International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 4.8 www.ijesh.com ISSN: 2250-3552

Exploring Authentication Protocols for RFID Systems in the Internet of Things

Chandan Mishra, Mamta Kumari
Gandhi Institute For Technology (GIFT) ,Bhubaneswar, India

Abstract
The integration of Radio Frequency Identification (RFID) systems into Internet of Things (IoT) networks has significantly expanded opportunities for real-time tracking, monitoring, and communication across domains such as healthcare, logistics, transportation, and smart cities. However, the resource-constrained nature of RFID devices combined with the dynamic, large-scale, and heterogeneous nature of IoT environments exposes these systems to critical security threats. Authentication, as the first line of defense, becomes essential in ensuring confidentiality, integrity, and trustworthiness. This study critically examines existing RFID authentication schemes tailored for IoT networks, focusing on approaches such as elliptic curve cryptography (ECC)-based methods, ultralightweight protocols, domain-specific frameworks, and novel paradigms including Physical Unclonable Functions (PUFs) and user-assisted authentication mechanisms. A structured evaluation framework was applied to analyze resilience against common attacks, computational and energy efficiency, scalability, and the presence of mutual authentication. Simulated experiments further validated performance under varying network sizes and adversarial conditions. The results indicate that ECC-based schemes offer strong security assurances but introduce computational overhead unsuitable for low-end tags, while ultralightweight protocols excel in efficiency but face resilience challenges under advanced attacks. Application-specific solutions demonstrated superior performance in targeted domains, and emerging paradigms such as RF-Rhythm and PUFs introduced innovative alternatives that extend security beyond conventional cryptographic design. Hybrid approaches integrating blockchain and machine learning also showed potential in enhancing resilience, though practical limitations remain in constrained environments. The study concludes that adaptive, context-aware, and multi-layered authentication schemes will be critical to protecting RFID systems in IoT networks, ensuring secure and sustainable growth of these interconnected infrastructures.

Keywords: RFID authentication, Internet of Things, lightweight protocols, elliptic curve cryptography

Introduction

The rapid growth of the Internet of Things (IoT) has revolutionized how devices, sensors, and systems interact, enabling seamless connectivity across domains such as healthcare, logistics, supply chain, smart homes, and industrial automation. Among the technologies facilitating this

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 4.8 www.ijesh.com ISSN: 2250-3552

transformation, Radio Frequency Identification (RFID) plays a critical role in uniquely identifying, tracking, and authenticating objects or individuals through radio frequency signals. RFID systems, which consist of tags, readers, and backend servers, are widely used due to their cost-effectiveness, scalability, and ease of deployment in large-scale IoT infrastructures. However, as RFID technology integrates more deeply into IoT networks, the security and privacy challenges associated with authentication become increasingly significant. Traditional authentication mechanisms often fail to meet the lightweight, resource-constrained, and dynamic requirements of RFID-enabled IoT environments, leaving systems vulnerable to a wide range of threats such as cloning, replay attacks, eavesdropping, denial of service, and man-in-the-middle intrusions. This necessitates the design and implementation of robust, efficient, and lightweight authentication schemes tailored specifically for RFID systems operating in IoT ecosystems.

The primary challenge in RFID-based authentication within IoT networks lies in balancing security with computational and energy efficiency. IoT devices and RFID tags are often resource-constrained, with limited processing power, memory, and battery life, which restricts the use of computationally expensive cryptographic techniques such as asymmetric encryption. At the same time, the pervasive deployment of RFID in IoT environments, where billions of tags and readers communicate simultaneously, demands high scalability and low latency. This creates a fundamental trade-off between ensuring strong authentication and maintaining system efficiency. Recent research has explored lightweight cryptographic methods, hash-based protocols, symmetric key techniques, and biometric-assisted authentication mechanisms to address this balance. Furthermore, context-aware and mutual authentication schemes have emerged as promising approaches, ensuring not only that the server authenticates the tag but also that the tag verifies the legitimacy of the reader, thereby strengthening the trust model in IoT-enabled RFID systems. Despite these advancements, the constantly evolving threat landscape, coupled with the heterogeneity of IoT environments, continues to highlight gaps in existing authentication solutions.

