ISSN: 2395-7852

# International Journal of Advanced Research in Arts, Science, Engineering & Management

Volume 10, Issue 3, May 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 6.551

+91 9940572462 +91 9940572462 ijarasem@gmail.com www.ijarasem.com

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 6.551 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 10, Issue 3, May 2023 |

# Prevention against Probabilistic Cloning Attacks in Anonymous RFID Systems

**Mr. K. Balachander[1], K. Kasthuri[2] , P. S. Nivetha Shree[3], K. Yuvanthi[4]**

[1]Associate Professor, Department of Computer Science and Engineering, Velammal Institute of Technology, Panchetti, Chennai, India

[2]Department of Computer Science and Engineering, Velammal Institute of Technology, Panchetti, Chennai, India

[3]Department of Computer Science and Engineering, Velammal Institute of Technology, Panchetti, Chennai, India

[4]Department of Computer Science and Engineering, Velammal Institute of Technology, Panchetti, Chennai, India

**ABSTRACT:** Radio frequency identification (RFID) is used in staff Id-cards for attendance.The technology used is Cyber Security in the domain Internet of Things(IOT)This project focuses on how RFID is hackable. For example, RFID metro card-when the hardware which we designed is brought near another targeted RFID card, then the data of Unique Identification(UID) from Targeted card will be copied automatically to the hardware which we designed. so we will be having the full data of targeted RFID card in our hardware. Radio Frequency Identification (RFID) refers to a wireless system comprised of two components: tags and readers. The reader is a device that has one or more antennas that emit radio waves and receive signals back from the RFID tag.

## I. INTRODUCTION

The RFID reader is a network-connected device that can be portable or permanently attached.Radio Frequency Identification (RFID) refers to a wireless system comprised of two components: tags and readers. The reader is a device that has one or more antennas that emit radio waves and receive signals back from the RFID tag. It uses radio waves to transmit signals that activate the tag. Once activated, the tag sends a wave back to the antenna, where it is translated into data.While your RFID card is safe in your wallet, a hacker scans the card in your pocket without you knowing.

The attacker can then siphon money or steal information without you knowing about it.It can range up to 100 m.RFID can scan items from inches to feet away, depending on type of tag and reader. RFID tags come in a variety of shapes and sizes and are either passive or active. Passive tags are the most widely used, as they are smaller and less expensive to implement. Passive tags must be “poweredup”by the RFID reader before they can transmit data.

Radio-Frequency Identification (RFID) is an emerging technology which has been widely applied in various scenarios , such as tracking, object monitoring, and social networks.Cloning attacks can severely disturb the RFID systems, such as missed detection for the missing tags.Although there are some techniques with physical architecture design or complicated encryption and cryptography proposed to prevent the tags from being cloned, it is difficult to definitely avoid the cloning attack.In this paper, we conduct the first comprehensive and systematic survey of RFID clone prevention and detection solutions.

The architecture-succinctness and cost-effectiveness of RFID tags promise their proliferation as well as allure security and privacy breaches.Cloning attack using clone tags to impersonate genuine tags can lead to unimaginable threats because RFID applications equate tag genuineness to the authenticity of tagged objects.

Cloning of RFID tags may lead to considerable financial losses and worse reputation in many commercial applications, while being attractive for adversaries.One way to address tag cloning is to use the visibility that RFID traces provide to detect cloned tags as soon as they enter the system.This paper presents a series of probabilistic techniques to enable reliable detection of cloned tags in cases where the visibility is incomplete.

In RFID system hackers create duplicate cards. After creating duplicate cards they will place the hardware near the RFID-ID cards.Then the data will be read from RFID-ID cards. After the data us read then we have to place the duplicate card over the hardware. Then the copied data will be written on the duplicate card.So that the hacker will use the duplicate card as original I'd card.

Paper is organized as follows. Section 1 describes about the RFID cards and its use. In section2wedescribed about how cloning attacks disturbs RFID systems and reliable detection of cloned tags and breaching .In section 3 we described how RFID system works in our project.

## II. RELATED WORKS

Zeshan Ali, Etienne Perret, Nicolas Barbot, Romain Siragusa, David Hely had dedicated to the authentication of manufactured products is proposed. The proposed technique is an extension of chipless radio frequency identification (RFID) with the prevention of tags' cloning due to the use of natural randomness in the fabrication process. For the first time, we proposed a methodology to characterize the chipless RFID tags for the purpose of authentication. The proposed method has a high level of security due to the employment of a database of authenticity. With a nonintrusive and nondestructive operation, the proposed method has promising possibilities for authentication applications, for example, the chipless tags can be inserted (or hidden) in the product packaging.

