong to the same color family if they are very similar to one another. This is because jumper wires come in such a wide variety of colors. Generally speaking, there are three primary types of jumper cables. The male jumper wires have pins on the ends, which makes it simple to attach them to a variety of different components. On the other hand,

female jumper wires do not have this pin attached to these wires. Jumper wires that connect males to males are used for the vast majority of component connections.

4. Result and Discussion

The door is first secured with a lock before being opened. It is necessary for the user to scan the tag in order to receive access to the door. Figure 2, which can be found further down on this page, depicts the initial point of the system.

Figure 2. Door Lock System

The following are two outcomes that could occur as a result of scanning the tag: Figure 3 and Figure 4. When one of these scenarios occurs, the user is notified by the system through the LCD screen whenever the tag corresponds to the information being displayed.

Figure 3. Door Unlock System

In the event that the tags do not correspond, the user will be able to view a notification on the LCD screen, and the individual who is attempting to open the door will be denied entry.

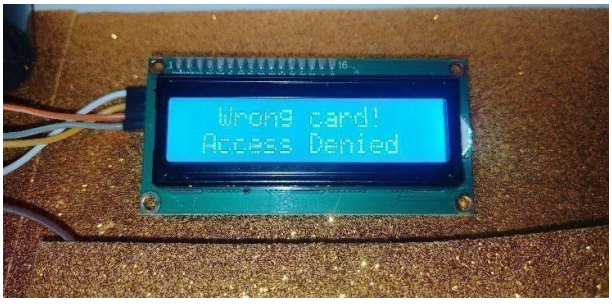

Figure 4. Message Informing the Tag Being the Wrong One

Like the way RFID responds when it detects a registered serial number. The Arduino Mega will react rapidly, support more users, and have push button functionality. This gadget is simple to use and helpful for people who are

keeping items in the room, according to the testing results and analysis. Otherwise, the Arduino program will run commands directly to the proximity sensor as input and activate the buzzer as an indicator if the door is forced open.

Valid and invalid cards were used to test the system; when a valid card is inserted, the electromagnetic door lock opens and the LCD shows "ACCESS GRANTED." However, if the card is invalid, the door lock stays locked, the LCD shows "DECLINED," and the GSM Module makes a call to the administrator. The Buzzer and Delay Sound based on the RFID Card is shown in Table 2.

Table 2. Buzzer and Delay Sound Based on RFID Card

RFID Tag Number	Delay Applied	Buzzer Sound
AUTHENTICATEDTAG	200	HIGH
WRONG TAG	200	HIGH \ LOW
WRONG TAG	200	HIGH \ LOW

When an RFID tag is detected by the reader, the door will open and close automatically after a certain amount of time has passed. This will occur after the door has been detected. The database is first searched in this application to find information about user authentication. In order to prevent unwanted entries, the door won't open if the user has no prior records in the database.

To tabulate results or outcomes, you might consider tracking the performance, success, or status of various components or aspects of the RFID-based door lock system we can use a table with measurable metrics. The Measurable Metrics of RFID-Based Door Lock System is shown in Table 3.

Table 3. Measurable Metrics of RFID-Based Door Lock System

S. No.	Metric/Outcome	Value/Measurement
1.	RFID Tag Recognition Rate	98%
2.	Unauthorized Access Attempts	1
3.	Servo Motor Reliability	95%
4.	Power System Uptime	99%
5.	User Interface Feedback Speed	1.5 seconds
6.	Anti-Theft Measures Success	99%
7.	Integration with Home Security	97%
8.	System Response Time	0.3 seconds
9.	Environmental Robustness	-10 to 45 degrees Celsius

Using an RFID door lock system in home security, especially with Arduino, offers several advantages for making your locks keyless and enhancing theft prevention. RFID technology is more secure than traditional locks and keys

since RFID cards or tags are difficult to replicate. It is an additional layer of protection. When there is no requirement for physical keys, the likelihood of unauthorized key duplication is significantly reduced. You can program RFID cards or tags with specific permissions for different users, allowing you to control who has access to your home. Arduino-based systems can be integrated with other IoT devices and smart phones, enabling you to monitor and control your locks remotely. RFID systems can log access attempts, helping you track who entered your home and when, which can be useful in case of security breaches or theft. RFID systems provide quick and convenient access, as users only need to present their RFID card or tag to unlock the door. Visible RFID readers and the knowledge of a keyless system can act as a deterrent to potential thieves. Arduino allows for flexibility and integration with other smart home devices and systems, creating a holistic security setup. RFID locks are generally low-maintenance, reducing the need for regular lock replacements and rekeying. While there may be an initial setup cost, RFID systems can be cost- effective in the long run compared to replacing lost keys and rekeying locks. Overall, RFID door lock systems with Arduino provide an efficient, secure, and convenient way to enhance home security and reduce the risk of theft. However, it's essential to implement such a system carefully to ensure its reliability and effectiveness.

