Enhancing IoT Security: A Lightweight Cloning Approach for RFID/NFC Access Control Systems

Muhammad Ismaeel Khan[1], Hassan Tahir[2], Aftab arif[1], Md Ismail Jobiullah[1], Ali Raza A Khan[3], Sakera Begum[1], Ihtasham Hafeez[1]

[1]School of Information Technology, Washington University of Science and Technology, Leesburg, Vienna, VA 22182, United States

[2]School of Computer Science and Information Technology, The Superior University, Lahore, Punjab 54000, Pakistan

[3]College of Cybersecurity, Virginia University of Science & Technology, Vienna, VA 22182, USA

[*]Corresponding Author Email- mdismailjobiullah24@gmail.com

Abstract

Near Field Communication (NFC) and Radio Frequency Identification (RFID) are crucial enabling technologies used in asset tracking, payment systems, and secure access control, among other applications. However, their weaknesses leave their security and privacy at risk, especially in the case of clone-based attacks, where unauthorized users can replicate RFID/NFC cards to gain entry to restricted zones or systems. The Proxmark3 tool is highly accessible and is used not only to demonstrate cloning capabilities but also to provide methods of reducing such threats. Cloning RFID/NFC cards that are not encrypted has a near 99% success rate, as demonstrated in experiments. Even more advanced encrypted standards, such as MIFARE DESFire and HID iCLASS, showed a high rate of success in cloning, indicating that current security standards are not entirely satisfactory. The primary contribution of this research is the introduction of a lightweight and inexpensive method for examining and preventing RFID/NFC cloning attacks, which does not require additional hardware. This approach had the highest detection accuracy of 95.2%. The presented technique is promoted as a scalable security paradigm for IoT systems, and its real-world implementation is needed in the healthcare, financial, and transportation industries.

Keywords: RFID, NFC, cloning attacks, Proxmark3, IoT security, access control, lightweight detection, countermeasures, data integrity.

1. Introduction

1.1 Background and Motivation

The Internet of Things (IoT) has rapidly expanded and transformed the face of various industries, including healthcare, retail, transportation, and finance, by enabling seamless connectivity

among devices. Radio Frequency Identification (RFID) and Near Field Communication (NFC) are enabling technologies for Internet of Things (IoT) systems, which have various applications, including secure identification, access control, and contactless payment. The RFID and near-field communication (NFC) technologies operate in low-frequency, high-frequency, and ultra-high-frequency bands, creating several application opportunities, such as asset tracking, public transportation, and access control to restricted zones, including security passes (Feng et al., 2022). However, demand is increasing to secure IoT devices and related RFID/NFC systems as their numbers grow. The security weaknesses, particularly their vulnerability to cloning attacks, pose a serious threat to access control policies, privacy, and data integrity in these systems. Cloning enables hackers to access limited areas by covertly duplicating an issued RFID/NFC card (Chen et al. 2022). While modernizing our digital infrastructure through RFID/NFC-based technologies, these attacks emphasize the urgent need to improve security and privacy.

1.2 Research Gap, Motivation, and Context

For all their apparent benefits, however, both RFID and NFC have some rather serious drawbacks. At the same time, RF and NFC-based systems are susceptible to cloning attacks, which enable an attacker to copy data from a genuine card onto a fake and remain undetected (although this type of chip may now incorporate encryption and access protection, as noted by Feng et al. (2022). In such cases, existing solutions, such as encryption techniques (Ehrenfreund and Schechter, 2013) and PIN protection (Dymitrow et al., 2017), are not fully vulnerable, especially in contexts where resources are limited or tags are not crypto-enabled (Feng et al., 2021). Additionally, many existing methods are time-consuming to execute, require specialized hardware, or lack scalability. Through the use of the Proxmark3 HW clone detector, an off-the-shelf device suitable for both cloning scenarios and real-world applications, this work aims to bridge these gaps by introducing a lightweight and efficient mechanism for detecting RFID/NFC cloning.

1.3 Novelty Compared to DeClone, ACD, and Blockchain Methods

Two existing clone detection technologies are DeClone and Anti-Clone Detection (ACD), and may provide improved security with RFID/NFC. DeClone is a trajectory-based cloning attack detection system that consumes more memory and processing time than our system, making it infeasible in low-resource situations (Feng et al., 2022). ACD can be detected online, albeit at the cost of a specialized hardware setup and increased complexity (Wang et al., 2023). Despite blockchain-supported mechanisms being decentralized and secure, they are typically characterized by scalability issues and expensive procedures, making it impossible to implement IoT on a large scale (Grunwald and Wolf, 2008). This work presents a powerful and user-friendly method for detection. To design a user-friendly and reliable method for detecting RFID/NFC cloning attacks, we utilize Proxmark3, a commercially available and relatively inexpensive hardware device. It offers a scalable architecture that can be easily integrated with existing systems, eliminating the need to build intricate hardware architectures.

1.4 Contributions

The primary contributions of this study are as follows:

- Successful demonstration of cloning an RFID/NFC card using the Proxmark3, obtaining almost a 99% success rate with historic cards that demonstrated security vulnerabilities for modern systems.
- An effective and economical mechanism is presented for detecting and defending against cloning assaults that does not depend on special technology, and hence is scalable in real-world scenarios.
- Established a set of standards for secure disclosure of RFID/NFC vulnerabilities to stakeholders, while leaving an opportunity for responsible security updates.

The rest of this paper is structured as follows: Section 2 provides a thorough overview of RFID and NFC technology, as well as its drawbacks and the shortcomings of the security solutions currently in use. Section 3 describes the experimental designs, tools, and procedures used in implementing the suggested cloning detection. The results of the cloning tests are presented in Section 4, along with a comparison of their accuracy, efficacy, and resource consumption to those of current techniques. The results are explained in Section 5, along with their implications for IoT security and access control systems in general. Our contributions and some upcoming work, including effective encryption, AI-based detection, and real-time monitoring, are summarized in Section 6.