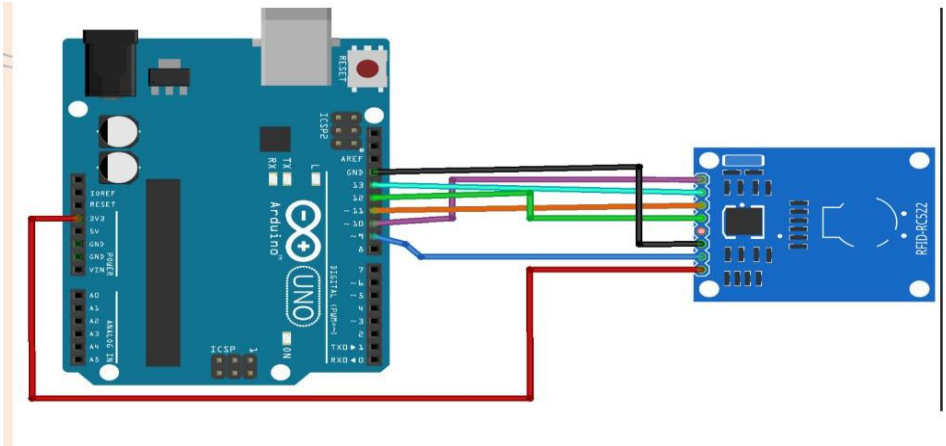
Mikko Lehtonen,Florian Michahelles have told about cloning of RFID tags may lead to considerablefinancial losses and worse reputation in many commercial applications, while being attractive for adversaries. One way to address tag cloning is to use the visibility that RFID traces provide to detect cloned tags as soon as they enter the system. However, RFID traces always represent historic events without giving certainty where the traced objects currently really are. Furthermore, imperfect read rates can lead to missing reads. As a result, the visibility is not always perfect, which makes detection of cloned tags harder and less reliable. These findings suggest that reliable detection of cloned tags is possible if missing reads are addressed and the supply chain is precisely modeled.

Honglong Chen, Senior Member, IEEE, Xin Ai, Kai Lin proposed Radio frequency identification (RFID) systems have achieved wide applications in various scenarios, such as warehouse management, logistic tracking, and smart transportation, etc. Despite the enormous benefits from the RFID systems, the security issues are still of great concern, such as the cloning attacks. In this paper, we focus on the detection of probabilistic cloning attacks for the anonymous RFID systems, in which each cloned genuine tag suffers attacks from its clone tags with a certain probability. We propose an efficient Detection protocol Against the Probabilistic cloning attacks in anonymous RFID systems named DAP, which can detect the probabilistic cloning attacks.Kai Bu, Member, IEEE, Minyu Weng, Yi Zheng, Bin Xiao Radio-Frequency Identification (RFID) is one of the driving technologies for Internet of Things (IoT). The architecture-succinctness and costeffectiveness of RFID tags promise their proliferation as well as allure security and privacy breaches. The cloning attack using clone tags to impersonate genuine tags can lead to unimaginable threats because RFID applications equate tag genuineness to the authenticity of tagged objects.

Xin Ai, Honglong Chen Radio-Frequency Identification (RFID) is an emerging technology which has been widely applied in various scenarios, such as tracking, object monitoring, and social networks, etc. Cloning attacks can severely disturb the RFID systems, such as missed detection for the missing tags. Although there are some techniques with physical architecture design or complicated encryption and cryptography proposed to prevent the tags from being cloned, it is difficult to definitely avoid the cloning attack. Therefore, cloning attack detection and identification are critical for the RFID systems.

## III. PROPOSEDSYSTEM

The architecture of our system is illustrated below. Figure 1 shows the overall architecture of the system. The major component of the system are Rfid-Idcards , hardware, jumperwires.



### 3.1 DESCRIPTION

#### 3.1.1 ARDUINO UNO

Arduino is an open-source platform used for building electronics projects. Arduino consists of both a physical programmable circuit board (often referred to as a microcontroller) and a piece of software, or IDE (Integrated Development Environment) that runs on your computer, used to write and upload computer code to the physical board.

The Arduino platform has become quite popular with people just starting out with electronics, and for good reason. Unlike most previous programmable circuit boards, the Arduino does not need a separate piece of hardware (called a programmer) in order to load new code onto the board -- you can simply use a USB cable.