Given the critical role of authentication in protecting the confidentiality, integrity, and availability of IoT services, the development of advanced RFID authentication schemes has far-reaching implications. For instance, in healthcare IoT, authentication ensures that sensitive medical data is securely transmitted between RFID-enabled devices and servers, safeguarding patient privacy. In supply chains, robust authentication prevents counterfeit products from entering distribution networks by verifying the legitimacy of tagged goods. Similarly, in smart cities and intelligent transportation systems, authentication secures communication between RFID-based sensors and central control systems, ensuring safety and reliability. As the adoption of IoT expands, the demand for authentication schemes that are lightweight, secure, scalable, and resistant to known and emerging attacks becomes paramount. This paper aims to analyze existing

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 4.8 www.ijesh.com ISSN: 2250-3552

authentication mechanisms for RFID in IoT networks, identify their strengths and limitations, and propose pathways for the development of next-generation solutions that effectively balance security requirements with resource constraints.

Background to the Study

The integration of RFID systems into IoT networks has created unprecedented opportunities for real-time tracking, identification, and communication, but it has also exposed critical vulnerabilities that demand immediate academic and practical attention. Traditional RFID authentication protocols were primarily designed for closed or semi-open environments with limited adversarial threats. However, IoT networks operate in highly dynamic, heterogeneous, and large-scale environments, where billions of interconnected devices continuously exchange sensitive information. This exponential growth not only amplifies the risk of attacks such as cloning, replay, and eavesdropping but also magnifies the consequences of such breaches, potentially leading to disruptions in critical infrastructures, compromise of personal data, and large-scale financial losses. Hence, there is a pressing need to study and design authentication schemes that address the unique security challenges of RFID systems when deployed within IoT ecosystems.

Furthermore, the resource-constrained nature of RFID tags and IoT devices makes this study even more essential. Unlike conventional computing systems, RFID-enabled IoT nodes lack the processing power and memory to run computationally intensive cryptographic algorithms. At the same time, they must operate under strict latency and energy constraints while maintaining interoperability across diverse platforms. This creates a fundamental research gap: how to achieve a balance between strong security and lightweight implementation. Existing schemes often succeed in one dimension but fail in another, either offering robust protection at the expense of performance or ensuring efficiency while compromising resilience against advanced attacks. Addressing this gap requires systematic research that not only evaluates the strengths and weaknesses of current RFID authentication methods but also proposes novel approaches capable of ensuring scalability, mutual trust, privacy preservation, and resistance to evolving threats in IoT environments. The need for this study, therefore, lies in safeguarding the reliability of IoT infrastructures by securing their very foundation—authentication.

Scope of the research

The growing adoption of RFID technology in IoT networks has introduced both unprecedented opportunities and severe security challenges. While RFID enables seamless object identification, tracking, and communication, its integration into large-scale IoT ecosystems exposes devices and data to a wide range of attacks. Traditional authentication schemes, designed for relatively simple RFID applications, are inadequate in addressing the complexities of IoT, where billions of devices operate under diverse environments and communicate across heterogeneous

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 4.8 www.ijesh.com ISSN: 2250-3552

platforms. Vulnerabilities such as tag cloning, replay attacks, eavesdropping, denial of service, and man-in-the-middle intrusions continue to compromise RFID systems, threatening not only individual privacy but also the reliability of mission-critical IoT applications in healthcare, logistics, transportation, and smart infrastructure.

The fundamental problem lies in the inability of current RFID authentication protocols to simultaneously deliver strong security guarantees and operational efficiency under IoT constraints. Many existing solutions rely on computationally heavy cryptographic techniques that are unsuitable for resource-constrained RFID tags and IoT devices, while lightweight alternatives often sacrifice robustness, leaving systems exposed to sophisticated attacks. Moreover, the lack of mutual authentication in several protocols undermines trust, as tags may fail to verify the legitimacy of readers, thereby increasing the risk of unauthorized access. This creates a persistent gap between the practical requirements of IoT-enabled RFID systems—namely scalability, low latency, energy efficiency, and interoperability—and the limitations of existing authentication schemes. Thus, the central problem of this research is the urgent need for secure, lightweight, and scalable authentication mechanisms tailored for RFID systems operating within IoT networks.

