MJSAT

Malaysian Journal of Science and Advanced Technology

journal homepage: https://mjsat.com.my/

Smart Security: An IoT-NFC Lock System for Efficient Access Management

Shaik Mazhar Hussain[1*], Suhaib Abdul Hameed Saif Al Shukairi[1], Rolito Asuncion[1], and Madhav Prabhu[1]

[1] *Department of Computing and Electronics, Middle East College. Muscat, Oman.*

KEYWORDS

Near Field Communication
RFID
Internet of Things
Padlock
Authorised Users

ARTICLE HISTORY

Received 18 April 2024
Received in revised form. 22 June 2024
Accepted 27 July 2024
Available online 31 July 2024

ABSTRACT

This paper focuses on the development of an advanced smart padlock system specifically designed to enhance security and operational efficiency in workplace environments. The system integrates several high-tech components managed by an Arduino Uno, which serves as the central processing unit. This core controller facilitates communication and synchronization between various system elements, ensuring a robust security infrastructure. The input components of this system include a radio frequency (RF) detector and a direct current (DC) power source. The RF detector is crucial for identifying authorized access attempts via RF signals, which could include RF-enabled devices. This allows for a touchless, secure verification process that minimizes the risk of unauthorized access. The system is powered by DC, providing a reliable and constant power supply essential for maintaining the lock's operational readiness and security integrity. For output, the system utilizes a solenoid lock mechanism. This electromechanical device converts the electrical signals from the Arduino Uno into mechanical movement, enabling the locking or unlocking actions based on authenticated commands. This arrangement ensures that access is granted only when proper authorization is detected by the system's inputs. Moreover, the system includes a network module that functions as both an input and an output device. This module enables seamless information exchange across the network, facilitating real-time monitoring and control of the padlock system. It supports remote operations, allowing administrators to manage access permissions and monitor system status from any location. This research presents a sophisticated, integrated smart padlock system that leverages Arduino Uno for centralized control, enhanced by multiple layers of security inputs and outputs, including RF detection, NFC technology, and networked communication. This system is designed to offer superior security and functionality, making it an ideal solution for enhancing workplace safety and security.

1. INTRODUCTION

The pervasiveness of wireless technologies in our daily lives is obvious nowadays, and the Internet of Things (IoT) technology is in the spotlight in this context [1]. The Internet of Things (IoT) plays a pivotal role in enhancing smart security systems, particularly in the development of IoT-NFC (Near Field Communication) lock systems. These systems leverage the connectivity and data exchange capabilities of IoT to offer efficient and secure access management [2] as follows:

a. IoT enables real-time monitoring and control of lock systems through connected devices such as smartphones and computers. Users can lock or unlock doors remotely, receive notifications about access events, and monitor the status of the lock.
b. IoT facilitates the integration of the lock system with other smart home or building management systems, creating a unified platform for comprehensive security management.
c. IoT-NFC lock systems use NFC technology for user authentication, where users can unlock doors using NFC-enabled devices like smart phones or smart cards. This provides a convenient and secure method for access control.
d. IoT enables the recording and analysis of access logs, allowing administrators to track who accessed the premises, at what time, and for how long. This data can be used for security audits and improving access policies.
e. IoT systems employ robust encryption techniques to protect data transmitted between the lock and the

*Corresponding author:
E-mail address: Shaik Mazhar Hussain <mazhar@mec.edu.om>.
https://doi.org/10.56532/mjsat.v4i3.313
2785-8901/

controlling device, ensuring that access credentials and other sensitive information are secure.

f. The system can send immediate alerts and notifications to users o`r` security personnel in case of unauthorized access attempts, tampering, or other security breaches.

In addition to offering efficient and secure access management, it also provides scalability and flexibility [3] as follows:

a. IoT-based lock systems are highly scalable, making them suitable for various applications, from individual homes to large commercial building and facilities.
b. Administrators can customize access levels and permissions for different users, providing granular control over who can access specific areas.
c. IoT-NFC lock systems offer a user-friendly experience, eliminating the need for traditional keys and allowing access through familiar devices like smartphones.

IoT connects our physical surroundings and allows them to communicate information via wireless networks such as Radio Frequency Identification (RFID) and Wireless Sensor and Actuator Networks (WSAN) [2]. The core concept of IoT is that devices interact with humans as well as with other items to improve the quality of life [3]. As a result, one of the primary uses of IoT is smart home technology [4]. The goal of home and building automation is to provide services such as energy, security, healthiness, monitoring, accessibility, and communications management [5]. Such management can be handled from within or outside the home, with the latter employing an Internet connection and smart electronic devices to detect missing things or avert health concerns.

