

Double-Layered Authentication Door-Lock System Utilizing Hybrid RFID-PIN Technology for Enhanced Security [†]

Aneeqa Ramzan ^{1,*}, Warda Farhan ¹, Itba Malahat ¹ and Namra Afzal ²

¹ Faculty of Computer Science and Engineering, Ghulam Ishaq Khan (GIK) Institute of Engineering Sciences and Technology, Topi 23640, Pakistan; warda.farhan1764@gmail.com (W.F.); itbamalahat@gmail.com (I.M.)

² Department of Biomedical Engineering and Sciences, National University of Sciences and Technology (NUST), Islamabad 44000, Pakistan; namra_afzal@uet.edu.pk

* Correspondence: aneeqaramzan@gmail.com

[†] Presented at the 3rd International Conference on Modern Technologies in Mechanical & Materials Engineering (MTME2025), Topi, Pakistan, 16–17 April 2025.

Abstract

Radio frequency identification (RFID) is popular and attaining momentum in manifold sectors, including, but not limited to, pharmaceuticals, retail, defense, transport, healthcare and currently security. Utilizing RFID solely as a solution does not result in effective security. Conventional systems have integrated only one solution, such as GSM, cryptography, wireless sensors, biometrics or a One-Time Password (OTP); however, the security provided is limited since each incorporated technology has its disadvantages. Our paper proposes improving the conventional methods in the field by proposing an intelligent door-lock system prototype implementing two-step authentication, providing double-layered security provisions in, for instance, highly sensitive zones. The suggested technique, firstly based on RFID technology and then a password (PIN) during the authentication process, results in a hybrid system that is more accurate and efficient compared to a traditional, single-method system. The Arduino micro-controller is interfaced with RFID, with a keypad that receives the input to the micro-controller, a Liquid Crystal Display to output the authentication status and finally a motor connected to the door for automation within a limited time-frame. Adding biometric verification, such as fingerprints and face recognition, can enhance the proposed design further by providing an additional layer of security from external intruders.

Keywords: authentication; hybrid; prototype; RFID; UID; SPI; PIN; Arduino; servo motor; LCD; security; IoTs



Academic Editor: Hamza Mohsin

Published: 13 August 2025

Citation: Ramzan, A.; Farhan, W.; Malahat, I.; Afzal, N. Double-Layered Authentication Door-Lock System Utilizing Hybrid RFID-PIN Technology for Enhanced Security. *Mater. Proc.* **2025**, *23*, 19. <https://doi.org/10.3390/materproc2025023019>

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

A variety of conventional safety methods—including security guards, metal detectors and surveillance cameras—are adopted to safeguard valuables and high-security zones, such as bank vaults, scientific chambers and military and intelligence zones. Owing to the increased significance of security, it is incontrovertibly crucial for engineers and scientists to devise novel, intelligent and efficient automated solutions employing identification, authentication and authorization as the access control foundation [1]. Radio frequency identification is a category of automatic identification and capture technology for objects embedded with, for instance, RFID cards or tags. There is no electronic circuit in this chipless communication technology, the design of which is based on a metallic surface's resonance [2,3]. The Internet of Things (IoT), transportation, Supply Chain Management

(SCM) and medicine—fields in which sustained research is being conducted to develop novel technological solutions—comprise the applications of RFID [4]. Traditional door-locks that employed mechanical locking without any security provisions are being replaced by intelligent, mechatronics methodologies, which not only provide security but also aid elderly and disabled individuals living alone [5]. The technique we developed makes use of two distinct security technologies, resulting in a hybrid and efficient door-lock system. The following are the issues with the existing methods for door-lock systems:

- Manual door-locks employ keys that are often difficult to insert/remove from the lock;
- Manual doors sometimes have misaligned door latches;
- Automated, battery-operated doors face failures due to power discharge;
- Some automated door-locks either become stuck or cease to function in scenarios of system glitches;
- Electronic doors can be breached by unauthorized personnel;
- Conventional automated doors employ GSM, resulting in a lack of cost effectiveness;
- Locks based solely on passwords do not provide adequate security.

We have discussed ways to overcome the above stated issues in our proposed solution of a hybrid autonomous door-lock system in the methodology section.

2. The Literature Survey

We have conducted a thorough review of various applications of RFID and its use in lock systems, which are explored in the subsections below.

