International Journal of Computers and Applications

ISSN: 1206-212X (Print) 1925-7074 (Online) Journal homepage: www.tandfonline.com/journals/tjca20

A secure and efficient identity-based RFID mutual Authentication scheme for IoT using elliptic curve cryptography

Md Ozaif, Mahfooz Alam, Suhel Mustajab, Mohd Mustaqeem & Nadeem Khan

To cite this article: Md Ozaif, Mahfooz Alam, Suhel Mustajab, Mohd Mustaqeem & Nadeem Khan (2025) A secure and efficient identity-based RFID mutual Authentication scheme for IoT using elliptic curve cryptography, International Journal of Computers and Applications, 47:5, 424-437, DOI: 10.1080/1206212X.2025.2491075

To link to this article: https://doi.org/10.1080/1206212X.2025.2491075

Published online: 29 Apr 2025.

INTERNATIONAL JOURNAL OF COMPUTERS AND APPLICATIONS
2025, VOL. 47, NO. 5, 424–437
https://doi.org/10.1080/1206212X.2025.2491075

A secure and efficient identity-based RFID mutual Authentication scheme for IoT using elliptic curve cryptography

Md Ozaif [a], Mahfooz Alam [b], Suhel Mustajab [a], Mohd Mustaqeem [a] and Nadeem Khan[a]

[a]Department of Computer Science, Aligarh Muslim University, Aligarh, India; [b]Department of MCA, G. L. Bajaj Institute of Technology and Management, Greater Noida, India

ABSTRACT

Existing ECC-based RFID authentication protocols exhibit vulnerabilities to various attacks. A new ECC-based authentication protocol is proposed to address these issues, ensuring mutual authentication, confidentiality, and resistance to SCA. The proposed protocol minimizes computational time and enhances privacy features without additional calculations. Security and privacy comparisons with existing schemes show the improved protocol's effectiveness in mitigating threats. The study emphasizes practical implementation and detailed security analysis, highlighting the protocol's efficiency and security enhancements. Further, it discusses emerging security solutions, including encryption algorithms, secure key exchange protocols, and anomaly detection techniques, to mitigate potential risks and enhance the overall security posture of IoT and RFID systems. By understanding and addressing these security concerns, organizations and individuals can fully leverage the transformative power of IoT and RFID technologies while safeguarding sensitive data and ensuring the integrity and reliability of interconnected systems.

ARTICLE HISTORY
Received 1 September 2024
Accepted 4 April 2025

KEYWORDS
Internet of things; ECC; RFID; side channel attack; authentication method; AVISPA tool

1. Introduction

The Internet of Things (IoT) refers to a connected network of physical objects, devices, and sensors capable of gathering, transmitting, and exchanging data through the Internet. These networked devices can automate many processes, enhance decision-making, and deliver various services, all while exchanging data without human intervention. However, people can interact with these devices to set up, give instructions, or access the data [1,2]. Since the inception of IoT in 2008, the field has experienced significant growth [3]. In 2010, 7.5 billion devices were connected to the internet. It is estimated that by 2025, there will be more than 30 billion IoT device connections, averaging approximately four IoT devices per person [4]. IoT extends the power of the internet beyond computers and smartphones to a vast array of everyday objects, making them 'smart' and capable of enhancing various aspects of our lives. However, given the increasing connectivity of IoT devices, they need to be protected from any security threats [5]. The IoT concept has numerous applications in a variety of industries, including household appliances, healthcare, security, etc [6]. It is expanding quickly and will soon be an inseparable part of our daily life, its architecture is typically divided into three layers.

- **Sensing Layer**: Collects data from the physical world through sensors and devices.
- **Network Layer**: Transmits data from IoT devices to the processing layer.
- **Data Processing Layer**: Filters, normalizes, and analyzes the received data to derive actionable insights [7].

1.1. Iot security challenges

Implementing IoT security involves measures and practices designed to protect interconnected devices and networks within the IoT ecosystem from potential threats and vulnerabilities [8]. It involves safeguarding data, securing communications, and ensuring the integrity and privacy of connected devices. With the growing number of IoT devices, addressing security risks is crucial to prevent unauthorized access, data breaches, and potential harm to individuals and infrastructure. Effective security measures, such as encryption, authentication, and timely updates, are essential for maintaining the trustworthiness and dependability of IoT systems. Despite these measures, IoT systems remain vulnerable to a variety of attacks, including:

- Side-Channel Attacks (SCA): Exploit power consumption or timing information to extract cryptographic keys.
- Replay Attacks: Intercept and retransmit authentication messages to gain unauthorized access.
- Man-in-the-Middle (MITM) Attacks: Alter communication between devices by intercepting and manipulating data.
- Impersonation Attacks: Exploit weak identity management to impersonate legitimate devices.
- Cloning Attacks: Create duplicate devices by exploiting insecure storage of cryptographic parameters.
- Denial-of-Service (DoS) Attacks: Overwhelm systems with excessive requests, rendering them unavailable to legitimate users.
- Key Compromise Impersonation (KCI) Attack: A KCI attack occurs when an adversary compromises the private key of a

CONTACT Mahfooz Alam mahfoozalam.amu@gmail.com, malam.cs19@gmail.com Department of MCA, G. L. Bajaj Institute of Technology and Management, Greater Noida-201306, U.P., India

legitimate entity and uses it to impersonate another entity in the system, bypassing authentication mechanisms.

1.2. Elliptic Curve Cryptography (ECC) in IoT and RFID

Elliptic Curve Cryptography (ECC) has emerged as a beacon of lightweight cryptographic strength, particularly relevant for Radio-frequency Identification (RFID) systems where computational simplicity is crucial [9]. The application of ECC in RFID signifies a significant advancement in balancing stringent security demands with the inherent resource constraints of RFID tags. ECC's ability to provide high levels of security with relatively small key sizes results in reduced power consumption and faster computations, making it a perfect match for the lean nature of RFID technology [10–12]. This synergy between ECC and RFID not only strengthens tag-to-reader communications against sophisticated attacks but also supports ongoing research into lightweight cryptography, striving for the highest efficiency and security in the ever-expanding scope of wireless identification.

RFID technology, harnessed within the purview of security and authentication, has seen a significant evolution with the integration of ECC [13]. ECC's strength lies in its lower computational overhead and higher security per bit of key size, making it ideally suited for resource-constrained environments like RFID systems [14]. This melding of technologies brings forth a paradigm where the compactness of RFID tags' compactness synergizes with ECC's robustness, paving the way for a new generation of secure, efficient, and scalable authentication mechanisms. These advancements not only bolster the security landscape of RFID applications but also open new avenues for research, focusing on optimizing the balance between computational efficiency and cryptographic strength [15]. In order to facilitate safe and effective device authentication, the proposed strategy incorporates RFID technology into IoT networks. In IoT networks, RFID tags – whether active, passive, or semi-passive – are essential for tracking and identifying physical things. The ECC-based authentication protocol addresses resource limitations and security issues common to IoT environments , which guarantees safe communication between RFID tags, readers, and backend systems. The system works with IoT-enabled active tags, which may have extra sensors or communication features enabling direct communication with IoT networks, even if it is made to be agnostic to the type of RFID tag.

RFID-based mutual authentication schemes using ECC are vulnerable to various threats, including side-channel attacks (SCA). For instance, power analysis attacks can exploit power consumption patterns or execution time variations to extract private cryptographic keys. Replay attacks happen when a hacker uses weak challenge-response protocols to intercept and retransmit authentication messages. If encryption and mutual authentication are not correctly implemented, attackers can change communication between the tag and server through Man-in-the-Middle (MITM) attacks. If adversaries are able to determine tag identities due to inadequate tag identification methods, impersonation attacks may be possible. If ECC keys are not changed on a regular basis, cloning attacks can generate duplicate tags by taking advantage of the insecure storage of cryptographic parameters. Also, by taking advantage of ECC's increased processing requirements, Denial-of-Service (DoS) attacks might overload the server with too many authentication requests, preventing authorized access. The contributions of this paper are summarized as follows.

- We show that protocols [16–25] are vulnerable to SCA attacks, contrary to their claims. Our analysis reveals that these schemes fail to achieve certain important security goals, as highlighted in [25].
- We propose an improved ECC-based authentication protocol design to minimize computational costs compared to protocols [16–27]. The security analysis demonstrates that our protocol provides mutual authentication, confidentiality, anonymity, and resistance to SCA.
- We present the implementation results of our proposed protocol in an RFID system to demonstrate its practicality and feasibility, utilizing SCA attacks in our evaluation. We present detailed security and performance comparisons between our protocol and related existing schemes.

The rest of this paper is structured in the following manner: Section 2 outlines the review papers on RFID technologies. Section 3 introduces the system model, RFID protocols reliant on ECC, and the essential vulnerability criteria needed for their effective implementation. Section 4 proposes a secure authentication scheme for RFID systems based on ECC. Section 5 provides an in-depth analysis of performance and functionality disparities, while the discussion is presented in Section 6.

2. Literature review

RFID authentication protocols play a critical role in ensuring the security and integrity of RFID systems. Recent research has focused on leveraging ECC to enhance the security of RFID authentication protocols. The literature review on RFID authentication protocols covers various aspects of lightweight RFID authentication protocols suitable for different applications. The review also includes an analysis of mutual authentication protocols, cryptographic solutions, and security challenges faced by RFID systems. This segment presents a review of prior studies on authentication protocols for RFID systems based on ECC and delineates the novel contributions of this paper. Several RFID protocols have been devised to address the diverse security and privacy challenges inherent in RFID systems. A recent exhaustive examination of existing protocols in this domain can be found in Avoine's RFID Security and Privacy Lounge. In the realm of public key cryptography (PKC), a significant majority of researchers have favoured ECC-based protocols due to their capacity to deliver high security using smaller key dimensions, alongside streamlined and effective computational processes.

In 2014, Zhao introduced [17] a novel protocol and demonstrated a vulnerability in Liao and Hsiao's protocol [28], wherein adversaries can extract the private key stored in the tag through a key compromise attack. The analysis reveals that Liao and Hsiao's protocol fails to uphold any security or privacy assurances as discussed in [19].