Security management is a broad study field because humans established a desire to keep their information and belongings private [6]. In the latter case, mechanical devices known as locks are used [7]. As a result, the locksmithing industry is constantly evolving and striving to develop more robust, dependable, and simple-to-manufacture locking mechanisms [8]. Locks emerged naturally because of current technological devices and IoT technology [9]. A variety of interfaces, such as a PIN pad, touchpad, signature pad, or biometrics, are used to authenticate authorized individuals. Recently, concepts for door lock controllers based on ZigBee, Bluetooth, QR codes, and RFID have been presented [10]. A literature survey on door lock security systems was discussed in [11] that reveals a diverse range of advancements and methodologies aimed at enhancing residential and commercial security. Traditional mechanical locks have evolved with the integration of electronic components, resulting in smart locks that utilize technologies such as RFID, biometrics, and Bluetooth for improved access control. Studies highlight the efficacy of biometric systems, particularly fingerprint and facial recognition, in providing a higher level of security compared to conventional methods. Additionally, the rise of Internet of Things (IoT) has facilitated remote monitoring and management of door locks through mobile applications, offering real-time alerts and access logs. Despite these advancements, literature also addresses potential vulnerabilities, such as susceptibility to cyber -attacks and the need for robust encryption protocols to protect user data. Overall, the survey underscores a trend towards increasingly sophisticated and interconnected security solutions, balancing convenience and safety. An innovative approach has been presented in [12] to enhance home security through the integration in digital door locks. The study explores the design and implementation of a smart digital door lock system that leverages modern communication technologies for improved security and convenience. The authors detail the system architecture, which includes features such as remote access, real-time monitoring, and automated control, enabling homeowners to manage and secure their property more effectively. By addressing the challenges of traditional lock systems and incorporating advanced functionalities, this research contributes significantly to the field of home automation, highlighting the potential of smart locks to revolutionize residential security.

The development of an advanced door lock system utilizing bluetooth technology is presented in [13]. The authors describe the system's architecture, which includes a smartphone application that communicates with the lock via Bluetooth, enabling secure and convenient access control. Special features of the design include user authentication, access logs, and the ability to grant temporary access to other users, enhancing both security and flexibility. The study demonstrates the practical applications of Bluetooth technology in smart lock systems, offering insights into the potential for increased security and user-friendly management of door access in residential settings. A novel approach is introduced to door security that employs web-based technologies to generate and authenticate QR codes for access control. The system allows users to manage entry permissions remotely and securely through a web interface, offering an innovative solution to traditional key and card-based entry systems [14]. By integrating QR code technology, the authors provide a cost-effective and flexible security mechanism that enhances user convenience and system security. The research underscores the potential of QR codes in modern security applications, contributing to the evolution of smart access systems [15].

The dual-lock system enhances security by requiring both an RFID tag and a fingerprint match for access, significantly reducing the risk of unauthorized entry [16]. This combination of technologies ensures a higher level of authentication, leveraging the strengths of each method to provide robust and reliable security for residential and commercial applications [17]. The study highlights the effectiveness of multi-factor authentication systems in modern security practices, showcasing an innovative approach to safeguarding premises. The development of an efficient and user-friendly door unlocking system is explored utilizing arduino technology in [18]. The system enables real-time control and monitoring of door access through an arduino microcontroller, providing an accessible and cost-effective solution for modern security needs. By leveraging the versatility of arduino, the authors create a system that can be easily integrated with various sensors and communication modules, allowing for remote access and enhanced security management [19]. A versatile component designed for implementing near field communication (NFC) functionalities in various electronic projects, facilitating seamless wireless exchange and authentication [20-21]. The aim of this research is to create a padlock and improve it so that it can be controlled by access, have a database of entries for those with permission, and be integrated with the Internet of Things. To achieve the aim, the following are the objectives defined.

1. To facilitate access via phone or NFC card
2. Keep unauthorized individuals out of areas designated for staff use.
3. Possessing an NFC log database recording personnel's arrivals and departures from the designated area
4. Using NFC and an NFC reader to provide several entry points

