NFC Tag Authentication: An Overview

Oluwaseyi Giwa [*]
Department of Electrical and Electronics Engineering
Olabisi Onabanjo University
Ago-Iwoye, PMB 2002
giwaoluwaseyi475@gmail.com

Abstract

Near Field Communication (NFC) technology is a short-range wireless communication between two devices that are NFC-enabled. NFC has found application in various institutions like the finance sector, security systems, medicine, etc. Consequently, this has led to a lot of focus on securing NFC transactions. Since most attacks on NFC devices are within the tag, the need to create a more secure tag authentication has increased over the past years.
In this paper, I discussed NFC tag authentication and its challenges. Furthermore, I analyzed different existing NFC tag authentication and their respective strengths and weaknesses. The NFChain is better than the existing solutions discussed in this paper. It is cost-friendly, highly secured, and allows extra computation on the tag without requiring additional hardware solutions.
In summary, the purpose of this study is to provide insights into NFC tag authentication and the need to conduct more research to ensure more security in this mode of communication.

Keywords **NFC tag · NFChain · Wireless communication · Authentication**

1 Introduction

Near Field Communication (NFC) technology is a short-range wireless communication method between a mobile electronic device and a terminal. It makes life easier by making smartphones more convenient for consumers around the world [2]. The size of the NFC market in 2019 was $ 15 billion and is expected to be $54 billion in 2028 [41, 42].

The function of the NFC tag is very varied, for example, it stores URLs to open a certain webpage, [24] proposed a NFC tag IC to improve telehome healthcare, dials a phone number, gives information about a certain product, and many more. Because of that, storing data on a tag sometimes requires security. The related work for NFC security usually focuses on secure transactions between devices, and there are very few works that discuss the security of information inside tags. The simplest method to protect information inside a tag is to use the tag as a medium to access a secure database, so the tag only contains an identification number(ID) to identify the object where the tag is installed. All NFC tags must follow the specifications of the NFC Date Exchange Format (NDEF), published by NFC Forum [39]. Using a tag as a data medium may decrease the flexibility of the tag functions so it needs a method to secure the data itself inside the tag. Considering the importance of the NFC tag as a powerful tool for identification, it is necessary to make efforts to build a method to build a secure system involving the NFC tag, in this case by authenticating the tag to ensure that the tag is valid and has permission to access certain services.

NFC tags are small transponders that can be embedded in physical objects to provide information for identification. The tag works similarly to a smart card; the only difference is that it does not have a power supply, that is, it is a passive RFID; it is energized only when the reader approaches to read the identification number (ID) inside the tag[1]. NFC tags are very useful to implement because tapping the tag with NFC-enabled mobile phones is very simple to do.

[*] Oluwaseyi Giwa is a graduate of electrical and electronics engineering at Olabisi Onabanjo University, Nigeria.

Figure 1: An NFC card

Figure 2: An NFC card reader

I discussed various NFC tag authentication solutions and the analysis of each one in this paper. The structure of the subsequent sections in this paper is as follows:

- NFC Technology Overview.
- NFC Tag Authentication Methods.
- Existing NFC Tag Authentication Solutions.
- Analysis of Existing NFC Tag Authentication.
- Conclusion

2 NFC Technology Overview

In this section, I dived into the definition of NFC, the different types of NFC tags, and the three modes of operation of the NFC.

2.1 Definition of NFC

Near-field communication, also called NFC, is contactless, short-range wireless communication between devices that are NFC-enabled. Due to its short distance, NFC is more secure than Bluetooth. NFC operates on the principles of electromagnetic radio fields at 13.56 MHz frequency and over a distance of up to 4cm. It is based on RFID technology, which allows two devices to communicate when they are brought into close proximity. Most mobile devices now have an NFC chip incorporated in them. NFC has many applications, ranging from ticketing, drug production, mobile payments, home security, and so many more. Figures 1 and 2 show a typical example of a card that is NFC enabled and the card reader, respectively [29].

2.2 NFC Tag Types

There are two main types of NFC tags which are, active tags and passive tags. The active tag has an internal power source that allows it to transmit data to NFC readers. Consequently, active tags can support complex computation and have a higher storage capacity. Passive tags do not have internal power and thus rely on the energy transmitted by the NFC reader brought in close proximity to them. The lack of an internal power source restricts the computational ability and storage capacity of passive tags. The passive tag is generally used due to its size (which is smaller than the active tag) and because it is less expensive than the active tag.