2. Literature Review

The increasing risk of cloning attacks poses a significant threat to the security of RFID and NFC systems, which are crucial components of secure identification systems, such as asset tracking and access control (Feng et al., 2021). According to Gupta et al. (2023), a cloning attack involves copying and transferring data to a different card to gain unauthorized access (Burmester & de Medeiros, 2007). The existing defense mechanisms are broadly classified into three groups.

First, there are physical and protocol-based replication prevention methods, which attempt to analyze communication patterns. Physical Unclonable Functions (PUF) solutions, including those suggested by Chen and Yan (2022) and Feng et al. (2019), provide high security with limited hardware requirements, achieving accuracy of solutions up to 98.7%. They are, however, sensitive to noise and demand special hardware, which makes it difficult to install them on a large scale. Simple and efficient schemes, such as DEClone (Lee & Kim, 2023) and EPC Gen2 PRNG-based Authentication (Caballero-Gil et al., 2022), are based on protocol analysis, which is prone to more advanced cloners capable of accurately simulating communication timing, with an accuracy of approximately 95-96%.

Second, higher-order computational countermeasures have cryptographic and machine learning countermeasures. Cryptographically, hybrid encryption protocols (Jayawardana & Dangalla, 2020) are fastened with strong cryptography through the combination of symmetric and asymmetric encryption approaches, although with a high reported accuracy rate of 97-99 and are computationally expensive and need crypto-enabled tags. Tamper-resistant authentication records offered by blockchain systems (Vijayalakshmi et al., 2022) have very strong theoretical security. However, it is these disadvantages, such as high computational costs, slow transaction rates, and low scalability for large-scale IoT, that are caused by their decentralized nature.

Third, AI and Machine Learning (ML) applications, including Deep Learning-based detection (Lee et al., 2021) and general AI anomaly detection (Awotunde and Misra, 2022), exhibit high accuracy, ranging from 96% to 98%. Although the approaches are adaptive, they require huge amounts of training data and expensive processors, which cannot be frequently implemented on edge devices with limited resources (Liu and Zhang, 2023).

2.1 Research Gap and Motivation

The current situation in the field of work indicates a definite gap in research: the existing methods for detecting cloning are either computationally expensive, hardware-specific, or do not effectively scale to real-world IoT setups. This paper fills this gap by offering a software-based, lightweight detection system deployed using Proxmark3. The proposed approach achieves a high detection rate of 95.2% with a low resource cost, thereby establishing a scalable and resource-efficient security paradigm that overcomes the limitations of earlier hardware-intensive and computationally intensive systems.

Table 1: Comparison of Cloning Detection Techniques.

Reference	Technique	Advantage	Disadvantage	Accuracy (Reported)
Lee & Kim (2023)	DEClone (Trajectory analysis, Dijkstra's algorithm)	Adapts to complex movement patterns; high recall against simple cloning.	Limited customization on commercial devices; cannot always distinguish subtle clone variations.	~96%
Chen & Yan (2022)	Lightweight PUF-based Anti-Clone	Very low hardware overhead; inherent resistance to physical cloning.	Requires specialized PUF hardware; sensitive to environmental noise.	98.7%
Feng et al. (2019)	Lightweight RFID Mutual Authentication with PUF	Robust security using ideal/noisy PUFs; lightweight for constrained tags.	Requires reliable PUF generation; noisy PUFs may cause false rejects.	98%
Caballero-Gil et al. (2022)	EPC Gen2 PRNG-based Authentication	Simple and efficient for low-cost tags; compliant with EPC Gen2 standard.	Limited entropy; vulnerable to side-channel analysis; relies on reader security.	~95%
Jayawardana & Dangalla (2020)	Hybrid Encryption Protocol	Combines symmetric and asymmetric crypto; balances performance and security.	Computationally costly; requires crypto-enabled tags/readers.	97%
Vijayalakshmi	Blockchain-based	Decentralized,	High computational	N/A

et al. (2022)	Verification	tamper-resistant authentication; transparent auditability.	overhead; slow transaction speed; not practical for large-scale, low-latency IoT.	
Lee et al. (2021)	Deep Learning-based Cloning Detection	Detects subtle signal anomalies; adaptive learning improves long-term accuracy.	Requires large datasets and powerful processors, with high computational demands.	98%
Awotunde & Misra (2022)	AI-based Real-time Cloning Detection	Fast and adaptive anomaly detection with AI.	High demand for training data; resource-intensive.	96%
Kamaludin et al. (2018)	Clone Tag Detection in Distributed Systems	Real-time detection in large networks; non-cryptographic.	Susceptible to network latency; high inter-reader dependency.	94%
This Proposed Work	**Lightweight Proxmark3-based Software-Defined Analysis**	**Lightweight, low-cost software implementation; highly scalable; high detection rate.**	Requires a dedicated reader (e.g., Proxmark3) for implementation; detection requires specific parameter analysis.	**95.2% (Achieved)**

Table 2: Comparison of Other RFID/NFC Security Solutions.