In 2017, Izza et al. [18] introduced a robust RFID authentication mechanism aimed at facilitating protected healthcare support and diagnostics while maintaining patient privacy in an IoT setting. This enhanced protocol is structured into two primary components: authentication and secure data transmission. Through rigorous evaluation using Burrows–Abadi–Needham (BAN) logic and random oracles alongside informal security assessments, [15] demonstrates resilience against significant security threats such as impersonation and privileged insider attacks, among others. The protocol ensures confidentiality, bidirectional authentication, and anonymity between the reader tag and the healthcare server, enhancing the patient data security framework. Moreover, Zheng et al., 2017 [22] introduced an enhanced version of the protocol originally developed by Tian and his team, designed to withstand de-synchronization and traceability attacks. Tian et al. had earlier developed a highly lightweight protocol, known as Random Access Permutation Protocol (RAPP), which leveraged permutation functions alongside XOR, permutation, and left rotation operations to fulfill the security requirements of RFID systems. This protocol was engineered to counter various threats,

including tango, disclosure, replay attacks, and de-synchronization within RFID environments. However, Ahmadian and his team later pointed out a vulnerability in Tian's protocol, indicating it could not effectively defend against de-synchronization attacks. Following this, [22] an approach based on the ECDLP-Random key, as detailed in their research, to address these security challenges.

In 2018, Naeem et al.'s protocol [19] analyzed a newly introduced RFID authentication protocol designed for IoT infrastructures. In [19] proved that the protocol, originally proposed in [20], lacks scalability, being limited to supporting just a single tag. Naeem went on to propose enhancements to the [20] scheme, making it not only secure but also scalable for application in various IoT settings. Additionally, these proposed modifications significantly lessen both computational and communication cost. Further, Alamr et al., 20 introduced a novel RFID authentication protocol [20], which utilizes elliptical curves and employs the Elliptic Curve Diffie-Hellman (ECDH) protocol as a key exchange method to establish secure communication between the tag and the reader. The ECDH protocol allows each party to possess its own public-private key pair and generate a new, modifiable key for encrypting the communication. This protocol is based on the Elliptic Curve Discrete Logarithm Problem (ECDLP) and the Elliptic Curve Factorization Problem (ECFP). The ECFP involves finding the points [s]P and [t]P such that the quantity Q equals [s]P + [t]P. Yang et al., 2018 [23] introduced an upgraded lightweight RFID authentication protocol tailored specifically for the IoT. Designed to meet the unique requirements of IoT settings, this protocol offers improved security and efficiency. The proposed protocol's main objective is to streamline the RFID system authentication procedure used in IoT situations, providing strong protection against security flaws while reducing computing load. By harnessing lightweight cryptographic methods, the protocol strikes a balance between security and efficiency, rendering it well-suited for IoT devices with limited resources. In summary, the proposed work contributes to the advancement of authentication mechanisms in RFID-based IoT systems, thereby bolstering the overall security stance of IoT deployments.

In 2020, the author Benssalah et al., presents a novel RFID authentication protocol tailored specifically for IoT environments [21]. This protocol relies on ECC, leveraging its strengths to secure IoT systems effectively. This authentication protocol's main goal is to address the efficiency and security issues that come with RFID-based IoT applications. Because the protocol uses ECC, it minimizes computational load and provides strong security, making it perfect for low-resource IoT devices. In essence, the proposed work centres on enhancing authentication mechanisms in RFID-enabled IoT setups using ECC, thereby contributing to the progress of secure and efficient IoT implementations. Moreover, Sowjanya et al., 16, recently proposed a scheme in [16]. It is highly efficient, requiring only three elliptic curve multiplications on the tag side. However, it is not scalable, as an exhaustive search on the reader side is necessary to determine the Diffie-Hellman key to decrypt the message and retrieve the basic information. Furthermore, if the secret key of the reader or tag is compromised, the tag's identity can be exposed. This protocol is compared with those in [29–31], all of which have several shortcomings, such as a lack of resistance to session-specific temporary information attacks and time synchronization attacks.

In 2021, Arslan and Bingöl introduced a secure, privacy-focused, and effective authentication protocol for RFID based on ECC [32]. This work included a thorough performance and security evaluation of the proposed protocol, with comparisons to existing schemes. Moreover, the protocol was implemented in an actual RFID system to showcase its real-world applicability. To the best of our knowledge, this scheme stands out as the most effective RFID authentication protocol utilizing ECC implemented in practice, fulfilling all essential security and privacy requirements, including both backward and forward privacy. According to Aloui's protocol 2021 [24], the tag accepts a random message Rr from the reader without validating it beforehand. The tag is required to complete the entire authentication process before determining the legitimacy of the request. Consequently, the tag lacks the capability to prevent a high volume of potential requests or manage inquiries from unauthorized readers. Consequently, the protocol may be susceptible to denial-of-service attacks.

In 2022, Noori et al. [26], introduced a scheme based on ECC to establish a mutual authentication within RFID technology in the IoT. The proposed scheme has lower computational costs, lower communication costs, while improving security against common RFID attacks. Despite its advantage, the protocol still faces high computational overhead for resource-constrained IoT devices and also lacks in providing MIMT, Impersonation, SPA, and DEMA. In 2023, Timouhin et al. [27], introduced a new ECC-based RFID authentication protocol designed to enhance security in IoT environments. The proposed protocol ensured mutual authentication, confidentiality, integrity, anonymity, and availability. It reduced computational and communication overhead while offering strong resistance against replay, tracking, and denial-of-service attacks. The scheme could not provide security against SPA and DEMA attacks. The comparative analysis is presented in Table 1 based on the existing literature review.

3. System model

RFID tags are an important component of an RFID-based system; thus, it is important to look into the complete system design and its collaborative operation. An RFID system has various interconnected components, including tags, readers, middleware, databases, and application software, collaboratively facilitating seamless data gathering, transmission, and processing. The combined performance of these components determines the overall system efficiency, covering aspects such as data accuracy, security, and real-time processing capabilities. Based on power supply sources, RFID tags are classified into three categories: active, passive, and semi-passive tags. The RFID system includes readers, which are positioned between the tags and the back-end server and function as interrogators. An RFID system typically comprises numerous tags, readers, and a back-end server [24]. A standard model of an RFID system is shown in Figure 1. RFID systems use radio frequency (RF) technology to enable wireless communication between tags and readers for various identification and authentication purposes. In some instances, the tag contains only a unique identification code, such as an Electronic Product Code (EPC). This identification code is written onto the tag and is unmodifiable.

3.1. Components of an RFID system

RFID systems need to be safeguarded, especially when they are utilized in sensitive or essential applications. RFID system security requirements aim to preserve data integrity, confidentiality, and availability, as well as to protect against unauthorized access and harmful assaults. RFID functions by transmitting and receiving signals using an antenna and an integrated circuit (IC) [31,33]. It primarily consists of two components: the RFID tag and the RFID reader. The RFID tags, equipped with an IC and an antenna, transmit data to the RFID reader, also known as an interrogator. The reader converts these radio waves into a more usable form of information. The data gathered from the RFID tags is then sent via a communication interface to a host computer system, where it can be stored in a

Table 1. A Comparative Analysis of RFID Syste ng ECC of Existing Works.

References		tosystem	Threat Model	Advantages / Secure against such attacks	Weakness/ Limitations
Zhao's scheme 2014 [17]	ECC		Key compromise, impersonation, replay, server spoofing, DoS, tracking, cloning	MITMA, Replay, Key Compromise, DoS, Location Tracking Cloning, Server Spoofing, and De-synchronization represent various security threats.	Does not provide tag anonymity, location privacy, data integrity, or backward and forward privacy.
Izza et al., protocol 2017 [18]	ECC, On Digita Messa	' hash function, ature with covery (DSMR)	Dolev – Yao Threat Model	DoS, MITMA, key compromise	Attacks using desynchronization techniques can occur on the communication channel.
Zheng et al., Protocol 2017 [22]	ECC		Cloning, tracking, DoS, and system internal attacks	MITMA, Impersonation, Replay, Location tracking, Key compromise, Cloning, Server spoofing, DoS, De-synchronization	Considering that only the channel Security of Secret Keys Against SCA attacks is not safe
Naeem et al., protocol 2018 [19]	ECC		Replay, impersonation , MITM, and tracking attacks	MITMA, Replay, Key Compromise, DoS, Location Tracking Cloning, Server Spoofing, and De-synchronization are all security concerns or threats.	This protocol does not consider SCA attacks.
Yang et al., 2018 [23]	ECC		Replay, impersonation, and modification attacks	MITMA, Replay, Key Compromise, DoS, Location Tracking Cloning, Server Spoofing, and De-synchronization represent various security threats	During data transmission, Yang's protocols are susceptible to SCA vulnerabilities.
Alamr et al., protocol 2018 [20]	ECC, Elli Diffie-Hellman (ECDH)	urve	MITM, replay, and impersonation attacks	MITMA, Impersonation, Replay, Key compromise, Location tracking, Cloning, Server spoofing	This scheme does not provide a DoS attack.
Benssalah et al., protocol 2020 [21]	ECC		SCA, impersonation, replay, and identity disclosure attacks	MITMA, Impersonation, Replay, Key compromise, Location tracking, DoS, Cloning, Server spoofing, De-synchronization	This scheme does not achieve SCA attack and does not provide forward and/or backward privacy, contrary to their claim [21].
Sowjanya et al., 16 [16]	ECC		MITM, impersonation , replay, and key compromise attacks	Mutual Authentication, Anonymity, Perfect Forward Secrecy, DoS.	Desynchronization attack, Scalability, SCA attack, Backward secrecy.
Aloui et al., protocol 2021 [24]	ECC		Replay, impersonation , MITM, and cloning attacks	Replay, Location tracking, MITMA, Cloning, Server spoofing, SPA	This protocol is not resistant to DEMA and DPA attacks.
Noori et al., 26 [26]	ECC		MITM, replay, eavesdropping, and forging attacks	Lower computational cost, communication cost, and elliptic curve point multiplication time Resistant to replay, MITM, and forging attacks validated using the AVISPA tool	It may have a higher computational cost for ultra-lightweight RFID devices Implementation may require optimizing elliptic curve parameter selection.
Timouhin et al., 27 [27]	ECC		Spoofing, tracking, and DoS attacks	Secure authentication between RFID tags, readers, and servers Resistance against spoofing, tracking, and denial of service attacks	Potential synchronization issues in large-scale RFID deployments, and may require additional optimizations for real-time IoT applications

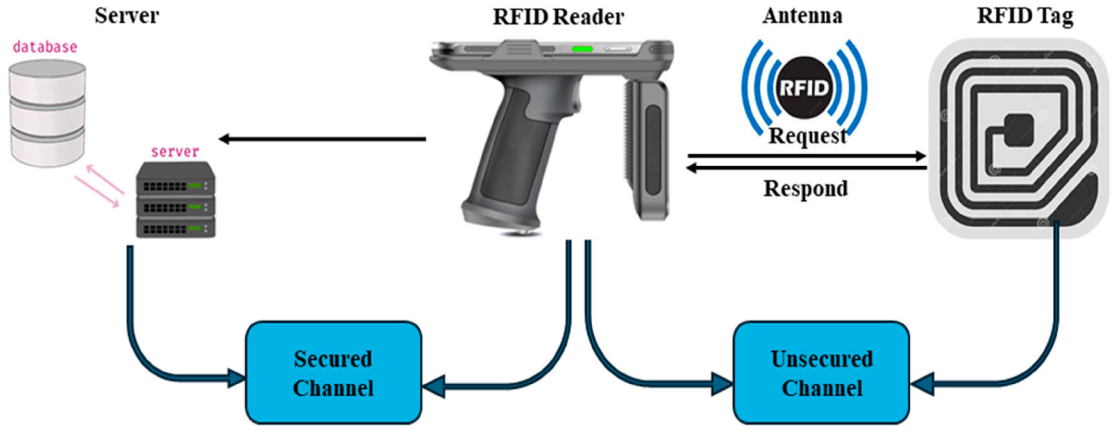

Figure 1. The components of RFID tags, RFID readers, and backend systems.

database and analyzed later [34]. The following figure illustrates this process.