2.1. Applications of RFID

Divya et al., in [6], delve into RFID technology, emphasizing its role in real-time object monitoring and information communication. A systematic mapping study (SMS) involving 219 rigorously selected studies from various digital libraries explores the multifaceted landscape of research into RFID, revealing the trends, publication patterns and research gaps.

2.1.1. Digital Applications

Haibi et al. introduced RFID technology and its components, including tags, readers and middleware. This paper emphasized the role of middleware in RFID systems, detailing the management functions, presenting the unique BTMiddleware, a lightweight solution comprising a MongoDB NoSQL database for real-time Big Data handling [2]. Rouchdi et al., in [7], elucidate the RFID architecture, components, functions and middleware roles. Subsequently, Role-Based Access Control is explored to fortify the access to RFID data. This study introduces the UIR middleware technique and the BagTrac application, simplifying live visualization and manipulation of the luggage transport process, contributing to refining luggage tracking. In [8], Haibi et al. also aim to improve the traceability of airport baggage by incorporating RFID systems into baggage tracking processes, focusing on the design and implementation of a tracking system which encompasses BTMiddleware and the BagTrac application, enabling users to track their luggage via smartphones. Gabsi et al. present a unique radio frequency identification authentication protocol in [3] based on Elliptic Curve Cryptography (ECC) that addresses the security weaknesses in the existing ECC-based protocols. The protocol proposed here is analyzed rigorously using the AVISPA analysis tool and High-Level Protocol Specification Language (HLPSL).

2.1.2. RFID Tags

In [9], Kusic et al. introduce a low-cost RFID tag designed through ink-jet printing-technology. Operating at 13.56 MHz, the passive RFID tag employs an inductive-capacitive

resonant circuit. Good et al. present a practical implementation of a secure, passive off-the-shelf front-end RFID tag in [10]. The custom 0.18 μm ASIC integrates an ultra-low-power AES design, a unique random number generator and a novel protocol that indicates 64-bit security against various attack methods on analysis. In [11], Haibi et al. focus on two aspects to enhance RFID technology's applicability. Firstly, a metal mountable tag-antenna is designed to cover European (865–867 MHz) and U.S. (902–928 MHz) UHF RFID bands. A cost-effective and easily tunable antenna uses a microstrip configuration with an open bent stub feed-network for conjugate matching with the Monza R6 chip made by Impinj (Seattle, WA, USA) impedance. This RFID middleware architecture leverages Role-Based Access Control (RBAC) and NoSQL databases, enabling efficient access management to RFID data.

2.1.3. Wearable Applications

Khan et al., in [4], present the patterns, fabrication and testing of two chipless octagonal-shaped RFID tags intended for wearable applications. Turner et al., in [12], present a dual-mode RFID tag that features bi-directional communication and data logging functionality and integrates an IC capable of communicating with two SPI peripherals: a pressure sensor and a memory chip. The tag autonomously records pressure data at set intervals, while the bi-directional communication enables wireless data downloading via standard SPI protocols.

2.1.4. Other Applications

In [13], Lee et al. introduce an intelligent RFID-based system combining fuzzy association rule mining and recursive process mining algorithms to connect the production process parameters with product quality. The recursive nature of the approach continually refines the process parameters to enhance the quality assurance. The study [14] by Wang et al. integrates the Internet of Things and Deep Learning principles into research into a tennis robot, analyzing Mask R-CNN and IoT-based RFID for tennis robot positioning. An intelligent real-time image recognition tennis robot is developed to enhance the positioning accuracy and recognition efficiency. In [15], Herrojo et al. conducted a comprehensive review of chipless RFID technology, a recent advancement with the potential for low-cost tags without ASICs, elucidating the pros and cons of the technology. Equally, [16] presents an innovative RFID-based cashless and secure payment system for vending machines, combined with Arduino and GSM. Despite database storage challenges and the initial costs, this proposed methodology surpasses traditional vending machines regarding its security, improved sensing and communication. Ramzan et al. presented an intelligent shopping booth (SSB) for students that employed RFID technology in a vending machine (VM), providing a cashless and user-friendly environment and improving the communication and sensing capabilities in [17].