5. Conclusion

The overarching objective of this research is to develop a door lock system that is not only robust but also secure through the use of user-friendly design. The program itself will not be significantly altered if the components are changed to ones of a similar type rather than the original ones. If it is possible to achieve the same functionality in a significantly smaller form factor, such as by utilizing an Arduino Nano board, then its practicality in real-world scenarios will be significantly improved. Comparatively speaking, the lock and key system provides very little protection in comparison to other contemporary security systems. This is due to the fact that it is simple for someone to make duplicate keys without permission. In comparison with the conventional method, RFID cards offer strong authentication. The keypad functions as an additional security measure. The door will stay locked even if the RFID tag is misplaced or ends up in the hands of unauthorized personnel thanks to the keycode. Without a doubt, the most affordable security system available to all users is the lock and key system. While RFID readers and tags are slightly more expensive than lock and key systems, they also offer significantly higher security. When you compare the price of an excellent lock with the cost of an RFID, the cost of the RFID is actually not that high. However, the project is comparatively more expensive than conventional options due to its multiple components. This project could be enhanced by incorporating several features to enhance its user-friendliness. For example, it is feasible to incorporate fingerprint input functionality. Additionally, it is feasible to create an Android application that functions as a client for the project. This app will promptly notify the user in the event that an unauthorized individual enters the room, aside from the legitimate user. Lastly, considering the aforementioned constraints, the project may benefit from some more recent digital technologies such as voiceprint identification, retinal scanning, and iris scanning for user authentication. In this manner, home doors and gates will be able to benefit from more sophisticated, quick, and user-friendly security provided by this Arduino-based door locking system. Important elements of the system include an electronic door lock that is enabled with RFID technology and an Arduino UNO that is protected with a password. Electronic lock systems are significantly superior to mechanical ones when it

comes to safety-related concerns. The purpose of this research was to develop an electronic door lock system with the intention of automating homes. With an Arduino microcontroller serving as the primary controller, the system is equipped. The Arduino is a piece of hardware that is extremely advantageous. It is possible to put them to a wide range of different uses. Additional parts must be added to Arduino in order for it to receive and send data.

Declarations

Source of Funding

The study has not received any funds from any organization.

Competing Interests Statement

The authors have declared no competing interests.

Consent for Publication

The authors declare that they consented to the publication of this study.

Authors' Contributions

All the authors took part in literature review, research, and manuscript writing equally.

References

[1] Okafor, C.S., Nnebe, S.U., Alumona, T.L., Onuzuluike, V.C., & Jideofor, U.C. (2022). Door access control using rfid and voice recognition system. International Journal for Research in Applied Science and Engineering Technology, 10(3): 157–163.

[2] Finkenzeller, K. (2010). RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication. John Wiley & Sons.

[3] Jiji Wiselin, S., Sreeja, B.S., Sureshkumar, K., Joshitha, C., Nandhini, V.I., Shetty, R., Suneri, K., & Yazhini (2015). Design of a novel RF MEMS dual and quad output switches for satellite payload applications. International Journal of Applied Engineering Research, 10(14): 34339–34345.

[4] Sovacool, B.K., & Del Rio, D.D.F. (2020). Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies. Renewable and Sustainable Energy Reviews, 120: 109663.

[5] Stead, M.R. (2020). Spimes: A Multidimensional Lens for Designing Future Sustainable Internet Connected Devices. Lancaster University, United Kingdom.

[6] Rao, A.K., & Reddy, T.R. (2022). A comprehensive study on the development of an automated RFID-based security system for residential and industrial applications. Turkish Journal of Computer and Mathematics Education, 13(03): 1542–1549.

[7] Suresh Kumar, K., Gayathri, G., Arthi, A., & Sathishkumar, V. (2023). Artificial Intelligence Supported Instinctive Irrigation System (IIS) Using Arduino and Zigbee in Wireless sensor Network. International Journal of Advanced Research Trends in Engineering and Technology, 10(6): 1–11.

[8] Ugwoke, F., Etuk, E., Iroegbu, C., & Nwabueze, S. (2022). A Bluetooth Enhanced Smart Home Automation System Using Arduino Board. Rivers State University Journal of Biology & Applied Sciences, 2(2).