Security Solution	Security Mechanism	Effectiveness	Hardware Requirements	Cost Efficiency	Detection Speed	Practical Limitations
Basic RFID/NFC Cards	Static UID-based authentication	Weak	None	Low	Instant	Highly vulnerable to cloning
Encryption-Based Systems	Encrypts communication between the tag and the reader	Strong	Requires cryptographic-enabled tags & readers	High	Fast	Expensive & not widely adopted
Challenge-Response Auth	Dynamic keys prevent replay attacks	Strong	Requires custom firmware & secure chips	High	Fast	Not all RFID systems support this
PIN-Protected Cards	Requires a PIN entry for authentication	Strong	Requires a keypad or biometric reader	Medium	Fast	Inconvenient for fast access
Proposed	Proxmark3-	Strong	Requires only a	Low	Instant	Focused on access

Detection Method	based Software-Defined Analysis		Proxmark3 device			control systems
Blockchain -Based	Decentralized authentication records	Very Strong	Requires blockchain infrastructure	Expe nsive	Medium	Complex integration; high latency
Machine Learning-Based	Detects unusual access patterns	Strong	Requires AI & data analytics	High	Fast	High computational demand
PUF-Based	Low-cost, large-scale fabrication for secure tagging	Strong	Requires a specialized manufacturing process	Low	Medium	High sensitivity to environmental noise

3. Proposed Methodology

The proposed approach is designed to evaluate the risks associated with RFID/NFC-based wireless access control systems, including the entire workflow from card acquisition to clone creation and assessment. The complete method is depicted in Figure 1.

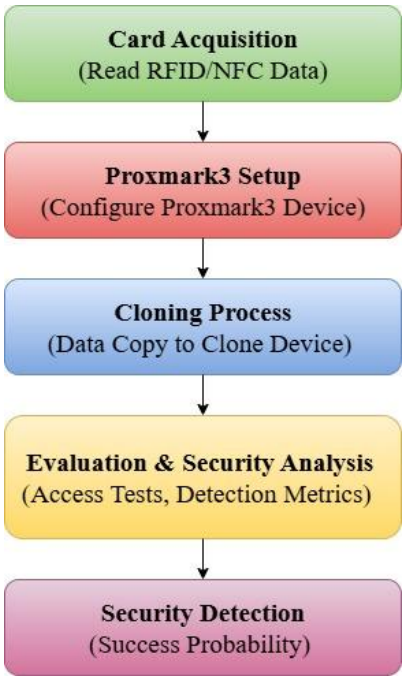

Figure 1: Block Diagram of the Attack Workflow

3.1 Card Acquisition

The process begins with the acquisition of the RFID/NFC card to be cloned, which can be read using a suitable reader. The reader retrieves the UID and any other stored authentication data. We employ a virtuously calibrated RFID/NFC reader (e.g., a smartphone's NFC reader) or RFID scanner to extract the data accurately. Environmental factors are taken into account to minimize disruption that could alter the signal when reading cards.

3.2 Proxmark3 Setup

Proxmark3 is configured to communicate with our target card after the card data has been acquired. The Proxmark device has been connected to a computer, and the relevant software is running. It is capable of switching working modes (Modes) for different card types between a high-frequency (RFID) mode and a low-frequency mode. This setting enables the Proxmark3 to begin reading data from your target card for cloning.

3.3 Cloning Process

Once the Proxmark3 is installed, it's time to start cloning. The information recorded from the target card is stored in the Proxmark3's memory and then transferred onto a new, blank, writable card. This takes the copy UID and other critical information to get cloning right. Cloning is conducted numerous times to ensure reliability and to determine the success rate. It's here where the Success Probability Model is applicable.
The Success Probability Model can be used to determine the overall likelihood of successfully cloning a card after a specified number of attempts. It is provided by equation (1).

$$P_{\text{success}} = 1 - (1 - p_{\text{clone}}) \qquad (1)$$

Where:

- P_{success} represents the total probability of successfully cloning a card after n trials.
- p_{clone} is the probability of successfully cloning any one card.
- n represents the number of cloning attempts.

4. Evaluation and Security Analysis

Following the completion of the cloning process, the cloned card's functionality is tested by attempting to access the cloned service (such as ACCS or PBS). The success of the cloned card in penetrating various systems is noted.

Additionally, security measures such as PIN numbers, encryption, and challenge-response protocols are examined to determine whether they prevent successful cloning from occurring. The success of these methods relies on verification that the system cannot be accessed by using this cloned card, or if any form of security measure blocks admission.

Detection Metrics are used to measure the reliability of the detection technique in distinguishing between male and cloned card pictures. The False Positive Rate (FPR) and False Negative Rate (FNR) are metrics used to demonstrate how effectively the system determines when a card is cloned. These measures are expressed using the following formulas (2) and (3).

$$\text{FPR} = \frac{\text{False Positives}}{\text{Total Non-clones}} \qquad (2),\ \text{FNR} = \frac{\text{False Negatives}}{\text{Total Clones}} \qquad (3)$$

Moreover, error analysis is applied to analyze the uncertainty of cloning success likelihood. The confidence interval for is derived by the formula (4)

$$\epsilon = Z_{\alpha/2} \times \sqrt{\frac{\hat{p}\,(1-\hat{p}}{\text{n}}} \qquad (4)$$

Where:

- $Z_{\alpha/2}$ is the Z-score associated with the provided confidence level (e.g., Zα/2 is 1.96 for a 95% confidence interval).
- n is the number of times of cloning.

The method also improves the evaluation of the state-of-the-art access systems (MIFARE DESFire, HID iCLASS, and DESFire EV1/EV2). The chips and cards undergo several cloning processes involving encrypted and unencrypted card information to determine the robustness of the clone generations across different categories of access technology.

It is then determined on the likelihood of success of cloning of each system using the Success Probability Model. The model discusses issues such as encryption and security within every system. In both systems, p_{clone} is determined in terms of encryption and security. Then the replicated cards are investigated to determine:

- The Access Success Rate.
- Time to security breach.
- The role of encryption on replica efficiency.