2.2. RFID-Based Lock Systems

Mathew et al., in [1], surveyed automatic access control and identification techniques with regards to preventing unauthorized access. Old-fashioned lock systems, password-based door-locks and RFID-only-based systems provide inadequate security. RFID, One-Time Passwords (OTPs), cryptography, GSM, biometrics and wireless sensors were also used in door-lock security systems. In [5], Agarwal et al. introduce an innovative remote door-lock control system based on Arduino devices using RF modules. The system comprises Node-1 (a portable remote) and Node-2 (a door-mounted unit). The system's limitations include RF communication constraints, and future enhancements could involve transitioning to IoT technology for remote control. Ahtsham et al. introduce an innovative door-lock system that combines password-based security with AES-128 and SHA-512 crypt-

tographic algorithms in [18] that includes an Android app for remote management, sensors for unauthorized entry detection and actuators for secure access control.

2.3. Pin/Password-Based Lock Systems

The research paper [19] by Orji et al. presents a digital door-lock security system using a micro-controller and a keypad designed to ensure security. This solution employs a 4×4 keypad with PIN input, a Liquid Crystal Display (LCD) and a servo motor for door-locking/unlocking. Prabhakar et al. [20] present an Arduino-controlled secure door-locking system that initially locks the door with a servo motor, requiring users to input a password on a keypad. Successful authentication unlocks the door briefly, while incorrect attempts trigger a buzzer, with three consecutive failed attempts locking the system and displayed an “Access Denied” message. Owners receive SMS notifications on the door’s status via a GSM modem and can control the system through SMS commands. Baikerikar et al. [21] focus on creating a secure, smart door-lock system for rental properties, households and bank lockers, which requires the owners to set a unique PIN for each new guest renting the premises. Guests can conveniently unlock the door using an OTP, establishing a user-friendly system, particularly beneficial for hotel-like setups. Makandar et al. [22] presents a cost-effective approach to enhancing security by using economic components and accessible code development libraries, rendering it a notable alternative to more advanced security systems like fingerprints or RFID.

3. The Proposed Technology

3.1. RFID Technology

In 1945, an apparatus used for spying purposes, named “The Thing”, developed by Nikitin et al. in [23], with an embedded device was gifted to the U.S. ambassador by the Soviet Union to spy on his conversations. It operated based on the back-scattering technique and was first published about/explained by H. Stockman in 1948 [24]. The RFID tag in Figure 1 transmits data by quickly switching its internal impedance. This changes how much of the reader’s RF signal is reflected back, as shown in Figure 2. Furthermore, the reader then interprets these variations as binary data. This process is key to how passive RFID systems communicate—efficiently and without needing a battery inside the tag.

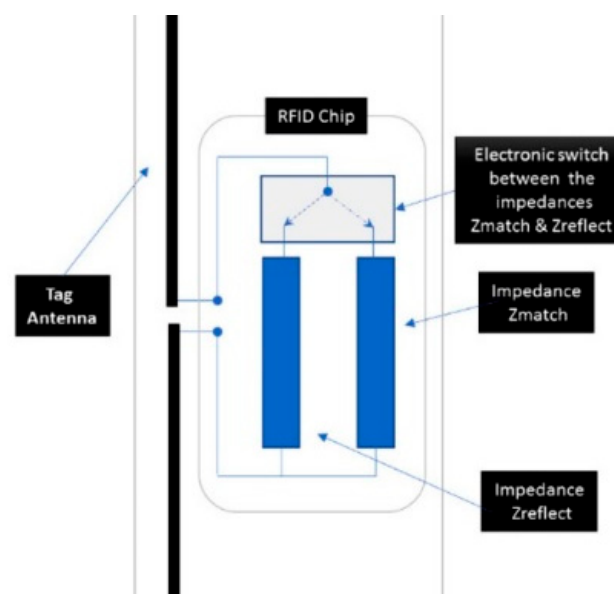


Figure 1. The simplified structure of an RFID tag.

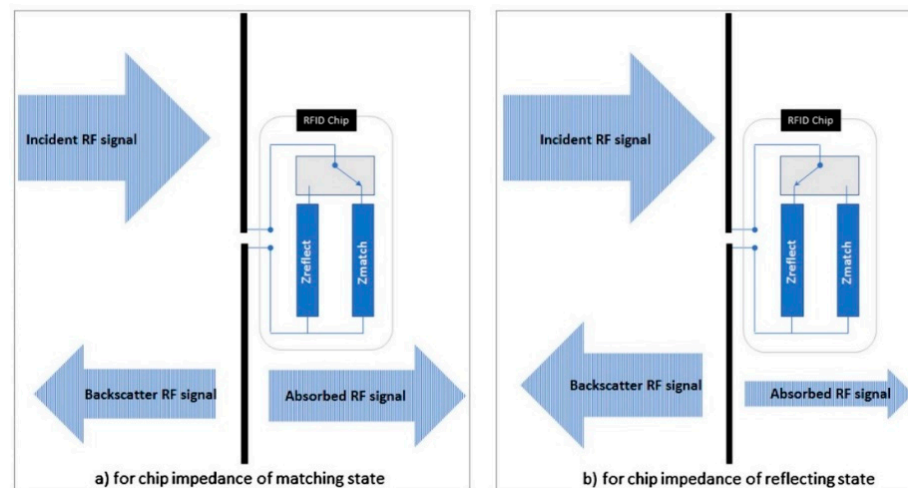


Figure 2. The behavior of an RFID tag in different impedance states.