#### 3.1.2 RFID TAGS

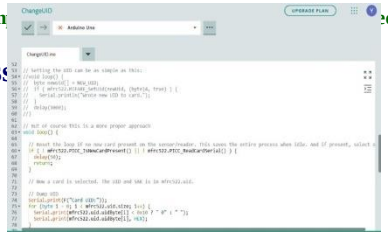
RFID tags are a type of tracking system that uses smart barcodes in order to identify items. RFID is short for “radio frequency identification” ,and as such, RFID tags utilize radio frequency technology. These radio waves transmit data from the tag to a reader, which then transmits the information to an RFID computer program. RFID tags are frequently used for merchandise, but they can also be used to track vehicles, pets, and even patients with Alzheimer’s disease. An RFID tag may also be called an RFID chip.

An RFID tag works by transmitting and receiving information via an antenna and a microchip — also sometimes called an integrated circuit or IC. The microchip on an RFID reader is written with whatever information the user wants.


#### 3.1.3 RFID BLOCKER

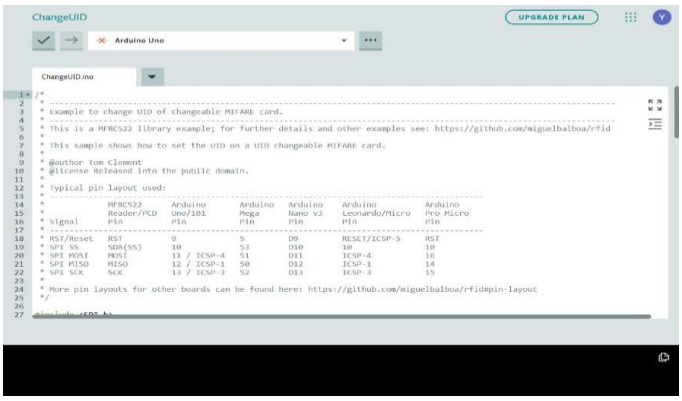
RFID-blocking shields block any signals to RFID-enabled cards so that no one can access the information without your permission. Remember, it's not just your money they can steal, but also your personal details, including full names and addresses.

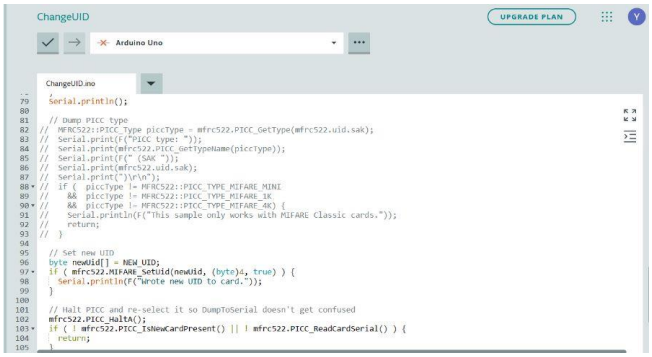
RFID blocking systems reduce the transmitted signal power of the reader, preventing the microchip in the RFID card from working. This ensures RFID card security. Essentially, RFID readers transmit signals which power the microchip



in the card, the microchip in the card then powers up and send data back to the reader. This can be prevented by either deflecting/blocking RFID signals, or by transmitting a signal that interferes with the reader but this only works with one frequency and often a certain type of technology

## IV. FEATURE EXTRACTION






## V. EXPERIMENT RESULTS

## VI. CONCLUSION AND FUTURE ENCHANCEMENT

Many may first notice RFID tags in security and health applications.People will also begin to experiment with personalized applications. RFID will become a component in home-management systems, which will help to schedule shopping, laundry, and other tasks. Provide awareness on these attack to public. We can provide awareness regarding these attacks so they can protect their RFID and Near Field Communication cards.

Clone tags can impersonate genuine tags and thus impose unimaginable threats to various RFID applications. Due to resource constraints of tags, it is not affordable to prevent RFID cloning using complex cryptographic techniques. Although unique physical characteristics of tag chips can be used to identity tags, they are susceptible to environmental factors and may need certain enhancements over tag hardware. We therefore need detection solution to check whether clone tags exist in an RFID system. We systematically classify existing clone prevention and detection solutions.
Our motive is to educate people regarding RFID cloning attack. RFID users shoulduse RFID blocker to prevent this attack. RFID system should produce encryption to protect RFID users data.

