International Journal of Modern Computation, Information, and Communication Technology
2026;9(1):9-16.
ISSN: 2581-5954

Enhancing Security and Privacy in Radio Frequency Identification Systems Using Symmetric Cryptosystem Algorithm

Balakumar Vijayaraman[1*], Sakthidevi I[2]

[1]*MPLS Network Operations Centre, Bharat Sanchar Nigam Ltd.,*
Bengaluru, Tamil Nadu, India.
[2]*Department of Information and Technology, Adhiyamaan College of Engineering (Autonomous),*
Hosur, Tamil Nadu, India.

[*]*Corresponding author: vinbalakumar@gmail.com*

Abstract. Privacy and security vulnerabilities in RFID systems remain a pressing concern as the technology sees wider adoption for automatic identification and real-time tracking. These vulnerabilities are not purely technical, addressing them involves interconnected economic, ethical, and social challenges alongside the technological ones. This work presents recent investigations into RFID privacy and security flaws, with a focus on developing solutions that are affordable, practical, reliable, scalable, adaptable across organizations, and durable, while still meeting RFID's core privacy and security requirements. A central obstacle in meeting these requirements is that RFID tags typically operate under severe resource constraints such as limited power, memory, and processing capacity — which restricts the cryptographic techniques that can be applied. In cryptography, information is encoded so that only an intended recipient can decipher it; for RFID, this study addresses the constraint problem by optimizing cryptographic processes specifically for resource-limited devices, aiming to make effective use of available computing power while minimizing any negative impact on device functionality. The proposed cryptographic approach was evaluated for its computational efficiency and its impact on RFID device operation under real-time conditions. Results show that the proposed system achieves an average processing time of 0.12 seconds, indicating that meaningful security gains can be achieved without significantly compromising device responsiveness. It is important to note that outcomes may vary depending on implementation specifics, the comprehensiveness of the security measures applied, and the system's ability to adapt to evolving security threats. This study synthesizes the sociological and technological context behind existing proposals for protecting individual privacy and RFID system integrity and is intended as a resource for both generalist readers and domain experts.

Keywords: Radio Frequency Identification System, Authentication, Privacy, Security and Symmetric Cryptosystem Algorithm.

INTRODUCTION

RFID is one of the numerous technologies that make up the Internet of Things (IoT) and may be used to keep tabs on a single item or an entire warehouse. The healthcare industry, supply chains, logistics, and asset tracking have all made extensive use of this technology. However, for RFID-based IoT applications to realize their full potential, they need a high degree of security and privacy, and they are sadly exposed to several assaults and dangers. Therefore, offers a set of securities and privacies principles for RFID, complete with rules for modelling, mitigation, and the attack vectors [1]. Examine how the model stacks up against the state of the art and highlight where they fall short relative to established best practices. This methodology entails the following steps: (i) identifying the securities and privacies guidelines feature; (ii) highlighting the security goal for RFID-based IoT application; (iii) analyzing the feature in relation to RFID industrial standards; (iv) summarizing attacks and threats against RFID applications; and (v) deriving sets of securities and privacies guidelines for RFID application in accordance's with security goals. Also, (VI) highlights the current mitigation techniques to execute suggested recommendations, and (vii) characterizes guidelines derived in relation to the concerned parties. Finally, details the key caveats of the study that need more investigation and lists the many problems plaguing modern security measures [2].

To effectively circumvent several security and privacy concerns, RFID authentication techniques have increasingly adopted the usage of elliptic curves cryptography (ECCs). Despite the use of ECC's robust

Received: 18.01.2026 Revised: 18.03.2026 Accepted: 29.03.2026

cryptographic primitives, current authentication techniques fall well short of achieving the needed degree of security and anonymity. In this study, we examined recent ECC-based RFID authentication systems. The authors assert that their approaches satisfy critical security and privacy needs. However, critical weaknesses in the schemes are shown that they have alleged [3]. Use transmitted messages in an unsecured channel to attack protocol, taking advantage of message relations that point to a particular tag to demonstrate that their system does not guarantee tag anonymity/intractability, forward or backward security, or good performance. Further, it shows that the methods by Kumar et al. and Agrahari and Varma do not provide forward and backward securities because they are not built to remove the benefit of an opponent acquiring complete knowledge of a tag from by attack specification. Further, it demonstrates that the forward and backward security of the approach is compromised when the pseudonym of a tag is conveyed via an unsecured channel without any kind of updating [4].