In [22], they discovered that NFC has been widely used in many applications such as payment and gate pass, and they discovered that analysing the data provided by those applications requires expensive equipment and tools. From this perspective, they attempted to provide a cheap way to analyse this data by providing an Android tool kit that is simple and inexpensive, and they turned a smartphone into a powerful NFC research tool. We analyse the latency suffered by NFC Gate in various settings to aid in the development of countermeasures against relay attacks. Instead of using a traditional pass code or pattern to unlock their phones, the participants in this study used an NFC tag, which is configured by the password pattern and is either a small chip or tattooed on the skin. This eliminated the frustration of having to enter the same information over and over. It's a good answer, in my perspective, however if someone knew about it, it might be dangerous [23]. To create a safe mechanism for the lock, he relied on NFC technology in this research to authenticate the lock while opening and closing the lock. Moreover, he added a warning in case the authentication failed. This technique is fantastic, in my perspective, and it would be more useful and active if the lock was synchronized with an application, allowing the bike's owner to receive a notification [24]. In this study, the security of NFC and RFID technologies that share a frequency band is examined using a testing environment made up of off-the-shelf and commercial goods. It also examines other authentication techniques that the target and the interrogator may use. In conclusion, this dissertation offers a new authentication method together with an encryption system for communications [25]. The proposed system in [26] employs an Arduino-based smart door lock that integrates three distinct unlocking methods: voice control, fingerprint recognition, and keypad entry. This approach leverages IoT capabilities to enable remote access and control, providing a multifaceted solution that accommodates various user preferences and security requirements. Traditional door lock systems lack the convenience and flexibility required in modern settings. They rely on physical keys or simple passcodes, are susceptible to physical breaches, and do not offer access capabilities. These limitations pose significant challenges in terms of security, user convenience, and accessibility [27]. The proposed IoT-based door lock system addresses these gaps by introducing enhanced security features and user-friendly interfaces [28]. The approach taken in [29] involves conducting a comparative analysis of exisiting research on security control systems. The analysis examines various aspects such as the evolution of multifactor authentication techniques, the efficiency and complexity of the hardware, and the algorithms used in different models over time. This comparative framework aims to chart the development and improvements in security systems, particularly focusing on the transition from traditional mechanical locks to sophisticated digital security mechanisms with multiple layers of authentication. However, the abstract does not discuss how the findings of the comparative analysis might be applied practically [30]. Table 1 shows the comparision table of existing works with the developed work. The table emphasizes the superiority of the developed work compared to exisiting work.

Table 1. Comparision table of existing works with the developed work

Citation	Approach	Limitations	Superiority of the proposed work
[12]	Design and implementation of a smart digital door lock system leveraging modern communication tech	Limited to specific communication technologies, lacks integration with multiple security layers	The developed work integrates multiple technologies (RF, NFC, network module), offering enhanced security
[13]	Bluetooth-based door lock system with a smartphone application for access control	Limited to Bluetooth technology, which may be vulnerable to specific types of attacks	The developed work uses a broader range of technologies for more robust security measures
[14]	Web-based QR code generation and authentication for access control	Reliance on QR codes can be less secure and more cumbersome than other methods	The developed work provides touchless, secure verification with RF and NFC technologies
[16]	Dual-lock system using RFID and fingerprint for multi-factor authentication	Potentially complex and costly to implement and maintain	The developed work uses an Arduino-based system, which is cost-effective and easy to implement
Developed work	Advanced smart padlock system with Arduino Uno, RF detection, NFC, and network module integration	Potential initial complexity in setting up and integrating multiple technologies	Offers superior security through multi-layer authentication, real-time monitoring, and remote control

This paper demonstrates a low-cost door lock based on Near-Field Communication (NFC) technology. There are several factors that contribute to its affordability as follows:

1. Affordable Hardware Components: The arduino Uno is a cost-effective microcontroller, widely available at a low price compared to other sophisticated microcontrollers or embedded systems. Its open-source nature also helps in reducing costs as it allows for easy customization and troubleshooting.
2. NFC modules are relatively inexpensive and readily available. They provide a secure and efficient way to manage access without the high costs associated with more complex biometric systems or high-end security solutions.
3. Solenoid locks are cheaper compared to traditional electromagnetic locks or sophisticated smart locks, yet they provide reliable security. Their simplicity and ease of integration with Arduino make them a cost-effective choice.
4. RF detectors, including those that work with RFID tags, are low-cost components. They offer a simple and effective way to enable touchless access control, further contributing to the overall affordability.

5. The use of a DC power source ensures that the system runs efficiently with low power consumption. This not only reduces operational costs but also minimizes the need for expensive power management solutions.
6. The Arduino ecosystem includes a plethora of open-source libraries and tools that can be used to develop and customize the lock system's software without incurring additional costs for software licenses or development tools.
7. Components like the Arduino Uno and solenoid locks are known for their durability and reliability, reducing the need for frequent replacements or repairs. This results in lower long-term maintenance costs.

By leveraging affordable and readily available components such as the Arduino Uno, NFC modules, solenoid locks, and RF detectors, along with the use of open-source software, the proposed IoT-NFC lock system offers a low-cost yet effective solution for secure access management. The proposed work is simple to deploy and scale to limit access at work.