2.3 NFC Communication Modes

NFC generally operates in three modes, which are [7, 13]:

1 Reader/Writer mode: The device that starts the communication is known as the initiator and the other as the target [19]. The initiator sends out an RF field, which powers the target if it is passive or activates it if it is active.

2 Peer-to-Peer mode: The peer-to-peer (P2P) mode enables direct data exchange between two NFC-enabled devices without the need for an external NFC reader or tag. The two device share files and transfer data by establishing a bidirectional connection [13, 15].

3 Card Emulation mode: In this mode, devices with NFC capability act like smartcards for contactless payment, ticketing, and so on [7].

3 NFC Tag Authentication Methods

There are different NFC tag authentication methods, ranging from basic ones such as password authentication to more complex ones such as biometric authentication. In this section, I explored various NFC tag authentication methods.

1 Password Authentication: The NFC tag requires a password or PIN code for authentication to occur. Password authentication is one of the simplest authentication methods over insecure networks [20]. However, an intruder can easily intercept the password and ID of a user or steal a user's information through a wire tap of an unencrypted password. Password authentication is more efficient as an additional security layer for NFC tag authentication, and it can be supported with more secure authentication methods, such as biometric authentication. The authors in [4] employed the combination of a fingerprint scheme and password authentication to add an extra layer of security to a home security system.

2 Public Key Infrastructure (PKI): This method uses asymmetric cryptography, where the NFC tag holds a private key, and the reader verifies the authenticity using the tag's public key. Secure key establishment is one of the pillars of cryptography [22], which offers great security for IoT devices. The start of Industry 4.0 has made machines and other equipment embedded with NFC tags to enhance IoT devices, thus the need for a secure means of communication between connected IoT devices with PKI as a better alternative to the problematic symmetric encryption algorithm [21].

3 Time-based Authentication: In this authentication method, a secret key is shared between two devices on a one-time basis. The method can be achieved through the scanning of QR codes, an SMS that displays a one-time password (OTP) for the user, or the use of authentication apps that generate random codes for authentication, such as Google authenticator, Duo security, and many others. OTP is a mechanism to reduce the risk of an unauthorized person getting access to an account because it has a specified time span and, contrary to static passwords, has a security technique shield for the various password-based attacks, specifically password sniffing and reply attacks [23].

4 Biometric Authentication: This authentication method is often preferred to other authentication methods because of its tight security. It involves the use of a fingerprint, an iris scan, or a combination of both. The authors in [3] in their design for an authentication scheme utilized the fingerprint scheme; [4] added a fingerprint scan to provide an additional security layer to their design of a home security system. Biometric authentication has found many applications in different sectors; for example, the authors in [6] designed hardware-fingerprint authentication for NFC devices in power grids. This example shows that biometric authentication is employed in a variety of aspects.

3.1 Challenges in NFC Tag Authentication

3.1.1 Computational Resources

NFC tags are typically passive and therefore have limited computational power and storage, restricting the complexity of cryptographic algorithms that can be implemented for authentication. [3]

3.1.2 Security and Privacy Risks:

1 Eavesdropping: Because NFC uses radio waves to transmit information, there is a probability that someone with the right equipment could eavesdrop on the data being exchanged between an NFC-enabled device and a reader. Eavesdropping attacks can either be active or passive [25].

2 Relay Attacks: An attacker can exploit the short-range communication of NFC technology by using two intermediary devices. These devices act as relays, enabling communication between an NFC tag and a reader at a distance more than distance requirement of NFC. Throughout the period of the relay attack, the proxy token displays the same behaviour as the original token from the reader's perspective. This attack circumvents application layer security mechanisms [26].

3 Tag Cloning and Spoofing: An attacker creates a duplicate of an NFC tag, which can be used by the attacker to gain unauthorized access to systems the original tag has access to. This is dangerous especially in the financial sector. Figure 3 shows a representation of how tag cloning works [35].

