future internet

MDPI

Review

A Systematic Literature Review on Authentication and Threat Challenges on RFID Based NFC Applications

Ismail El Gaabouri [1,*], Mohamed Senhadji [1], Mostafa Belkasmi [1] and Brahim El Bhiri [2,*]

[1] ICES Team, ENSIAS, Mohammed V University in Rabat, Rabat 10000, Morocco; mohamed.senhadji@ensias.um5.ac.ma (M.S.); mostafa.belkasmi@ensias.um5.ac.ma (M.B.)
[2] Smartilab Laboratory, EMSI, Rabat 10000, Morocco
[*] Correspondence: ismail_elgaabouri@um5.ac.ma (I.E.G.); b.elbhiri@emsi.ma (B.E.B.)

Abstract: The Internet of Things (IoT) concept is tremendously applied in our current daily lives. The IoT involves Radio Frequency Identification (RFID) as a part of the infrastructure that helps with the data gathering from different types of sensors. In general, security worries have increased significantly as these types of technologies have become more common. For this reason, manifold realizations and studies have been carried out to address this matter. In this work, we tried to provide a thorough analysis of the cryptography-based solutions for RFID cards (MIFARE cards as a case study) by performing a Systematic Literature Review (SLR) to deliver the up-to-date trends and outlooks on this topic.

Keywords: RFID; cryptography; IoT; smart cards; security; systematic literature review

check for updates

Citation: El Gaabouri, I.; Senhadji, M.; Belkasmi, M.; El Bhiri, B. A Systematic Literature Review on Authentication and Threat Challenges on RFID Based NFC Applications. *Future Internet* **2023**, *15*, 354. https://doi.org/10.3390/fi15110354

Academic Editor: Claude Chaudet

Received: 5 September 2023
Revised: 30 September 2023
Accepted: 10 October 2023
Published: 27 October 2023

1. Introduction

Radio Frequency Identification (RFID) is a method of remotely gathering and storing data that employs two types of RFID devices [1,2]. The first type is the RFID tags (transponders), which require each object to be marked in order to be identified in the system (a unique identifier). There are three types of tags [3]. The first are active ones, which transmit their ID signal on a continuous schedule due to the on-board battery. Next are passive tags, which depend entirely on the radio energy transmitted from the reader, because there is no battery supply. The third type comprises semi-active tags, for which the tag is supplied with a battery to manage its demands for regular measurements (such as temperature). Contrary to the transponders, RFID readers are a collection of devices that acquire data from RFID tags to track objects. Readers have better resources and frequently connect to back-end databases (where each tag is indexed) and can perform complex computations, such as implementing cryptographic solutions [4]. These tags all acknowledge periodicity. A tag can be assigned to one of four frequency ranges [5]: Low Frequency (LF), High Frequency (HF), Ultra-High Frequency (UHF), and Super-High Frequency (SHF). Since tags can only store a limited amount of information due to resource constraints, back-end databases are essential to the completion of the RFID system.

Currently, RFID-based applications are widely used in several domains; we can mention industry and military as instances. Due to the enormous growth of this field, RFID tags and readers are an ideal target for attackers to counterfeit. Hence, several security threats and risks have been identified while implementing this technology, which can cause data breaches and information alteration, which reflects directly on the credibility of their generated information content. To overcome these menaces, several authentication schemes have been proposed in order to provide trustable communications between different RFID system parts. The term RFID has been known since the third decade of the past century when it was first applied in the military. In this paper, we considered carrying out a Systematic Literature Review (SLR) on the RFID authentication security approaches that seem to be extremely advantageous. Therefore, different solutions will be discussed with the intention of providing the present and forthcoming research orientations. This article is organized as follows. The research methodology is presented in Section 2. Furthermore, the challenges for and threats to the RFID technology are highlighted in Section 3. Section 4 provides the suggested cryptography-based solutions in the literature. Section 5 highlights the open discussion to address future perspectives. Finally, Section 6 recapitulates the paper.

2. Research Methodology

In order to respond to our research questions and obtain an in-depth understanding of the highlighted subject, our SLR was conducted in the following manner.

2.1. Elementary Exploration

In order to provide strong research results, our search process was based on the usage of keywords that complied with our theme. The keywords utilized are presented as given below:

- Keyword 1 = "Mifare" && "Threats";
- Keyword 2 = "Mifare" && ("Security" OR "Authentication").

To gather studies that satisfied our SLR objective, various publishers' online platforms were considered. Google Scholar, Scopus, ACM Library, IEEE Xplore, and SpringerLink were the databases adopted. e considered. Google Scholar, Scopus, ACM Library, IEEE Xplore, and SpringerLink were the databases adopted. The results found (journal articles/conference articles/book chapters) were classified based on some specific exclusion and inclusion criteria, and these will be presented in detail in the following section.

2.2. Extraction Criteria and Primary Results

The chosen studies were clustered after a three-pass approach, which was extract, classify, and store. Table 1 highlights the criteria for the exclusion and inclusion process.

Table 1. Exclusion and inclusion criteria.

Exclusion Criteria	Inclusion Criteria
Publications came from predatory journals or conferences.	Journals' and conferences' credibility.
Published before 2012.	Published after 2012.
Studies not written in English.	Studies written in English.
The studies did not address smart card RFID security.	The studies directly addressed smart card RFID security.

Tables 2 and 3 present each of the two keywords' results, respectively.

Table 2. Keyword 1 results.

Database	All References	After 2012	After 2017	English Only and after 2017
Google Scholar	877	556	217	186
Scopus	52	31	13	13
ACM library	18	14	6	6
IEEE Xplore	1	1	1	1
SpringerLink	147	99	52	52
Total	1095	701	289	258

Table 3. Keyword 2 results.

