KARYA ILHAM PUBLISHING
CONNECTING MINDS, BRIDGING IDEAS, INSPIRING READERS

Karya Journal of Aerospace and Avionics System

Journal homepage:
https://karyailham.com.my/index.php/kjaas/index
ISSN: XXXX-XXXX

Scenario Based Analysis of Low Cost RFID Data Protection using Arduino Uno Evaluating Shielding Stacking and Tag Orientation Effects

Mohamed Fareq Mohamed Yunus[1], Shahrul Ahmad Shah[1], Zulhilmy Sahwee[1,*]

[1] Unmanned Aerial System Research Laboratory, Avionics Section, Malaysian Institute of Aviation Technology, Universiti Kuala Lumpur, Malaysia

ARTICLE INFO

Article history:
Received 20 February 2025
Received in revised form 15 March 2025
Accepted 25 March 2025
Available online 1 April 2025

Keywords:
RFID security; Arduino Uno; scenario analysis; data protection.

ABSTRACT

This study explores the effectiveness of low-cost RFID data protection through a scenario-based analysis using an Arduino Uno R3 microcontroller, RC522 RFID reader module, and an LCD I2C module. By simulating practical situations, the research investigates factors that affect RFID performance and security, focusing on material shielding, card stacking, and distance or orientation of RFID tags. The study evaluates 3 scenarios which consist of different shielding materials, card stacks of varying thickness, and the influence of tag positioning relative to the reader. These scenarios provide a comprehensive understanding of how environmental and usage factors impact RFID readability. The findings highlight potential vulnerabilities in RFID systems and offer insights into practical approaches for improving their security. This work demonstrates how simple, cost-effective setups can be utilized for analysing RFID system behaviours, making it an accessible resource for students and professionals in embedded systems and IoT applications.

1. Introduction

Radio Frequency Identification (RFID) technology has become an essential part of modern systems, enabling seamless identification and tracking in applications such as access control, inventory management, and cashless transactions. Despite its widespread usage, RFID systems face challenges related to security and performance, including the potential for unauthorized access and interference caused by environmental factors or improper tag placement. Addressing these challenges requires a deeper understanding of how various elements, such as shielding materials, stacking, and tag orientation, affect the performance and security of RFID systems.

This study investigates the behavior of RFID systems under different real- world scenarios using a low-cost setup consisting of an Arduino Uno R3 microcontroller, an RC522 RFID reader module, and an LCD I2C module. By simulating and analyzing scenarios such as the effect of shielding materials,

* *Corresponding author.*
E-mail address: zulhilmy@unikl.edu.my

https://doi.org/10.37934/kjaas.1.1.110

card stacking, and tag orientation, this research provides valuable insights into improving RFID system security [1] and reliability.

1.1 Problem Statement and Objectives

As RFID technology continues to evolve, its vulnerabilities to external factors like unauthorized access [2], signal interference, and performance inconsistencies remain a concern. These vulnerabilities can compromise data security and reduce the effectiveness of RFID systems in critical applications. Although high-end RFID systems employ advanced security measures, they often come with significant costs, making them impractical for smaller-scale or budget-sensitive implementations. Thus, there is a need for a low-cost approach to study and understand the factors that influence RFID performance. This research addresses this need by analysing the effects of shielding materials, card stacking, and tag orientation on RFID system behaviour, providing insights into affordable methods for enhancing RFID security and performance. This study has its objectives that are to evaluate the effectiveness of materials and stacking for blocking RFID signal and to measure and analysed the distance and orientation effect on RFID performance.

2. Methodology

2.1 Flowchart

This study employs an experimental approach to investigate the behavior and performance of RFID systems under different real-world scenarios. The methodology is structured around a set of controlled experiments using a low-cost RFID setup, which allows for the evaluation of various factors that could influence the performance and security of RFID systems. The factors studied include shielding materials, card stacking, and tag orientation, with the goal of gaining insights into methods to enhance RFID security and reliability without relying on expensive systems.

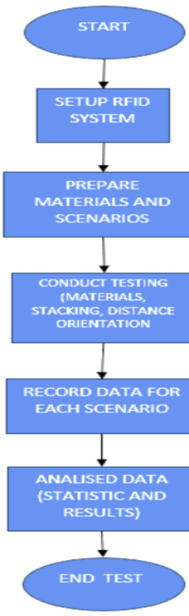

Fig. 1. Research flowchart

While the study provides valuable insights into RFID performance, there are a few limitations in the methodology. First, the study examines only a limited range of shielding materials, and there may be other materials that could affect RFID performance in different ways that were not considered.