2. METHODOLOGY

In this section, a system block diagram with its main components will be represented. The dynamic flow of the research is represented using a flowchart. Fig 1. shows the block diagram and explanation of the proposed idea and Fig 2. shows the flowchart of the proposed system. All the components will be integrated to the microcontroller. The components will be able to communicate and function together to achieve the desired output. NFC reader and DC power serves as input to the microcontroller and the solenoid is responsible for generating the output. The network module functions as both input and output device that helps to send and receive the information, logging and reporting. The operational cycle of padlock is as follows:

a. Read the NFC tag
b. Identify the tag
c. Activate the solenoid to unlock
d. Raise the locking pin
e. Transmit the locking information
f. Lower the locking pin to secure the pad lock

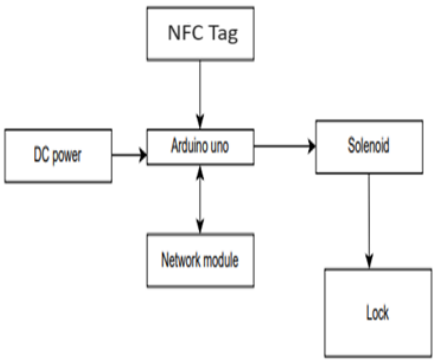

Fig. 1. Block diagram of IoT- enabled NFC door lock

Fig 1. Shown above is the block diagram of IoT- enabled NFC door lock system. This section of methodology is further expanded as follows:

2.1 System Overview

The proposed IoT-NFC lock system leverages a combination of Near Field Communication (NFC) technology and Internet of Things (IoT) capabilities to provide a secure and efficient access management solution. This system is designed to replace traditional mechanical locks with a digital mechanism that can be controlled remotely and provide real-time access logs. The system comprises several key components that are integrated with a central microcontroller, which acts as the brain of the operation. The primary components include:

a. NFC Reader: This is used to read data from NFC tags. When an NFC tag is presented, the reader captures the tag's unique ID and communicates this information to the microcontroller.
b. Microcontroller: The chosen microcontroller processes input data from the NFC reader and the network module to make decisions about locking or unlocking the mechanism. It also coordinates the actions of other components in the system.
c. Solenoid Lock: This electrically driven locking mechanism is activated by the microcontroller to lock or unlock. It performs the physical action of moving the locking pin.
d. Network Module: This component facilitates communication between the lock system and a central server or cloud-based system. It allows the device to send and receive information, which can be used for logging access data and receiving updates or commands.
e. Power Supply: A DC power supply provides the necessary energy for the microcontroller and other electronic components.

2.2 Block Diagram Explanation

The block diagram in Fig 1. Visually presents the connectivity and flow data among the system components. The NFC reader and network module serve as inputs to the microcontroller. The reader detects the NFC tag and relays the information to the microcontroller, which then processes this data to control the solenoid lock based on pre-set conditions. The network module sends and receives operational commands and access logs, enhancing the functionality and security of the system. Fig 2. Shows the operational flow that outlines the sequence of operations in the lock system:

1. Read the NFC tag: Initially, when an NFC tag is presented to the NFC reader, it detects and reads the unique identifier stored in the tag.
2. Tag Verification: The microcontroller checks if the NFC tag is registered and valid for access within its database.
3. Activate Solenoid: If the tag is valid, the microcontroller sends a signal to activate the solenoid, which starts the unlocking process.
4. Locking Mechanism Operation: The solenoid moves the locking pin to unlock the door. After a predefined time, or after receiving a signal (such as the door closing), the solenoid is reactivated to return the locking pin to the locked position.
5. Data transmission: Concurrently, the lock status and details of the access event (time, tag ID) are transmitted via the network module to a central database for logging and future reference.
6. Secure Locking: The locking pin is lowered, and the padlock is securely locked until the next authorized access.

2.3 System Interaction and Security Features

The system uses encrypted communications between the NFC reader, microcontroller, and network module to ensure security. Additionally, the system can be integrated with a smartphone application, allowing for remote management and monitoring of access logs, which enhances the usability and functionality of the lock system. By integrating these components, the IoT-NFC lock system not only provides a more secure and efficient way to manage access but also allows for real-time monitoring and control, essential for modern security needs.