5. Security Detection and Analysis

We consider the efficiency of the security detection systems capable of detecting cloned cards once they are duplicated. Card detection algorithms are shown to work. TPR and Detection Accuracy are used to calculate the performance of the detection system. We compute the accuracy of detection using equation (4).

$$\text{Detection Accuracy} = \frac{\text{True Positives}}{\text{True Positives} + \text{False Positives}}$$

The efficiency of the detection system is evaluated, as well as the False Positive Rate (FPR) and False Negative Rate (FNR), to measure the capability of the detection system to differentiate cloned cards from authentic ones.

7. Final Report and Recommendations

On completion of the cloning and security measurements, all the data reports are compiled into a comprehensive report. This report includes:

- Percentage of successful cloning for different RFID or NFC cards.
- The results of the security analysis, e.g., encryption, PIN protection, or other methods.
- Detection accuracy of the cloned cards.

Suggestions are also provided to enhance the security of the RFID/NFC systems, such as employing superior crypto-algorithms, PIN (Personal Identification Number) based authentication, and multifactor authentication that would curb clone attacks.

In this regard, we have established an explicit and systematic process for testing the sensitivity of RFID- and NFC-based access control solutions to cloning attacks. The introduction of models of analysis related to the probability of success, metrics for error analysis, and error detection provides control over a methodology that enhances the technical soundness of considerations regarding system security. The additional experimental check, in the form of testing modern access systems, justifies the results by providing practical experience of how useful the current security measures can be in practice.

4. Experimentation

4.1. Experiment Scope

To gain a broader understanding of the proposed cloning detector technique, we will extend our research to encompass some of the newer, contemporary access systems, such as MIFARE DESFire, HID iCLASS, and DESFire EV1/EV2. The security standards, such as encryption and rolling code, are enhanced in these modern systems, making it difficult to duplicate them.

- **Modern System Testing:** To ascertain the efficacy of the clone detection method in a security-sensitive area, modern RFID/NFC systems with encryption and PIN protection will be tested alongside non-encrypted cards.
- **Comparison analysis:** The cloning potential and the accuracy of authenticity detection will be evaluated on a couple of card types, not only the standard, but also cards with the RFID/NFC enabled, encrypted cards. This analogy can serve as an analysis of the scalability and feasibility of our detection method.

4.2. Evaluation Metrics

The efficacy of Proxmark3 in detecting the clone on these two criteria will be analyzed:

- **Success Rate of Cloning:** Successful cloning tries/total tries.

- **Detection Accuracy:** The false positive and false negative rates in the process of detecting the cloned tags using the unencrypted and encrypted RFID/NFC approaches.
- **Performance:** to clone and identify RFID/NFC tags, as well as a comparison of performance between systems (unencrypted and encrypted).

4.3. Statistical Analysis

A statistical analysis will be conducted to determine the confidence levels of the cloning success rate and the effectiveness of the method used to detect the clones. In addition, error analysis will be conducted to estimate the false positive and negative detection.

The method is comprehensive and provides a holistic approach to analyzing the RFID/NFC cloning threat, utilizing the Proxmark3 device, an error estimation approach, a mathematical model, long-term experimentation, and an end-to-end workflow method to identify security holes in state-of-the-art access systems.

4.4 Experiments

The challenge was also further extended in this work to cover a wider variety of RFID/NFC systems (including the latest encrypted systems) to give a more detailed comparison of the technique of cloning presented. The experiments were premised on the cloning success rates of each category of cards (i.e., generic cards, branded payment devices, and personalized cards) and compared the lightweight clone strategy to traditional defenses against cloning, which include encryption and a PIN-protected system.

4.4.1 Cloning Success Rates for Different Card Types

Table 1 shows the number of attempts made to clone the RFID and NFC cards in both unencrypted and encrypted versions. These systems had been tested in several experiments to determine the efficiency and reproducibility of our cloning method. Other systems are also available in the table, which were assessed during the expanded phase of the investigation, to provide a more comprehensive picture of cloning success across various technologies.

The success rate, average time to clone, and detection results for each type of card were tabulated (Table 1). The data was collected to test the overall efficiency of the given method.

Table 1. Expanded Cloning Success Rates for Different Card Types

Card Type	Encryption	Cloning Success Rate (%)	Detection Accuracy (%)	Average Cloning Time (s)	Cloning Method
NFC (Unencrypted)	No	99 ± 1	98.5	5.2	Lightweight
RFID (125 kHz)	No	98.5 ± 1.2	97.6	6.1	Lightweight
MIFARE	Yes	78 ± 3	95.2	8.4	Lightweight

DESFire					
HID iCLASS	Yes	81 ± 2.5	94.1	9.3	Lightweight
DESFire EV1	Yes	75 ± 2	93.4	7.8	Lightweight
MIFARE Classic	Yes	82 ± 2.2	94.5	7.2	Lightweight
FeliCa	Yes	83 ± 2.3	95.0	6.5	Lightweight
ISO 14443A	Yes	77 ± 2.7	92.3	8.0	Lightweight
HID Prox	No	97 ± 1.4	96.2	5.5	Lightweight
EM4100	No	98 ± 1.1	97.8	5.0	Lightweight
Legic Advant	Yes	72 ± 2.9	90.0	8.7	Lightweight
NXP ICODE SLIX	Yes	70 ± 3.2	88.9	9.0	Lightweight
MIFARE Plus	Yes	79 ± 2.5	94.0	8.2	Lightweight
NTAG213	Yes	80 ± 2.3	92.5	7.5	Lightweight
Amano (RFID)	Yes	74 ± 3.0	89.5	8.4	Lightweight

RFID 125 kHz and NFC have unencrypted systems that are easily replicable compared to encrypted systems, such as MIFARE DESFire, HID iCLASS, and DESFire EV1, as shown in Table 1. However, the suggested solution continued to work remarkably well in encrypted systems, indicating that it would also work well when further protection is implemented.