Database	All References	After 2012	After 2017	English Only and after 2017
Google Scholar	5690	3640	1660	1150
Scopus	238	92	42	42
ACM library	59	34	14	14
IEEE Xplore	26	20	11	11
SpringerLink	376	250	122	115
Total	6389	4036	1849	1332

The number of results found after a full extraction was 7484 based on the date of publication (2017–2022). Only 2138 out of 7484, which represents 28.56% of the existing references, were investigated in this SLR:

- Another metric was taken into consideration, which was the language utilized by the authors. Thus, only results written in English were included. Due to this metric, the number of explored studies decreased from 2138 to 1590, which represents 74.36% of the results we obtained after the first extraction.
- Checking for duplicates in the 1590 studies included in the SLR should be performed to avoid a study being double-analyzed or -checked. As a result, the number of studies decreased from 1590 to 915 (57.54%).
- Last, but not least, an extraction built on the title, abstract, and scope of research was deemed for the sake of organizing the work. Further, to further scrutinize the existent implementations that had a quite similar vision as ours, 202 out of the 915 (22.07%) were selected to be utilized to accomplish the intended SLR (first full extraction). The distribution of these studies by year is shown in Figure 1 and Table 4.

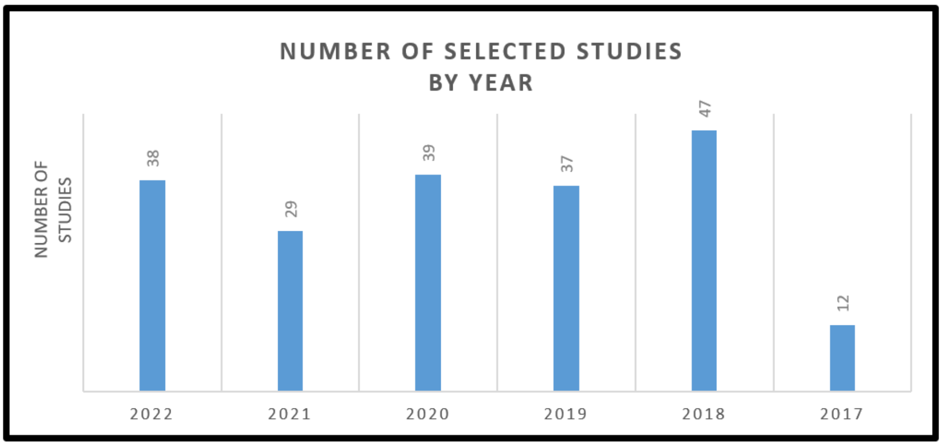

Figure 1. Studies' distribution by year.

Table 4. Number of selected studies by year.

Year of study	2017	2018	2019	2020	2021	2022	All
Total of number of studies	38	29	39	37	47	12	202

- Another criterion that was borne in mind was the article's availability and its perceived compliance. At this stage, we determined whether the realized study had a strong link with our principal insight. Only 32 out of the 202 studies were selected to go through the realization process (final extraction); see Figure 2.

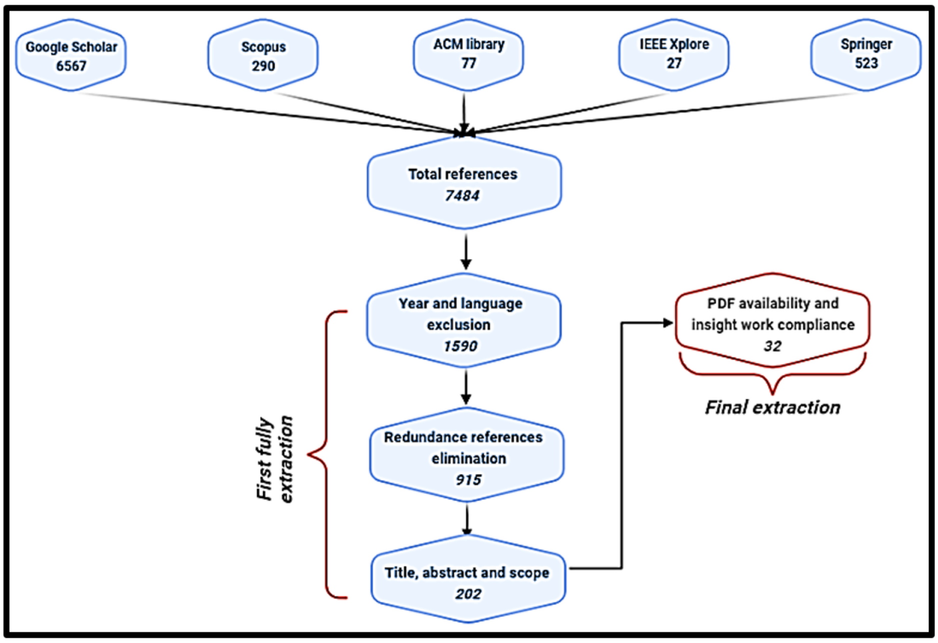

Figure 2. Studies' extraction and inclusion process.

3. RFID Security and Threats

Currently, RFID tags and readers play a key role in helping to save users' time, and we can mention transport cards, companies' access control cards, and medical records [6]. For this reason, security is necessary to promote this type of technology, as a data violation can have some serious detriments. Hence, before going through the analysis of the studies, obtaining sufficient knowledge about the security challenges, issues, and threats of RFID was necessary with the purpose of emphasizing the topic problem. Due to RFID devices' small capacities, many challenges are faced in expanding their utilization, and the principal ones will be discussed to offer an overview of these constraints.

3.1. RFID Challenges

As mentioned, each RFID system is composed of three main components; therefore, the challenges for each part of the system will be highlighted. In general, RFID suffers from inflexibility issues, as usually, the readers ought to be fixed in place. Moreover, and more precisely, commercial devices are expensive to re-design or reproduce since they come as a black box with limited information [7]; at this point, manufacturers restrict users' ability to make profound changes. Furthermore, message collisions can be spotlighted as another challenge that can reduce the system's efficiency, since the same communication channel is used by the diverse tags utilized. Frequency interferences, the read speed ratio, and energy wastage are some of the problems that can also be encountered. In addition, the read range and energy-gathering limitation comprise another set of challenges because the communication range relies on the device's available power [8].

The previously mentioned challenges could lead to security issues that reflect the normal system workflow and may lead to information loss, which is pivotal in some cases, for instance, healthcare or industry. To overcome this issue, several suggestions have been presented to secure RFID communications and protect the confidentiality, integrity, and privacy of users.