Sensors, RFID tags, actuators, and mobile phones are just some of the gadgets that make up the IoT. There is no human involvement in communication between these devices. People, assets, items, and more may all be monitored with the use of RFID technology. These gadgets have several security flaws, including limited storage space and weak batteries. Replays, disclosures, tracking, offline guessing, and denials of service attacks are only some of the various types of attacks that might compromise a system's security. Researchers have proposed several different security strategies over the last several decades to address these flaws [5]. That's why we are here to talk about how RFID systems may be attacked and what kinds of safeguards have been recommended to prevent them. The average annual number of papers, annual growth rate, and total number of citations were retrieved as basic metrics. Using the open-source Python program ScientoPy, key concepts were identified, and pertinent indications were evaluated [6].

The following sections elaborate on these findings: First, present the Applications Section, which is divided into the subheadings IoT, Supply Chains Managements, Localizations, Traceability, Logistic, Ubiquitous Computing, Healthcare, and Access Controls; second, present the Securities and Privacies Sections, which is divided into the subheadings Authentications, Privacy, and Ownership Transfers; and third, present the Discussions Sections. This paper's goal is to provide the readers with an overarching picture of where RFID is at in the grand scheme of things by presenting a variety of interpretations, each informed by a unique set of motives and experiences [8]. The problem statement is discussed below. Typically, the problem statement for improving RFID security and privacy using a symmetric cryptosystem algorithm centre on resolving security flaws and possible threats. Unauthorized access to RFID communication might make it possible for hackers to intercept and decode private information while it is being sent. Information misuse, possible data breaches, and compromised confidentiality. RFID systems with weak or insufficient authentication procedures run the risk of exposing sensitive data to unauthorized devices. The contributions are as follows:

- A thorough assessment and careful selection of symmetric cryptosystem algorithms that are suitable for RFID applications.
- Considering elements like speed, resource economy, and security strength, optimal cryptographic algorithms aid in effective and safe data protection.
- Creation of secure key management procedures adapted to the needs of RFID technology.
- Secure symmetric key creation, distribution, and storage are ensured by robust key management, which lowers the possibility of unwanted access and cryptographic assaults.
- Symmetric encryption methods are included in RFID systems to safeguard the privacy of data while it is being sent.
- Encryption protects private data by keeping others from reading RFID data and taking care of issues with interception and eavesdropping.
- Improvement of symmetric cryptography-based authentication methods to guarantee safe RFID tag and reader verification.
- RFID data is more reliable when tamper detection systems are in place to stop unwanted changes and guarantee information correctness.
- Improved privacy safeguards reduce the possibility of privacy breaches, comply with privacy standards, and address concerns about the security of personal data.
- Together, these contributions aid in the creation of an RFID system that is more private and secure by using Symmetric Cryptosystem methods.
- The goal is to provide a strong framework that tackles issues, safeguards private data, and guarantees the privacy, integrity, and confidentiality of RFID data in a range of applications.

The literature survey is discussed in section 2. After that, the proposed system is discussed using a Symmetric cryptosystem algorithm for enhancing security and privacy in RFID in section 3. Then, the results and discussion for the given dataset are discussed to reduce the time taken in section 4. Finally, the conclusion provides the overall performance of the RFID system and recommendations for future work.

LITERATURE SURVEY

Better patient care and safety may be achieved via the widespread use of RFID technology in healthcare systems. However, there are security flaws in these systems that put patients' personal information and credentials at risk. Improved privacy and security for RFID-based healthcare systems, which intend to contribute to the state of the arts, is the focus of this article. More particularly, it proposes a lightweight RFID protocol that protects patients' privacy in the IoT domains by using pseudonyms instead of actual IDs to establish authenticated tag-to-reader communication [9]. Extensive testing has shown that the suggested protocol is safe from a wide range of security threats. This article presents high-level overviews of RFID technology's use in health care systems and compares the obstacles these systems confront to industry standards. It then analyses the suggested RFID authentication techniques for IoT-based healthcare systems, evaluating their merits and shortcomings. To solve the problems with anonymity and traceability that plague currents solutions, we presented a new protocol. Also showed that the suggested protocol was more secure and required less computing power to implement than competing solutions. Finally, the suggested lightweight RFID protocol preserved patient privacy by employing pseudonyms rather than actual IDs, and it was secure against known threats.