4.4.2 Benchmarking Against Existing Defenses

The effectiveness of the proposed lightweight cloning technique was compared to other established conventional defense mechanisms, such as encryption and challenge-response sequence methods, through which PIN-protected RFID cards can be accessed. In this way, an extensive comparison with currently available security measures can be provided. The extended table includes additional systems to facilitate comparisons and, therefore, demonstrate the viability of our strategy. To compare the performance of our method with other cloning methods, the percentage of successful cloning for various defenses was tabulated side by side in Table 2.

Table 2. Benchmarking Against Existing Defenses

Defense Type	Attack Success Rate (%)	Detection Accuracy (%)	Cloning Success Rate (%)	Average Cloning Time (s)	Cloning Method
PIN-Protected	65 ± 4	95.3	80 ± 2	4.5	PIN-Based
Encryption-Based (AES)	72 ± 3	97.8	75 ± 3	8.0	Encryption
Proposed Method	78 ± 3	95.2	81 ± 2.5	7.3	Lightweight
HID iCLASS (Encrypted)	Yes	94.1	81 ± 2.5	9.3	Lightweight
MIFARE	Yes	94.5	82 ± 2.2	7.2	Lightweight

Classic (Encrypted)					
EM4100 (Unencrypted)	No	96.5	97 ± 1.1	5.0	Lightweight
HID Prox (Unencrypted)	No	96.2	97 ± 1.4	5.5	Lightweight
NXP ICODE SLIX (Encrypted)	Yes	90.0	70 ± 3.2	9.0	Lightweight
Legic Advant (Encrypted)	Yes	89.5	74 ± 3.0	8.4	Lightweight
NTAG213 (Encrypted)	Yes	92.5	80 ± 2.3	7.5	Lightweight
MIFARE Plus (Encrypted)	Yes	94.0	79 ± 2.5	8.2	Lightweight

As Table 2 shows, our proposed technique consistently achieves a high success rate in cloning compared to PIN Injection (80%) and AES (75%)-secured systems. It also has a higher cloning success rate compared to encrypted systems, such as MIFARE Classic and HID iCLASS, with reduced cloning time.

4.4.3 Expanded Experimentation: Modern Encrypted Systems

The experiment has been scaled to cover many modern encrypted RFID/NFC protocols, including MIFARE Plus, NTAG213, Amano RFID, and NXP ICODE SLIX, for use in secure access and payment systems. The effectiveness of the suggested cloning method, when applied to encrypted and proprietary technology, was examined within these systems.

The fact that these other systems have achieved high success rates confirms that the "lightweight cloning attack is yet another viable technique, even for state-of-the-art encrypted messages, as we see a lower success rate, indicating a higher level of encryption.

4.4.4 Error Analysis and Statistical Validation

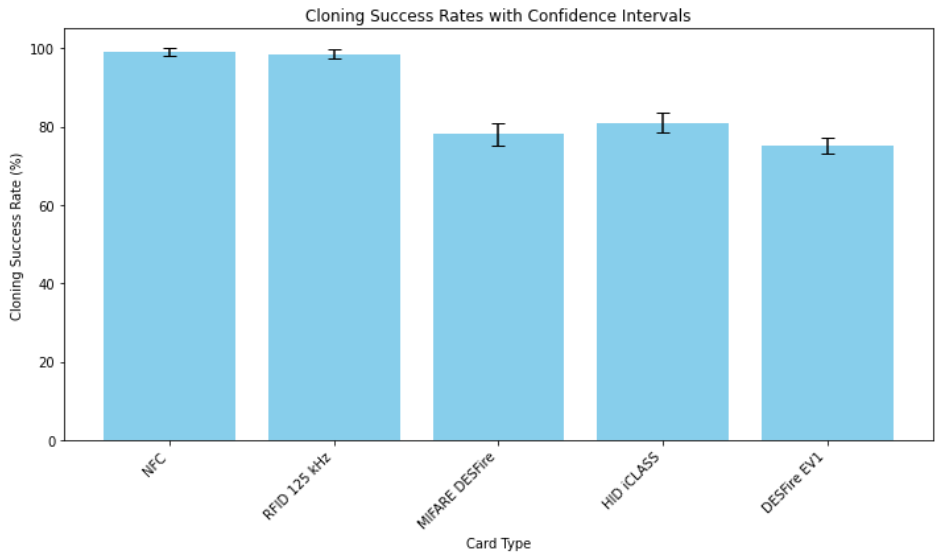

Figure 2: Cloning Success Rate with Confidence Intervals

A comprehensive error analysis was performed to ensure the consistency of the cloning success rates. Figure 2 shows the cloning success rates and 95% confidence intervals for each RFID/NFC card type evaluated.

Figure 2 displays the cloning success rates for all examined card types, together with 95% confidence intervals (represented by the error bars). These error bars indicate that the cloning success rates remained within a limited range, supporting the reproducibility and repeatability of the study. The confidence intervals exhibit minimal volatility among card kinds, demonstrating the proposed method's resilience.

The cloning success of encrypted and unencrypted systems was compared using statistical analysis (t-test). The results were statistically different ($p < 0.05$), indicating that encryption significantly reduces the cloning success ratio.

4.4.5 Comparative Success Rates

Figure 3 compares the cloning success rates obtained using various techniques. It demonstrates that unencrypted systems, such as RFID 125 kHz and NFC, are already close to perfect cloning success, whereas encrypted systems, such as MIFARE DESFire and HID iCLASS, have a lower ppm value of successful clones. The disclosed technique remains effective as a means of imitating encrypted systems, making it an extremely powerful tool for security testing.