Passive battery-less RFID systems incorporating radio frequency (RF) electromagnetic fields comprise an RFID card/tag, a reader with an operational frequency of 13.56 MHz and a database for storing UIDs (unique identification numbers) and further details on the card holder. Modern RFID, i.e., a contactless, unitary-identification (having stored UIDs), secure and economical electronic identification technology inspired by anti-theft and capacitive-inductive resonant systems, was born a decade later. It is now employed in applications like logistics, access control, car keys, traceability, passports, ticketing and payments, etc. [25]. An RFID card/tag consists of an electron micro-chip and a spiral inductive antenna that aids in the identification of the stored UID as an exclusive feature. The RFID reader is used for power in passive RFID, and it radiates a frequency of 13.56 MHz using an EM field. RFID must be in the range of a RFID card (less than 1 m), but not in the line of sight, to read UIDs saved to a specific card [16]. We have compared between the RFID technologies accessible globally and the specifications chosen for the proposed method in Table 1.

Table 1. RFID: globally accessible and chosen specifications in hybrid door-lock system.

Category	Available Worldwide	Selected in Hybrid Door-Lock System
Model	Variety of Models	MFRC522
Type	Passive/ Active	Passive
Battery	Battery-less/Battery Operated	Battery-less
Host Interface	I2C/SPI	SPI
Tag Reader Strength	High/Very Low	Very Low
Bytes in UID	4/7 Bytes	4 Bytes
Frequency Range	LF (kHz), HF and UHF (MHz), SHF (GHz)	HF (MHz)

3.2. RFID Interfacing with the SPI Bus Protocol

Serial Peripheral Interface (SPI) is a fast communication protocol that transfers data sequentially between devices in the SPI master-to-slave mode or the SPI slave-to-master mode, as shown in Figure 1 [11]. SPI is a key interface used by RFID, as it is ideal for short-distance communication. In the proposed methodology, an Arduino Mega micro-controller is used as the master and RFID RC522 acts as the slave during master-to-slave serial communication. Serial-Clock, Master-Output Slave-Input, Master-Input Slave-Output and

Slave-Select (which allows the slave to initiate communication with the master when set on low) are the four key bus lines of the Serial Peripheral Interface bus protocol. In SPI, data communication is carried out using an 8-bit data shift register which transfers one bit of data from the master to the slave during one clock pulse and in the next pulse transfers one bit from slave to master. In this manner, it takes 16 clock pulses to exchange 8 bits of master data and 8 bits of slave data.

Our proposed methodology shown in Figure 3 addresses the problems discussed in the introduction. It shows a flowchart of the hybrid security technology. Unique identification and four-digit passwords/PINs are first stored in the database; the system is then initialized for testing, after which point the RFID UID is taken as the first input. The system checks the specific UID in the stored database, and on a successful match, it allows the system to proceed to the next step, which is obtaining the second input from the user via PIN entry. If any input does not match with the database, it displays unauthorized access; the door will not be unlocked, with the system reverting to its initial stage. On successful validation of both inputs in our hybrid system, the system displays authorized access and initializes automatic locking by driving a motor; the door will be unlocked and allow the user to enter the sensitive location.