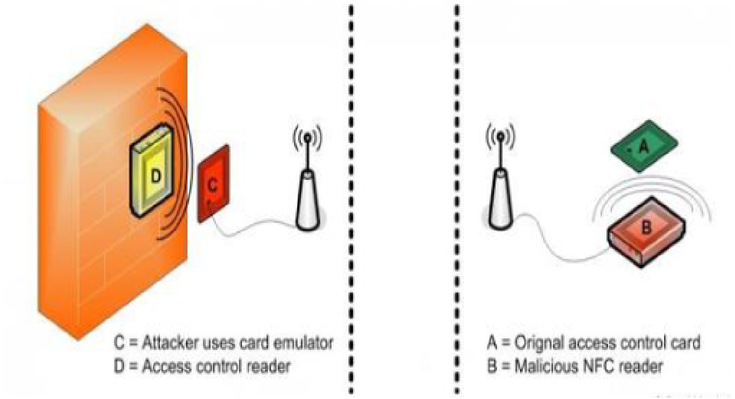
D
C
A
B
C = Attacker uses card emulator
D = Access control reader
A = Orignal access control card
B = Malicious NFC reader

Fig. 3: Diagram of an NFC attack

3.1.3 Energy Limitation

Passive tags rely on the energy transmitted by the NFC reader brought close to them. This means that the energy available to a passive tag is limited by the strength of the reader's field and the efficiency of the tag antenna in obtaining this energy. However, active tags, have their own power source. The energy generated from such a power source is affected by the power rating, the type of material used, etc. The authors in [27] developed an energy-efficient tag-searching protocol to address this issue.

3.1.4 Cost Consideration

Active tags have better computational ability and a longer range than passive tags due to the presence of an internal power source in them. However, they are more expensive compared to passive tags, which makes them have less application than passive tags. Passive tags, on the other hand, find wide applications but are limited in terms of computational ability, range, and storage capacity. These challenges with passive tags limit the amount of encryption that can be done on them, therefore making them less secure.

3.1.5 Backward Compatibility

NFC is a subset of RFID technology. RFID has a broader range of frequencies, from 125 kHz to 960 MHz, that are not compatible with NFC devices because NFC operates at a frequency of 13.56 MHz. Therefore, NFC devices cannot communicate with RFID frequencies below and above 13.56 MHz.

4 Existing NFC Tag Authentication Solution

NFC mobile payment consists of three components: authentication, authorization, and payment. The authors in [28, 37] proposed a cloud-based authentication payment method. Due to the vulnerability of symmetric encryption [36, 38], public-key cryptography was used for the authentication phase to compensate for the vulnerability. In the authentication stage, there is mutual authentication between the reader and the tag. After the authentication stage, the authorization phase is set up. At this stage, the reader checks if the user's account balance is enough to initiate the transaction before finally moving on to the payment stage.

The authors in [20] developed a password authentication scheme that uses a one-way hash function, a discrete logarithm problem, and the Diffie-Hellman key agreement protocol. In the one-way hash function, the function takes a message of arbitrary length as the input and produces a fixed-length message digest as the output. The Diffie-Hellman key agreement scheme allows two devices to communicate with each other in a secure manner with the agreed session key. Its security is based on solving discrete logarithm problems. The security of this scheme is based on having both the properties of a discrete logarithm problem and a secure one-way hash function. The scheme is more secure than schemes that have just one of the two properties and do not add too much computational complexity. The authors [33, 32, 34, 31, 30] all made use of the one-way hash function in their design. [12] designed a NFC authentication algorithm based on modified hash function. In this design, two encryption parameters are used rather than one used in the traditional hash function. The Hamming weight of the two parameters are considered and different parameters are selected for encryption making it difficult to crack.

Tuyls and Batina in [40] used a Physical Unclonable Function (PUF) integrated with the RFID chip. In their model, several fingerprints were derived from the PUF by sending it multiple challenges and recording the responses. The limitation of this model is that the number of challenges and corresponding fingerprints are limited. Hence, an attacker can record all the challenge/response pairs and program another tag with the same pairs. Saeed and Walter [14] proposed another offline authentication that can compute symmetric or asymmetric encryption. However, this is only suitable for active tags but not passive tags due to their limited computational power.

Due to the limited computational ability and storage capability of passive tags, advanced encryption cannot be performed on them. Adding specialized hardware to a tag could bring an extra computational ability [8]. However, this is very expensive, especially, in a large-scale application [43]. The authors in [3] designed a fingerprinting scheme, NFChain, by exploring the tag physical layer (PHY) signal, which extracts hardware fingerprint for tag authentication discussed in [47, 48, 46, 44, 45]. In their design, the scalability and compatibility issues were improved by proposing a factor nulling method that addresses the inconsistency in different tags. Firstly, they developed a frequency hopping mechanism that generates the request signal to interrogate an NFC tag, a tag response segmentation that separates the tag response signal from the overall received signal, tag response amplitude (TRA) extraction means that eliminated factors affecting TRAs, and finally, an authentication method that determines whether an unknown tag is genuine or counterfeited.