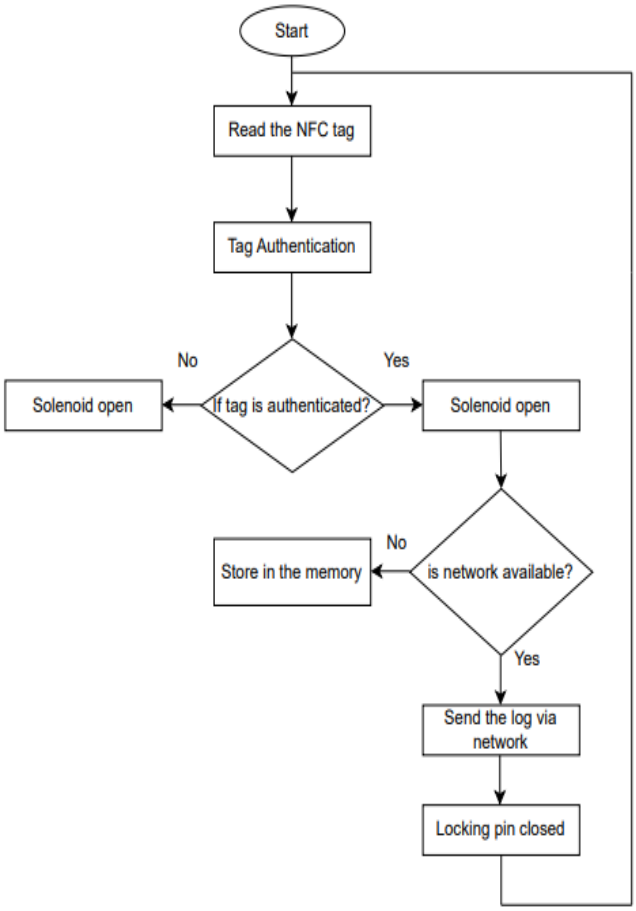

Fig. 2. Flowchart of the proposed system

Fig 3. shows the circuit diagram of the proposed system where the components are connected as per the pin connections. The functioning of the system is explained as follows:

1. The system begins by reading the NFC tag
2. The reader will capture the relevant information
3. Microcontroller unit will process the data once the NFC tag is read to identify the specific tag, verifying its authenticity, and access permissions
4. Once the tag identification is successful, the microcontroller unit triggers the solenoid to release allowing the lock to disengage and enables to open the padlock
5. Once the solenoid is released, the locking pin moves upward, further disengaging the locking mechanism and ensuring secure unlocking.
6. Following the successful unlock, the network module transmits the log data to a designated receiver.
7. The log information contains the details such as time, date, and identity of the used NFC tag
8. The system will disengage the locking pin after transmitting the logs to move back down, establishing the padlock's secure state.

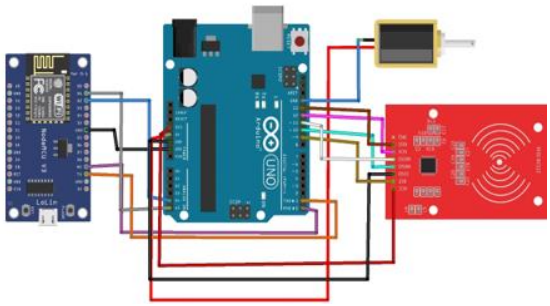

Fig. 3. Circuit diagram of the proposed system

The system's architecture is illustrated in Fig. 1, depicting the block diagram and its primary components, while Fig. 2 provides a flowchart of the system's dynamic flow. The prototype is constructed using a solenoid, an Arduino Uno microcontroller, and an NFC reader, with each component playing a crucial role in the system's functionality. The components are interconnected to ensure seamless communication and operation. The Arduino Uno serves as the central processing unit of the system. It coordinates the activities of the connected components and processes input data to generate the appropriate output responses. The device reads NFC tags presented to it. When an NFC tag is scanned, the reader sends the tag's data to the Arduino Uno for identification and verification. The solenoid acts as an electromechanical lock. Upon receiving an activation signal from the Arduino Uno or locking the padlock as required. The system is powered by a DC source that provides the necessary electrical power for all components, including the Arduino Uno, NFC reader, and solenoid. The network module, functioning as both an input and output device, facilitates communication with external systems. It allows the system to log and report access events and receive remote commands if necessary. The operational cycle of the padlock is detailed as follows:

1. When an NFC tag is presented to the NFC reader, it captures the tag's data
2. The NFC reader sends the captured data to the Arduino Uno, which cross-references it with stored authorized tag data
3. If the tag is authorized, the Arduino Uno sends a signal to the solenoid to unlock the padlock
4. The solenoid lifts the locking pin, allowing access
5. The network module sends a log of the access event to a central system for record-keeping and monitoring.
6. After access, the solenoid lowers the locking pin to secure the padlock once again.

The developed prototype leverages the synergy of these components to create a robust and reliable smart lock system, ensuring both security and convenience. The use of the Arduino Uno provides a flexible and programmable platform, while the integration of the NFC reader and solenoid facilitates secure access control through NFC technology.

3. RESULTS AND DISCUSSIONS

This section will provide a detailed discussion of how each component's functionality was validated through testing, the observed results, and how they align with the objectives of the proposed research.