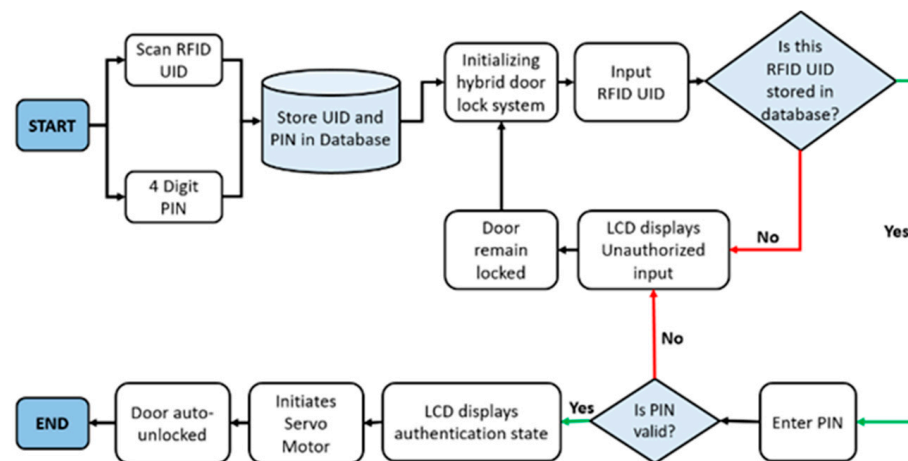


Figure 3. Flowchart of hybrid door-lock system.

3.3. The Hybrid Security System: RFID- and Keypad-Based

An intelligent double-authentication door-locking system that uses RFID-PIN technology provides an extra layer of protection for access control in areas that require heightened security measures. This system combines two distinct authentication methods—RFID (radio frequency identification) and a PIN (personal identification number)—to ensure that only authorized individuals are granted access to the secure location. Here is how such a system might work:

3.3.1. Components of the System

- *The RFID Reader:* This device reads the RFID tags or cards that authorized personnel possess. Each RFID tag contains a unique identifier, and when presented to the reader, it communicates this identifier to the system.
- *The PIN Keypad:* The PIN keypad allows authorized individuals to input their personal identification number. The PIN adds an additional layer of security to the system.
- *The Control Unit:* The control unit is the brain of the system. It processes inputs from the RFID reader and the PIN keypad, validates them and then decides whether to grant access or not.

- *The Lock Mechanism:* The lock mechanism controls physical access to the location. It is electronically controlled by the control unit, which triggers the lock to open or remain closed based on the authentication outcome.

3.3.2. The Authentication Process

- *Initial Request:* An individual approaches the door and initiates the authentication process.
- *RFID Authentication:* The individual puts forth their solution of using an RFID card or tag with the RFID reader. The reader communicates the PIN to the control unit.
- *PIN Authentication:* After successful RFID authentication, the system prompts the individual to enter their PIN on the keypad.
- *Dual Authentication:* The control unit compares the RFID identifier with the authorized database and checks whether the entered PIN matches the authorized individual's PIN.
- *Access Decision:* If both the RFID and PIN authentications are successful and match the authorized records, the control unit triggers the lock to open. If either authentication fails or both authentications fail, the lock remains secured, and access is denied.

3.4. A Description of the Hardware and Electrical Components

The system combines RFID detection and a keypad-based password for enhanced security. Users must provide both a valid RFID unique identifier (UID) and a four-digit PIN. This data is processed by an Arduino AT-Mega 2560 micro-controller of Arduino LLC (Turin, Italy). The RFID UID is checked, and if valid, the system prompts for the password. Upon correct entry, the door unlocks for 5 s via a servo motor, and the status is displayed on a 16×4 LCD. If the UID or the password is incorrect, "WRONG PASSWORD" is shown, and the door remains locked.

The system features a 4×4 keypad for PIN entry, an MFRC522 RFID module manufactured by NXP Semiconductors (Eindhoven, Netherlands) that uses passive RFID tags and a 5 V power supply or a WAPDA backup for uninterrupted operation. The Arduino is programmed via a laptop, but after detachment, it operates autonomously using batteries. Electronic components complete the circuitry to ensure high security and efficiency. The hardware and electrical components are shown in Figure 4.