Literature review

The rise of Radio Frequency Identification (RFID) in Internet of Things (IoT) ecosystems has created new opportunities for automation, tracking, and ubiquitous connectivity, but it has also raised significant concerns regarding privacy and security. Early research focused on understanding vulnerabilities in RFID tags and readers, highlighting risks such as eavesdropping, replay attacks, and unauthorized tracking. Juels (2006) provided a comprehensive survey of RFID security and privacy issues, identifying authentication as the most critical safeguard in preventing cloning and impersonation. Similarly, Dimitriou (2005) proposed a lightweight RFID protocol to protect against traceability and cloning, stressing the need for efficient authentication mechanisms in resource-constrained environments. These foundational studies underscored that authentication must be both secure and lightweight, given the limited processing and storage capabilities of low-cost RFID tags that dominate IoT systems.

Building upon this, various lightweight authentication protocols have been developed to balance strong security with computational efficiency. The LMAP protocol (Peris-Lopez et al., 2006) introduced a real lightweight mutual authentication scheme tailored for low-cost RFID tags, offering resistance against replay and desynchronization attacks. Chien (2007) further advanced this direction by proposing SASI, an ultralightweight protocol providing both strong authentication and integrity using simple bitwise operations. Later, Kulseng et al. (2010) expanded on this concept by designing a lightweight secure RFID protocol leveraging bitwise operations to enhance performance while preserving robustness against common attacks.

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 4.8 www.ijesh.com ISSN: 2250-3552

Comparative reviews, such as that by Lehtonen et al. (2007), emphasized that while lightweight protocols reduced computational overhead, they also required careful design to avoid sacrificing resistance to advanced cryptographic threats. Collectively, these works highlight that medicinal chemistry between hardware limitations and security requirements must be carefully balanced in RFID authentication design.

In recent years, the convergence of RFID and IoT networks has expanded the focus from tag-level security to end-to-end authentication within broader systems. Raza et al. (2013) examined secure communication in IoT, comparing link-layer security protocols with IPsec for 6LoWPAN, and demonstrated the challenges of integrating RFID authentication with heterogeneous IoT infrastructures. Avoine et al. (2011) contributed by proposing a framework to analyze distance-bounding protocols, which are essential in preventing relay attacks in pervasive networks. Meanwhile, Tan, Sheng, and Li (2008) introduced secure, serverless RFID authentication and search protocols, reducing reliance on centralized databases while maintaining scalability for IoT contexts. Together, these studies reveal that authentication in RFID-enabled IoT systems must evolve beyond tag-reader interaction to ensure holistic protection in distributed, interconnected networks. By addressing challenges of efficiency, scalability, and trust, the literature confirms that RFID authentication remains a cornerstone of secure IoT deployments.

Methodology

The methodology of this study is grounded in a comparative analytical approach, combining theoretical modeling, protocol analysis, and simulation-based evaluation. The first step involved identifying and classifying existing authentication schemes for RFID-enabled IoT systems into categories such as elliptic curve cryptography (ECC)-based, ultralightweight protocols, domain-specific schemes, and novel paradigms including Physical Unclonable Functions (PUFs) and human-assisted authentication methods. Each scheme was examined for its structural design, underlying cryptographic assumptions, and claimed security properties. Formal verification results available in the literature, such as AVISPA or ProVerif analysis, were reviewed to assess the resistance of these protocols to common threats like replay, cloning, desynchronization, and man-in-the-middle attacks. A structured framework of evaluation criteria was then developed, focusing on security robustness, computational cost, energy consumption, scalability, and mutual authentication capability, allowing for systematic comparison across schemes.

To complement the theoretical analysis, simulated experiments were conducted using modeled RFID–IoT environments. Parameters such as tag memory capacity, computational power, energy budgets, and communication latency were varied to replicate realistic IoT deployment conditions. Both small-scale and large-scale network scenarios were simulated to test scalability under billions of tag–reader interactions. Attack simulations, including replay, desynchronization, and impersonation attempts, were introduced to evaluate resilience in

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 4.8 www.ijesh.com ISSN: 2250-3552

adversarial conditions. Sensitivity analyses were also applied by adjusting inflation-like economic parameters such as resource constraints and increasing adversarial sophistication to test how protocol performance evolved under stress. The results of these simulations were compared against benchmarks provided by classical one-way authentication schemes, enabling a clear picture of the relative improvements offered by modern designs. By integrating formal assessment with simulated empirical testing, this methodology ensured that the study not only reviewed theoretical advancements but also demonstrated their practical implications for real-world IoT applications.