[9] Makanjuola, P.O., Shokenu, E.S., Araromi, H.O., Idowu, P.O., & Babatunde, J.D. (2022). An RFID-Based Access Control System Using Electromagnetic Door Lock and an Intruder Alert System. Journal of Engineering

[10] Ho, G., Leung, D., Mishra, P., Hosseini, A., Song, D., & Wagner, D. (2016). Smart locks: Lessons for securing commodity internet of things devices. In Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, Pages 461–472.

[11] Epstein, D.M. (2007). Lincoln and Whitman: Parallel Lives in Civil War Washington. Random House.

[12] Senatore, A. (2009). Advances in the automotive systems: An overview of dual-clutch transmissions. Recent Patents on Mechanical Engineering, 2(2): 93–101.

[13] Schemmel, J., Brüderle, D., Grübl, A., Hock, M., Meier, K., & Millner, S. (2010). A wafer-scale neuromorphic hardware system for large-scale neural modeling. In 2010 IEEE International Symposium on Circuits and Systems (ISCAS), Pages 1947–1950, IEEE.

[14] Kabilan, M., Manikandan, V., & Suresh Kumar, K. (2023). Synergizing IoT, IoE, GSM Technology, and Deep Learning Models for Advanced Security Applications: A Comprehensive Overview. Irish Interdisciplinary Journal of Science & Research, 7(4): 38–46.

[15] Yasmeen, N., & Doss, S. (2023). Intelligent Systems Powered Hourly Attendance Capturing System. In 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI), Pages 1536–1541, IEEE.

[16] Khalimov, R., Rakhimbayeva, Z., Shokayev, A., Kamalov, B., & Ali, M.H. (2020). Development of intelligent door locking system based on face recognition technology. In 2020 11th International Conference on Mechanical and Aerospace Engineering (ICMAE), Pages 244–248, IEEE.

[17] Bhargava, A., & Ochawar, R.S. (2014). Biometric access control implementation using 32 bit arm cortex processor. International Conference on Electronic Systems, Signal Processing and Computing Technologies, Pages 40–46, IEEE.

[18] Frederick, O.E., & Olaiya, O.O. (2020). Design of a Hybridized Security Door System with Password-Based Access and SMS Notification. FEPI-JOPAS, 2(2): 11–22.

[19] Adetoyi, O.E. (2017). Development of Smart Card Door Access Control System. International Journal of Electronics Communication and Computer Engineering, 8(1): 41–44.

[20] Mishra, J. (2018). Development of a Digital Rain-Sensing Irrigation Pump Controller and an Android Enabled Bluetooth Paddlewheel Flowmeter. Doctoral dissertation, University of Arkansas.

[21] Akanbi, C.O., Ogundoyin, I.K., Akintola, J.O., & Ameenah, K. (2020). A prototype model of an IoT-based door system using double-access fingerprint technique. Nigerian Journal of Technological Development, 17(2).

[22] JosephNg, P.S., Brandon Chan, P.S., & Phan, K.Y. (2023). Implementation of Smart NFC Door Access System for Hotel Room. Applied System Innovation, 6(4): 67.

[23] Liu, B., Duan, S., & Cai, T. (2010). Photovoltaic DC-building-module-based BIPV system—Concept and design considerations. IEEE Transactions on Power Electronics, 26(5): 1418–1429.

[24] Jayakumar, A., Suresh Kumar, K., Ananth Kumar, T., & Sundaresan, S. (2021). Design of MIMO Cylindrical DRA's Using Metalstrip for Enhanced Isolation with Improved Performance. In Contemporary Issues in Communication, Cloud and Big Data Analytics: Proceedings of CCB 2020, Pages 149–158, Singapore: Springer Singapore.

[25] Pawar, M.D., & Kokate, R.D. (2021). Convolution neural network based automatic speech emotion recognition using Mel-frequency Cepstrum coefficients. Multimedia Tools and Applications, 80: 15563–15587.

[26] Saleem, Yasir, Noel Crespi, Mubashir Husain Rehmani & Rebecca Copeland (2019). Internet of things-aided smart grid: technologies, architectures, applications, prototypes, and future research directions. IEEE Access, 7: 62962–63003.

[27] Jabbar, Waheb A., Tee Kok Kian, Roshahliza M. Ramli, Siti Nabila Zubir, Nurthaqifah S.M. Zamrizaman, Mohammed Balfaqih, Vladimir Shepelev & Soltan Alharbi (2019). Design and fabrication of smart home with internet of things enabled automation system. IEEE Access, 7: 144059–144074.

[28] Arifin, R.D.H., & Sarno, R. (2018). Door automation system based on speech command and PIN using Android smartphone. In 2018 International Conference on Information and Communications Technology, Pages 667–672, IEEE.