3.1.1. RFID reader

The RFID reader plays a crucial role in tag identification, consisting of a transmitter, microprocessor, receiver, and antenna. This device emits electromagnetic waves containing a signal directed towards the target for identification. Subsequently, it captures signals that carry data from the tags. RFID readers can be stationary or portable, and their antennas are available in various shapes [35]. RFID readers authenticate and encrypt communication with RFID tags to ensure data integrity, confidentiality, and authenticity [36]. Authentication protocols can be symmetric, asymmetric, or lightweight, verifying tag identity and preventing unauthorized access. Encryption schemes protect data from eavesdropping and tampering, using symmetric or asymmetric cryptography, or lightweight mechanisms like stream ciphers or block ciphers. Security challenges in RFID systems include physical, logical, and protocol issues, impacting authentication and encryption effectiveness [37]. Various attacks like tag disabling, cloning, tracking, and replay attacks pose security risks, emphasizing the need for robust security measures in RFID systems [38]. Mutual authentication protocols based on ECC enhance RFID security, resisting attacks like impersonation and replay attacks [39]. ECC offers advantages in security and efficiency due to its smaller key size and strong encryption capabilities [40].

3.1.2. RFID tag

RFID tags function as small data storage units connected to objects, assets, or humans, facilitating efficient tracking and management in diverse applications [29]. RFID tags possess antennas that enable efficient communication with RFID readers within a specific frequency band, which is crucial to their performance. These interactions enable the transfer of data from the tag to the reader, hence enabling the extraction of stored information. RFID tags function as essential elements within a comprehensive RFID system, which encompasses readers, middleware, databases, and application software. The efficiency of an RFID system relies on the collaboration of its components to facilitate smooth data collecting, processing, and decision-making.

According to [30], RFID technology facilitates real-time tracking and administration of products; nevertheless, its efficiency is dependent upon the interaction among tags, readers, and backend systems. RFID readers acquire tag information and transmit it to a central database through middleware, where the data is processed, analyzed, and incorporated into enterprise applications. Security measures integrated into RFID tags, including encryption, are essential for protecting unique identifiers and sensitive data. However, the comprehensive security of the system is dependent upon network security protocols, authentication methods, and access controls throughout the entire RFID infrastructure [31]. The success of an RFID deployment depends on the collaboration among hardware, communication protocols, and data management strategies, which ensures accuracy, security, and operational efficiency.

3.1.3. Backend server

In RFID systems, back-end systems, or servers, serve as central components responsible for processing, storing, and managing RFID data collected from readers [41]. These servers, encompassing software, databases, and servers, play a pivotal role in integrating RFID data with other business processes such as inventory management or connected devices. They interact with multiple readers, receiving data and performing data processing and analysis tasks. Security measures implemented within servers are paramount to ensuring data integrity, confidentiality, and access control. As highlighted by [42], these security functionalities include validating and processing data received from readers, as well as enforcing authentication and authorization policies to safeguard against unauthorized access and data breaches. Servers leverage security protocols to verify the authenticity of both readers and tags, ensuring that only legitimate data is processed and stored securely [43].

3.2. Iot integration in the system model

In order to provide safe and effective device and object authentication, the suggested system model integrates RFID technology into the larger IoT ecosystem. This concept allows physical things to be uniquely identified and monitored within IoT networks by attaching RFID tags to them. As gateways, RFID readers receive information from the tags and send it to cloud-based systems or backend servers for processing and analysis. IoT systems may now automate procedures, improve decision-making, and provide services based on real-time data from RFID-tagged devices. The proposed ECC-based authentication protocol ensures secure communication between RFID tags, readers, and backend systems, addressing the resource constraints and security challenges typical of IoT environments. By providing mutual authentication, confidentiality, and resistance to attacks such as replay and impersonation, the protocol enhances the overall security of IoT deployments. This integration of RFID and IoT enables scalable, efficient, and secure solutions for applications such as supply chain management, healthcare, and smart cities.

3.3. Assumptions and threats model

The protocol assumes that the RFID tag and reader are secure, and the communication channel is secure. However, it is vulnerable to various attacks, such as replay attacks, man-in-the-middle attacks, Server Spoofing, DoS attacks, and impersonation attacks [24,44]. Based on the provided research papers, [16–27] protocol is identified as vulnerable to MITM attack, while Impersonation Attacks are mentioned in the protocols [16–25]. Key Compromise Attacks are addressed in the papers [17,19,20,22,25]. Additionally, DoS attacks are discussed in the works by [9,15,17,20–23,25]. Cloning attacks are highlighted in the papers [9,17,19–25]. Furthermore, Server Spoofing is mentioned in the papers by [17,19–25].

Information about Side-Channel Attacks (SCA) exploits has been disclosed by analysing physical attributes of the system, such as power usage or electromagnetic radiation [45,46]. Protocols should be designed employing defences to mitigate SCA, such as using constant-time algorithms, secure hardware implementation, or randomizing power consumption. SCA can be avoided through ECC itself is able to withstand specific SCA, like basic power analysis or timing attacks, due to its inherent mathematical properties [25].

Studies by [34,47] explore the vulnerabilities of various RFID authentication protocols employing ECC against hardware attacks, especially SCA. Their findings underscore the susceptibility of these protocols to Analysing differential electromagnetic attack (DEMA) fields and differential power analysis (DPA) and other forms of SCAs, highlighting deficiencies in safeguarding secret keys and resisting unauthorized access. Despite the rigorous cryptographic mechanisms embedded within these protocols, the lack of robustness against SCA is a significant challenge in ensuring the integrity and security of RFID systems. Consequently, there is a pressing need for further research and development efforts aimed at enhancing the resilience of ECC-based RFID authentication protocols against hardware-based attacks, thus fortifying the overall security posture of RFID-enabled systems.

The existing approaches for RFID authentication protocols using ECC face several challenges and limitations. The applicability of asymmetric systems such as ECC for RFID remains an unresolved research challenge, primarily due to constraints related to tag expenses, gate count, and power allocation. It is crucial to meticulously design the ECC architecture and asymmetric mutual authentication protocol to guarantee both security and efficiency [48]. Employing ECC crypto-systems within RFID systems aims to ensure confidentiality and mutual authentication. However, the hardware vulnerabilities of encryption block within tags can be exploited by hardware attacks such as side-channel analysis (SCA) and fault attacks (FA) [49]. These attacks, as highlighted by, pose a significant threat to the security of RFID systems. While SCA attacks on contactless devices like RFID are more intricate compared to contact devices, they are not beyond the realm of feasibility. While RFID authentication protocols integrate symmetric encryption cryptographic primitives to mitigate SCA attacks, there is a lack of protocols specifically addressing the security of encryption blocks against SCA attacks. This gap in the literature highlights the need for further research to ensure the security of encryption blocks against SCA attacks. The need to develop lightweight ECC implementation designs explicitly for RFID applications arises from the resource constraints of RFID systems. However, the development of these architectures is still an active area of research, and the search for optimal solutions continues.

3.4. ECC in IoT security

ECC is emerging as a promising solution to enhance security measures within IoT networks [50]. As an asymmetric encryption method, ECC secures data transmission across public networks through the exchange of public keys [34,51]. The need to balance security, speed, and hardware resource utilization has made the hardware implementation of the ECC algorithm a major emphasis during the past 10 years. The efficacy of ECC algorithms is highly dependent on arithmetic operations within the foundational GF, which are either prime order domains GF (p) or binary fields GF (2^m). Both types offer comparable security levels, but GF (2^m) is noted for its simplicity and ease of implementation in hardware. In these fields, addition and subtraction operations are efficiently performed using modulo-2 arithmetic. Specifically, an EC defined across the finite field GF (2^m) the binary field follows the equation $y^2 + xy = x^2 + ax^2 + b$, optimizing for both performance and security in cryptographic applications [52]. These curves have unique properties that make them suitable for cryptographic operations.

Previously, RSA was the dominant public key encryption method until the full advent and adoption of ECC. ECC's security hinges on the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP). Advancements in solving RSA's complex problems necessitated an increase in operand sizes to 3072 bits to achieve a 128-bit security level, whereas ECC achieves the same security with just 256 bits [53]. The strength of ECC largely depends on the choice of curve; thus, organizations such as the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO) have endorsed specific ECC curves to ensure secure cryptographic encryption [54]. ECC is recognized for providing robust IT solutions, ensuring confidentiality, authenticity, reliability of data transmission, and non-repudiation. Furthermore, the Diffie-Hellman key exchange mechanism, integral to ECC, secures principal communications over public networks through the use of public and private keys [55].

ECC-based solutions, such as mutual authentication, secure key exchange, digital signatures, and encryption, ensure data security in RFID systems by preserving confidentiality, integrity, and authenticity [56]. These solutions involve the exchange of encrypted challenges and responses between tags and readers to ensure that only authenticated entities communicate. Secure key exchange is facilitated by ECC protocols like ECDH, which establish confidential keys for subsequent encrypted communication [57]. In [58] digital signatures, such as ECDSA, verify the source and integrity of RFID data, ensuring this encryption has not been tampered with. Using ECC with a symmetric algorithm protects RFID data, allowing access only to authorized parties.

RFID systems are susceptible to attacks like network scanning, tracking, and eavesdropping since they rely on wireless communication routes between cards and card readers [20]. However, by offering an effective security plan for RFID networks, ECC-based solutions can aid in securing this technology. In Figure 2, we have shown that ECC involves a secure information exchange process that enhances security while maintaining efficiency. The server initiates authentication by generating a challenge which the RFID tag must respond to. The tag uses ECC to generate a cryptographic response. Upon receiving this response, the server verifies it using ECC algorithms to ensure its validity. If the response is verified, authentication is successful. This process ensures that the exchange of information between the server and the RFID tag remains secure, leveraging the strong cryptographic capabilities of ECC to prevent unauthorized access and ensure data integrity.