Patient administration has been substantially simplified, healthcare personnel costs have been cut, and patients have received improved treatment because of RFID technology's broad use in the "smart" home and hospital settings. The privacy and security of hospitals and patients might be jeopardized by careless usage of RFID tags, which could lead to real injury for patients and harm to the hospitals' reputations as well. RFID-based medical monitoring systems serve a crucial role in protecting both patients' confidentiality and the confidentiality of their medical records. However, designing an efficient and effective authentication strategy for RFID medical monitoring systems is difficult because of the limited resources of RFID tags/readers [10]. This paper proposes ultra-light-weighted RFID security authentication protocols using cloud servers that can effectively resist forgery attacks, replay attacks, de-synchronization attacks, and denials of services attacks while certify the cloud servers, and thus reducing the resources overheads and meeting the security requirement of the RFID systems. The suggested authentication protocol is better suited for scaling to large-scale authentication, as seen by the security analysis and experimental findings, which also demonstrate that it can reach greater security objectives at a lower cost.

Applications built on top of the IoT place a premium on protecting the confidentiality and integrity of data associated with connected devices. The three phases of a physical object's life cycle—before, during, and after production—help to make sense of its complex security and privacy concerns. This motivates the proposal of security architecture for the IoT based on the notion of physical objects. Physical objects at various phases of production have their security and privacy needs assessed, together with the technology used to safeguard them, based on the security architecture. Potential security and privacies concern that IoT items might encounter in ubiquitous computing environments are described considering the evolution of IoT technology. Possible strategies for overcoming these obstacles are also highlighted [11]. The widespread uses of RFID technology in healthcare settings have increased the technology's profile as a useful component of the IoT. RFID identification systems, however, have been under increasing scrutiny due to security and privacy concerns. A concern with existing RFID protocols is that they often rely on a backend server to maintain the specifics of the tagged items, which may be compromised if an attacker were to launch a successful assault on the server. This research presents security-improved RFID authentication protocols for healthcare environments by using in-distinguish-ability obfuscation, which stops private information from leaking out of the server. Meanwhile, adapt the protocol to work in a cloud setting, where the data from the tags is kept in an off-site location. Protocols are, to the best of my knowledge, the first to use in-distinguish-ability obfuscations in the context of RFID authentication systems. Protocols are both practical and scalable, and they have been thoroughly examined to meet most of the RFID security requirements.

The IoT has evolved, matured, and steadily impacted human life in many new application domains in recent years. These domains include anything from wearable gadgets and smart manufacturing to smart homes and ambient intelligence. While IoT has enormous promises, it is still a research question on how best to protect users' privacy and security. Not all the existing security methods and methodologies can be readily applied to IoT-based

systems since they were originally designed for centralized and dispersed information systems. Due to unusual features like low uptime, high scalability, constant flux, and restricted resources, IoT systems need a paradigm shift to design novel security and privacies solutions [12]. First, provide high-level reviews of securities and privacy in the IoT. After establishing the background for IoT systems, pinpoint four primary features that provide novel difficulties for today's security methods. RFID, wireless sensors networks (WSNs), and mobile delay tolerant networks (MDTNs) form the backbone of many IoT-based systems and detail the specific threats and challenges related to these technologies from the perspectives of these characteristics and IoT security requirements. Possible solutions to the problems and dangers posed by the IoT are also discussed [13].