The limitation of RFID is highly recommended to be taken into consideration while applying any sort of implementation to find a suitable solution. Consequently, cryptography-based schemes are deployed to reinforce RFID communications' security. The primary concern of cryptography is to safeguard data from being eavesdropped on or sniffed, but it needs some computational and storage abilities to be undertaken.

Resource limitations comprise the main challenge confronted by any RFID application, where heavy computational cryptosystems cannot be supported [8]. For example, passive tags' lifespan is a necessity. The latter only supports simple operations such as rotate and XOR. At this stage, conventional crypto primitives utilization might lead to an increase in heat, fast energy wastage (tag lifespan decreasing), and tag damage. As a result, ultra-lightweight schemes can be implemented to fit this type of tag. For semi-passive or semi-active tags, we can have some moderate resources that can support some advanced operations such as checksums, random number generation, hash functions, and mutual authentication. However, active tags consist of small batteries and have a good storage ability, so they are efficient enough to perform heavy computational operations without restrictions. In this regard, classical crypto-primitives can be used to offer strong security to the system, and we can mention Public Key Cryptography (PKC) schemes such as Elliptic Curve Cryptography (ECC) and Rivest, Shamir, and Adelman (RSA). In addition to symmetric key encryption, we can highlight the Advanced Encryption Standard (AES) and other computationally heavy algorithms. Besides this, communication protocol issues should be accommodated; therefore, anti-collision protocols are used to avoid tag message collisions. For instance, multi-access methods are implemented to identify exactly the tags where the signals came from and to decrease the collision number, which reflects positively on the throughput and number of transmitted bits. These methods are classified into four main categories as follows [9]:

- **Code division multi-access:** This is built by multiplying the tag ID by a pseudo-random sequence before the data transmission. This method offers security to the communication between the reader and the tag; however, it has some high demands such as computation, along with enhancing the complexity.
- **Frequency division multi-access:** This refers to the utilization of frequency ranges for the sake of recognizing tags. At such a level, each tag must belong to a specific frequency. FDMA seems expensive to implement and it is not designed for general employment.
- **Space division multi-access:** Its main concern is to split the channel into distinct areas to enhance the channel's connection capability. Unfortunately, SDMA is extremely costly and requires some complex designs for the antennas.
- **Time division multi-access:** This approach is widely used and covers many anti-collision algorithms. TDMA divides the transmission channel between tags to ensure the reader's identification ability at separate times to overcome interference. This method is not costly and reduces the number of tag interrogations after each successful response (broadcast message response).

3.2. RFID Security Threats

Although RFID-based systems are tremendously used currently, several security threats are confronted in their implementation. These can be faced at the physical level or the communication level. This section presents the most common threats that can harm the RFID system and may lead to some serious breaches that reduce user information privacy. Data alteration, ID cloning, communication interruption, and tag tracking are some attacks that need in-depth consideration to address them:

- **Tracking:** This is known as the act of reading RFID tags without the proper authorization by the use of a considerable number of RFID readers to gather their identifiers, and these identifiers can be personal credit card numbers [10].
- **Counterfeiting:** This attack manipulates the tag, where a smaller amount of information is needed. Here, circumventing the security mechanisms utilized is the main objective of the counterfeiting threat [10].
- **Eavesdropping:** This attack is based on saving the read intercepted communication with the intention to be re-used for analysis and as a baseline for another type of attack such as tag cloning attacks [7].

- **Tags cloning:** Its major purpose is to duplicate a reliable tag as a copy to be used for unauthorized access to the reader's information with the intention of extracting data to be stored in another tag. Tag cloning leads to several damages such as the manufacturer's reputation and some serious financial losses [7].
- **Physical attacks:** Its main concern is to tamper with the tag physically by damaging one of its components or disrupting its normal performance by glitching the tag's clock or changing the transmitted radio frequencies, and we can mention side channel and timing attacks [10].
- **DoS attack:** The is a denial of service, where the intruder tries to take the tag out of service. Consequently, no information will be leaked or occupied. However, it reduces the RFID system's efficiency and faithfulness. The concept of realizing a DoS attack is to interfere with the signals of the channels used for the tags' radio frequency communications [10].

4. RFID Security Solutions

With the intention to provide a pervasive understanding of the suggested cryptography schemes in the literature for RFID, this section presents the prominent studies, pointing out each study's main objective, the methods utilized, and the domain of implementation, which are presented in Table 5.

Table 5 illustrates the overall analysis of the selected studies that were used to perform this SLR. The results exemplify that many types of encryption schemes can be applied to secure RFID-based applications, and the diversity of solutions comes from the fact that RFID is implemented in several domains, healthcare and voting applications being quite common. As such, medical records or citizens' votes should not be shared and may lead to crucial outcomes: patient's lives may be negatively affected, and the privacy of the results of elections can be compromised, which reflects on their credibility.

Figures 3 and 4 clarify the worldwide RFID applications, where 21 countries were identified based on the 32 analyzed studies. Simultaneously, the variety of disciplines where this technology is implemented is given. We can mention electronic payments, healthcare, and remote education, among other disciplines, a fact that requires thorough scrutiny.

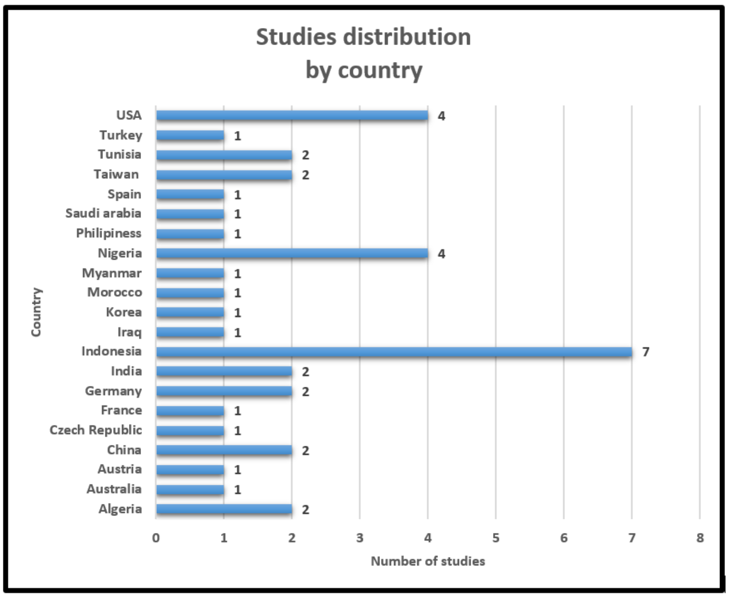

Figure 3. Studies' distribution by country.