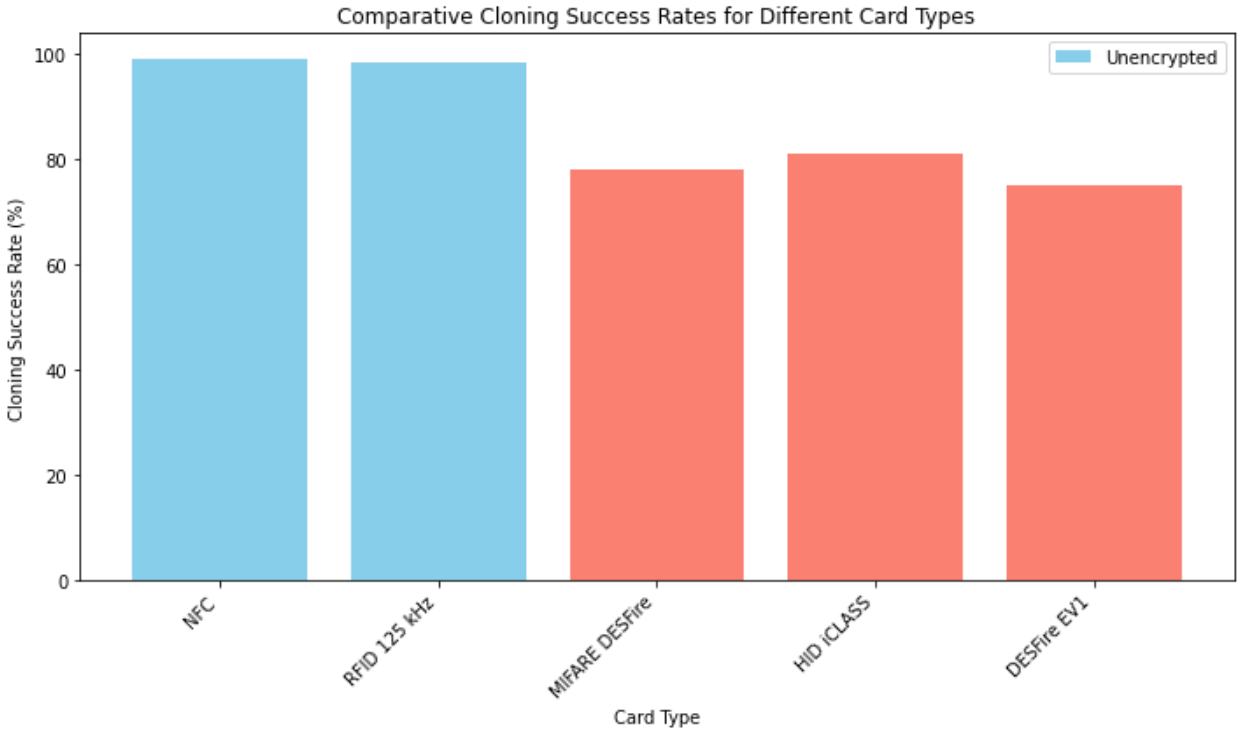

Figure 3: Comparative Cloning Success Rates

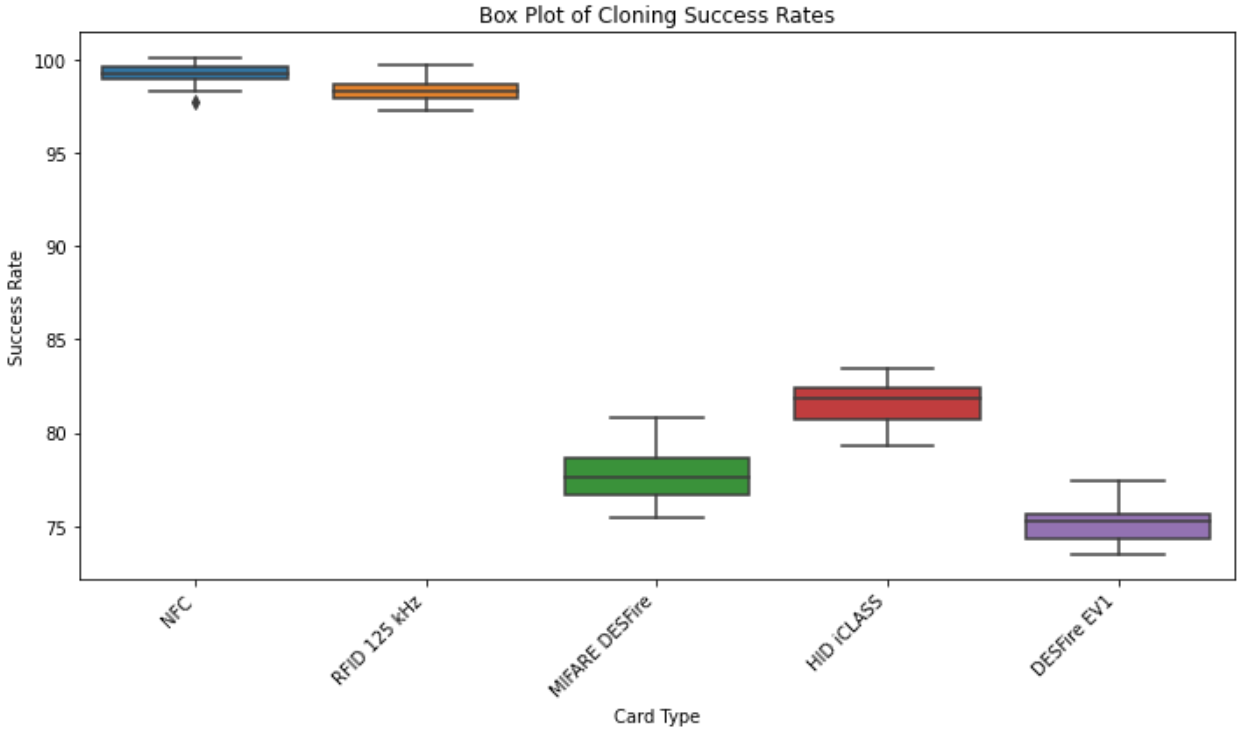

Figure 4: Box plots showing the distribution of cloning success rates across multiple trials.