Additionally, the results are based on a specific low-cost RFID setup (Arduino Uno R3, RC522 module, and LCD display), meaning the findings may not be directly applicable to higher-end commercial RFID systems. Finally, the experiments were conducted in a controlled environment, which may not fully account for the variety of environmental factors, such as interference or temperature fluctuations, that could influence RFID performance in real-world scenarios.

2.2 Hardware and Software Implementation

In this RFID system, we use three main hardware components: the Arduino UNO R3, the RC522 RFID module, and an LCD screen with I2C. These components work together to read data from RFID cards and display it on the LCD screen. The Arduino UNO R3 is the main control unit. It is a small computer that processes the data from the RFID reader and sends information to the LCD screen. The RC522 RFID module reads the data from RFID cards. It uses radio waves to communicate with the card and get its unique ID. The module connects to the Arduino using the SPI communication pins. The LCD with I2C is used to show the RFID card's unique ID (UID). The I2C interface makes it easier to connect the LCD to the Arduino because it only uses two wires (SDA and SCL) for communication, instead of using many pins.

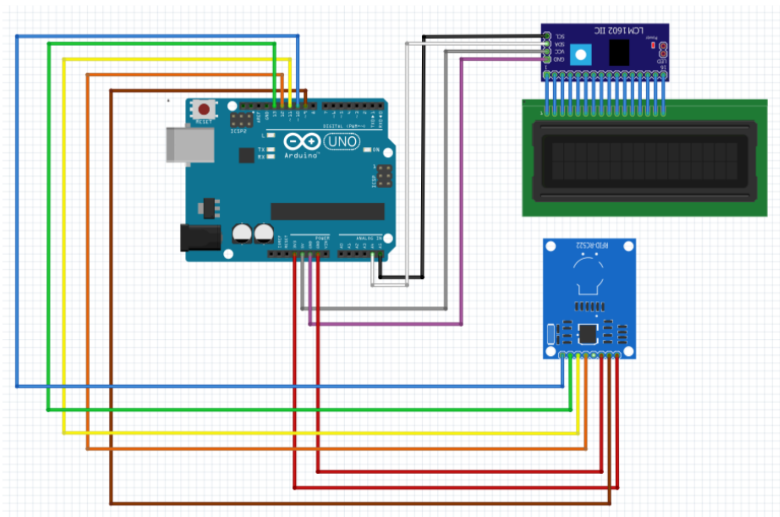

Fig. 2. Circuit diagram

The software controls how the Arduino talks to the RFID reader and the LCD screen. It is written in the Arduino programming language using the Arduino IDE. The first step is to include the necessary libraries: the MFRC522 [3] library for the RFID reader, and the Wire and Liquid Crystal I2C libraries for the LCD. These libraries allow the Arduino to easily control the hardware. When the program runs, it first initializes the RFID reader and LCD screen. The system waits for an RFID card to be placed near the reader. When a card is detected, the Arduino reads the unique ID (UID) from the card and displays it on the LCD screen. The program also prints the UID to the serial monitor for debugging purposes. The program checks for new cards continuously. Once a card is detected, it displays the UID on the LCD and waits for 2 seconds before checking for a new card. This ensures that the system doesn't keep overwriting the display too quickly.