Table 5. Analysis of the suggested RFID security schemes.

Authors and	Main Objective	Year	Country	Method Utilized	Discipline
Adeniji, O.D. et al. [11]	Guaranteeing multi-level security for NFC smart cards by combining Huffman code and AES.	2022	Nigeria	Huffman code and AES	Multi-discipline
Olaniyi, O.M et al. [12]	The proposal of a secure NFC e-voting-based application to enhance the digitization of democratic decision-making trustworthiness.	2022	Nigeria Austria Morocco	Multi-Factor and Authentication (MFA)	e-voting
Raj, K.V et al. [13]	Increasing the use ofa multipurpose smart card by applying a proficient crypto algorithm.	2022	India	RC6 over AES and Blowfish SHA-256 for authentication	Multi-discipline
Arslan, A et al. [14]	Enhancing the ID17 scheme to overcome the mentioned protocol weaknesses.	2021	Turkey	ECC, brainpoolP160r1, and Digital Signature (DSA)	Multi-discipline
Dreyer, J et al. [15]	A novel approach to exchange public keys authentically via NFC (no third-party smuggling.)	2021	Germany	Challenge–response scheme	Multi-discipline
Noprianto et al. [16]	Introduced a data security technique built on keys' and access conditions' dynamic altering.	2021	Indonesia	Dynamic key utilization	Multi-discipline
Benamara N.K et al. [17]	Proposed a face authentication system based on deep learning facial biometry and RFID cards.	2021	Algeria	VGG-16, RESNET-50 RESNET-34 models	e-payment
Basjaruddin N.C et al. [18]	Applying homomorphic encryption NFC system security.	2020	Indonesia	Homomorphic cryptography (Paillier cryptosystem)	Airport baggage tracing

Table 5. *Cont.*

Authors and	Main Objective	Year	Country	Method Utilized	Discipline
Damayani, S et al. [19]	Suggested the usage of AES-256 for key storage and SHA-256 for authentication, with the intention to provide robust data protection.	2020	Indonesia	Homomorphic cryptography (Paillier cryptosystem) SHA-256 and AES	e-voting
Chikouche, N. et al. [20]	Suggested an efficient protocol built on a post-quantum cryptosystem to secure RFID and NFC wireless communications.	2020	Indonesia	McEliece cryptosystem	
Alamer, A. et al. [21]	Proposed a modified approach (4 IVs and key pairs) to enhance Mickey cryptosystem Version 2.0 security providence.	2019	Australia Saudi-Arabia USA	Mickey 2.0 stream cipher	Healthcare
Arulmozhi, P. et al. [22]	Suggested a lightweight three-pass authentication scheme to verify the token.	2019	India USA Australia	Three-pass authentication tokenization TEA/RF-TEA	Multi-discipline
Zhang, Y. et al. [23]	The major intention was to provide full supply chain traceability by integrating several security features such as cryptography and blockchain (no consensus needed needed due to end entities' trust).	2019	USA	ECDSA SHA-256 10 BytesCRC (integrity)	Supply chain
Kang, J. et al. [24]	Presented a secure RFID-suitable data-transmission protocol that offers protection against several attacks.	2019	Korea	Challenge–response process (PRNG + CRC)	Multi-discipline
Eka Putra, I.G.S et al. [25]	Suggested a logging-based application, where the MD5 algorithm was utilized against several attacks to offer smart card data privacy.	2019	Indonesia	MD5	Multi-discipline
Nilar Soe et al. [26]	Offered a secure access control system based on the utilization of the ECDSA algorithm to overcome inaccurate payment issues.	2019	Myanmar	PKI infrastructure based on ECDSA	Electronic payment

Table 5. *Cont.*

Authors and	Main Objective	Year	Country	Method Utilized	Discipline
Lamia Rzouga et al. [27]	Fulfillment of a secure biometric built-in application for access control by integrating watermarking techniques.	2019	Tunisia	Wavelet packet decomposition and Gabor filter extractor	Multi-discipline
Isa Mulia Insan et al. [28]	The application of the MFA scheme with usage of fingerprints and smart cards as security factors.	2019	Indonesia	Multi-Factor Authentication scheme (MFA)	Parking gate
Abdulsalam, Y.S. et al. [29]	Proposed an enhanced TEA ciphering algorithm to secure RFID-based healthcare application factors.	2018	Nigeria	TEA algorithm and Yarrow PRNG	Healthcare
Mine Cetinkaya et al. [30]	The intention was to allow RFID tags to be configured and to gather keys in a secure way, without the necessity of a direct computer connection to the sensor.	2018	Germany	AES-128	Multi-discipline
He Xu et al. [31]	A mutual verification-based protocol with the integration of PUF and Kulseng's verification to offer efficient security against desynchronized attacks.	2018	China	Mutual verification (physical unclonable function + Kulseng verification)	Multi-discipline
Excel B. et al. [32]	Enhanced the RC5's slow encryption speed by a generated random number for keys' generation (speed up key expansion process).	2018	Philippines	Enhanced RC5	Electronic payment
Lukas Malina et al. [33]	A zero-knowledge-based cryptography scheme was suggested, where Schnorr's identification scheme was used to provide the proof of knowledge and ECC for data size moderation.	2018	Czech Republic	Schnorr's scheme ECC	Multi-discipline
Baolong Liu et al. [34]	The utilization of a hash-based scheme to identify the reader and tag, each part being identified by half of the generated hash. BAN was implemented for protocol correctness.	2018	China	SHA3-224 Burrows–Abadi–Needham (BAN)	Multi-discipline