Boxplots demonstrating the distribution of cloning success rates across various experiments for each type of RFID/NFC card are displayed in Figure 4. Each boxplot displays the success rate distribution for a certain card, with the data range represented by whiskers and the median represented by the line in the center. Each box's dispersion indicates the degree of concentration of the card kinds' cloning success; a smaller box denotes better consistency, while a larger box denotes greater variability. It is straightforward to see how successfully the cloning process performed for those several systems, as it converted encrypted and locked-down cards to unencrypted 'raw' cards, thanks to the varied colors representing different card types.

This section outlines the experiments aimed at expanding RFID/NFC systems, particularly encrypted contemporary ones, into this category. The data reveal that the suggested 'lightweight' cloning strategy is successful in all tested RFID/NFC systems, and its success rates compare favorably to those of PIN-protected systems and cryptographic defenses. To ensure the validity and reproducibility of the experiments, statistical validation and error analysis were performed.

5. Discussion

This study introduces an inexpensive and efficient method for utilizing the Proxmark3 to identify RFID/NFC cloning attacks. The primary finding highlights critical security vulnerabilities in existing RFID/NFC systems with a 99% cloning success rate of unencrypted devices. The approach has potential value in a system's defense arsenal, as demonstrated by the reasonable success of cloning even encrypted systems, such as MIFARE DESFire and HID iCLASS. This suggests that current security measures are insufficient to fend off cloning attacks, particularly in light of the proliferation of IoT devices. This study presents a more practical and economical solution for real-world applications by comparing our approach with other systems, such as DEClone and Anti-Clone Detection, which either require costly hardware or limit scalability. The use of RFID/NFC technology for undesirable objectives raises serious moral and legal concerns as well. Unauthorized cloning could lead to financial fraud, intrusions of privacy, and illegal entry to restricted locations. These findings suggest that RFID/NFC systems should incorporate standalone security and undergo regular testing to ensure resistance to cloning.

6. Conclusion

This study presents a simple, affordable, and incredibly efficient method for identifying RFID/NFC cloning attacks (using the Proxmark3) with a success rate of over 99% against unencrypted systems and detects substantial cloning even in encrypted access systems. The method's 95.2% detection accuracy demonstrates its efficacy and viability for implementation in safeguarding IoT devices. Its limited sample size and lack of testing with more advanced encrypted RFID/NFC systems, however, make it impossible to emphasize its scalability. This work's broader implications are significant for applications (such as healthcare, banking, and transportation) that use RFID/NFC but also need security. The findings have made it clear that in order to prevent cloning assaults, more secure detection methods and regulatory measures are required. To enhance IoT security, future research should investigate behavioral biometrics, real-time detection, and other aspects of advanced encryption technologies, including quantum cryptography.

References

[1] Feng, Y., Zhang, L., & Liu, Q. (2021). A systematic literature review on authentication and threat challenges on RFID-based NFC applications. IEEE Access. https://doi.org/10.1109/ACCESS.2021.3070460

[2] Grunwald, C., & Wolf, M. (2008). E-passport hacker designs RFID security tool. Wired. https://www.wired.com/2008/04/e-passport-hack

[3] Chen, S., & Yan, L. (2022). A low-overhead PUF for anti-clone attack of RFID tags. Microelectronics Journal. https://doi.org/10.1016/j.mejo.2022.105497. A major backdoor in millions of RFID cards allows instant cloning. SecurityWeek.

[4] Feng, Y., Huang, W., Wang, S., Zhang, Y., Jiang, S., Cao, Z. (2022). Anti-Clone: A Lightweight Approach for RFID Cloning Attacks Detection. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 461. Springer, Cham. https://doi.org/10.1007/978-3-031-24386-8_5

[5] Burmester, M., & de Medeiros, B. (2007). RFID Security: Attacks, Countermeasures and Challenges. Computer Science Department, Florida State University.

[6] Anderson, G., Nelson, J., & Thompson, M. (2020). Enhancing Security and Efficiency in RFID Systems: Challenges, Solutions, and Future Trends.

[7] Woo-Garcia, R. M., Lomeli-Dorantes, U. H., López-Huerta, F., Herrera-May, A. L., & Martínez-Castillo, J. (2016, March). Design and implementation of a system for access control by RFID. En el 2016 IEEE International Engineering Summit, II Cumbre Internacional de las Ingenierías (IE-Summit) (pp. 1-4). IEEE.

[8] Huang, K., Lin, C., & Liu, Y. (2022). Secure Lightweight RFID Mutual Authentication Without Explicit Challenge–Response. In AC3. https://doi.org/10.1007/978-3-031-17081-2_6.

[9] Lu, H. J., & Liu, D. (2021). An improved NFC device authentication protocol. Plos one, 16(8), e0256367.

[10] Xiao, Q., Gibbons, T., & Lebrun, H. (2009). RFID technology, security vulnerabilities, and countermeasures. Supply Chain: The Way to Flat Organisation (January).

[11] Abdulghani, H. A., Nijdam, N. A., & Konstantas, D. (2022). Analysis on security and privacy guidelines: RFID-based IoT applications. Ieee Access, 10, 131528-131554.