Logistics, supply chain visibility, access controls, the military, and the agri-food industry are just some of the industries that have benefited from RFID adoption on a worldwide scale. When used in an IoT setting, RFID's many security features keep sensitive information safe during transit between a tag and a reader. Despite these benefits, there are still several security and privacy concerns with these systems that an attacker may exploit. Additionally, there is an immediate need for secure authentications and sensitive data protections due to the expanding IoT [14]. To defend RFID systems from the large variety of assaults they are susceptible to, several different authentication procedures based on cryptographic primitives have been studied and put into use. The Elliptic Curve Integrated Encryption Scheme (ECIES) is one such cryptosystem that appears in several cryptographic norms. It has become widely used in RFID applications because of the mutual authentications and data integrity it provides. This research provides an innovative, safe, ECC-based RFID authentication system that satisfies the privacy and security requirements of previously published techniques. First, provide a review of different ECC-based RFID authentication methods and point out the ways in which these protocols are vulnerable to server spoofing, tracking, and impersonation attacks. After that, the protocols are compared to others in terms of computing efficiency and safety. The last step in the development of the protocol is to represent it in High-Level protocol specifications Languages (HLPSL) and run it through the Automated Validations of Internet Security Protocol and Application (AVISPA) analysis tools [15].

The paper reviews RF attacks' impact on wireless communication security and privacy, categorizing effects and proposing solutions to mitigate risks across various systems [16]. The IoT faces data security challenges [17]. Researchers propose RFID-based solutions, highlighting vulnerabilities in existing protocols and introducing a secure, lightweight alternative using Plr operations. The integration of RFID technology in transportation enhances operations but introduces security challenges, including data breaches and unauthorized access, necessitating effective mitigation strategies [18]. RFID technology's expansion necessitates enhanced security [19]. A DNA TRIKKY-based mechanism is proposed for mutual authentication, improving hash functions and outperforming existing protocols in efficiency and security [19]. The IoT leverages RFID technology for automation and traceability, particularly in healthcare. A new lightweight RFID protocol addresses security vulnerabilities found in existing systems [20]. The adaptive security framework for IoT combines AI, blockchain, and quantum-resistant cryptography to enhance security, utilizing adaptive orchestration and Digital Twins for threat mitigation [21].

PROPOSED SYSTEM

Concerns about RFID's privacy implications centre on the technology's potential for covert monitoring and inventorying. When an RFID reader queries a tag, the tag responds without notifying its owner or the person carrying it. Therefore, covert scanning of tags is a real concern in areas where the read range allows for it. Even RFID tags that encrypt their data using cryptographic techniques (which go into shortly) still give out their own unique IDs, as seen above. Thus, an RFID-tagged individual may be tracked covertly by the dissemination of a constant serial number to surrounding readers. Such tracking is achievable even if the serial numbers assigned to a fixed tag are completely arbitrary and contain no useful information. When the tag serial number is paired with the other identified details, the risk of privacy increases using a symmetric cryptosystem algorithm. For instance, a store may correlate a customer's credit card transaction with the serial numbers of the tags she is wearing. Then, utilizing networks of RFID readers, both inside and outside of stores, marketers could identify and profile the customer. Of course, RFID isn't the only technology with an issue with covert tracking. Many other kinds of wireless gadgets, such as Bluetooth-enabled ones, are also vulnerable. Figure 1 shows the system architecture of the proposed system.

Certain tags, in particular tags, convey information about the products to which they are affixed, in addition to their unique serial numbers. Both the "General Manager," often the item's maker, and the "object class," typically

a product number or SKU (stock keeping unit) for information, are included in EPC tags. As a result, those who wear tags may be susceptible to undercover audits of their possessions. A reader can invisibly determine what she is wearing and thus learn a great deal, including the kinds of medication she is carrying and what illness she might be suffering from, the RFID-enabled loyalty card she is carrying, and where she shops, her preferred clothing size and accessories, and so on.