4. Proposed Identity-Based RFID Mutual Authentication Scheme on ECC

The proposed Identity-Based RFID Mutual Authentication Scheme on ECC intends to improve the RFID system's efficiency and security

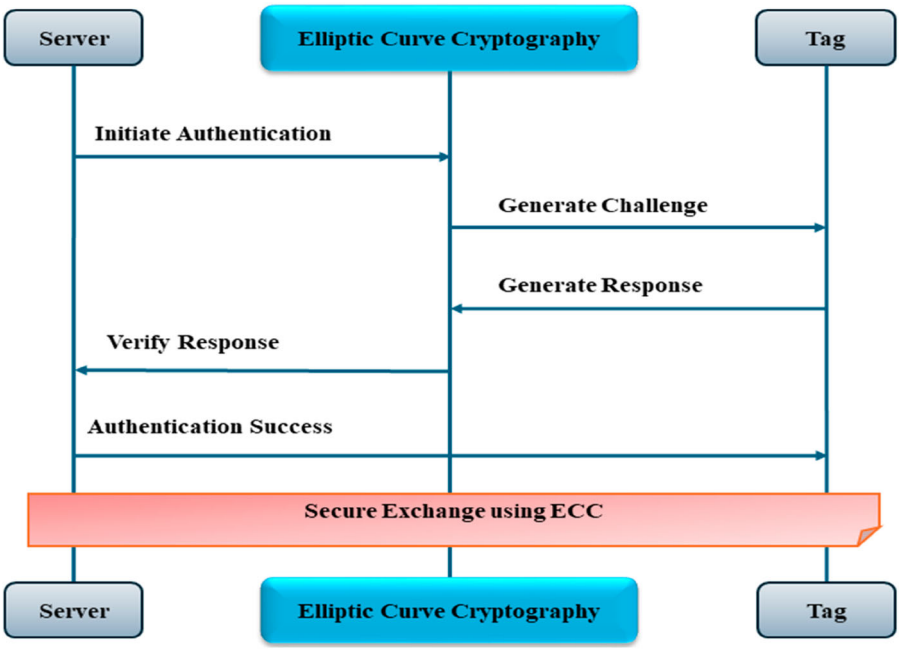

Figure 2. The secure information exchange in the Authentication Protocol in RFID utilizing ECC. Figure 2

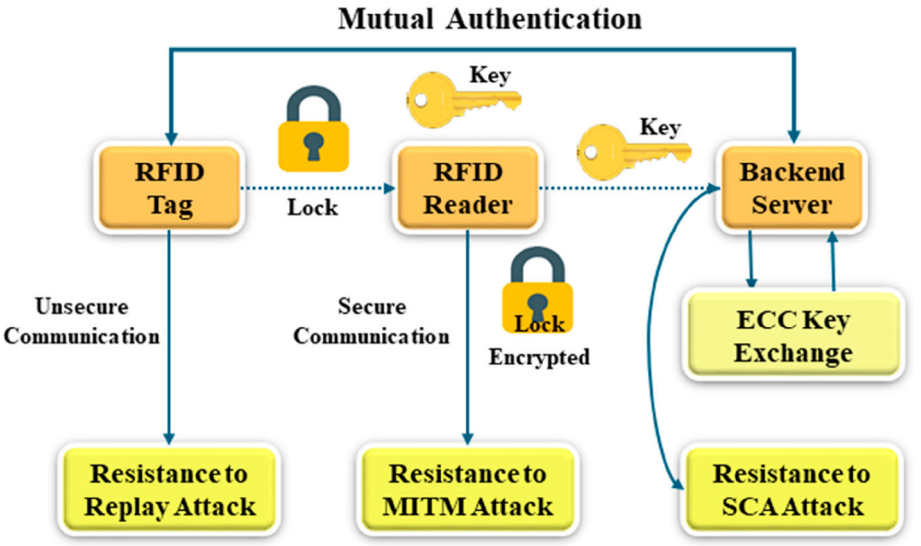

Figure 3. Depicts a general overview of the proposed model.

in IoT. The scheme makes use of ECC's built-in advantages, such as its capacity to offer strong security with reduced key sizes, which makes it perfect for RFID tags with limited resources. By ensuring mutual authentication between the RFID tag and the reader, the protocol guards against unwanted access and mitigates a number of threats, such as SCA, replay, and MITM. The protocol guarantees the secrecy, integrity, and validity of the communication between the tag and the reader by employing key exchange mechanisms and encryption based on ECC. The plan is also made to reduce communication and computation overhead, which makes it appropriate for low-power Internet of Things devices.

Figure 3 shows the safe communication flow between the RFID tag, reader, and backend server. The process of mutual authentication, in which the tag and the reader confirm each other's identities in order to create a secure connection, is highlighted in the diagram. The use of ECC for encryption and key exchange is essential to this system since it offers a strong defense against several threats, such as SCA, replay attacks, and MITM attacks. The 'Lock Encrypted' symbol indicates that the communication is protected by encryption, guaranteeing the integrity and confidentiality of the data. The difference between secure and insecure communication channels emphasizes how crucial it is to put robust security mechanisms in place to safeguard private information sent back and forth between the tag and the reader.

ECC algorithms are implemented in a way that they are resistant to Figure, which is important for RFID tags that might be physically accessible to attackers [59]. Modifications to elliptic curves for low-frequency operations involve adjustments at the mathematical level, enhancing their applicability [60]. At the hardware level, the effectiveness of ECC implementations, particularly the scalar multiplication algorithm, is significantly influenced by the choice of hardware architecture. This tailored approach optimizes resource use

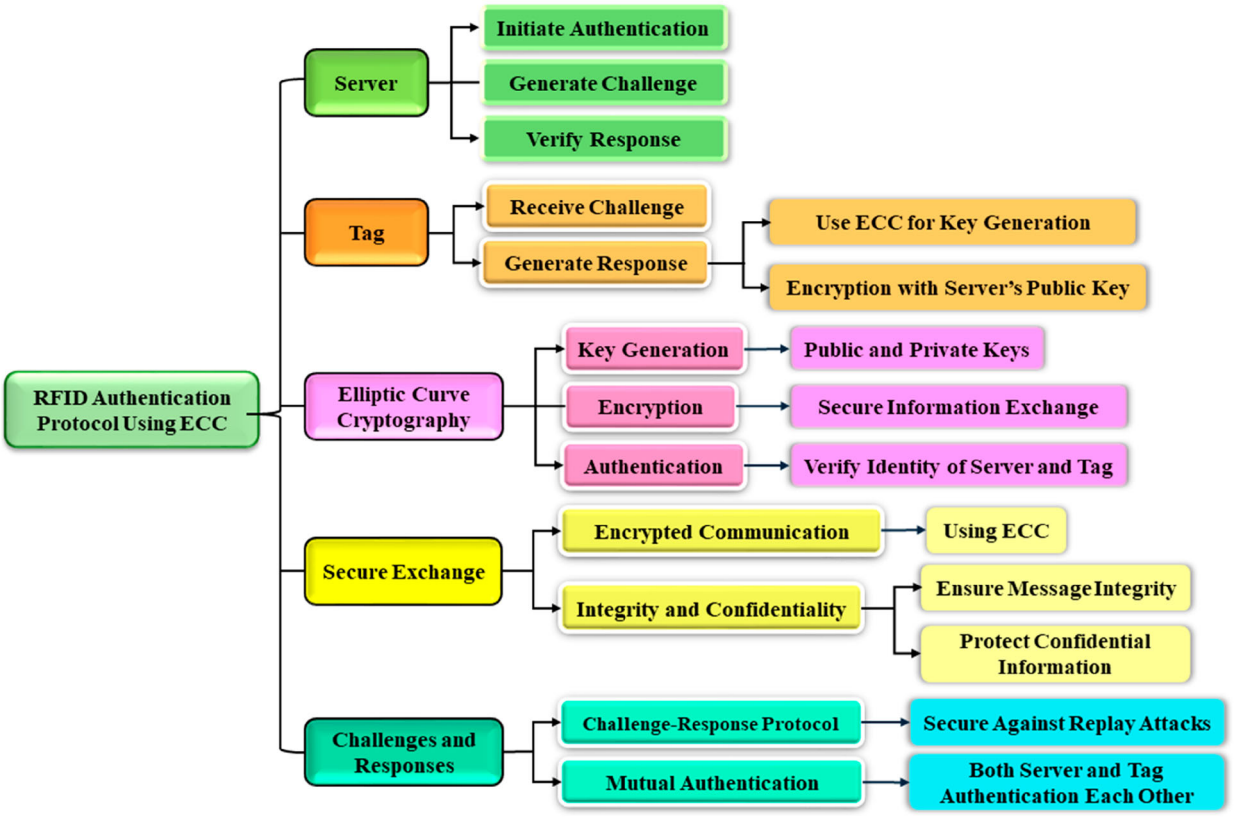

Figure 4. Verification, Establishment, and Management of an RFID System Using ECC.

in RFID applications, leveraging ECC's benefits to enhance security efficiently. The RFID authentication protocol using ECC ensures the secure establishment and management of information exchange as depicted in Figure 3. This process involves mutual authentication where both the server and the RFID tag authenticate each other using a challenge-response protocol. ECC is utilized for key generation, encryption, and verifying the integrity and confidentiality of messages, making the system secure against replay attacks. By encrypting communications with the server's public key and generating unique challenges and responses, the protocol ensures that confidential information remains protected throughout the authentication process, as shown in Figure 4.

4.1. Key establishment and management

Key establishment and management are critical aspects of cryptographic systems, ensuring secure and efficient communication between parties [61]. Securely generate cryptographic keys using random number generators. Keys can be symmetric (shared) or asymmetric (public-private) [62] as depicted in Figure 4.

4.1.1. Data encryption

To ensure secure communication, the process typically starts with generating an ECC key pair, containing both a private and a public key [63]. While the private key remains confidential, the public key is shared openly. In scenarios involving two parties, an ECC-based key exchange protocol like ECDH is utilized to create a mutual secret key, which is then used for symmetric encryption. Employing the agreed-upon secret key, information is encrypted using a symmetric encryption method such as Advanced Encryption Standard (AES) [64]. This process involves dividing the data into segments and encrypting them using the symmetric key. Eventually, the encrypted data is securely transmitted, ensuring the inclusion of necessary details like the public key and any additional parameters required for decryption, thereby ensuring its secure delivery to the intended recipient [34].