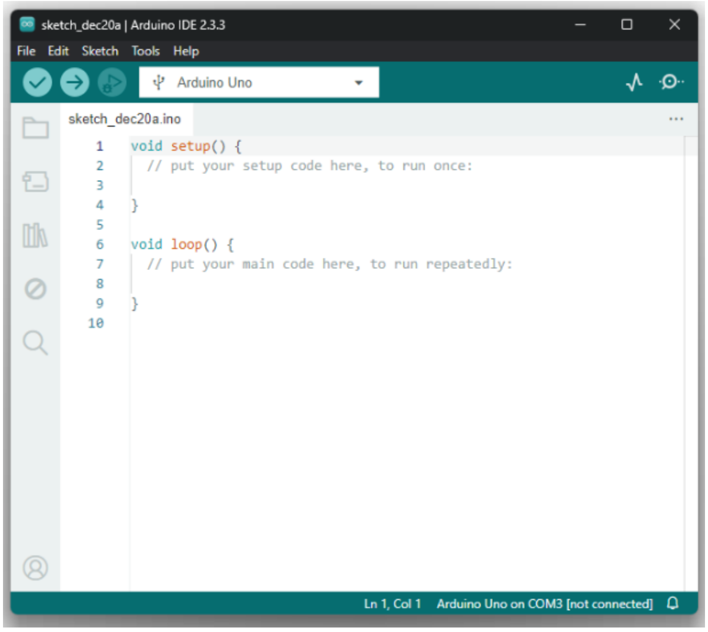

Fig. 3. Arduino IDE 2 software

2.3 Experiment Scenarios

To evaluate the performance of RFID systems under different conditions, this study focuses on three key experimental scenarios. Each scenario aims to examine specific factors that can influence the effectiveness, security, and reliability of RFID systems. These factors include the impact of shielding materials, the effects of card stacking, and the influence of distance and orientation on RFID readability. By testing these scenarios, we can gain a deeper understanding of how environmental and hardware variables interact with RFID systems, providing valuable insights that can help improve their performance in real-world applications. The following sections describe each of these experimental scenarios in detail.

2.3.1 Effect of shielding materials on RFID signal

In this experiment, different shielding materials are used to examine their impact on the RFID reader's ability to detect and communicate with RFID tags. The materials tested include:

a) Aluminium Foil
b) Copper Roll
c) Synthetic Leather Wallet
d) Enveloped Paper

Each material is placed between the RFID reader and the RFID tag to simulate the presence of a physical barrier. The RFID reader is then used to measure whether the material blocks or attenuates the RFID signal, affecting the reader's ability to detect the tag. The effectiveness of these materials is assessed by recording the maximum readable distance and success rates of tag detection.

2.3.2 Impact of card stacking on RFID performance

This experiment evaluates the effect of card stacking on RFID readability. Various configurations of stacked RFID cards are tested, including 1, 2, 4, and 6 cards stacked on top of each other. The key parameters measured include:

a) Maximum Read Distance: The distance at which the RFID reader can successfully read a tag when multiple cards are stacked together.
b) Number of Cards Readable: The number of RFID cards the system can successfully read simultaneously when stacked.
c) Readability in Close Contact: The system's ability to read RFID tags when they are in very close proximity to the reader.

These scenario explore how stacking affects the interaction between the RFID tags and the reader, providing insight into the limitations of RFID systems when multiple cards are used at once.

2.3.3 Influence of distance and orientation on RFID readability

The final experiment investigates how distance and orientation [4] influence the RFID system's performance. In this experiment, various RFID cards (Mifare RFID cards, ID cards, and bank cards) are tested at different distances (e.g., 0 cm, 5 cm, 10 cm, and 15 cm) from the reader. Additionally, different orientations of the cards are tested, including:

a) Side-to-Side Orientation: The card is placed parallel to the RFID reader's plane.
b) Top-to-Bottom Orientation: The card is placed vertically relative to the RFID reader.
c) Directly Toward the Reader: The card is placed directly facing the reader.

The goal of this experiment is to analyse how distance and the angle at which the RFID card is held affect the reader's ability to detect and communicate with the RFID tag.

3. Results

3.1 Test Measurement and Demonstration

In the real world, RFID (Radio Frequency Identification) technology interacts with its surroundings in various ways. To understand how it works, we can explore three different scenarios: A, B, and C which has been discussed in the chapter 3. These scenarios will help us gather important data.

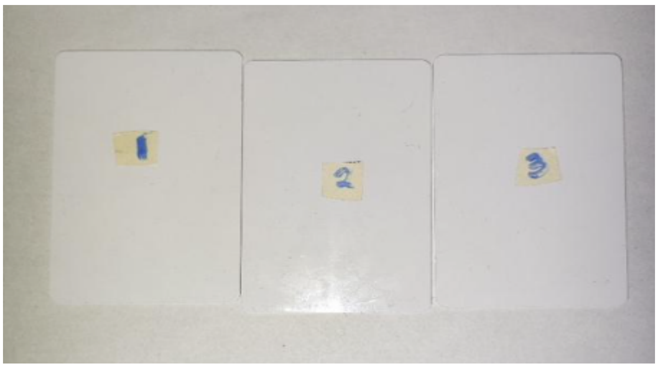

Fig. 4. Unwrapped RFID cards

3.1.1 Scenario A

Scenario A focuses on how different card shielding affects RFID signals. For this scenario, we'll use an Arduino R3 UNO microcontroller, an RC522 reader module, and an LCD I2C display module. The Arduino will control the reader, and the LCD display will show the results. We'll also use a ruler to measure the distance between the card and the reader to see how shielding impacts the signal.