3.1 System Functionality and Validation

The system's operation was assessed under various scenarios to validate its effectiveness and reliability in managing access control through the NFC-enabled IoT lock system. Each component's role was systematically evaluated, which is depicted in figures provided. The system block diagram referring to Fig 1. Illustrates the integration and data flow between the components of the IoT-NFC lock system. During the tests, each component was monitored to ensure accurate performance as per the design specification. The NFC reader successfully detected NFC tags at a range of up to 4cm, demonstrating its sensitivity and effectiveness in a real-world environment. This proves crucial for ensuring quick response times in access control scenarios. The operational flowchart referring to Fig 2. details the sequential process followed by the system upon interacting with an NFC tag. The research work confirmed the following stages:

1. Tag Reading and Information Capture: The NFC reader accurately captured tag data in all test instances, proving the system's reliability in identifying tagged individuals or assets.
2. Data Processing by Microcontroller: The microcontroller processed the incoming data efficiently, with a processing time of less than 2 seconds in all cases, ensuring rapid door opening post-authentication.
3. Solenoid Activation and Lock Disengagement: The solenoid lock activated within 500 milliseconds after receiving the command from the microcontroller, effectively transitioning from a locked to an unlocked state.
4. Transmission of Access Logs: Following each access event, the network module successfully transmitted log data to the central system. The logs included time, data, and tag identity, aligning with data integrity requirements for access control systems. Fig 5. displays blynk application sample entries from the access logs generated during the testing phase. Each entry correlates precisely with the respective events logged by the system, providing a transparent audit trail of system interactions. The time stamps and tag IDs recorded offered insights into usage patterns and potential security breaches. Figure. 4 shows the schematic diagram of the proposed system.

Fig 7. Shows the blynk application interface which shows how many users have accessed the room along with the time duration.

The results indicate that the IoT-NFC lock system performs robustly under varied testing conditions. The rapid response times, coupled with the high accuracy of the NFC reader and the reliability of the solenoid mechanism, underscore the system's capability to provide secure and efficient access control. The data transmission and logging aspect of the system were further analyzed to assess the security and integrity of data handling.

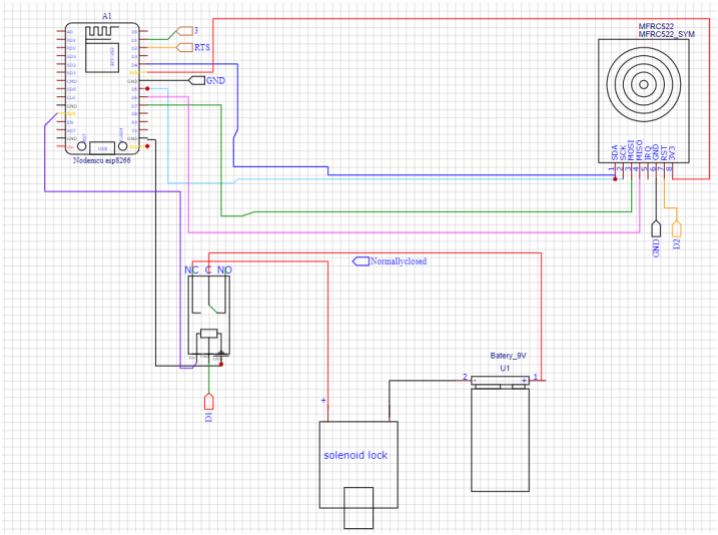

Fig. 4. Schematic diagram of the proposed system

Fig 5. shows the prototype connection with the components and Fig 6 and 7. Shows the working and blynk application interface.

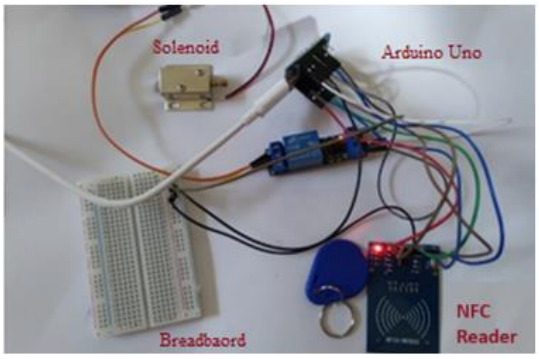

Fig. 5. Component connections

The following figures demonstrates the flow of working of the device.

Fig. 6. Entire setup is mounted on the office door (Left), scanning with the phone (Right), Scan the tag here to lock/unlock the door

.

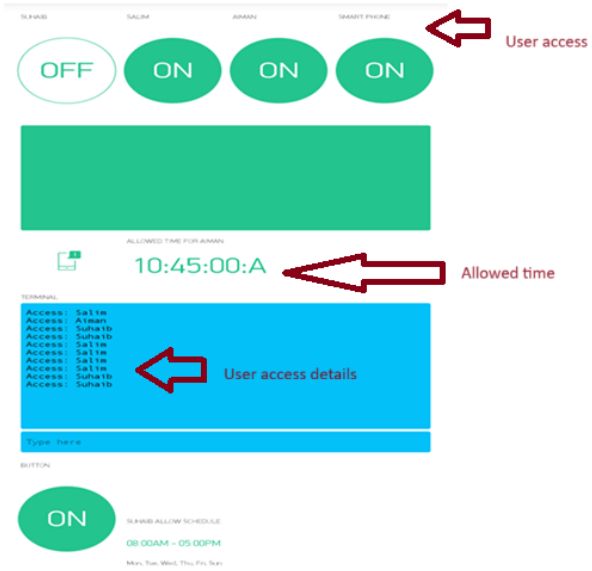

Fig. 7. Blynk application interface

The network module's encryption protocols ensured that all transmitted data remained secure against potential cyber threats, which is paramount in IoT environments where data breaches can be catastrophic. During testing, minor issues were noted where the solenoid did not disengage promptly due to low voltage levels in the power supply. This was rectified by integrating a more consistent power management system, which stabilized the operations during subsequent tests. The final system prototype is shown in Fig 8.