4.1.2. Decoding encrypted data

To start the decryption procedure, obtain a private key from the ECC key pair utilized in the encryption process, if required, as it plays a crucial role in generating the shared secret key necessary for symmetric decryption [65]. If encryption employs a key agreement protocol [66], use the recipient's private key and the sender's public key to implement this protocol and create a shared secret key. Then, utilize this mutual secret key to decrypt the encrypted data symmetrically, applying the same symmetric encryption method and settings used during encryption. Process each block of data individually to retrieve the original plaintext [67]. Lastly, verify the integrity of the decrypted data by checking for any modifications during storage or transmission, employing methods like digital signatures or Message Authentication Codes (MACs).

4.1.3. Tag ownership transfer

Theprocess of transferring ownership of a tag is more complex than simple tag-to-reader authentication or mutual authentication due to the involvement of both the existing and prospective owners. This transfer process is intricately linked to the tag's authenticity by its reader [68]. Recently, an authentication protocol that facilitates tag ownership transfer using hash and XOR operations. They assert that their protocol ensures the untraceability of tags, even in the presence of sophisticated adversaries, thereby enhancing security during the ownership transfer phase.

4.1.4. Cryptographic hash functions

Cryptographic hash functions, such as SHA-256, can be effectively utilized in RFID systems to ensure data integrity [69]. Hash functions produce consistent hash values of a specific size that uniquely identify the input data, allowing for the detection of any modifications or tampering of the RFID data. This approach serves as a strong technique to safeguard the genuineness and completeness of RFID data, especially when combined with techniques like ECC.

4.1.5. Privacy-preserving protocols

To address privacy concerns, cryptographic techniques like pseudonyms and anonymous authentication can be used. Pseudonyms protect the identity of the tag by using temporary identifiers instead of permanent ones, and anonymous authentication protocols allow tags to authenticate without revealing their unique identifiers [70].

4.2. Registration phase

In this section, we will fully explain the Registration phase. In the proposed scheme, it is assumed that the communication between the reader and the back-end server is secure, while the communication between the tag and the reader is not secure. The symbols and terms used to describe the system are listed below.

n and q denote large prime numbers.–
r_1 signifies a random number generated by the reader.
r_2 represents a random number generated by the tag.
f_q denotes the finite field of q representing a finite field.
a and b are two parameters of an elliptic curve.
p represents a prime number generation of E
X_s signifies the private key generated by the server.
P_s represents the public key generated by the server, calculated as $P_s = X_s.P$
K denotes the identity of the tag.
P_t signifies the confidential key exchanged between the tag and the server.
IDS represents the tag's unique identity pseudonym.
$h()$ Represents a secure irreversible hashing algorithm that maps finite binary inputs to integers in the specified range $[2, n^2]$.

4.2.1. Our ECC algorithm design and improvement scheme

Our ECC algorithm design and improvement scheme for the RFID authentication process aims to enhance security and efficiency. In this scheme, both the tag and the reader mutually authenticate one another. The authentication process is summarized in Figure 5.

4.2.2. Authentication phase

The authentication phases are as follows:

Step 1. Server to Tag (Initialization):
During the initialization phase of communication from the server to the tag takes in the following manner-

- The server generates a random number $\boldsymbol{r_1}$ from the set of integers ($\boldsymbol{In}$).
- It computes $\boldsymbol{R_s} = \boldsymbol{r_1}.\boldsymbol{p}$, where $\boldsymbol{p}$ is a point on an elliptic curve.
- The server sends $\{\boldsymbol{R_s}\}$ to the tag to initiate the authentication process.

This step establishes the foundation for secure communication by generating and exchanging cryptographic parameters.

Step 2. Communication from Tag to Server (Authentication Request):

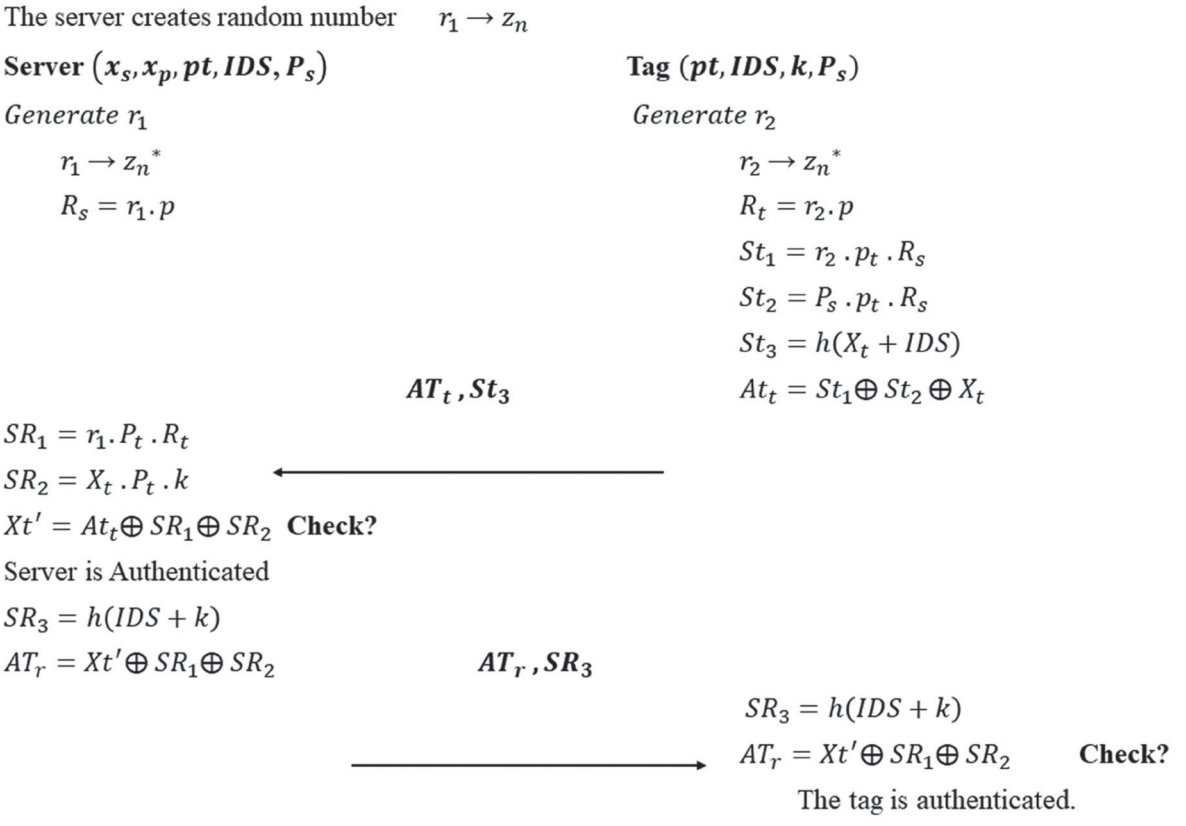

Figure 5. A Proposed Scheme.

Tag Action:
The tag generates a random number r_2 from the set of integers (In).
It computes:

- $R_t = r_2.p$,
- $St_1 = r_2 p_t R_s$,
- $St_2 = P_s p_t R_s$
- $St_3 = h(X_t + IDS)$
- $AT_t = St_1 \oplus St_2 \oplus Xt$

The tag sends AT_t, St_3 to the server. In this step the tag request authentication from the server by sending computed cryptographic values.
Step 3. Server to Tag (Authentication Response):
Server Action:
The server computes:

- $SR_1 = r_1 P_t$
- $SR_2 = Xt.P_t$ k
- $Xt' = AT_t \oplus SR_1 \oplus SR_2$

The server verifies if p_t exists in its database:

- If p_t is not found, the session is terminated.
- If p_t is found, the server proceeds to compute
- $SR_3 = h(IDS + k)$
- $AT_r = Xt' \oplus SR_1 \oplus SR_2$.

The server sends AT_r, SR_3 to the tag. This step ensures the integrity and authenticity of the server's response, enabling secure communication.
Step 4. Tag Verification:
Tag Action:
The tag compares the received SR_3 with the computed value AT_r.

- If SR_3 matches $\mathbf{AT_r}$, the server is authenticated.
- If SR_3 does not match $\mathbf{AT_r}$, the tag terminates the session to prevent potential security breaches.

This step ensures the integrity and authenticity of the server's response, completing the mutual authentication process.

5. Performance evaluation

The performance evaluation of RFID authentication protocol security using ECC involves assessing various aspects such as computational costs, storage memory requirements, and communication costs incurred under the schemes. This evaluation aims to compare the level of security offered by each protocol by examining whether they satisfy a set of security properties under a multi-level adversarial model. The security properties examined typically include tag anonymity, tag authenticity, reader authenticity, session unlinkability, forward secrecy, and desynchronization resilience. Additionally, the evaluation includes analysing the overhead in terms of computational costs, storage memory requirements, and communication costs to determine the efficiency and effectiveness of the ECC-based RFID authentication protocols.

5.1. Tags and reader computational cost (s) overhead analysis

The computational cost of elliptic curve operations is determined by their execution time. For instance, performing elliptic curve scalar multiplication on a 160-bit key using a 5 MHz processor takes approximately $T = 0.064$ s. Since the time taken for the hash function (T_h) on both the Server and Tag is very low. So, we can neglect this in our calculations [71]. If T_m represents the running time required for multiplication on the Tag, the approximate running time for a square operation is $T_m = T \times 0.064$. Similarly, the running time for addition is approximately $T_a = (T_a \times T/20)$. For the Server, if T' is the running time for multiplication, the square operation takes T'/5, and the addition operation takes approximately $T_a = (T_a \times T'/20)$.

Table 2. Comparison of computational cost.

Protocol	Tag's Total running time (s)	Reader Total running time (s)	Total cost
[16]	$3T_m + 2T_a = 0.1984$ s	$6T_m + 2T_a = 0.3904$ s	0.5888s
[17]	$5T_m + 2T_a = 0.3264$ s	$5T_m + 2T_a = 0.3264$ s	0.6528s
[18]	$3T_m$+$6T_h = 0.192$ s	$4T_m$+$7T_h = 0.256$ s	0.448s
[19]	$5T_m$+$2T_h + T_a = 0.3232$ s	$5T_m + 2T_h + T_a = 0.3232$ s	0.6464s
[20]	$4T_m + T_a = 0.2592$ s	$4T_m + T_a = 0.2592$ s	0.5184s
[21]	$3T_m + 3T_h + T_a = 0.1952$ s	$3T_m + 3T_h + T_a = 0.1952$ s	0.3904s
[22]	$4T_m + 3T_a = 0.2656$ s	$4T_m + 3T_a = 0.2656$ s	0.5312s
[23]	$T_m T_h = 0.064$ s	$T_m T_h = 0.064$ s	0.128s
[24]	$4T_m + 3T_a = 0.2656$ s	$2T_m + T_a = 0.1312$ s	0.3968s
[26]	$4T_m + 2T_h = 0.2533$ s	$4T_m + 2T_h = 0.2533$ s	0.5066
[27]	$3T_m + 2T_h = 0.1902$ s	$3T_m + 2T_h = 0.1902$ s	0.3804s
Proposed	$2T_m$+T_h+$T_a = 0.1312$ s	$64T_m$+T_h+$T_a = 0.0672$ s	0.1984s

Based on the notations provided, we compared the computational cost of our proposed protocol with eleven existing protocols, as shown in Table 2. The results show that our protocol is superior to others in terms of computational efficiency. Although the [23] protocol has a lower computational cost, it lacks security against SCA. Our proposed protocol addresses these vulnerabilities, providing enhanced security without significantly increasing computational cost. The incorporation of SCA-resistant techniques results in a marginal rise in computational complexity relative to protocols that do not mitigate SCA. This trade-off is essential for ensuring robust security, as SCA weaknesses may result in the extraction of private keys and compromise the entire system.