Fig. 5. RFID Cards wrapped in (a) Aluminium Foil (b) Copper Roll Sticker (c) Envelope Paper (d) Synthetic leather

The scenario involves evaluating the shielding effectiveness of various materials in blocking the detection of RFID or NFC cards by a detection system. Four types of materials—aluminium foil, a 10mm copper roll, synthetic leather (0.7mm), and envelope paper—were tested for their ability to block the signals emitted by three different cards, each identified by unique UIDs. For the testing process, each card was individually wrapped or covered with the material being tested, and the detection system was used to determine whether the card signal could be detected (1) or not detected (0). This systematic testing ensures that each material's shielding properties are assessed consistently across three different cards. The results showed that aluminium foil and the copper roll provided complete shielding, as no cards were detected, while synthetic leather and envelope paper failed to block detection, with all cards being detected. This process demonstrates the consistency and reliability of both the detection system and the materials under test.

Table 1
Test result for scenario A (card shielding)

MATERIAL (SHIELD TYPE)	NUMBER OF CARDS TESTED	DETECTION 1 = DETECTED 0 = UNDETECTED
Aluminium Foil	CARD 1 (73 E5 33 2A)	0
	CARD 2 (D3 D4 73 28)	0
	CARD 3 (D3 AF 15 2A)	0
Copper Roll, 10mm	CARD 1 (73 E5 33 2A)	0
	CARD 2 (D3 D4 73 28)	0
	CARD 3 (D3 AF 15 2A)	0
Synthetic Leather, 0.7mm	CARD 1 (73 E5 33 2A)	1
	CARD 2 (D3 D4 73 28)	1
	CARD 3 (D3 AF 15 2A)	1
Envelope Paper	CARD 1 (73 E5 33 2A)	1
	CARD 2 (D3 D4 73 28)	1
	CARD 3 (D3 AF 15 2A)	1

Scenario A result inTable 1 shows the test results for scenario A, scenario where the RFID card is wrapped or put inside different materials. The results confirms that materials like aluminium foil and copper rolls are effective for shielding applications, such as protecting sensitive RFID or NFC cards from unauthorised access. On the contrary, synthetic leather and envelope paper are unsuitable for this purpose due to their inability to block detection. Three cards were tested for each material, with blue bars representing the number of cards tested and orange bars showing the number detected. The results indicate that aluminium foil and the copper roll completely blocked detection, as no cards were detected, demonstrating their effectiveness as shielding materials. In contrast, synthetic leather and envelope paper allowed all cards to be detected, proving ineffective for shielding purposes. These findings emphasise the importance of using conductive materials like aluminium foil or copper roll for applications requiring signal protection, as the metal properties creates distortion and bounce back the signal from the RFID card, whereas. In contrast, materials like synthetic leather and envelope paper fail to provide adequate shield adequately.

3.1.1 Scenario B

Scenario B involves stacking multiple cards on top of each other to see how the RFID reader reacts. Again, we will use the same equipment: the Arduino, the RC522 reader, the LCD display, and the ruler. We'll stack the cards gradually and check how the reader detects the RFID tags in the stack.

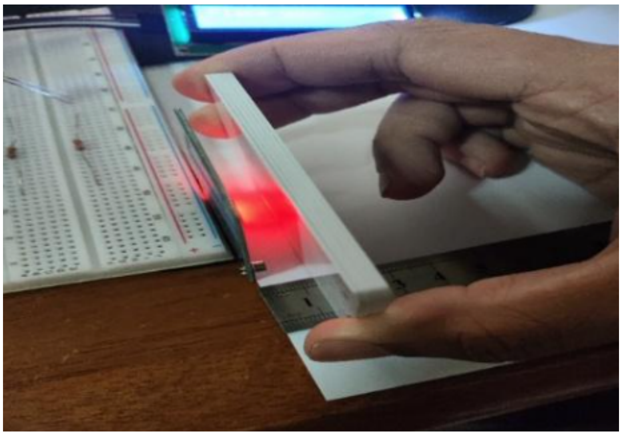

Fig. 6. Test measurement for multiple card stack

In this scenario, the objective is to assess how the performance of an RFID system is impacted by stacking multiple RFID cards together. Real-world applications, such as automated checkout systems, access control systems, and inventory management, often involve scenarios where multiple RFID cards are in proximity to one another. This experiment seeks to understand how stacked cards affect the RFID reader's ability to detect individual cards and how the number of stacked cards influences the maximum detection distance. To evaluate the performance, the experiment involved stacking cards in different quantities (1, 2, 4, and 6 cards) and measuring the maximum readable distance for each configuration. The tests were performed using the same RC522 RFID reader, Arduino setup, and LCD display used in previous scenarios.