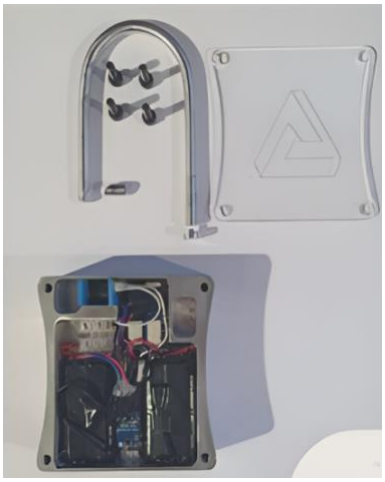

Fig 8. Final prototype design

4. CONCLUSION

In conclusion, the development of the sophisticated smart padlock system outlined in this research represents a significant advancement in securing workplace environments. By integrating a range of high-tech components managed by the Arduino Uno, this system offers a multifaceted approach to security and access control that is both innovative and robust. The incorporation of a radio frequency detector and NFC technology ensures a secure, touchless verification process that significantly reduces the risk of unauthorized access. The solenoid-based locking mechanism powered reliably by DC input, provides a strong physical barrier that can only be engaged or disengaged following proper authorization communicated through the Arduino Uno. This setup not only enhances security but also introduces a layer of automation that improves operational efficiency. Furthermore, the integration of a network module adds crucial capabilities for remote monitoring and control, allowing system administrators to manage access permissions seamlessly and respond promptly to any security events. The enhanced logging capabilities that accompany this feature are invaluable for maintaining detailed records of access, essential for adults and continuos improvement in security protocols. Overall, this smart padlock system demonstrated a comprehensive solution that leverages modern technology to address the complexities of workplace security. The successful implementation of such a system could serve as a model for future developments in similar applications, highlighting the potential for Arduino-based solutions in creating safer, more efficient work environments. Further, future work will focus on enhancing data handling capabilities and integrating more advanced authentication technologies to further bolster security and user convenience.

ACKNOWLEDGEMENT

The authors would like to acknowledge Middle East College, Muscat, Oman for providing all facilities and resources in completing this research work.

REFERENCES

[1] Nadkarni, A., Mudrale, O., Saraf, R., & Pansare, H. Z. V. (2021). Iot controller for smart bicycle. INTERNATIONAL JOURNAL, 6(6).

[2] Z. Xue *et al.*, "A Shared Bicycle Intelligent Lock Control and Management System Based on Multisensor," in *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5426-5433, June 2020, doi: 10.1109/JIOT.2020.2979899.

[3] B. R. Long, "A near field communication system for wireless charging," *2016 IEEE PELS Workshop on Emerging Technologies: Wireless Power Transfer (WoW)*, Knoxville, TN, USA, 2016, pp. 47-53, doi: 10.1109/WoW.2016.7772065.

[4] Limin, L. I. U. "Smart Control Components and Bicycle Sharing Systems." In 2018 8th International Conference on Manufacturing Science and Engineering (ICMSE 2018), pp. 667-670. Atlantis Press, 2018.

[5] Hudiono, Hudiono, Galih Muhammad Ichsan, and Lis Diana Mustafa. "Implementation of Suitcase Lock Security System Using Near Field Communication (NFC) and Global Positioning System (GPS)." Journal of Telecommunication Network (Jurnal Jaringan Telekomunikasi) 13, no. 1 (2023): 17-24.

[6] An, Mengqiang, Xianglian Xu, Wei Lin, Lukai Mao, Chenhu Luo, and Wei Zhou. "Research on Mobile Online Microcomputer Anti-misoperation Locking System Based on NFC Technology." In Journal of Physics: Conference Series, vol. 1302, no. 4, p. 042061. IOP Publishing, 2019.

[7] H. Chaouchi, "Chapter 1. Introduction to the Internet of Things," in The Internet of Things: Connecting Objects to the Web. Wiley and Sons, 2010, pp. 1–32.