The proposed scheme is designed to provide robust security against a variety of attacks, including key compromise and impersonation attacks. In the proposed scheme, even if an adversary compromises the private key of one entity, they cannot impersonate another entity without knowing the random numbers and other parameters used in the authentication process.

Further, we provide a comparative analysis of each of the 11 protocols. Table 2 and Figure 6 detail the number of scalar multiplications required by the tag and reader for each protocol and calculate the total computation time based on the previously stated assumption of 0.064s per scalar multiplication. Furthermore, Table 2 and Figure 6 compare the calculation costs with several related works. The results indicate that, compared to the protocols in [16–27], our improved version requires less computational time to perform the total number of scalar multiplication operations needed. Furthermore, our protocol does not require any additional calculation to provide enhanced capabilities and additional privacy features. These properties make our protocol the least computationally time-consuming protocol.

5.2. Comparison of security and privacy with existing schemes

We focus on the security analysis of various proposed protocols. Table 3 evaluates the security and vulnerability of different protocols against wireless and physical attacks that RFID systems may encounter.

Through a number of important measures, such as mutual authentication, ECC-based encryption, resistance to side-channel attacks, and a challenge-response system, the suggested RFID authentication scheme improves security. Strong defense against a

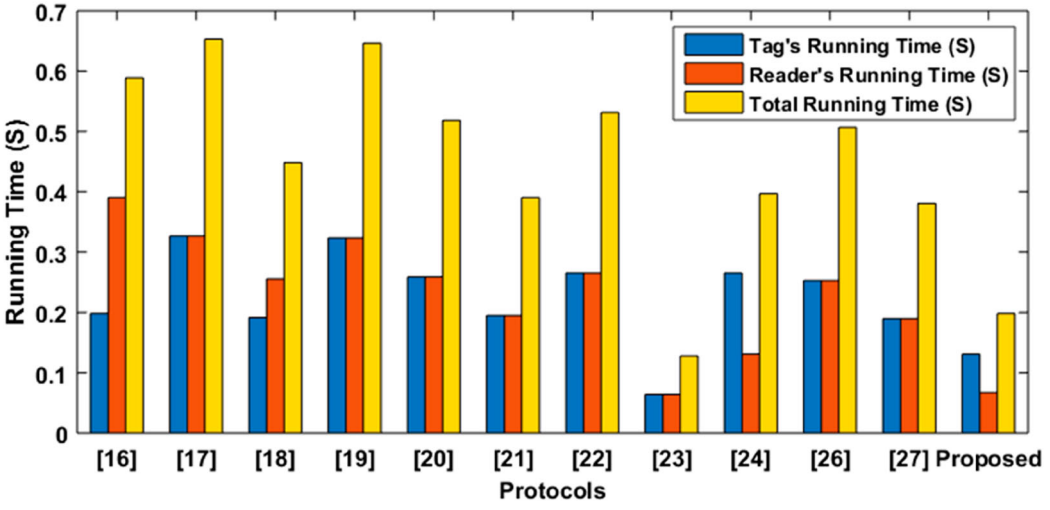

Figure 6. Comparison of Tag and Reader and Total Computational Cost.

Table 3. Comparison of Security and Privacy (Yes: indicates protection from such attacks. No: vulnerable to such attacks. '-' denotes lack of treatment.).

Protocols	Replay	MITM	Impersonation	Key compromise	DoS	Server spoofing	Cloning	SCA	SPA	DEMA
[16]	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No
[17]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	-	No	No
[18]	Yes	-	-	Yes	Yes	-	-	No	No	No
[19]	Yes	Yes	Yes	-	Yes	-	No	-	Yes	No
[20]	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	No
[21]	Yes	Yes	-	Yes	Yes	No	Yes	-	No	No
[22]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
[23]	Yes	Yes	Yes	-	-	Yes	-	No	-	No
[24]	-	Yes	Yes	-	-	-	-	-	Yes	No
[26]	Yes	-	-	-	Yes	Yes	-	Yes	No	No
[27]	Yes	-	-	Yes	Yes	Yes	Yes	Yes	No	No
Proposed	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

variety of attacks, such as replay, impersonation, man-in-the-middle, and key compromise attacks, is guaranteed by these features. The security features of the scheme have been confirmed by rigorous verification utilizing the AVISPA tool. Table 3 provides a comprehensive overview of the security components.

6. Discussion

The paper discusses various RFID authentication protocols using ECC, which provide mutual authentication and demonstrate resilience against major security attacks. However, these protocols have limitations and vulnerabilities, such as the inability to resist SCA, DoS attacks, and desynchronization attacks. The quantity of data sent between the RFID tag and the reader during the authentication process is referred to as the 'communication cost' in relation to RFID systems. It is crucial to minimize the communication cost to reduce power consumption and improve system efficiency.

6.1. Practical considerations

The AVISPA tool is a powerful formal verification tool used in the research paper to analyse and verify the security properties of cryptographic protocols [72]. AVISPA employs a variety of formal methods, including the Strand Spaces, and the applied pi-calculus, to rigorously analyse the security aspects of protocols [73]. It allows researchers to model and simulate the behaviour of protocols, detect vulnerabilities, and verify security properties such as confidentiality, integrity, authentication, and availability. By using AVISPA, researchers can assess the robustness of their protocols against various security threats, including MITM attacks, replay attacks, and impersonation attacks [71]. The program offers a methodical way to assess cryptographic protocols' level of security, ensuring that they meet the desired security requirements before deployment in real-world applications. Our proposed scheme is verified using AVISPA tools as shown in Figure 7 and Figure 8.

6.2. Future research directions

Future research directions in RFID authentication systems using Elliptic Curve Cryptography focus on several key areas, as follows:

- Lightweight Authentication Protocols: Developing lightweight authentication protocols that can be efficiently implemented on low-cost RFID tags while maintaining robust security is crucial. ECC-based protocols are particularly suitable due to their computational efficiency, making them ideal for resource-constrained environments.
- Energy Efficiency: RFID systems often operate in environments where energy efficiency is critical. The research aims to develop ECC-based protocols that minimize power consumption while maintaining security, thereby enhancing the longevity of RFID devices.
- Security Analysis and Improvement: Continuous security analysis and improvement of ECC-based RFID authentication protocols are necessary to address potential vulnerabilities and ensure robustness. This includes cryptanalysis of existing protocols and the development of new, more secure protocols. Integrating ECC-based RFID authentication protocols with other technologies, such as wireless sensor networks and the IoT, can enhance the

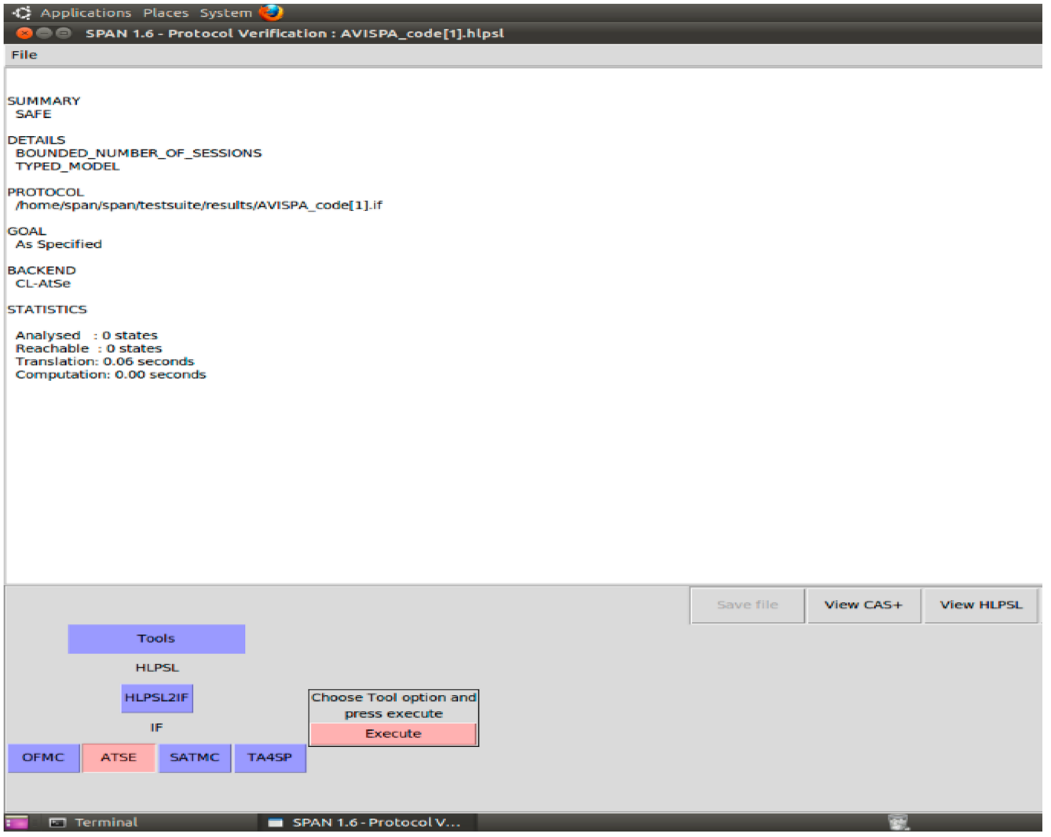

Figure 7. Analysis of our protocol using AVISPA's ATSE Backend module yielded favourable results.