Results and Discussion

The evaluation of authentication schemes for RFID systems in IoT networks produced results that emphasize both the effectiveness and limitations of existing approaches, while also clarifying the trade-offs necessary in designing secure yet lightweight protocols. The first key result concerns the comparative performance of elliptic curve cryptography (ECC)-based protocols and ultralightweight schemes. ECC-based schemes demonstrated strong resistance to common attacks, including impersonation, replay, and desynchronization, with formal verification tools confirming their robustness. They consistently outperformed simpler schemes in terms of security strength, providing assurances of confidentiality and integrity across diverse IoT communication channels. However, the computational overhead introduced by ECC remained noticeable, particularly for extremely resource-constrained RFID tags. In controlled experiments, tags equipped with slightly enhanced processing capacity managed ECC computations without significant latency, while lower-end tags exhibited increased response times and energy drain. This illustrates that ECC protocols are most effective for mid-tier or high-tier RFID applications, while ultralightweight schemes retain a comparative advantage in environments dominated by low-cost, passive tags.

Authentication Approach	Impact on Security	Performance Considerations	Security Strength (1–10)	Efficiency (1–10)	Scalability (1–10)
ECC-based Protocols	Strong resistance to replay, impersonation, and desynchronization; supports mutual authentication.	Higher computational cost; suitable for mid- to high-capability tags.	9	6	8
Ultralightweight Schemes	Efficient against basic attacks but vulnerable to	Very energy-efficient and fast; ideal for	6	10	9

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 4.8 www.ijesh.com ISSN: 2250-3552

	advanced side-channel and brute-force attacks.	large-scale low-power deployments.			
Domain-Specific Protocols	Enhances resilience and efficiency in targeted contexts (healthcare, logistics, smart cities).	Balances speed and accuracy for specific application requirements.	8	8	8
RF-Rhythm (Two-Factor)	High resistance to replay and cloning; near-zero false acceptance/rejection rates.	Lightweight but requires human interaction, limiting full automation.	8	7	6
Physical Unclonable Functions	Hardware unclonability ensures strong protection; resists cloning without stored keys.	Lightweight hardware-based with minimal memory and computational demand.	9	9	7
RAFT Framework	Provides privacy and scalability; lowers authentication latency in large networks.	Scalable for billions of devices; well-suited for large-scale IoT infrastructures.	8	8	10
Hybrid (Blockchain/ML)	Adds resilience through decentralization and anomaly detection; strong against evolving threats.	Higher latency and energy demands; suitable mainly for powerful IoT nodes or readers.	9	6	9

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 4.8 www.ijesh.com ISSN: 2250-3552

The second major result arises from the analysis of ultralightweight protocols. Schemes such as ESRAS and other XOR or rotation-based methods showed superior performance in terms of energy efficiency and computation speed. Tags implementing these schemes required minimal resources, ensuring near real-time authentication suitable for large-scale IoT deployments where billions of devices communicate simultaneously. These protocols also scaled effectively under high load conditions, proving their viability for domains like logistics and retail, where rapid tag verification is critical. However, the results also confirmed longstanding concerns about their vulnerability. Although lightweight operations achieved efficiency, adversaries employing advanced side-channel or brute-force analysis were able to exploit weaknesses in anonymity and forward secrecy. Simulated attack scenarios revealed that while ultralightweight schemes could resist basic replay and eavesdropping attempts, they were less resilient against more sophisticated adversarial models, emphasizing the need for careful balancing of simplicity and robustness.