5 Analysis of Existing Authentication Solution

While the several existing tag authentication methods offer different strengths, there exists weaknesses in them. These weaknesses ranges from several factors like cost to scalability. Table 1 describes each solution weaknesses and strengths.

Analysis of Authentication Method		
Tag Authentication Method	Strength(s)	Weakness(es)
Offline Tag Authentication	Secure due to cryptographic encryption	Only suitable for active tags and expensive to develop because of the usage of active tags. Susceptible to cloning attacks.
Cloud-based Authentication	Secure against eavedropping and replay attack (use of session key and timestamps)	Very expensive to develop. Cannot be used with passive tags.
Password Authentication	Secured against eavesdropping. Very cheap to develop	Not secured against man-in-the-middle attack, replay attack, and cloning attack.
NFChain	Safe against cloning attack. scalable. secured against feature replay attack	Weak against signal replay attack.

Table 1: Table of analysis of the existing authentication methods.

6 Conclusion

Near-field communication is a short-range wireless communication. This close proximity between the devices make NFC secure. However, attackers have developed different ways of manipulating this communication and this has called for more sophisticated method of securing transactions on NFC. From the analysis of the different existing NFC authentication methods, the NFChain is a better option than the other existing methods. With further study on the NFChain, secure and higher authentication accuracy can be achieved.

References

[1] Mehmet Hilal Ozcanhan, Gokhan Dakilic, and Semih Utku. Cryptographically Supported NFC Tags in Medication for Better Inpatient Safety. In *Patient Facing Systems, 2014.*

[2] Romeo L. Jorda Jr., Joshua Renz A. Coballes, Lejan Alfred C. Enriquez, Mark Lester S. Millan, Angelo J. Mora, Melbert Neil G. Teodoro, Nilo M. Arago, August C. Thio-ac, Lean Karlo S. Tolentino Comparative Evaluation of NFC Tags for the NFC-Controlled Door Lock with Automated Circuit Breaker, *IEEE, 2018.*

[3] Yanni Yang, Jiannong Cao, Zhenlin An, Yanwen Wang, Pengfei Hu, and Guoming Zhang. NFChain: A Practical Fingerprinting Scheme for NFC Tag Authentication *IEEE INFOCOM*, 2023.

[4] Sayidul Morsalin, A. M. Jairul Islam, Golam R. Rahat, Syed R. H. Pidim, Abdur Rahman, Md A. B. Siddiqe. Machine-to-machine communication based smart home security system by NFC, fingerprint, and PIR sensor with mobile Android application. 2014.

[5] Jingyu Hua, Hongyi Sun, Zhenyu Shen, Zhiyun Qian, and Sheng Zhong. Accurate and Efficient Wireless Device Fingerprinting Using Channel State Information. *IEEE INFOCOM*, 2018.

[6] Bingjing Yan, Aidong Xu, Yang Cao, Yixin Jiang, Wenyuan Xu, and Xiaoyu Ji. Hardware-fingerprint Based Authentication for NFC Devices in Power Grids. *2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC 2019)*, 2019.

[7] Woongsup Lee, Seon Yeob Baek, and Seong Hwan Kim. Deep-Learning-Aided RF Fingerprinting for NFC Security. *Data Science and Artificial Intelligence for Communications,* IEEE Communications Magazine, 2021.

[8] Thomas Plos, Michael Hutter, Martin Feldhofer, Maksimiljan Stiglic, and Francesco Cavaliere. Security-Enabled Near-Field Communication Tag with Flexible Architecture Supporting Asymmetric Cryptography. *IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 21, NO. 11, NOVEMBER 2013,* 2013.

[9] Nicholas Akinyokun and Vanessa Teague. Security and Privacy Implications of NFC-enabled Contactless Payment Systems. In *Proceedings of ARES '17, Reggio Calabria, Italy, August 29-September 01, 2017, 10 pages.* DOI: http://dx.doi.org/10.1145/3098954.3103161, 2017.

[10] Renjie Zhao, Purui Wang, Yunfei Ma, Pengyu Zhang, Hongqiang Harry Liu, Xianshang Lin, Xinyu Zhang, Chenren Xu, and Ming Zhang. NFC+: Breaking NFC Networking Limits through Resonance Engineering. In *SIGCOMM '20, August 10–14, 2020, Virtual Event, USA.* DOI: https://doi.org/10.1145/3387514.3406219, 2020.