## REFERENCES

1. "Guardrfid," https://www.guardrfid.com/solutions/healthcare.
2. X. Ai, H. Chen, K. Lin, Z. Wang, and J. Yu, "Nowhere to Hide: Efficiently Identifying Probabilistic Cloning Attacks in Large-Scale RFID Systems," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 714–727, 2021.
3. C. Bertoncini, K. Rudd, B. Nousain, and M. Hinders, "Wavelet Fingerprinting of Radio-Frequency Identification (RFID) Tags," IEEE Transactions on Industrial Electronics, vol. 59, no. 12, pp. 4843 – 4850, 2012.
4. K. Bu, X. Liu, J. Luo, B. Xiao, and G. Wei, "Unreconciled Collisions Uncover Cloning Attacks in Anonymous RFID Systems," IEEE Transactions on Information Forensics and Security, vol. 8, pp. 429–439, 2013.
5. K. Bu, M. Xu, X. Liu, J. Luo, S. Zhang, and M. Weng, "Deterministic Detection of Cloning Attacks for Anonymous RFID Systems," IEEE Transactions on Industrial Informatics, vol. 11, no. 6, pp. 1255–1266, 2015.
6. H. Chen, Z. Wang, F. Xia, Y. Li, and L. Shi, "Efficiently and Completely Identifying Missing Key Tags for Anonymous RFID Systems," IEEE Internet of Things Journal, vol. 5, pp. 2915–2926, 2018.
7. H. Chen, G. Xue, and Z. Wang, "Efficient and Reliable Missing Tag Identification for Large-Scale RFID Systems with Unknown Tags," IEEE Internet of Things Journal, vol. 4, no. 3, pp. 736–748, 2017.
8. X. Chen, J. Liu, X. Wang, H. Liu, D. Jiang, and L. Chen, "Eingerprint:Robust Energy-related Fingerprinting for Passive RFID Tags," in Proc.of USENIX NSDI, 2020.
9. X. Chen, J. Liu, X. Wang, X. Zhang, Y. Wang, and L. Chen, "Combating Tag Cloning with COTS RFID Devices," in Proc. of IEEE SECON, 2018, pp. 1–9.
10. E. Y. Choi, D. H. Lee, and J. I. Lim, "Anti-cloning Protocol Suitable to Epcglobal Class-1 Generation-2 RFID Systems". "Guardrfid," https://www.guardrfid.com/solutions/healthcare.
11. X. Ai, H. Chen, K. Lin, Z. Wang, and J. Yu, "Nowhere to Hide: Efficiently Identifying Probabilistic Cloning Attacks in Large-Scale RFID Systems," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 714–727, 2021.
12. C. Bertoncini, K. Rudd, B. Nousain, and M. Hinders, "Wavelet Fingerprinting of Radio-Frequency Identification (RFID) Tags," IEEE Transactions on Industrial Electronics, vol. 59, no. 12, pp. 4843 – 4850, 2012.
13. K. Bu, X. Liu, J. Luo, B. Xiao, and G. Wei, "Unreconciled Collisions Uncover Cloning Attacks in Anonymous RFID Systems," IEEE Transactions on Information Forensics and Security, vol. 8, pp. 429–439, 2013.
14. K. Bu, M. Xu, X. Liu, J. Luo, S. Zhang, and M. Weng, "Deterministic Detection of Cloning Attacks for Anonymous RFID Systems," IEEE Transactions on Industrial Informatics, vol. 11, no. 6, pp. 1255–1266, 2015.
15. H. Chen, Z. Wang, F. Xia, Y. Li, and L. Shi, "Efficiently and Completely Identifying Missing Key Tags for Anonymous RFID Systems," IEEE Internet of Things Journal, vol. 5, pp. 2915–2926, 2018.
16. H. Chen, G. Xue, and Z. Wang, "Efficient and Reliable Missing Tag Identification for Large-Scale RFID Systems with Unknown Tags," IEEE Internet of Things Journal, vol. 4, no. 3, pp. 736–748, 2017.
17. X. Chen, J. Liu, X. Wang, H. Liu, D. Jiang, and L. Chen, "Eingerprint:
18. Robust Energy-related Fingerprinting for Passive RFID Tags," in Proc.of USENIX NSDI, 2020.
19. X. Chen, J. Liu, X. Wang, X. Zhang, Y. Wang, and L. Chen, "Combating Tag Cloning with COTS RFID Devices," in Proc. of IEEE SECON, 2018,pp. 1–9.
20. E. Y. Choi, D. H. Lee, and J. I. Lim, "Anti-cloning Protocol Suitable to Epcglobal Class-1 Generation-2 RFID Systems".


# International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| Mobile No: +91-9940572462 | Whatsapp: +91-9940572462 | ijarasem@gmail.com |

www.ijarasem.com