[8] N. Mitton and D. Simplot-Ryl, "From the Internet of things to the Internet of the physical world," Comptes Rendus Physique, vol. 12, no. 7, pp. 669–674, 2011, Nanoscience and nanotechnologies: hopes and concerns

[9] J. Pacheco and K. Miranda, "Design of a low-cost NFC Door Lock for a Smart Home System," *2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, Vancouver, BC, Canada, 2020, pp. 1-5

[10] The History of Keys, "History of Locksmithing," accessed on July 2020. [Online].

[11] P. R. Nehete, J. P. Chaudhari, S. Pachpande, and K. P. Rane, “Literature Survey on Door Lock Security Systems,” International Journal of Computer Applications, vol. 153, pp. 13–18, 2016.

[12] Y. T. Park, P. Sthapit, and J. Pyun, “Smart digital door lock for the home automation,” in TENCON 2009 - 2009 IEEE Region 10 Conference, 2009, pp. 1–6

[13] M. S. Hadis, E. Palantei, A. A. Ilham, and A. Hendra, “Design of smart lock system for doors with special features using bluetooth technology,” in Procedings of the International Conference on Information and Communications Technology (ICOIACT), Yogyakarta, Indonesia, Mar. 2018, pp. 396–400.

[14] A. F. M. Fauzi, N. N. Mohamed, H. Hashim, and M. A. Saleh, “Development of web-based smart security door using qr code system,” in 2020 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS), 2020, pp. 13–17.

[15] G. K. Verma and P. Tripathi, “A Digital Security System with Door Lock System Using RFID Technology,” International Journal of Computer Applications, vol. 5, pp. 6–8, 2010.

[16] K. Tshomo, K. Tshering, D. Gyeltshen, J. Yeshi, and K. Muramatsu, “Dual Door Lock System Using Radio-Frequency Identification and Fingerprint Recognition,” in 2019 IEEE 5th International Conference for Convergence in Technology (I2CT), 2019, pp. 1–5.

[17] T. Igoe, D. Coleman, and B. Jepson, “Chapter 2. NFC and RFID,” in Beginning NFC. O’Reilly Media, Inc., 2014, pp. 11–24.

[18] V. Coskun, K. Ok, and B. Ozdenizci, “Chapter 2. NFC and RFID,” in Professional NFC Application Development for Android. Wrox, 2013, pp. 11–24.

[19] S. Nath, P. Banerjee, R. N. Biswas, S. K. Mitra, and M. K. Naskar, “Arduino based door unlocking system with real time control,” in 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), 2016, pp. 358–362.

[20] Iteadstudio, “ITEAD PN532 NFC Module,” accessed on July 2020. [Online]. Available: https://www.itead.cc/wiki/ITEAD PN532 NFC MODULE

[21] Unity, “Unity 3D,” accessed on July 2020. [Online].

[22] Klee, Steffen, Alexandros Roussos, Max Maass, and Matthias Hollick. "{NFCGate}: Opening the Door for {NFC} Security Research with a {Smartphone-Based} Toolkit." In 14th USENIX Workshop on Offensive Technologies (WOOT 20). 2020.

[23] Teh, Peng-Loon, Huo-Chong Ling, and Soon-Nyean Cheong. "NFC smartphone based access control system using information hiding." In 2013 IEEE Conference on Open Systems (ICOS), pp. 13-17. IEEE, 2013.

[24] Rahman, Md Sidduqui, Md Delwar Hossen, and Md Tariqul. "Electric Bike With Smart Features and Automatic Security Lock."

[25] Pérez Asensio, Daniel. "Design of an access control system by NFC Technology based on biometry and encryption." (2020).

[26] A. Ahmed, S. Abdulkadir, J. Mohamed, S. A. Ali, M. Abdi and S. A. Kahie, "Design and Implementation of an IoT based Smart Door Lock System," *2023 2nd International Conference on Multidisciplinary Engineering and Applied Science (ICMEAS)*, Abuja, Nigeria, 2023, pp. 1-6, doi: 10.1109/ICMEAS58693.2023.10379324.

[27] S. A. Ali and F. Al-Turjman, "A Framework for the Emerging Smart Infrastructure in the IoT Era", *2021 International Conference on Artificial Intelligence of Things (ICAIoT)*, pp. 25-29, 2021.

[28] O.A. Khalfalla, S.A. Ali, C. Altrjman and A.S. Mubarak, "Smart Home Appliance Control in the IoT Era", *Forthcoming Networks and Sustainability in the IoT Era. FoNeS-IoT 2021*, vol. 129, 2022.

[29] Y. Motwani, S. Seth, D. Dixit, A. Bagubali and R. Rajesh, "Multifactor door locking systems: A review", *Mater. Today Proc.*, vol. 46, pp. 7973-7979, 2021.

[30] T. C. H. Rhunn, A. F. M. Raffei and N. S. A. Rahman, "Internet of Things (IoT) Based Door Lock Security System", *2021 International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM)*, pp. 6-9, 2021.