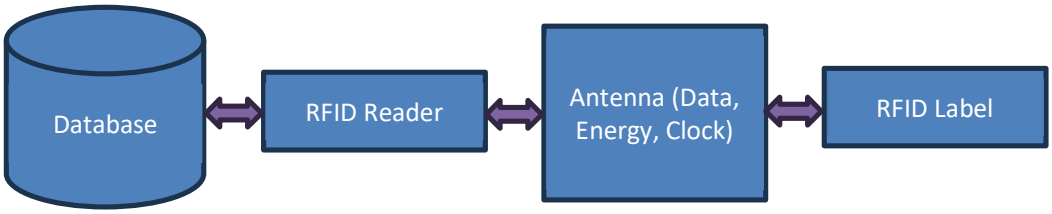

FIGURE 1. System architecture of the Proposed System

RFID is uniquely plagued by this stock-taking issue. Since RFID infrastructure is currently rare and fragmented, concerns associated with covert RFID monitoring and inventorying are of minimal significance at this time. As was just discussed, it will likely be quite some time before specific retail products are tagged. However, the privacy issue will become much more serious if RFID becomes ubiquitous. VeriSign's Discovery Service is an early indicator of the maturing RFID infrastructure. It standardizes the reporting of tag sightings among companies. Automatic toll payment transponders, which are little plaques mounted in the windshield's four corners, are becoming widespread. One well-known example involves a transponder whose data was subpoenaed and used to disprove the defendant's alibi in a divorce lawsuit. • Libraries RFID systems have been introduced in certain libraries to improve circulation, manage stock, and lessen the risk of librarians developing repetitive stress injuries. Privacy worries concerning RFID have been sparked, in part, by the USA Patriot Act's mandates that libraries track and record patrons' book choices.

The International Civil Aviation Organization (ICAO) has issued regulations enabling RFID-enabled passports and other forms of identification for international travel. The United States has made these requirements for admission into the country for nationals of 27 "visa waiver" nations. Delays have occurred because of technological difficulties and modifications to the mandate's technical requirements, in part because of lobbying by privacy groups. VeriChip is one of the few RFID devices that has sparked so much controversy among privacy activists because of its potential use in human implants. VeriChip is an RFID-implanted tag similar to those used for pets. The scanning of a patient's tag would allow a hospital to quickly and easily access her medical records. In fact, several medical facilities have already started testing out this technology. The VeriChip might also be used for the purpose of controlling who is allowed entry to a building.

RESULTS AND DISCUSSIONS

Must first question "Secure" and "private" against what to arrive at a rigorous definition of these terms for RFID tags? A formal model that describes the capabilities of possible attackers is the best solution. In cryptography, such a model often takes the form of an "experiment," a program that mediates interactions between a model adversary—typically represented as probabilistic algorithms or Turing machines—and a model runtimes environment that includes systems components (typically referred to as "oracles"). An RFID system model, for instance, would provide the attacker access to symbols for tags and readers. Most cryptographic models assume the adversary has unrestricted access to system components throughout execution. This makes perfect sense in terms of Internet security models: An attacker may theoretically get access to any computer in a network at any moment. For example, a server may receive requests from anywhere in the globe at any time. However, the notion that RFID system enemies would have constant access to tags is frequently unrealistic. Scanning a tag requires an attacker to be in close contact with it, which is unlikely in most settings. RFID security models should be modified to account for these considerations using a symmetric cryptosystem algorithm.

The inability to perform basic cryptographic operations means that low-cost RFID tags cannot offer effective security in robust models. Therefore, developing weaker security models that are reflective of actual threats and tag capabilities is an essential area of study. The "minimalist" security concept and supporting protocols are proposed, for instance, for inexpensive tags. This approach assumes that an attacker only scans a tag at certain

intervals and that tags only broadcast their data once every so often. To be more specific, the minimalist model presumes that there is a maximum number of times an adversary may scan a particular tag or attempt to spoof legitimate readers and that when this maximum is reached, the tag communicates privately with genuine readers. An enemy may only scan a target proximity card or attempt to obtain unlawful admittance to a facility ten times, for example, until the genuine cardholder successfully enters the building and is no longer within the adversary's eavesdropping range. Many cryptographic security models cannot adequately convey crucial aspects of RFID systems. In this research, see how to determine the mean of two different times. It uses the standard formula "(time1 + time2)/2" to get the average time and return the value.". Figure 2 shows the encryption performance of the proposed system, and Figure 3 shows the decryption performance of the proposed system.