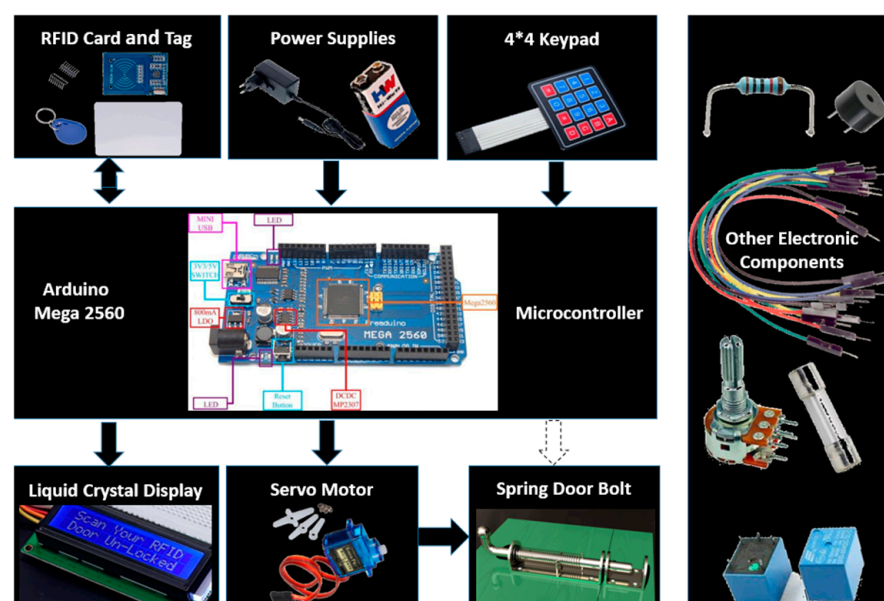


Figure 4. Block diagram of hybrid door-lock system.

4. Results

The final implementation of our hybrid door-lock system is completed by interfacing separate modules with the Arduino micro-controller software, hardware and electrical and mechanical parts. Figure 5 shows the Arduino interfacing step-wise in prototype building, i.e., with (1) a servo motor, (2) a servo motor and a keypad, (3) an LCD and (4) a motor–keypad–LCD. The final program is uploaded onto the Arduino, and all of the circuitry and components discussed in the proposed technology section are then assembled for final functioning. The response time or the time taken from RFID scanning to entering the PIN and to unlocking the door of the proposed system measured is within 5 s, whereas RFID detection completes in milliseconds. A total of 25 experiments were carried out to verify the system performance, yielding a 100% success rate.

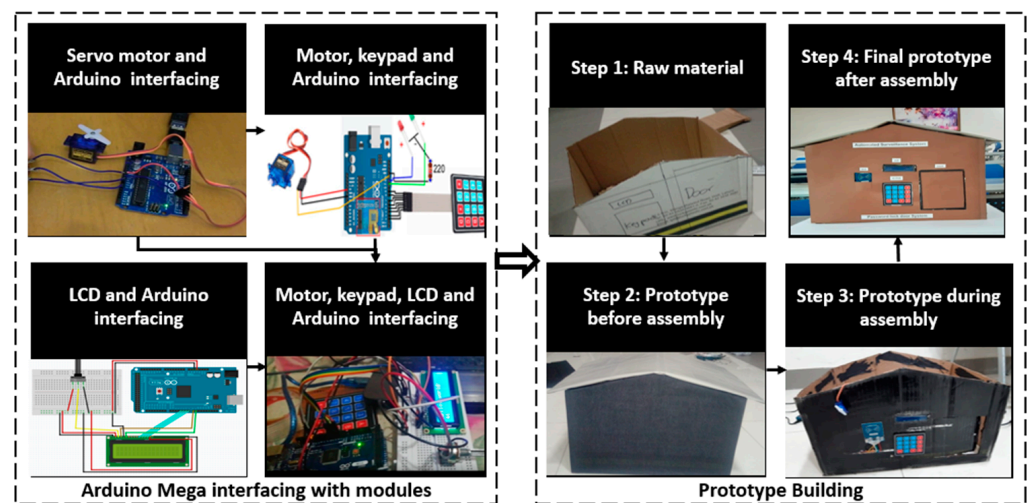


Figure 5. Hybrid door-lock system prototype building with Arduino Mega interfacing module.

5. Conclusions and Discussion

A smart door-lock system that utilizes RFID-PIN technology for double authentication is necessary for critical and confidential zones due to their elevated security requirements. The following are the key reasons for the system outlined:

- *Multi-Layered Security:* Combining RFID and PIN authentication creates a multi-layered defence against potential breaches, particularly for highly sensitive locations.
- *Mitigating Credential Theft:* By adding a PIN component, credential theft can be prevented, as an unauthorized person cannot enter without the corresponding PIN.
- *The Human Factor:* People can forget to lock doors, lose their access cards or even share them unintentionally. A hybrid system minimizes these risks by requiring a PIN only known to authorized individuals.
- *Protection against Lost Cards:* The hybrid system adds an extra layer of protection because even if a card is lost, the PIN is still required to gain entry to sensitive areas.
- *Accountability and Audit Trail:* The system provides a clearer audit trail of the access to the sensitive area, crucial for security investigations and compliance purposes.
- *Compliance Requirements:* The hybrid system can help meet compliance standards for sectors (like government and healthcare) subject to strict security regulation.
- *Deterrence:* The complexity of the system (since gaining unauthorized access requires both an RFID card and a PIN) reduces the likelihood of attempted breaches.
- *Dynamic Access Control:* A hybrid system allows for more sophisticated access control configurations in case the privileges are to be dynamically modified.
- *Emergencies and Threat Scenarios:* The RFID-PIN system facilitates swift changes to the access permissions in case of emergencies.