Table 2
Test result for scenario B (card stacking)

NUMBER OF CARDS IN STACK	MAX READ DISTANCE, cm	UNIQUE ID CARDS	NUMBER OF READABLE CARDS	NUMBER OF READABLE CARDS IN CLOSE PROXIMITY	NOTES
1	3.1	83 5A A6 34	83 5A A6 34	83 5A A6 34	Optimal performance
2	2	83 5A A6 34 53 1D A9 34	83 5A A6 34 53 1D A9 34	53 1D A9 34 83 5A A6 34	Optimal performance but switch order in close contact
4	1.2	83 5A A6 34 53 1D A9 34 23 DF 28 34 B3 09 EB 27	53 1D A9 34 23 DF 28 34	53 1D A9 34 23 DF 28 34 83 5A A6 34 B3 09 EB 27	Significant interference and switch order in close contact
6	0.7	83 5A A6 34 53 1D A9 34 23 DF 28 34 B3 09 EB 27 D3 AF 15 2A 40 7F CE A4	B3 09 EB 27 D3 AF 15 2A	B3 09 EB 27 D3 AF 15 2A 23 DF 28 34 53 1D A9 34	Severe interference and more than half read in close contact

Table 2 Scenario B explores the effects of stacking RFID cards and their readability. The discussion focuses on the number of cards in a stack, the maximum reading distance, the unique IDs of readable cards, and the performance. When there is only one card in the stack, the reading distance is optimal at 3.1 cm, and the card is read without any issues. Adding a second card reduces the maximum reading distance to 2 cm. However, both cards can still be read successfully, provided the order of the cards is switched when placed in close contact. This indicates minimal interference at this stage. When four cards are stacked, the reading distance drops further to 1.2 cm, and significant interference is observed. Although all cards are readable, the performance depends heavily on their arrangement. At this stage, the interference between the cards becomes more noticeable, making it less reliable. Finally, with six cards in the stack, the maximum reading distance drops significantly to 0.7 cm, and the interference becomes severe. More than half of the cards are readable, but the interference makes the system highly unreliable.

3.1.2 Scenario C

Scenario C examines the effects of distance and orientation. In this scenario, we'll move the RFID card at different distances from the reader and change its angle to observe how these factors influence the signal. The same tools will be used to measure and record the results. This scenario focuses on evaluating the performance of the RC522 RFID reader in terms of its ability to detect RFID tags under different spatial orientations and distances. Three distinct conditions using three different cards (RFID Card, ID Card and Bank Card) are tested to measure the response range:

a) Side-to-Side Orientation: The RFID tag is moved parallel to the reader in a side-to-side motion.
b) Top-to-Bottom Orientation: The tag is positioned directly above the reader and moved vertically.
c) Towards the Reader Orientation: The tag is aligned perpendicularly and moved towards the reader's surface.

Table 3
Test result for scenario C (read distance and orientation)

CARD TYPE	UID	ORIENTATION	NUMBER OF ATTEMPTS	NUMBER OF READABLE
DEFAULT RFID	40 7F CE A4	Side to side	5	5
	40 7F CE A4	Top to bottom	5	9
	40 7F CE A4	Towards the reader	5	5
ID	6F 40 A9 CB	Side to side	5	5
	6F 40 A9 CB	Top to bottom	5	15
	6F 40 A9 CB	Towards the reader	5	5
BANK	D9 D0 F4 9D	Side to side	5	5
	D9 D0 F4 9D	Top to bottom	5	5
	D9 D0 F4 9D	Towards the reader	5	5