Table 5. *Cont.*

Authors and	Main Objective	Year	Country	Method Utilized	Discipline
H Nurdiyanto et al. [35]	The usage of the IDEA cipher for an RFID-based parking application to identify, verify, and authenticate tags with the intention to improve the entire system's security.	2018	Indonesia Republic	IDEA cipher Burrows–Abadi–Needham (BAN)	Parking gate
Néstor Álvarez-Díaz et al. [36]	The usage of the IDEA cipher for an RFID-based parking application to identify, verify, and authenticate tags with the intention to improve the entire system's security.	2017	Spain USA	Homomorphic cryptography (the Paillier cryptosystem	Airport luggage control
Mohammed Issam Younis et al. [37]	A mutual authentication scheme to secure RFID system communications involves signing, issuing, and charging for verification.	2017	Iraq	PRNG (tag side) ECDSA + PBE (backend database)	Multi-discipline
Olayemi M et Olaniyi et al. [38]	Applying the enhanced-TEA cipher to secure clinical telediagnostic information and tags from being cloned or falsified.	2017	Nigeria	Pseudo-random TEA	Healthcare
Hung-Yu Chien [39]	Suggested a new ECC-based authentication scheme to secure RFID against active tracking attacks.	2017	Taiwan	ECC	Multi-discipline
Hung-Yu Chien [40]	A radio-frequency authentication scheme based on the usage of a challenge–response approach and AES cipher to protect tags from unauthorized identification and non-legitimate tracing.	2017	Taiwan	AES	Multi-discipline
Ratnadewi et al. [41]	They tried to implement the AES-128 algorithm to ensure data transmission privacy.	2017	Indonesia	AES-128 Burrows–Abadi	Multi-discipline
Yassine Naija et al. [42]	Proposed a low-cost mutual authentication that was built in.	2017	Tunisia France	PRESENT	Parking gate

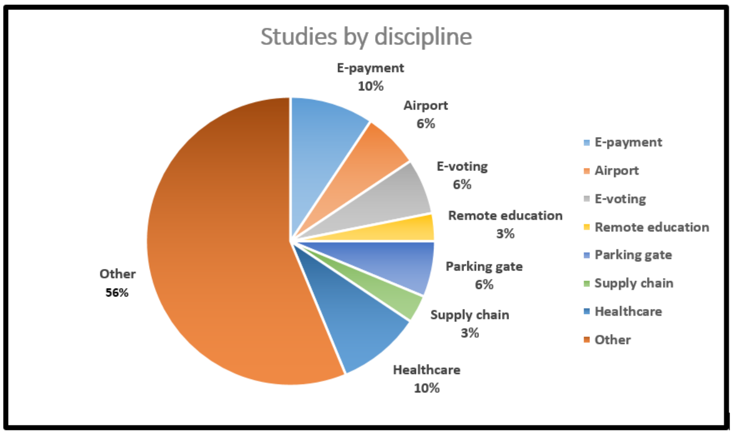

Figure 4. Studies' distribution by discipline.

To tackle this issue, the highly recommended AES-128 [30,40,41] can be used with a challenge–response scheme to prevent malicious accesses. Adeniji, O.D et al. [11] tried to combine the Huffman code with the aforementioned algorithm to mitigate malicious intrusions that could threaten the NFC card's information. Moreover, K.vivek Raj et al. [13] applied the sixth version of Rivest's code over AES or Blowfish (depending on the security needs) along with SHA-256 for authentication. On the other hand, Excel B. Villanueva et al. [32] implemented the fifth version of the same block cipher to be implemented for e-payment purposes. The TEA cipher is another block cipher algorithm that is considerably utilized, especially for healthcare applications [22,29,38], due to its low resource usage and healthcare applications' real-time information requirement. ECC can be seen as widely used, as in [14,39], where this approach was implemented alongside several techniques such as the Digital Signature Algorithm (DSA), SHA-256, and CRC, and it can be part of a blockchain-based e-payment application with no consensus, since the users are initially verified [23], or zero-knowledge- based cryptography within Schnorr's scheme [33]. At this level, ECC is used to moderate the size of the encrypted data. Further, challenge–response schemes are another kind of solution that can be applied where there are some resource limitations. These solutions are usually built in with the utilization of PRNG and CRC [15,24]. Moreover, the dynamic keys concept was utilized in [16], where each card has its own unique key and access conditions. Likewise, homomorphic cryptography schemes within the Paillier cryptosystem are perhaps worth considering, especially since this scheme is flexible enough to be used on its own [18] or with other cryptography schemes to scale up to adequate system security storage or authentication abilities [19]. In addition, some attempts have been made to gain security for different computing edges. The post-quantum McEliece cryptosystem has been carried out for remote education [20]. Watermarking and deep learning techniques canbe implemented for facial and fingerprint recognition [17,27]. Hashing algorithms are also exploited where the MD5 algorithm in [25] and SHA3-224 with Burrows–Abadi–Needham logic in [34] were used to increase integrity. Meanwhile, we can mention the IDEA cipher [35], Present [42], the modified Mickey 2.0 [21], and the multi-factor authentication schemes [12,27], among other alternative solutions that might replace the commonly used ones.

Table 5 and Figure 5 give a broad insight into where the studies on this topic were conducted. The findings can be used by new researchers to become accustomed with the different cryptography-based primitives employed for such environments, which are known for their resource limitations. This fact leads to a far-reaching consideration before any algorithm's integration. It was witnessed that a variety of authors have used encryption methods based on their application's necessities. A method may seem adequate for one application, but not for another.