- *Technology Advancements:* It can adapt to emerging threats by integrating novel authentication technologies.
- *Centralized Management:* The system allows administrators to control/monitor access permissions effectively.
- *Employee Training:* The system enforces security practices better by requiring employees to input unique PINs.

6. Future Work

In the future, our proposed system could be improved by integrating it with security systems such as surveillance cameras, alarms and access logs to create a comprehensive security network that enhances the overall effectiveness, from the data analysis to the collection and analysis of data, risk assessment and future improvements.

Author Contributions: Conceptualization, methodology, software, formal analysis, investigation, resources, data curation, writing, visualization, project administration, supervision, A.R.; validation, writing—review and editing, W.F. and I.M.; validation, writing—review and editing, supervision, N.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data generated in this study using RFID cards is described in the manuscript. No public datasets were used.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this paper:

RFID	Radio Frequency Identification
OTP	One-Time Password
UID	Unique Identification Number
LCD	Liquid Crystal Display
IoT	Internet of Things
SCM	Supply Chain Management
AES	Advanced Encryption Standard
SHA	Secure Hash Algorithm
SMS	Short Message Service
GSM	Global System for Mobile Communications
IC	Integrated Circuit
HLSL	High-Level Protocol Specification Language
ECC	Elliptic Curve Cryptography
UHF	Ultra-High-Frequency
LF	Low-Frequency
HF	High-Frequency
SHF	Super High-Frequency
RBAC	Role-Based Access Control
SSB	Smart Shopping Booth
VM	Vending Machine
WAPDA	Water and Power Development Authority (Power Supply in Pakistan)
NoSQL	Not Only SQL (Non-Relational Database)
SCL	Serial Clock Line (Part of the SPI Protocol)
MISO	Master-In Slave-Out