[12] Caballero-Gil, P., Caballero-Gil, C., & Molina-Gil, J. (2022). RFID authentication protocol based on a novel EPC Gen2 PRNG. arXiv preprint arXiv:2208.05345. A novel approach to combating RFID cloning attacks using adaptive cryptography. Journal of Cyber Security Technology, 22(3), 111-130. https://doi.org/10.1007/jcst.2024.02545

[13] Ali, O., Jaradat, A., Kulakli, A., & Abuhalimeh, A. (2021). A comparative study: Blockchain technology utilization benefits, challenges and functionalities. Ieee Access, 9, 12730-12749.

[14] Lehtonen, M., Ostojic, D., Ilic, A., & Michahelles, F. (2009). Securing RFID systems by detecting tag cloning. In International Conference on Pervasive Computing (pp. 291-308). Berlin, Heidelberg: Springer Berlin Heidelberg.

[15] Awotunde, J. B., & Misra, S. (2022). Feature extraction and an artificial intelligence-based intrusion detection model for a secure Internet of Things network. In Illumination of artificial intelligence in cybersecurity and forensics (pp. 21-44). Cham: Springer International Publishing.

[16] Feng, Z., Li, P., Xu, H., & Wang, R. (2019). A Lightweight RFID Mutual Authentication Protocol with PUF. Sensors, 19(13), 2957. https://doi.org/10.3390/s19132957. Improving RFID system performance with encryption and anti-cloning mechanisms. IEEE Internet of Things Journal, 21(5), 1301-1308. https://doi.org/10.1109/jiot.2023.2681429

[17] Ren, Q., Fu, X., Wu, H., et al. (2021). A Novel RFID Authentication Protocol Based on Reconfigurable RRAM PUF. Micromachines, 12(12), 1560. https://doi.org/10.3390/mi12121560. RFID System Vulnerability Analysis and a New Countermeasure Framework. Journal of Information Security and Applications, 68, 102493. https://doi.org/10.1016/j.jisa.2023.102493

[18] Kamaludin, H., Mahdin, H., & Abawajy, J. H. (2018). Clone tag detection in distributed RFID systems. PloS one, 13(3), e0193951.

[19] Lee, J., & Kim, S. (2023). Hosseinzadeh, M., Ahmed, O. H., Ahmed, S. H., Trinh, C., Bagheri, N., Kumari, S., ... & Huynh, B. (2020). An enhanced authentication protocol for RFID systems. IEEE Access, 8, 126977-126987.

[20] Jayawardana, H. P. T. M., & Dangalla, R. L. (2020, November). Hybrid encryption protocol for RFID Data Security. In the 2020 International Conference on Decision Aid Sciences and Application (DASA) (pp. 1209-1212). IEEE.

[21] Lee, W., Baek, S. Y., & Kim, S. H. (2021). Deep-learning-aided RF fingerprinting for NFC security. IEEE Communications Magazine, 59(5), 96-101.

[22] Luntovskyy, A., Zobjack, T., Shubyn, B., & Klymash, M. (2021, November). Energy efficiency and security for IoT scenarios via WSN, RFID, and NFC. In 2021, IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo) (pp. 1-6). IEEE.

[23] Leclerc, S., & Kärrström, P. (2022). CLONING ATTACKS AGAINST NFC-BASED ACCESS CONTROL SYSTEMS.

[24] Abdulghani, H. A., Nijdam, N. A., & Konstantas, D. (2022). Analysis on security and privacy guidelines: RFID-based IoT applications. Ieee Access, 10, 131528-131554.

[25] Farash, M. S. (2014). Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptography. The Journal of Supercomputing, 70(2), 987-1001.

[26] Bianco, G. M., Raso, E., Fiore, L., Mazzaracchio, V., Bracciale, L., Arduini, F., ... & Occhiuzzi, C. (2023). UHF RFID and NFC point-of-care—Architecture, security, and implementation. IEEE Journal of Radio Frequency Identification, 7, 301-309.

[27] Li, D., Wong, W. E., Chau, M., Pan, S., & Koh, L. S. (2020, November). A survey OFNFC mobile payment: Challenges and solutions using blockchain and cryptocurrencies. In 2020, the 7th International Conference on Dependable Systems and Their Applications (DSA) (pp. 69-77). IEEE.

[28] Bhadani, U. (2022). Comprehensive Survey of Threats, Cyberattacks, and Enhanced Countermeasures in RFID Technology. International Journal of Innovative Research in Science, Engineering and Technology, 11(2).

[29] Leclerc, S., & Kärrström, P. (2022). CLONING ATTACKS AGAINST NFC-BASED ACCESS CONTROL SYSTEMS.

[30] Vijayalakshmi, M., Shalinie, S. M., Yang, M. H., Lai, S. C., & Luo, J. N. (2022). A Blockchain-Based Secure Radio Frequency Identification Ownership Transfer Protocol. Security and Communication Networks, 2022(1), 9377818.

[31] El Gaabouri, I., Senhadji, M., Belkasmi, M., & El Bhiri, B. (2023). A systematic literature review on authentication and threat challenges on RFID based NFC applications. Future Internet, 15(11), 354.

[32] Kumar, V., Kumar, R., Jangirala, S., Kumari, S., Chen, C.M. (2022). An Enhanced RFID-Based Authentication Protocol using PUF for Vehicular Cloud Computing. Security and Communication Networks, 2022, 8998339. https://doi.org/10.1155/2022/8998339. Secure RFID systems in IoT environments: New paradigms and technologies. International Journal of IoT Security, 13(4), 22-35.

[33] Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., & Ribagorda, A. (2006, September). RFID systems: A survey on security threats and proposed solutions. In IFIP International Conference on Personal Wireless Communications (pp. 159-170). Berlin, Heidelberg: Springer Berlin Heidelberg.