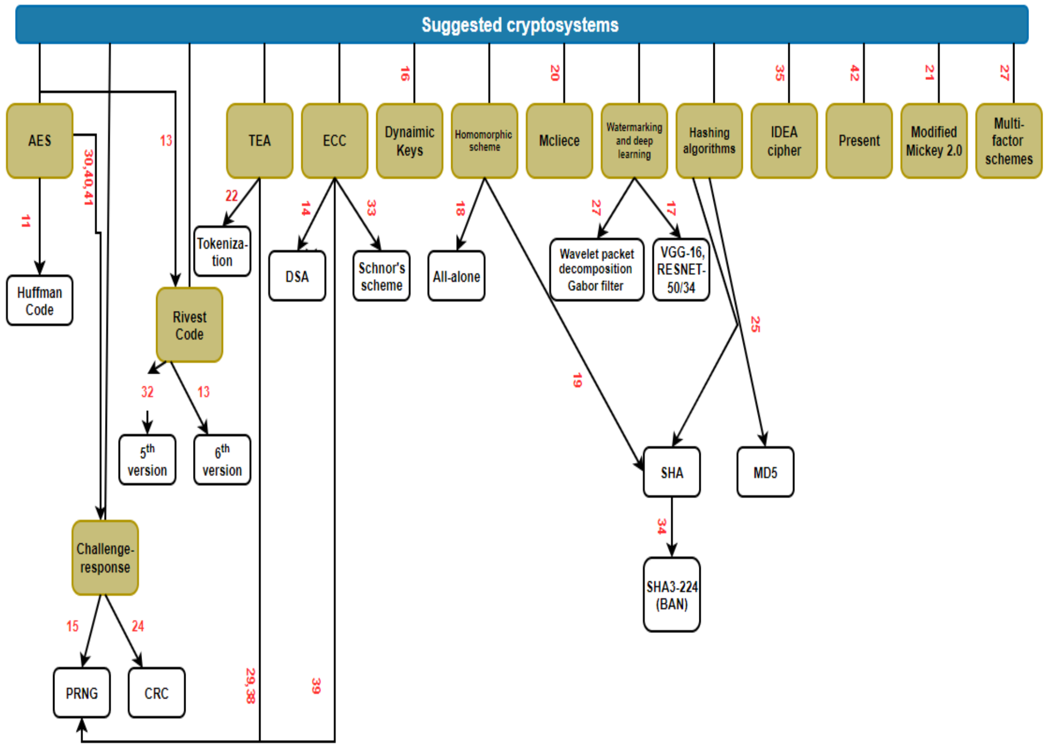

Figure 5. Graphical representation of Table 5 suggested cryptosystems.

5. Discussion

As stated above, many efforts have been made to surmount the highlighted issue, but plenty of the suggested proposals are quite heavy to be applied for general usage. First, the AES cipher can be mentioned as a robust algorithm that offers strong security, but the algorithm's operations are complicated to handle by RFID tags. At this scale, reducing round numbers can fix this problem. The TEA cipher seems resource-friendly; unfortunately, the cipher has several security flaws, since it does not offer adequate security strength. Applying ECC along with several techniques provides a strong security level, where both the data confidentiality and integrity are well proven, but it is burdensome for tags' and readers' resources. Challenge–response schemes are suitable as an efficient solution for tags with computational limitations; nevertheless, the PRNG and CRC techniques used to build the schemes do not lend vigorous certainty if an attacker has good computation capabilities. The dynamic keys concept is another endeavor proposed to address the RFID environment security issue, but this solution is intricate to employ because each tag is configured individually. Homomorphic cryptography appears as a good construct, but it is onerous to apply to conventional RFID systems with built-in memory storage because of its mathematical operations. For this reason, it is widely utilized when the system has external storage capacity (cloud storage). Post-quantum schemes can also be used, but this is unlikely; the level of complexity of these solutions is significant and needs considerable mathematical understanding for implementation. Watermarking and deep learning methods might offer some security features; even so, these require specific hardware such as high-resolution cameras (facial recognition) and fingerprint sensors to gather biometric information, a fact that is regarded as costly for regular applications. Hashing algorithms can offer the wanted system integrity, but some algorithms such as MD5 and SHA-1 are becoming vulnerable to some attacks, so carrying them out may cause security breaches and lead to sensitive information leakage. Among other solutions, some lightweight proposals sound relevant if applying some changes to their internal algorithmic cores in order to enhance their security performance; We can mention the IDEA, Present, Mickey, and Multi-factor authentication schemes, where the systemmust be reviewed to become superior cost–security tradeoff benchmarks. Based on these findings, there are plenty of suggestions that can be given as follows:

- **Healthcare applications:** Due to the real-time demand of data, low-cost cryptosystems are preferred, and we can mention the Tiny Encryption Algorithm (TEA) and Mickey ciphers. However, some critical changes must be made at the core of both algorithms because of the low resistance of to a manifold of types of attacks such as side channel attacks and the weak avalanche abilities, which reduce the cryptosystem's trustworthiness. For this reason, advanced or improved versions of both algorithms are suggested.
- **E-payment:** Because of the high sensitivity of the exchanged data between smart cards, readers, and connected databases that are related to banks, the higher the security, the more confident the system becomes. Therefore, it is suggested to employ the public key infrastructure concept within digital signatures to provide authenticity and confidentiality to users.
- **E-voting:** A card can be issued to every eligible citizen to vote in his/her country's elections. This can be a one-time utilization card, where robust cryptosystems are implemented to avoid vote corruption. Homomorphic cryptography along with other algorithms such as AES can be combined to offer the utmost possible security.
- **Other applications:** The cost, performance, and security trade-off must always be kept in mind by developers. Security requires computational abilities that obviously decrease the application's performance, a fact that directly enhances the cost and vice versa.

6. Conclusions

Securing tags and readers is a predominant requirement that needs to be undertaken, especially since RFID is widely used in numerous types of applications and implemented within a variety of life domains. This SLR presented the security challenges and threats along with the most-recent studies on cryptography schemes to resist several cyberattacks. The major intention of this work was to provide a thorough perspective for fresh researchers in this area. Encouraging suggestions were given such as elliptic curves' utilization as a preferential cryptosystem and lightweight crypto-primitives block and stream ciphers for asymmetric and symmetric approaches, respectively. Other proposals such as homomorphic encryption, post-quantum attempts, and the widely utilized challenge–response schemes for RFID smart card applications' security were included for completeness. In conformity with our SLR work, we can notice several gaps that can be addressed in the future to enhance the RFID system's trustworthiness and the ability to resist attacks. Innovative directions that seem promising for improving the security of RFID systems were suggested and remain open for future research.