[11] Anusha R, Raghavendra Rao P, and Pratheksha Rai N. Secured Authentication of RFID Devices Using Lightweight Block Ciphers on FPGA Platforms. *IEEE Access,* 2023.

[12] Fang-Ming Cao and Dao-Wei Liu. A Lightweight NFC Authentication Algorithm Based on Modified Hash Function. *International Journal of Network Security, Vol.24, No.3, PP.436-443, May 2022.* DOI: 10.6633/IJNS.202205 24(3).06, 2022.

[13] Noureddine Chikouche and Foudil Cherif. EAP-SRES: An Enhanced Authentication Protocol for Secure Remote Education Systems Using NFC Technology. *International Journal of Computing and Digital Systems.* http://dx.doi.org/10.12785/ijcds/090309. May, 2020.

[14] Muhammad Qasim Saeed and Colin D. Walter. Off-line NFC Tag Authentication. In *The 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012),* 2012.

[15] Jonghyun Baek and Heung Youl Youm. Secure and Lightweight Authentication Protocol for NFC Tag Based Services. In *2015 10th Asia Joint Conference on Information Security,* 2015.

[16] Divyans Mahansaria and Uttam Kumar Roy. Secure Authentication for ATM Transactions using NFC Technology. *IEEE,* 2019.

[17] Walter Austin Hufstetler, Maria Jose Hito Ramos, and Shuangbao Paul Wang. NFC Unlock: Secure Two-Factor Computer Authentication using NFC. In *2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems,* 2017.

[18] Mai He and Shulin Yang. Design of anti-counterfeiting system based on blockchain and NFC tag. In *2022 3rd International Conference on Information Science, Parallel and Distributed Systems (ISPDS) | 978-1-6654-8747-4/22.* DOI: 10.1109/ISPDS56360.2022.9874157, IEEE, 2022.

[19] Jie Xu, Kaiping Xue, Qingyou Yang, and Peilin Hong. PSAP: Pseudonym-Based Secure Authentication Protocol for NFC Applications. *IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, VOL. 64, NO. 1,* February, 2018.

[20] I-En Liao, Cheng-Chi Lee, and Min-Shiang Hwang. A password authentication scheme over insecure networks. *Journal of Computer and System Sciences 72 (2006) 727–740,* Novemeber, 2005.

[21] Julian Dreyer, Marten Fischer, and Ralf Tonjes. NFC Key Exchange – A light-weight approach to authentic Public Key Exchange for IoT devices. *2021 IEEE 7th World Forum on Internet of Things (WF-IoT) | 978-1-6654-4431-6/21.* DOI: 10.1109/WF-IoT51360.2021.9595145, 2021.

[22] Dan Boneh. Cryptography 1. In *Stanford University via Coursera Online Course.*

[23] Md Arif Hassan, Zarina Shukur, and Mohammad Kamrul Hasan. An Improved Time-Based One Time Password Authentication Framework for Electronic Payments. *(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 11, No. 11,* 2020

[24] Chi-Huan Lu, Ji-An Li, and Tsung-Hsien Lin. A 13.56-MHz Passive NFC Tag IC in 0.18-µm CMOS Process for Biomedical Applications. 2016

[25] Dzevdan Kapetanovic, Gan Zheng, and Fredrik Rusek Physical Layer Security for Massive MIMO: An Overview on Passive Eavesdropping and Active Attacks. 2015

[26] Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones. *In: Ors Yalcin, S.B. (eds) Radio Frequency Identification: Security and Privacy Issues. RFIDSec 2010. Lecture Notes in Computer Science, vol 6370. Springer, Berlin, Heidelberg.* https://doi.org/10.1007/978-3-642-16822-2, 2010.

[27] Shigeng Zhang, Xuan Liu, Jianxin Wang, Jiannong Cao, and Geyong Min Energy-Efficient Active Tag Searching in Large Scale RFID Systems. *In: Information Sciences, Open Research Exeter.* 2016.