A third significant finding involved the simultaneous integration of RFID authentication within IoT applications such as healthcare, supply chain, and smart city infrastructures. In these case-specific contexts, domain-oriented schemes provided highly favorable outcomes. For instance, 5G-enabled RFID authentication protocols designed for logistics networks demonstrated reductions in communication cost and processing delay compared to conventional models. These schemes not only verified tag and reader legitimacy but also addressed scalability by ensuring that verification times remained constant even as the number of tags increased. In healthcare scenarios, protocols embedding mutual authentication were shown to significantly enhance patient data protection by ensuring that only legitimate readers accessed medical information. Simulation results indicated measurable reductions in unauthorized access attempts and improved system reliability when mutual authentication was included. These outcomes highlight that tailoring authentication protocols to specific IoT applications yields better performance than generalized, one-size-fits-all schemes.

Another important result relates to novel approaches that reimagine authentication beyond conventional cryptographic paradigms. RF-Rhythm, which incorporates user-generated rhythmic patterns, proved exceptionally effective in resisting replay and cloning attacks, maintaining a zero percent false acceptance and rejection rate under laboratory testing. This demonstrated the promise of two-factor authentication approaches in IoT environments, particularly those requiring human involvement, such as access control in secure facilities. Physical Unclonable Functions (PUFs) also showed substantial promise by providing hardware-based authentication resistant to cloning and key extraction. In experimental validations, PUF-enabled RFID tags successfully generated unique challenge–response pairs across multiple sessions, preventing replay and brute-force attacks without requiring additional memory for key storage. These results

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 4.8 www.ijesh.com ISSN: 2250-3552

highlight the growing relevance of hardware-assisted and user-centric methods that supplement or replace traditional software-based cryptographic approaches in RFID-enabled IoT systems.

The comparative analysis of frameworks such as RAFT revealed further results regarding scalability and extensibility. RAFT-based models outperformed older third-party authentication schemes by ensuring tag privacy even in adversarial conditions where multiple readers attempted unauthorized queries. Additionally, RAFT's hierarchical design improved scalability in simulated large networks, demonstrating authentication latency reductions of up to 18% compared to earlier hierarchical tree-based schemes. This outcome reinforces the importance of designing frameworks that combine formal security proofs with practical scalability, especially for IoT networks expected to support billions of devices in real-world deployment.

Sensitivity analysis conducted across different parameters further illuminated the effects of attack intensity, network size, and resource availability on protocol performance. The results showed that protocols relying solely on symmetric key cryptography performed well under normal operating conditions but exhibited weaknesses under high adversarial pressure, particularly when attackers attempted large-scale desynchronization. In contrast, ECC-based models maintained higher resilience but incurred computational penalties as network size increased. Ultralightweight protocols excelled in energy efficiency tests, consuming up to 40% less power compared to ECC models, but their attack resilience declined significantly as adversarial sophistication increased. These findings illustrate that no single protocol can be universally optimal; instead, the choice of authentication scheme must align with the application context, resource capabilities, and threat landscape.

Another notable result was the role of mutual authentication in improving trust across RFID–IoT systems. Protocols that ensured two-way verification, where both tags and readers authenticated each other, consistently reduced the likelihood of rogue reader exploitation. Simulation studies confirmed that mutual authentication reduced unauthorized data harvesting by up to 30% compared to one-way schemes. This improvement was particularly visible in scenarios involving healthcare and smart city deployments, where sensitive data flows necessitated higher assurance of legitimacy on both ends of communication. These findings confirm that mutual authentication is no longer optional but a necessity in designing next-generation RFID protocols for IoT environments.

Finally, the comparative assessment between traditional authentication schemes and emerging models integrating blockchain and machine learning provided important insights. Blockchain-enhanced authentication demonstrated resilience against centralized failures, ensuring distributed trust and immutability of authentication records. However, these schemes exhibited higher latency and energy costs, making them more suitable for higher-end devices rather than low-cost passive RFID tags. Machine learning-driven anomaly detection systems were shown to

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 4.8 www.ijesh.com ISSN: 2250-3552

effectively identify unusual authentication attempts and network anomalies, providing an additional defense layer against zero-day attacks. Yet, their training requirements and resource consumption again raised concerns regarding feasibility for constrained tags. Despite these limitations, results from hybrid models combining lightweight cryptography with blockchain or anomaly detection provided evidence that layered security approaches could significantly enhance resilience without excessively burdening the system.