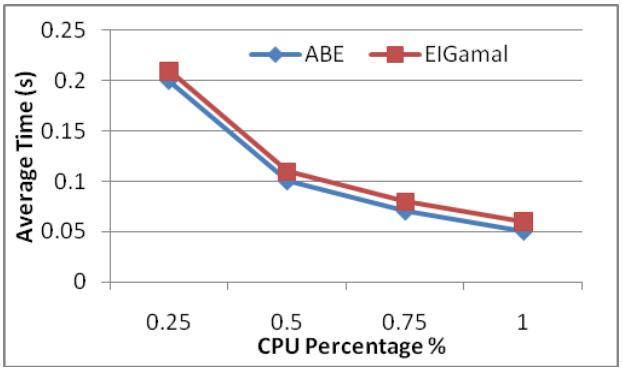

FIGURE 2. Encryption performance of the proposed system

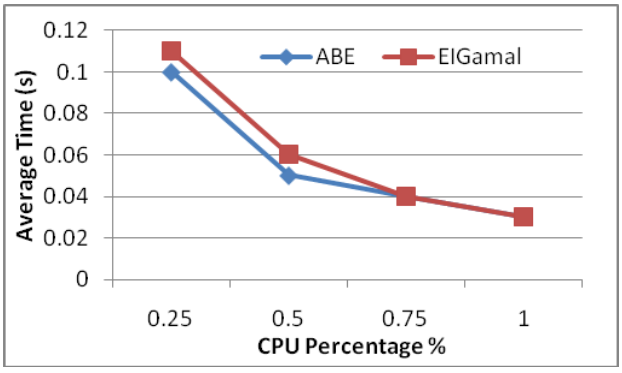

FIGURE 3. Decryption performance of the proposed system

For instance, the top-level protocol of communication between a tag and a reader may be captured by a basic cryptographic model. Anti-collision procedures and other elementary protocols are implemented at the lower levels. Identify the critical vulnerabilities in RFID system communication layers. They bring to light the dangers of insufficient random-number generations in RFID tags, among other difficulties. (As mentioned in the above footnotes, the Class-1 Gen-2 standard uses randomization to encrypt data in transit from the readers to the tag.) They've seen how many different RFID standards provide tracking challenges: The underlying standard of a tag might be used as a concise identifier. Threats to RFID systems' physical integrity have also been noted. An attacker may be able to single out individual tags by exploiting subtle differences in the signals they provide, such as those introduced during production. An RFID tag's unique "radio fingerprint" might render useless even the most advanced cryptographic privacy-preserving system.

CONCLUSIONS

A basic cryptographic model can capture the top-level communication protocol between a tag and a reader, while anti-collision procedures and other elementary protocols operate at the lower layers. Examining these layers reveals critical vulnerabilities in RFID system communication most notably, the risks posed by insufficient

random-number generation in RFID tags. (Notably, the Class-1 Gen-2 standard relies on randomization to encrypt data transmitted from readers to tags.) Differences across RFID standards also introduce tracking challenges: the underlying standard a tag conforms to can itself serve as a de facto identifier, undermining privacy even when other protections are in place. Threats to the physical integrity of RFID systems have also been identified. An attacker may be able to single out individual tags by exploiting subtle variations in their signal output, variations often introduced during manufacturing. This unique "radio fingerprint" can undermine even the most advanced cryptographic privacy-preserving system, since it allows tag identification independent of the cryptographic layer altogether.