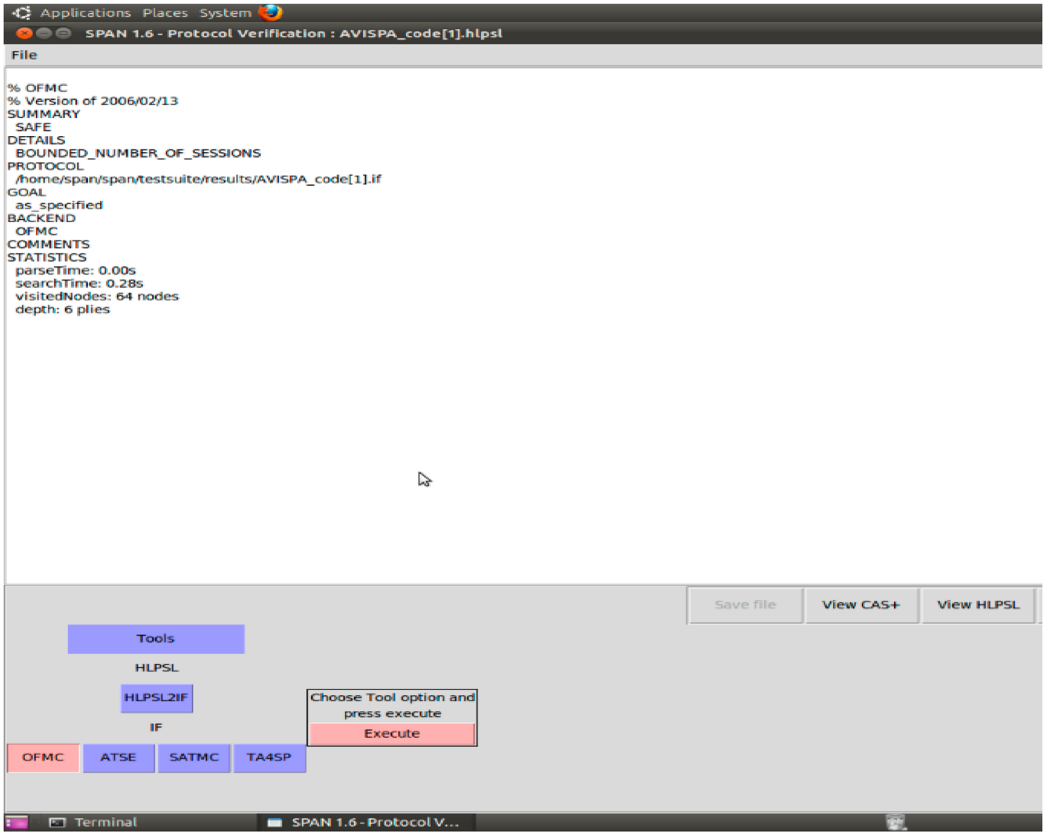

Figure 8. Analysis of our protocol using AVISPA's OFMC Backend module favourable results.

overall security and efficiency of these systems. This interdisciplinary approach can provide comprehensive security solutions for interconnected environments.

7. Conclusion

The proposed ECC-based RFID mutual authentication scheme mitigates significant vulnerabilities in current protocols, including SCA, replay attacks, and impersonation threats, while guaranteeing mutual authentication, confidentiality, and efficiency. Through the optimization of computational expenses and the utilization of ECC, the protocol attains enhanced performance relative to previous protocols, as indicated by comparative assessments and implementation outcomes. The incorporation of formal verification techniques such as AVISPA further supports its resilience against security risks. This research enhances the security of IoT and RFID systems by providing a scalable and lightweight solution appropriate for resource-limited contexts, while emphasizing the necessity of ongoing innovation to address growing threats in interconnected systems.

Author contributions

CRediT: **Md Ozaif:** Conceptualization, Methodology, Validation, Writing – review & editing; **Mahfooz Alam:** Conceptualization, Data curation, Formal analysis, Methodology, Supervision, Validation, Visualization, Writing – original draft, Writing – review & editing; **Suhel Mustajab:** Formal analysis, Resources, Supervision, Writing – review & editing; **Mohd Mustaqeem:** Data curation, Formal analysis, Writing – review & editing; **Nadeem Khan:** Data curation, Formal analysis, Validation, Writing – original draft

Disclosure statement

No potential conflict of interest was reported by the author(s).

Authors' contributions

MO and MA contributed to the main idea and methodology of the model. MO performs the implementation, data acquisition, and dataset of the model. SM, NK, and MM Each author contributed equally to this work. The data analysis, manuscript preparation, and editing are completed by all authors. All authors have read and agreed to publish a version of the manuscript.

ORCID

Md Ozaif http://orcid.org/0009-0004-7948-8367
Mahfooz Alam http://orcid.org/0000-0003-0668-9796
Suhel Mustajab http://orcid.org/0000-0002-9969-6110
Mohd Mustaqeem http://orcid.org/0000-0001-5055-5969

References

[1] Kumar S, Tiwari P, Zymbler M. Internet of things is a revolutionary approach for future technology enhancement: a review. J Big Data. 2019;6(111):1–21. doi:10.1186/s40537-019-0268-2
[2] Hassan R, Qamar F, Hasan MK, et al. Internet of things and its applications: A comprehensive survey. Symmetry (Basel). 2020;12(10):1674. doi:10.3390/sym12101674
[3] Ozaif M, Mustajab S, Alam M. Navigating challenges in IoT: applications, limitations, tools and open research direction. In: 2024 IEEE 13th International Conference on Communication Systems and Network Technologies (CSNT). IEEE; 2024 Apr. p. 525–531. doi:10.1109/CSNT60213.2024.10546141
[4] Khanh QV, Hoai NV, Manh LD, et al. Wireless communication technologies for IoT in 5G: vision, applications, and challenges. Wirel Commun Mob Comput. 2022;2022:1–12. doi:10.1155/2022/3229294
[5] Ozaif M, Mustajab S, Alam M. Exploration of secured data transmission in internet of things: A survey. In: 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT). Vol. 5. IEEE; 2024 Feb. p. 106–112. doi:10.1109/IC2PCT60090.2024.10486716
[6] Lone AN, Mustajab S, Alam M. A comprehensive study on cybersecurity challenges and opportunities in the IoT world. Security and Privacy. 2023;6(6):e318. doi:10.1002/spy2.318
[7] Ray PP. A survey on internet of things architectures. Journal of King Saud University-Computer and Information Sciences. 2018;30(3):291–319. doi:10.1016/j.jksuci.2016.10.003
[8] Aydos M, Vural Y, Tekerek A. Assessing risks and threats with layered approach to internet of things security. Meas Control. 2019;52(5-6):338–353. doi:10.1177/0020294019837991
[9] Lee CI, Chien HY. An elliptic curve cryptography-based RFID authentication securing e-health system. Int J Distrib Sens Netw. 2015;11(12):642425. doi:10.1155/2015/642425
[10] Eberle H, Gura N, Shantz SC, et al. A public-key cryptographic processor for RSA and ECC. In: Proceedings. 15th IEEE International Conference on Application-Specific Systems, Architectures and Processors. IEEE; 2004 Sep. p. 98–110. doi:10.1109/ASAP.2004.1342462
[11] Abbasinezhad-Mood D, Nikooghadam M. An anonymous ECC-based self-certified key distribution scheme for the smart grid. IEEE Trans Ind Electron. 2018;65(10):7996–8004. doi:10.1109/TIE.2018.2807383
[12] Abbasinezhad-Mood D, Ghaemi H. Dual-signature blockchain-based key sharing protocol for secure V2 V communications in multi-domain IoV environments. IEEE Trans Intell Transp Syst. 2024;25(10):13407–13407. doi:10.1109/TITS.2024.3410114
[13] Alexander Jr P, Baashirah R, Abuzneid A. Comparison and feasibility of various RFID authentication methods using ECC. Sensors. 2018;18(9):2902. doi:10.3390/s18092902
[14] Suárez-Albela M, Fraga-Lamas P, Fernández-Caramés TM. A practical evaluation on RSA and ECC-based cipher suites for IoT high-security energy-efficient fog and mist computing devices. Sensors. 2018;18(11):3868. doi:10.3390/s18113868
[15] Srinivas MB, Konguvel E. Era of sentinel tech: charting hardware security landscapes through post-silicon innovation, threat mitigation and future trajectories. IEEE Access. 2024;12:68061–68108. doi:10.1109/ACCESS.2024.3400624
[16] Sowjanya K, Dasgupta M, Ray S. An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems. Int J Inf Secur. 2020;19(1):129–146. doi:10.1007/s10207-019-00464-9
[17] Zhao Z. A secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem. J Med Syst. 2014;38:1–7. doi:10.1007/s10916-013-0001-1
[18] Izza S, Benssalah M, Drouiche K. An enhanced scalable and secure RFID authentication protocol for WBAN within an IoT environment. J Inf Secur Appl. 2021;58:102705.
[19] Naeem M, Chaudhry SA, Mahmood K, et al. A scalable and secure RFID mutual authentication protocol using ECC for internet of things. Int J Commun Syst. 2019;33:e3906. doi:10.1002/dac.3906
[20] Alamr AA, Kausar F, Kim J, et al. A secure ECC-based RFID mutual authentication protocol for internet of things. J Supercomput. 2018;74:4281–4294. doi:10.1007/s11227-016-1861-1
[21] Benssalah M, Sarah I, Drouiche K. An efficient RFID authentication scheme based on elliptic curve cryptography for internet of things. Wirel Pers Commun. 2020;117:2513–2539. doi:10.1007/s11277-020-07992-x
[22] Zheng L, Xue Y, Zhang L, et al. Mutual authentication protocol for RFID based on ECC. In: 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC). Vol. 2. IEEE; 2017 Jul. p. 320–323. doi:10.1109/CSE-EUC.2017.245
[23] Yang X, Yi X, Zeng Y, et al. An improved lightweight RFID authentication protocol for Internet of Things. In Proceedings of the International Conference on Web Information Systems Engineering; Zayed University, Dubai, United Arab Emirates, 2018 Nov 12–15; Springer: Cham, Switzerland; 2018.
[24] Alaoui HL, El Ghazi A, Zbakh M, et al. A highly efficient ECC-based authentication protocol for RFID. J Sens. 2021;2021:8876766. doi:10.1155/2021/8876766
[25] Dinarvand N, Barati H. An efficient and secure RFID authentication protocol using elliptic curve cryptography. Wirel Netw. 2019;25:415–428. doi:10.1007/s11276-017-1565-3
[26] Noori D, Shakeri H, Niazi Torshiz M. An elliptic curve cryptosystem-based secure RFID mutual authentication for internet of things in healthcare environment. EURASIP J Wirel Commun Netw. 2022;2022(1):64. doi:10.1186/s13638-022-02146-y
[27] Timouhin H, Amounas F, Azrour M. New ECC-based IoT authentication protocol for securing RFID systems. SN Computer Science. 2023;4(6):785. doi:10.1007/s42979-023-02220-2
[28] Liao YP, Hsiao CM. A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol. Ad Hoc Netw. 2014;18:133–146. doi:10.1016/j.adhoc.2013.02.004
[29] Ilie-Zudor E, Kemény Z, Van Blommestein F, et al. A survey of applications and requirements of unique identification systems and RFID techniques. Comput Ind. 2011;62(3):227–252. doi:10.1016/j.compind.2010.10.004

[30] Piramuthu S. Protocols for RFID tag/reader authentication. Decis Support Syst. 2007;43(3):897–914. doi:10.1016/j.dss.2007.01.003

[31] Khattab A, Jeddi Z, Amini E, et al. Rfid security. Vol. 11. Berlin, Heidelberg: Springer; 2017. p. 27–41.