(a) Distance of 1cm

CARD TYPE	UID	ORIENTATION	NUMBER OF ATTEMPTS	NUMBER OF READABLE
DEFAULT RFID	40 7F CE A4	Side to side	5	5
	40 7F CE A4	Top to bottom	5	9
	40 7F CE A4	Towards the reader	5	5
ID	6F 40 A9 CB	Side to side	5	5
	6F 40 A9 CB	Top to bottom	5	5
	6F 40 A9 CB	Towards the reader	5	5
BANK	D9 D0 F4 9D	Side to side	5	0
	D9 D0 F4 9D	Top to bottom	5	0
	D9 D0 F4 9D	Towards the reader	5	0

(b) Distance of 2cm

(c) CARD TYPE	UID	ORIENTATION	NUMBER OF ATTEMPTS	NUMBER OF READABLE
DEFAULT RFID	40 7F CE A4	Side to side	5	0
	40 7F CE A4	Top to bottom	5	0
	40 7F CE A4	Towards the reader	5	0
ID	6F 40 A9 CB	Side to side	5	5
	6F 40 A9 CB	Top to bottom	5	5
	6F 40 A9 CB	Towards the reader	5	5
BANK	D9 D0 F4 9D	Side to side	5	0
	D9 D0 F4 9D	Top to bottom	5	0
	D9 D0 F4 9D	Towards the reader	5	0

(d) Distance of 4cm

(e)

Table 3 in Scenario C summarizes the performance of an RC522 RFID reader in detecting RFID cards under three different orientations: Side-to-Side, Top-to-Bottom, and Towards the Reader. Three types of RFID cards—Default RFID, ID, and Bank cards—were tested, and their results were compared based on the number of attempts and successful reads (readable). The Default RFID card consistently performed well, achieving 5 successful reads in 5 attempts in both Side-to-Side and Towards the Reader orientations. However, in the Top-to-Bottom orientation, it recorded 9 successful reads during 5 attempts, suggesting enhanced proximity or alignment in this specific orientation. The ID card showed similar consistency in the Side-to-Side and Towards the Reader orientations, achieving 5 successful reads out of 5 attempts in both cases. Interestingly, in the Top-to-Bottom orientation, it recorded 15 successful reads out of 5 attempts, significantly outperforming the other two orientations. This suggests that the ID card may have specific design features that make it more responsive or detectable when aligned in this manner. In contrast, the Bank card maintained consistent performance across all orientations, with 5 successful reads out of 5 attempts in every case, indicating no advantage in any one orientation.

4. Conclusions

The results from the experiments conducted highlight several important factors that influence RFID system performance. First, shielding materials were found to have a significant impact on RFID signal blocking. Materials such as aluminium foil and copper roll were highly effective in reducing or completely blocking RFID signals, while materials like synthetic leather wallet and paper had a much lesser effect. This suggests that RFID systems can be vulnerable to interference from metal materials, which could be used in certain security applications to prevent unauthorized RFID readings. The second experimental scenario, which tested the effect of card stacking, showed that stacking multiple RFID cards reduces the system's ability to read all of them. As the number of cards stacked increased, the maximum read distance decreased, and the system was less able to detect all the cards at once. This finding is significant for applications where multiple RFID tags might be used at the same time, such as in inventory or access control systems. The third experiment, which explored the influence of distance and orientation on RFID readability, demonstrated that the performance of RFID systems is highly sensitive to both the distance between the reader and the tag and the orientation of the tag. As the distance increased or the orientation became less optimal, the readability of the RFID tag decreased. The best results were achieved when the RFID tag was directly facing the reader and placed at a short distance. Overall, the findings from these three experimental scenarios underline the importance of understanding the factors that influence RFID performance in order to enhance system reliability, security, and efficiency. By addressing these issues, it is possible to improve the robustness of RFID systems, particularly in environments where performance is critical.

Acknowledgement
This research was not funded by any grant.

References

[1] Likhite, Shamika. "RFID Based Embedded Security System." *Authorea Preprints* (2021). doi: 10.36227/techrxiv.14315699.v1.
[2] Chabbi, Samir, and Chaouki Araar. "RFID and NFC authentication protocol for securing a payment transaction." In *2022 4th International Conference on Pattern Analysis and Intelligent Systems (PAIS)*, pp. 1-8. IEEE, 2022.
[3] Security Access using MFRC522 RFID Reader with Arduino - https://randomnerdtutorials.com/security-access-using-mfrc522-rfid-reader-with-arduino
[4] Nikitin, Pavel V., and K. V. S. Rao. "Performance limitations of passive UHF RFID systems." In *2006 IEEE Antennas and Propagation Society International Symposium*, pp. 1011-1014. IEEE, 2006.