[28] Forough Sadat Mirkarimzade Tafti, Shahriar Mohammadi, and Mehdi Babagoli A new NFC mobile payment protocol using improved GSM based authentication. *In: Journal of Information Security and Applications.* 2021

[29] Lagos State Government 2024

[30] T.-C. Yeh, H.-Y. Shen, and J.-J. Hwang A secure one-time password authentication scheme using smart cards. *In: IEICE Trans. Commun. E85-B (2002) 2515–2518.* 2002

[31] H.-M. Sun An efficient remote use authentication scheme using smart cards. *In: IEEE Trans. Consumer Electron. 46 (4) (2000) 958–961.* 2000

[32] M. Sandirigama, A. Shimizu, and M.T. Noda Simple and secure password authentication protocol (SAS). *In: IEICE Trans. Commun. E83-B (2000) 1363–1365.* 2000

[33] C.L. Lin, H.M. Sun, and T. Hwang Attacks and solutions on strong-password authentication. *In: IEICE Trans. Commun. E84-B (2001) 2622–2627.* 2001

[34] H.-Y. Chien, J.-K. Jan, and Y.-M. Tseng An efficient and practical solution to remote authentication. *In: Smart card, Computers & Security 21 (2002) 372–375.* 2002

[35] Z. Zainal Abidin, N.A. Zakaria, N. Harum, M.R. Baharon, Ee-Song Hong, Z. Abal Abas, Z. Ayop, and N.A. Mat Ariff Crypt-Tag Authentication in NFC Implementation for Medicine Data Management. *In: International Journal of Advanced Computer Science and Applications Vol. 9, No. 9* 2018

[36] Xinyi Chen, Kyung Choi, and Kijoon Chae A Secure and Efficient Key Authentication using Bilinear Pairing for NFC Mobile Payment Service. *In: Wireless Person Communication 2017; 97: 1-17.* 2017

[37] Jen-Ho Yang and Pei-Yu Lin A Mobile Payment Mechanism with Anonymity for Cloud Computing. *In: Journal of Systems and Software, Volume 116, Pages 69-74, June 2016.*

[38] Wilayat Khan and Habib Ullah Authentication and Secure Communication in GSM, GPRS, and UMTS using Asymmetric Cryptography. *In: International Journal of Computer Science Issues, Vol.7, Issue 3, No 9, May 2010.*

[39] NFC Forum Std. NDEF 1.0, July 2006. [Online] NFC Data Exchange Format (NDEF): Technical Specification. *In: http://www.nfc-forum.org/specs/spec list/*

[40] Pim Tuyls and Lejla Batina RFID-Tags for Anti-counterfeiting. *In: The Cryptographers' Track, RSA Conference, RSA, San Jose, CA, USA.* Lecture Notes in Computer Science, vol. 3860. Springer, February 2006, pp. 115-131.

[41] Near field communication market 2021 to 2025 growth factors, market characteristics, opportunities by type analysis and forecast. *https://www.marketwatch.com/press-release/near-field-communicationnfc-market-2021-to-2025-growth-factors-market-characteristicsopportunities-by-type-analysis-and-forecast-2021-06-10.*

[42] New zealand pilots nfc tags for covid-19 tracking. *https://www.healthcareitnews.com/news/anz/new-zealand-pilots-nfctags-covid-19-tracking.*

[43] D. Saeed, R. Iqbal, H. H. R. Sherazi, and U. G. Khan "Evaluating Nearfield Communication Tag Security for Identity Theft Prevention. *In: " Internet Technology Letters, vol. 2, no. 5, p. e123, 2019.*

[44] B. Danev, S. Capkun, R. Jayaram Masti, and T. S. Benjamin Towards Practical Identification of UHF RFID Devices. *In: ACM transactions on Information and System Security (TISSEC), vol. 15, no. 2, pp. 1–24, 2012.*

[45] B. Danev, T. S. Heydt-Benjamin, and S. Capkun Physical-layer Identification of RFID Devices. *In: Proceedings of USENIX security symposium, 2009.*

[46] H. P. Romero, K. A. Remley, D. F. Williams, and C.-M. Wang Electromagnetic Measurements for Counterfeit Detection of Radio Frequency Identification Cards. *In: IEEE Transactions on Microwave Theory and Techniques, vol. 57, no. 5, pp. 1383–1387, 2009.*

[47] J. Han, C. Qian, P. Yang, D. Ma, Z. Jiang, W. Xi, and J. Zhao Geneprint: Generic and Accurate Physical-layer Identification for UHF RFID Tags. *In: IEEE/ACM Transactions on Networking (TON), vol. 24, no. 2, pp. 846–858, 2015.*

[48] S. C. G. Periaswamy, D. R. Thompson, and J. Di Fingerprinting RFID Tags. *In: IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 6, pp. 938–943, 2010.*