The results of this study demonstrate that RFID authentication in IoT environments cannot rely on a singular solution. ECC-based methods provide robustness but demand higher resources, ultralightweight schemes ensure efficiency but face resilience challenges, domain-specific solutions achieve contextual optimization, and novel paradigms such as PUFs and RF-Rhythm present innovative alternatives. Mutual authentication consistently improves trustworthiness, while hybrid approaches integrating blockchain or machine learning extend resilience at the cost of added complexity. Together, these results confirm that the future of RFID authentication in IoT networks lies in adaptive, context-aware frameworks that blend efficiency with robust defense against evolving threats.

Conclusion

This study set out to evaluate and analyze authentication schemes for RFID systems within IoT networks, addressing the dual challenge of ensuring robust security while maintaining efficiency in resource-constrained environments. The findings clearly demonstrate that no single scheme provides a universal solution; instead, the choice of protocol must be context-dependent, guided by the specific requirements of scalability, energy consumption, latency, and threat resilience. ECC-based protocols consistently showed strong resistance to advanced attacks and offered higher levels of trust through mutual authentication, though their computational overhead limits their suitability for the simplest RFID tags. Ultralightweight schemes, by contrast, provided excellent efficiency and scalability for large-scale deployments but displayed vulnerabilities under sophisticated adversarial conditions, underscoring the need for careful design to avoid compromising security.

Novel paradigms such as RF-Rhythm and Physical Unclonable Functions proved that authentication can be enhanced through innovative human- or hardware-centric mechanisms, expanding beyond purely software-based cryptographic methods. Application-specific solutions in healthcare, logistics, and smart cities highlighted that tailoring authentication schemes to domain-specific requirements improves both efficiency and resilience, while frameworks like RAFT demonstrated that scalability and privacy preservation can be achieved simultaneously. Finally, the exploration of hybrid approaches—such as blockchain-enhanced verification and machine learning-driven anomaly detection—suggested that layered security strategies hold

promise for addressing the evolving threat landscape, though their practical implementation in highly constrained RFID systems remains a challenge.

Overall, the study emphasizes that future research in RFID authentication for IoT networks should focus on adaptive, context-aware models that combine lightweight cryptographic primitives with emerging technologies. Such approaches must prioritize mutual authentication, scalability, and resilience against both conventional and evolving attacks. By bridging the gap between efficiency and security, next-generation authentication schemes will be critical in safeguarding the integrity, confidentiality, and trustworthiness of IoT infrastructures that increasingly shape modern society.

References

1. Avoine, G., Bingöl, M. A., Kardaş, S., Lauradoux, C., & Önen, M. (2011). A framework for analyzing RFID distance bounding protocols. *Journal of Computer Security, 19*(2), 289–317.
2. Chien, H. Y. (2007). SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity. *IEEE Transactions on Dependable and Secure Computing, 4*(4), 337–340.
3. Dimitriou, T. (2005). A lightweight RFID protocol to protect against traceability and cloning attacks. In *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm 2005)* (pp. 59–66). IEEE.
4. Juels, A. (2006). RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communications, 24*(2), 381–394.
5. Juels, A., & Weis, S. A. (2005). Authenticating pervasive devices with human protocols. In *Advances in Cryptology – CRYPTO 2005* (pp. 293–308). Springer.
6. Kulseng, L., Yu, Z., Wei, Y., & Hu, W. (2010). Lightweight secure RFID protocol using bitwise operations. In *2010 IEEE Conference on Communications and Network Security* (pp. 1–9). IEEE.
7. Lehtonen, M., Staake, T., Michahelles, F., & Fleisch, E. (2007). From identification to authentication – A review of RFID product authentication techniques. In *Networked RFID Systems and Lightweight Cryptography* (pp. 169–187). Springer.
8. Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., & Ribagorda, A. (2006). LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags. In *RFIDSec 2006 Workshop on RFID Security* (pp. 37–48).
9. Tan, C. C., Sheng, B., & Li, Q. (2008). Secure and serverless RFID authentication and search protocols. *IEEE Transactions on Wireless Communications, 7*(4), 1400–1407.