REFERENCES

[1]. H.A. Abdulghani, N.A. Nijdam, and D. Konstantas, 2022, "Analysis on Security and Privacy Guidelines: RFID-based IoT Applications," IEEE Access, 10, pp. 131528–131554.
[2]. A. Arslan, and M.A. Bingöl, 2022, "Security and Privacy Analysis of Recently Proposed ECC-Based RFID Authentication Schemes," Cryptology ePrint Archive, Article. 044.
[3]. A. Kumar, A.K. Jain, and M. Dua, 2021, "A Comprehensive Taxonomy of Security and Privacy Issues In RFID," Complex & Intelligent Systems, 7(3), pp. 1327–1347.
[4]. C. Munoz-Ausecha, J. Ruiz-Rosero, and G. Ramirez-Gonzalez, 2021, "RFID Applications and Security Review," Computation, 9(6), Article. 69.
[5]. M.A. Khan, S. Ullah, T. Ahmad, K. Jawad, and A. Buriro, 2023, "Enhancing Security and Privacy in Healthcare Systems Using a Lightweight RFID Protocol," Sensors, 23(12), Article. 5518.
[6]. X. Wang, K. Fan, K. Yang, X. Cheng, Q. Dong, H. Li, and Y. Yang, 2022, "A New RFID Ultra-Lightweight Authentication Protocol for Medical Privacy Protection in Smart Living," Computer Communications, 186, pp. 121–132.
[7]. X. Yao, F. Farha, R. Li, I. Psychoula, L.L. Chen, and H. Ning, 2021, "Security and Privacy Issues of Physical Objects in the IoT: Challenges and Opportunities," Digital Communications and Networks, 7(3), pp. 373–384.
[8]. S. Xie, F. Zhang, and R. Cheng, 2021, "Security Enhanced RFID Authentication Protocols for Healthcare Environment," Wireless Personal Communications, 117(1), pp. 71–86.
[9]. Y. Badr, X. Zhu, and M.N. Alraja, 2021, "Security and Privacy in the Internet of Things: Threats and Challenges," Service Oriented Computing and Applications, 15(4), pp. 257–271.
[10]. S. Gabsi, Y. Kortli, V. Beroulle, Y. Kieffer, A. Alasiry, and B. Hamdi, 2021, "Novel ECC-based RFID Mutual Authentication Protocol for Emerging IoT Applications," IEEE Access, 9, pp. 130895–130913.
[11]. A.K. Agrahari, and S. Varma, 2021, "A Provably Secure RFID Authentication Protocol Based on ECQV for the Medical Internet of Things," Peer-to-Peer Networking and Applications, 14(3), pp. 1277–1289.
[12]. S. Izza, M. Benssalah, and K. Drouiche, 2021, "An Enhanced Scalable and Secure RFID Authentication Protocol for WBAN Within an IoT Environment," Journal of Information Security and Applications, 58, Article. 102705.
[13]. A. Arslan, S.A. Çolak, and S. Ertürk, 2021, "A Secure and Privacy Friendly ECC based RFID Authentication Protocol for Practical Applications," Wireless Personal Communications, 120(4), pp. 2653–2691.
[14]. B. Chander, and K. Gopalakrishnan, 2022, "A Secured and Lightweight RFID-tag Based Authentication Protocol with Privacy-Preserving in Telecare Medicine Information System," Computer Communications, 191, pp. 425–437.
[15]. M. Shariq, K. Singh, M.Y. Bajuri, A.A. Pantelous, A. Ahmadian, and M. Salimi, 2021, "A Secure and reliable RFID authentication protocol using digital Schnorr cryptosystem for IoT-enabled healthcare in COVID-19 Scenario," Sustainable Cities and Society, 75, Article. 103354.
[16]. A. Maatallaoui, H. Touil, and L. Setti, 2023, "The Impact of Radio Frequency (RF) Attacks on Security and Privacy: A Comprehensive Review," 6th International Conference on Networking, Intelligent Systems & Security, pp. 1–23.
[17]. A.A. Khorasgani, M. Sajadieh, and M.R. Yazdani, 2023, "Reconstructing a Lightweight Security Protocol in the Radio-Frequency Identification Systems," IET Computers & Digital Techniques, 17(3–4), pp. 209–223.
[18]. M.J.C. Samonte, B.M.M. Rivera, L.F.S. Deldacan, and E.K.M. Liberato, 2024, "Analyzing Security Issues of Radio Frequency Identification Systems Integration in Transportation System," 12th International Conference on Information, Communication and Networks, pp. 431–438.
[19]. K. Kumar, 2024, "DNA TRIKKY Based Security Mechanism for Radio Frequency Identification

Protocol," IETE Journal of Research, 70(9), pp.7149.

[20]. K.Y. Tsai, Y.L. Wei, and P.S. Chi, 2025, "Lightweight Privacy-Protection RFID Protocol for IoT Environment," Internet of Things, 30, Article. 101490.

[21]. M. Elkhodr, 2025, "An AI-driven Framework for Integrated Security and Privacy in Internet of Things Using Quantum-Resistant Blockchain," Future Internet, 17(6), Article. 246.