Author Contributions: Methodology, I.E.G.; Validation, I.E.G.; Analysis, I.E.G.; Investigation, I.E.G.; Data collection, I.E.G.; Writing—original draft, I.E.G.; Results Validation, M.S., M.B. and B.E.B.; Supervision, M.S., M.B. and B.E.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors guarantee that none of their known financial conflict of interest or close personal ties have influenced the work reported in this publication.

Abbreviations

The following abbreviations are used in this manuscript:

BAN	Burrows–Abadi–Needham
CDMA	Code Division Multi-Access
CRC	Cyclic Redundancy Check
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
FDMA	Frequency Division Multi-Access
MD5	Message Digest 5
MFA	Multi-Factor Authentication
NFC	Near-Field Communications
PBE	Password-Based Encryption
PKI	Public Key Infrastructure
PRNG	Pseudo-Random Number Generation
RC	Rivest Code
RFID	Radio Frequency Identification
VGG	Visual Geometry Group
RESNET	Residual Neural Network
SHA	Secure Hash Algorithm
SDMA	Space Division Multi-Access
TDMA	Time Division Multi-Access
TEA	Tiny Encryption Algorithm

References

1. El Gaabouri, I.; Senhadji, M.; Belkasmi, M. A Survey on Lightweight Cryptography Approach for IoT Devices Security. In Proceedings of the 2022 5th International Conference on Networking, Information Systems and Security: Envisage Intelligent Systems in 5g//6G-based Interconnected Digital Worlds (NISS), Bandung, Indonesia, 30–31 March 2022; pp. 1–8.
2. El Mouaatamid, O.; Lahmer, M.; Belkasmi, M. Internet of Things Security: Layered classification of attacks and possible Countermeasures. *Electron. J. Inf. Technol.* **2016**, *9*, 66–80.
3. Baashirah, R.; Abuzneid, A. Survey on prominent RFID authentication protocols for passive tags. *Sensors* **2018**, *18*, 3584. [CrossRef] [PubMed]
4. Maarof, A.; Senhadji, M.; Labbi, Z.; Belkasmi, M. Security analysis of low cost RFID systems. In Proceedings of the 2014 5th Workshop on Codes, Cryptography and Communication Systems (WCCCS), El Jadida, Morocco, 27–28 November 2014; pp. 11–16.
5. Costa, F.; Genovesi, S.; Borgese, M.; Michel, A.; Dicandia, F.A.; Manara, G. A review of RFID sensors, the new frontier of internet of things. *Sensors* **2021**, *21*, 3138. [CrossRef]
6. Gupta, B.B.; Quamara, M. An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. *Concurr. Comput. Pract. Exp.* **2020**, *32*, e4946. [CrossRef]
7. Kumar, A.; Jain, A.K.; Dua, M. A comprehensive taxonomy of security and privacy issues in RFID. *Complex Intell. Syst.* **2021**, *7*, 1327–1347. [CrossRef]
8. Landaluce, H.; Arjona, L.; Perallos, A.; Falcone, F.; Angulo, I.; Muralter, F. A review of IoT sensing applications and challenges using RFID and wireless sensor networks. *Sensors* **2020**, *20*, 2495. [CrossRef]
9. Cmiljanic, N.; Landaluce, H.; Perallos, A. A comparison of RFID anti-collision protocols for tag identification. *Appl. Sci.* **2018**, *8*, 1282. [CrossRef]
10. Damghani, H.; Hosseinian, H.; Damghani, L. Investigating attacks to improve security and privacy in RFID systems using the security bit method. In Proceedings of the 2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI), Tehran, Iran, 28 February–1 March 2019; pp. 833–838.
11. Adeniji, O.D.; Akinola, O.E.; Adesina, A.O.; Afolabi, O. Text Encryption with Advanced Encryption Standard (AES) for Near Field Communication (NFC) Using Huffman Compression. In Proceedings of the Applied Informatics: 5th International Conference, ICAI 2022, Arequipa, Peru, 27–29 October 2022; pp. 158–170.
12. Olaniyi, O.; Dogo, E.; Nuhu, B.; Treiblmaier, H.; Abdulsalam, Y.; Folawiyo, Z. A Secure Electronic Voting System Using Multifactor Authentication and Blockchain Technologies. In *Blockchain Applications in the Smart Era*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 41–63.
13. Vivek Raj, K.; Navya, N.; Madhushree, P.; Anjali, K.; Soundarya, B. RFID-Based Secure Multipurpose Smart Card Using Arduino Module. In Proceedings of the Third International Conference on Intelligent Computing, Information and Control Systems: ICICCS 2021, Secunderabad, India, 14–17 July 2022; pp. 403–415.