[32] Arslan A, Bingöl MA. Cryptanalysis of Izza et al.'s protocol: An enhanced scalable and secure RFID authentication protocol for WBAN within an IoT environment. Cryptology EPrint Archive. 2021: 1–11.

[33] Baballe MA. A study on the components used in RFID system and its challenges. Global J Res Eng Comput Sci. 2021;1(1):21–27.

[34] Gabsi S, Kortli Y, Beroulle V, et al. Novel ECC-based RFID mutual authentication protocol for emerging IoT applications. IEEE Access. 2021;9:130895–130913. doi:10.1109/ACCESS.2021.3112554

[35] Ray BR, Chowdhury M, Abawajy J. Hybrid approach to ensure data confidentiality and tampered data recovery for RFID tag. Int J Networked Distrib Comput. 2013;1(2):79–88. doi:10.2991/ijndc.2013.1.2.2

[36] Hasan MK, Weichen Z, Safie N, et al. A survey on Key agreement and authentication protocol for internet of things application. IEEE Access. 2024;9:130895–130913. doi:10.1109/ACCESS.2021.3112554

[37] Bhagat V, Kumar S, Gupta SK, et al. Lightweight cryptographic algorithms based on different model architectures: A systematic review and futuristic applications. Concurr Comput: Pract Exp. 2023;35(1):e7425. doi:10.1002/cpe.7425

[38] Chai Q. Design and analysis of security schemes for low-cost RFID systems; Department of Electrical and Computer Engineering, University of Waterloo, Canada; 2012.

[39] Alamr AA, Kausar F, Kim JS. Secure mutual authentication protocol for RFID based on elliptic curve cryptography. In: 2016 international Conference on Platform Technology and Service (PlatCon). IEEE; 2016 Feb. p. 1–7. doi:10.1109/PlatCon.2016.7456822

[40] AlMajed H, AlMogren A. A secure and efficient ECC-based scheme for edge computing and internet of things. Sensors. 2020;20(21):6158. doi:10.3390/s20216158

[41] Rong C, Zhao G, Yan L, et al. RFID security. In: Computer and Information Security Handbook. Morgan Kaufmann; 2013. p. 345–361. doi:10.1016/B978-0-12-394397-2.00018-0

[42] Chen SM, Wu ME, Sun HM, et al. CRFID: An RFID system with a cloud database as a back-end server. Future Gener Comput Syst. 2014;30:155–161. doi:10.1016/j.future.2013.05.004

[43] Khalil G, Doss R, Chowdhury M. A comparison survey study on RFID based anti-counterfeiting systems. J Sensor Actuator Net. 2019;8(3):37. doi:10.3390/jsan8030037

[44] Mohsin SM, Khan IA, Abrar Akber SM, et al. Exploring the RFID mutual authentication domain. Int J Comput Appl. 2021;43(2):127–141. doi:10.1080/1206212X.2018.1533614

[45] Tsalis N, Vasilellis E, Mentzelioti D, et al. A taxonomy of side channel attacks on critical infrastructures and relevant systems. Crit Infrast Sec Res: Theor Met Tools Technol. 2019: 283–313. doi:10.1007/978-3-030-00024-0_15

[46] Zunaidi MR, Sayakkara A, Scanlon M. (2024). Systematic Literature Review of EM-SCA Attacks on Encryption. *arXiv preprint arXiv:2402.10030*.

[47] Abarzúa R, Valencia C, López J. Survey for performance & security problems of passive side-channel attacks countermeasures in ECC. Cryptology EPrint Archive. 2019: 1–43.

[48] Xiao M, Chen Q, Li Z, et al. Formal security analysis of ECC-based RFID in logic of events theory. Electronics (Basel). 2023;12(15):3286. doi:10.3390/electronics12153286

[49] Dubey A, Cammarota R, Suresh V, et al. Guarding machine learning hardware against physical side-channel attacks. ACM J Emerg Technol Comput Sys (JETC). 2022;18(3):1–31. doi:10.1145/3465377

[50] Qazi R, Qureshi KN, Bashir F, et al. Security protocol using elliptic curve cryptography algorithm for wireless sensor networks. J Ambient Intell Humaniz Comput. 2021;12:547–566. doi:10.1007/s12652-020-02020-z

[51] Bhandari R, Kirubanand VB. Enhanced encryption technique for secure iot data transmission. Int J Elect Comput Eng. 2019;9(5):3732. doi:10.11591/ijece.v9i5.pp3732-3738

[52] Leelavathi G, Shaila K, Venugopal KR. Elliptic curve crypto processor on FPGA using montgomery multiplication with vedic and encoded multiplier over GF (2 m) for nodes in wireless sensor networks. 2018 IEEE 13th International Conference on Industrial and Information Systems (ICIIS), Rupnagar, India; 2018. p. 207–210.

[53] Patel D, Patel B, Vasa J, et al. A comparison of the key size and security level of the ECC and RSA algorithms with a focus on cloud/fog computing. In: Choudrie J, Mahalle PN, Perumal T, etal, editors. ICT with intelligent applications. ICTIS 2023. lecture notes in networks and systems. Vol. 719. Singapore: Springer; 2023. p. 43–53.

[54] Gayoso Martínez V, Hernández Encinas L, Queiruga Dios A. Security and practical considerations when implementing the elliptic curve integrated encryption scheme. Cryptologia. 2015;39(3):244–269. doi:10.1080/01611194.2014.988363

[55] Akilan SS, Devprasad KD. Enhancing security in Wireless Body Area Networks (WBANs) with ECC-based Diffie-Hellman key exchange algorithm (ECDH). Technology and Health Care. 2024;32(6):4765–4784.

[56] Arslan A, Çolak SA, Ertürk S. A secure and privacy friendly ECC based RFID authentication protocol for practical applications. Wirel Pers Commun. 2021;120(4):2653–2691. doi:10.1007/s11277-021-08552-7

[57] Abusukhon A, Mohammad Z, Al-Thaher A. Efficient and secure key exchange protocol based on elliptic curve and security models. In: 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT). IEEE; 2019 Apr. p. 73–78. doi:10.1109/JEEIT.2019.8717496

[58] Al-Zubaidie M, Zhang Z, Zhang J. (2019). Efficient and secure ECDSA algorithm and its applications: A survey. *arXiv preprint arXiv:1902.10313*.

[59] Raso E, Bianco GM, Bracciale L, et al. Privacy-aware architectures for NFC and RFID sensors in healthcare applications. Sensors. 2022;22(24):9692. doi:10.3390/s22249692

[60] Álvarez-Bermejo JA, Lodroman A, López-Ramos JA. Distributed key agreement for group communications based on elliptic curves. An application to sensor networks. Math Methods Appl Sci. 2016;39(16):4797–4809. doi:10.1002/mma.3802

[61] Chandramouli R, Iorga M, Chokhani S. Cryptographic key management issues and challenges in cloud services. Secure Cloud Computing. 2013;1:1–30. https://doi.org/10.1007/978-1-4614-9278-8_1.

[62] Khan AG, Basharat S, Riaz MU. Analysis of asymmetric cryptography in information security based on computational study to ensure confidentiality during information exchange. Int J Sci Eng Res. 2018;9(11):992–999.

[63] Benssalah M, Djeddou M, Drouiche K. RFID authentication protocols based on ECC encryption schemes. In: 2012 IEEE International Conference on RFID-Technologies and Applications (RFID-TA). IEEE; 2012 Nov. p. 97–100. doi:10.1109/RFIDTA.2012.6404575

[64] Mahmud S. A study on parallel implementation of advanced encryption standard (AES) [Doctoral dissertation MS thesis], Computer Science, Independent University, Bangladesh; 2004.

[65] Sharma S, Chopra V. Data encryption using advanced encryption standard with key generation by elliptic curve Diffie-Hellman. Int J Sec Its Appl. 2017;11(3):17–28. doi:10.14257/ijsia.2017.11.3.02

[66] Abbasinezhad-Mood D, Mazinani SM, Nikooghadam M, et al. Efficient provably-secure dynamic ID-based authenticated key agreement scheme with enhanced security provision. IEEE Trans Dependable Secure Comput. 2020;19(2):1227–1238.

[67] Banoth R, Regar R. Asymmetric Key cryptography. In: Banoth R, Regar R, edotirs. Classical and Modern Cryptography for Beginners. Cham: Springer Nature Switzerland; 2023. p. 109–165.

[68] Kardaş S, Celik S, Arslan A, et al. An efficient and private RFID authentication protocol supporting ownership transfer. In: Avoine G, Kara O, editors. Lightweight Cryptography for Security and Privacy: Second International Workshop, LightSec 2013, Gebze, Turkey, May 6–7, 2013, Revised Selected Papers 2. Berlin, Heidelberg: Springer; 2013. p. 130–141.

[69] Sharma AK, Mittal SK. Cryptography & network security hash function applications, attacks and advances: A review. In: 2019 third International Conference on Inventive Systems and Control (ICISC). IEEE; 2019 Jan. p. 177–188. doi:10.1109/ICISC44355.2019.9036448

[70] Choudhury H. Anonymous RFID authentication for Iot in lte-a. In: Mandal JK, Kandarr D, Maji AK, editors. Proceedings of the International Conference on Computing and Communication Systems: I3CS 2016, NEHU, Shillong, India. Singapore: Springer; 2018. p. 673–687.

[71] Kumar S, Banka H, Kaushik B, et al. A review and analysis of secure and lightweight ECC-based RFID authentication protocol for internet of vehicles. Transact Emerg Telecommun Technol. 2021;32(11):e4354. doi:10.1002/ett.4354

[72] Vigano L. Automated security protocol analysis with the AVISPA tool. Electron Notes Theor Comput Sci. 2006;155:61–86. doi:10.1016/j.entcs.2005.11.052

[73] Armando A, Basin D, Boichut Y, et al. The AVISPA tool for the automated validation of internet security protocols and applications. In: Etessami K, Rajamani SK, editors. Computer Aided Verification: 17th International Conference, CAV 2005, Edinburgh, Scotland, UK, July 6–10, 2005. Proceedings 17. Berlin, Heidelberg: Springer; 2005. p. 281–285.