MOSI	Master-Out Slave-In
SS	Slave Select
HDLS	Hybrid Door-Lock System

References

- Divya, R.S.; Mathew, M. Survey on various door-lock access control mechanisms. In Proceedings of the 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT), Kollam, India, 20–21 April 2017.
- Haibi, J.A.; Yassini, K.E.; Oufaska, K. Suitcase traceability system via RFID and NoSQL database. In Proceedings of the SCA'18: 3rd International Conference on Smart City Applications, Tetouan, Morocco, 10–11 October 2018; pp. 1–6.
- Gabsi, S.; Kortli, Y.; Beroulle, V.; Kieffer, Y.; Alasiry, A.; Hamdi, B. Novel ECC-based RFID mutual authentication protocol for emerging IoT applications. *IEEE Access* **2021**, *9*, 130895–130913. [\[CrossRef\]](#)
- Khan, M.U.A.; Raad, R.; Foroughi, J.; Raheel, M.S.; Houshyar, S. An octagonal-shaped conductive HC12 and LIBERATOR-40 thread embroidered chipless RFID for general IoT applications. *Sens. Actuators A Phys.* **2021**, *318*, 112485. [\[CrossRef\]](#)
- Agarwal, A.; Mehandiratta, E.; Sanket, R.; Samkaria, R.; Gupta, T.; Singh, R.; Gehlot, A. Smart door-lock system for elderly, handicapped people living alone. *Int. J. Smart Home* **2016**, *10*, 155–162. [\[CrossRef\]](#)
- Haibi, A.; Oufaska, K.; El Yassini, K.; Boulmalf, M.; Bouya, M. Systematic mapping study on RFID technology. *IEEE Access* **2022**, *10*, 6363–6379. [\[CrossRef\]](#)
- Rouchdi, Y.; Haibi, A.; El Yassini, K.; Boulmalf, M.; Oufaska, K. A New RFID Middleware and BagTrac Application. In Proceedings of the International Conference on Advanced Intelligent Systems for Sustainable Development (AI2SD'2018), Tangier, Morocco, 12–14 July 2018; pp. 869–884.
- Haibi, A.; Oufaska, K.; El Yassini, K. Tracking Luggage System in Aerial Transport via RFID Technology. In Proceedings of the Third International Conference on Smart City Applications, Oujda, Morocco, 10–11 October 2018; pp. 289–299. [\[CrossRef\]](#)
- Kisic, M.; Dakic, B.; Damjanovic, M.; Blaz, N.; Zivanov, L. Design and simulation of 13.56 MHz RFID tag in ink-jet printing technology. In Proceedings of the 36th International Spring Seminar on Electronics Technology, Alba Iulia, Romania, 8–12 May 2013.
- Good, T.; Benaissa, M. A low-frequency RFID to challenge security and privacy concerns. In Proceedings of the 2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, Macau, China, 12–15 October 2009.
- Haibi, A.; Bouazza, H.; Bouya, M.; El Yassini, K.; Oufaska, K.; Boulmalf, M.; Lazaro, A.; Hadjoudja, A. A new compact metal mountable dualband UHF RFID tag antenna with an adapted middleware for transport and SCM fields. *Int. J. Commun. Antenna Propag.* **2021**, *11*, 106–117.
- Turner, M.; Naber, J. The design of a bi-directional, RFID-based ASIC for interfacing with SPI bus peripherals. In Proceedings of the 2010 53rd IEEE International Midwest Symposium on Circuits and Systems, Seattle, WA, USA, 1–4 August 2010.
- Lee, C.; Ho, G.; Choy, K.L.; Pang, G. A RFID-based recursive process mining system for quality assurance in the garment industry. *Int. J. Prod. Res.* **2014**, *52*, 4216–4233. [\[CrossRef\]](#)
- Wang, X. Tennis robot design via Internet of Things and deep learning. *IEEE Access* **2021**, *9*, 127460–127470. [\[CrossRef\]](#)
- Herrojo, C.; Paredes, F.; Mata-Contreras, J.; Martín, F. Chipless-RFID: A review and recent developments. *Sensors* **2019**, *19*, 3385. [\[CrossRef\]](#) [\[PubMed\]](#)
- Ramzan, A.; Rehman, S.; Perwaiz, A. RFID technology: Beyond cash-based methods in vending machine. In Proceedings of the 2017 2nd International Conference on Control and Robotics Engineering (ICCRE), Bangkok, Thailand, 1–3 April 2017.
- Lodhi, E.; Fenghua, Z.; Lodhi, Z.; Saleem, Q.; Xiong, G.; Wang, F. Design and Implementation of RFID based Smart Shopping Booth. In Proceedings of the 2019 6th International Conference on Information Science and Control Engineering (ICISCE), Shanghai, China, 20–22 December 2019.
- Ahtsham, M.; Yan, H.Y.; Ali, U. IoT based door-lock surveillance system using cryptographic algorithms. In Proceedings of the 2019 IEEE 16th International Conference on Networking, Sensing and Control (ICNSC), Banff, AB, Canada, 9–11 May 2019.
- Orji, E.Z.; Nduanya, U.I.; Oleka, C.V. Microcontroller Based Digital Door-lock Security System Using Keypad. *Int. J. Latest Technol. Eng. Manag. Appl. Sci.* **2019**, *8*, 92–97.
- Prabhakar, A.; Oza, S.; Shrivastava, N.; Srivastava, P.; Wadhwa, G. Password Based Door-lock System. *Int. Res. J. Eng. Technol.* **2019**, *6*, 1154–1157.
- Baikerikar, J.; Kavathekar, V.; Ghavate, N.; Sawant, R.; Madan, K. Smart door-locking mechanism. In Proceedings of the 2021 4th Biennial International Conference on Nascent Technologies in Engineering (ICNTE), Navi, Mumbai, India, 15–16 January 2021; pp. 1–4.
- Makandar, A.; Biradar, M.R.; Talawar, M.S. Digital door-lock security system using Arduino UNO. *Int. Res. J. Modern. Eng. Technol. Sci.* **2021**, *3*, 647–652.
- Nikitin, P. Leon Theremin (Lev Termen). *IEEE Antennas Propag. Mag.* **2012**, *54*, 252–257. [\[CrossRef\]](#)

24. Stockman, H. Communication by Means of Reflected Power. *Proc. IRE* **1948**, *36*, 1196–1204. [[CrossRef](#)]
25. Duroc, Y.; Tedjini, S. RFID: A key technology for Humanity. *C. R. Phys.* **2018**, *19*, 64–71. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.