14. Arslan, A.; Çolak, S.A.; Ertürk, S. A secure and privacy friendly ECC based RFID authentication protocol for practical applications. *Wirel. Pers. Commun.* **2021**, *120*, 2653–2691. [CrossRef]
15. Dreyer, J.; Fischer, M.; Tönjes, R. NFC Key Exchange-A light-weight approach to authentic Public Key Exchange for IoT devices. In Proceedings of the 2021 IEEE 7th World Forum on Internet of Things (WF-IoT), Yokohama, Japan, 26 October–11 November 2021; pp. 374–379.
16. Noprianto, N.; Wijayaningrum, V.N. Smart card security mechanism with dynamic key. *J. Infotel* **2021**, *13*, 197–204. [CrossRef]
17. Benamara, N.K.; Keche, M.; Wellington, M.; Munyaradzi, Z. Securing E-payment Systems by RFID and Deep Facial Biometry. In Proceedings of the 2021 1st International Conference on Artificial Intelligence and Data Analytics (CAIDA), Riyadh, Saudi Arabia, 6–7 April 2021; pp. 151–157.
18. Basjaruddin, N.C.; Ramadhan, S.; Asyikin, M.B.Z.; Indrianty, Y. Baggage Tracing and Passenger Management System in Airport Based on NFC Using Homomorphic Cryptography. In Proceedings of the International Seminar of Science and Applied Technology (ISSAT 2020), Online, 24–25 November 2020; pp. 296–301.
19. Suyitno, D.; Aladhirus, B.R.; Wardhani, R.W. Design and Implementation of Smart Card based Secure Key Storage The Blockchain E-voting Application. In Proceedings of the 2020 1st International Conference on Information Technology, Advanced Mechanical and Electrical Engineering (ICITAMEE), Yogyakarta, Indonesia, 13–14 October 2020; pp. 259–264.
20. Chikouche, N.; Cherif, F. EAP-SRES: An Enhanced Authentication Protocol for Secure Remote Education Systems Using NFC Technology. *Int. J. Comput. Digit. Syst.* **2020**, *9*, 3.
21. Alamer, A.; Soh, B.; Alahmadi, A.H.; Brumbaugh, D.E. Prototype device with lightweight protocol for secure RFID communication without reliable connectivity. *IEEE Access* **2019**, *7*, 168337–168356. [CrossRef]
22. Arulmozhi, P.; Rayappan, J.; Raj, P. A lightweight memory-based protocol authentication using radio frequency identification (rfid). In *Advances in Big Data and Cloud Computing: Proceedings of ICBDCC18*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 163–172.
23. Zhang, Y.; Guin, U. End-to-end traceability of ICs in component supply chain for fighting against recycling. *IEEE Trans. Inf. Forensics Secur.* **2019**, *15*, 767–775. [CrossRef]
24. Kang, J. Lightweight mutual authentication RFID protocol for secure multi-tag simultaneous authentication in ubiquitous environments. *J. Supercomput.* **2019**, *75*, 4529–4542. [CrossRef]
25. Putra, I.G.S.E.; Labasariyani, N.L.P. Design and Development of Login Security System Using Radio Frequency Identification. *Logic J. Ranc. Bangun Dan Teknol.* **2019**, *19*, 41–46. [CrossRef]
26. Soe, N.; Aung, T.H. Implementation of Secure Electronic Payment System Using RFID and ECC Digital Signature. *Int. J. Sci. Eng. Technol. Res.* **2019**, *8*, 6.
27. Rzouga Haddada, L.; Essoukri Ben Amara, N. Double watermarking-based biometric access control for radio frequency identification card. *Int. J. Microw. Comput. Aided Eng.* **2019**, *29*, e21905. [CrossRef]
28. Insan, I.M.; Sukarno, P.; Yasirandi, R. Multi-factor authentication using a smart card and fingerprint (case study: Parking gate). *Indones. J. Comput.* **2019**, *4*, 55–66.
29. Abdulsalam, Y.S.; Olaniyi, O.M.; Ahmed, A. Enhanced tiny encryption algorithm for secure electronic health authentication system. *Int. J. Inf. Privacy Secur. Integr.* **2018**, *3*, 230–252. [CrossRef]
30. Cetinkaya, M.; Dede, J.; Förster, A. An RFID Based Secure Key and Configuration Distribution for Contiki. In Proceedings of the EWSN, Madrid, Spain, 14–16 February 2018; pp. 189–190.
31. Xu, H.; Ding, J.; Li, P.; Zhu, F.; Wang, R. A lightweight RFID mutual authentication protocol based on physical unclonable function. *Sensors* **2018**, *8*, 760. [CrossRef]
32. Villanueva, E.B.; Gerardo, B.D.; Medina, R.P. Implementation of the Enhanced RC5 (ERC5) Algorithm in an RFID-based Payment Scheme. In Proceedings of the 2nd International Conference on Business and Information Management, Barcelona, Spain, 20–22 September 2018; pp. 6–10.
33. Malina, L.; Dzurenda, P.; Hajny, J.; Martinasek, Z. Secure and efficient two-factor zero-knowledge authentication solution for access control systems. *Comput. Secur.* **2018**, *77*, 500–513. [CrossRef]
34. Liu, B.; Yang, B.; Su, X. An improved two-way security authentication protocol for RFID system. *Information* **2018**, *9*, 86. [CrossRef]
35. Nurdiyanto, H.; Rahim, R.; Hidayat, R.; Harliana, P.; Gunawan, G.; Adam, H.; Sonatha, Y.; Azmi, M. Authentication Security in Radio Frequency Identification with IDEA Algorithm. In *Proceedings of the IOP Conference Series: Materials Science and Engineering*; IOP Publishing: Bristol, UK, 2018; Volume 384, p. 012042.
36. Álvarez-Díaz, N.; Caballero-Gil, P.; Burmester, M. A luggage control system based on NFC and homomorphic cryptography. *Mob. Inf. Syst. J.* **2017**, *2017*, 2095161 .
37. Younis, M.I.; Abdulkareem, M.H. ITPMAP: An improved three-pass mutual authentication protocol for secure RFID systems. *Wirel. Pers. Commun. J.* **2017**, *96*, 65–101 [CrossRef]
38. Olaniyi, O.M.; Arulogun, O.T.; Omotosho, A.; Onuh, V.O. Securing clinic tele-diagnostic system using enhanced tiny encrypted radio frequency identification and image steganographic technique. *Int. J. Telemed. Clin. Pract.* **2017**, *2*, 242–266. [CrossRef]
39. Chien, H.Y. Elliptic curve cryptography-based RFID authentication resisting active tracking. *Wirel. Pers. Commun.* **2017**, *94*, 2925–2936. [CrossRef]
40. Chien, H.Y. Efficient authentication scheme with tag-identity protection for EPC Class 2 Generation 2 version 2 standards. *Int. J. Distrib. Sens. Netw.* **2017**, *13*, 1550147717697321. [CrossRef]

41. Ratnadewi, R.; Adhie, R.; Hutama, Y.; Christian, J.; Wijaya, D. Implementation and performance analysis of AES-128 cryptography method in an NFC-based communication system. *World Trans. Eng. Technol. Educ.* **2017**, *15*, 178–183.
42. Naija, Y.; Beroulle, V.; Machhout, M. Low cost countermeasure at authentication protocol level against electromagnetic side channel attacks on RFID tags. *Int. J. Adv. Comput. Sci. Appl.* **2017**, *8*, 11. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.