Journal of
Cyber Security

Tech Science Press

https://doi.org/10.32604/jcs.2026.083953

ARTICLE

Lightweight Secure Authentication for IoT Devices: A Systematic Literature Review

Rayan Alenzi, Rayan Aldoghan* and M. M. Hafizur Rahman

Department of Computer Networks and Communications, College of Computer Sciences and Information Technology, King Faisal University, Al Ahsa, Saudi Arabia

*Corresponding Author: Rayan Aldoghan. Email: 226032032@student.kfu.edu.sa

Received: 14 April 2026; Accepted: 08 May 2026; Published: 1 July 2026

ABSTRACT: The rapid proliferation of Internet of Things (IoT) devices across smart homes, healthcare facilities, industrial networks, and smart cities has raised critical security concerns, particularly regarding device authentication. IoT devices are typically characterized by limited computational resources, constrained memory, and restricted energy budgets, which renders the deployment of traditional cryptographic protocols infeasible; consequently, lightweight authentication schemes are required. Although numerous lightweight authentication protocols have been proposed, a systematic risk evaluation of such protocols against established threat modeling frameworks remains largely absent from the existing literature. This paper presents a systematic literature review (SLR) based on the PRISMA methodology, encompassing 45 peer-reviewed articles published between 2021 and 2025 on lightweight secure authentication for IoT devices. The review integrates the STRIDE threat modeling framework for systematic threat identification with the DREAD risk assessment model for quantitative risk prioritization across authentication protocol categories. The protocols reviewed include Physical Unclonable Function (PUF)-based, Elliptic Curve Cryptography (ECC)-based, blockchain-based, multi-factor, Authenticated Encryption with Associated Data (AEAD)-based, post-quantum, and zero-knowledge proof authentication techniques. Our STRIDE-DREAD analysis indicates that, while ECC-based and PUF-based protocols exhibit the strongest overall risk mitigation profiles, considerable unmitigated risks persist across all categories, particularly in spoofing and information disclosure threats. The findings reveal critical gaps in real-world deployment validation, post-quantum readiness, cross-domain interoperability, and alignment with established risk management standards. This review contributes a risk-centric classification framework, quantitative risk scores per protocol category, and actionable research directions for the IoT security community.

KEYWORDS: IoT; lightweight authentication; risk assessment; STRIDE; DREAD; threat modeling; security protocol; PUF; ECC; blockchain; AEAD; mutual authentication; post-quantum cryptography

1 Introduction

The Internet of Things (IoT) has fundamentally transformed modern digital infrastructure, with billions of devices connected across diverse domains, including smart homes, healthcare, industrial automation, vehicular networks, and smart city ecosystems. Current projections estimate that the number of IoT-connected devices will surpass 30 billion worldwide by 2030, generating vast amounts of data and facilitating intelligent decision-making at the network edge. However, the expanding attack surface has simultaneously rendered IoT ecosystems primary targets for cyberattacks, including unauthorized access, data breaches, device impersonation, man-in-the-middle attacks, and denial-of-service attacks.

Authentication constitutes the first line of defense in IoT security, ensuring that only authorized devices and users can access network resources and communicate. Traditional authentication algorithms, including RSA, Diffie-Hellman key exchange, and certificate-based Public Key Infrastructure (PKI), offer strong security assurances but impose computational, memory, and energy demands that exceed the capabilities of resource-constrained IoT devices. Most IoT sensors and actuators employ 8-bit to 32-bit microcontrollers with limited RAM (typically less than 64 KB) and operate on battery power, rendering traditional cryptographic techniques infeasible [1–3].

This resource asymmetry has driven the development of lightweight authentication protocols. Various approaches have been explored by the research community, including hardware-based authentication using Physically Unclonable Functions (PUFs), mathematical schemes based on Elliptic Curve Cryptography (ECC), distributed approaches leveraging blockchain technology, Authenticated Encryption with Associated Data (AEAD)-based designs aligned with NIST lightweight cryptography standards, and emerging paradigms such as post-quantum cryptography and zero-knowledge proofs [4–6].

Despite the growing number of proposed lightweight authentication protocols, a critical gap persists: the absence of systematic risk evaluation of these protocols within the context of established threat modeling and risk quantification frameworks. Most existing reviews focus on security property analysis and performance comparison without employing structured risk assessment methods such as STRIDE for threat identification or DREAD for risk prioritization [7–10]. This paper addresses this gap by presenting a systematic literature review based on the PRISMA methodology that uniquely integrates threat analysis using the STRIDE framework with risk scoring using the DREAD model to evaluate lightweight IoT authentication protocols.

Unlike prior surveys, which predominantly catalogue security properties and computational metrics without structured risk quantification [8,10,11], this review makes four distinct contributions: (1) it is the first SLR to apply the combined STRIDE-DREAD framework systematically across all major lightweight IoT authentication categories; (2) it provides quantitative, cross-category risk scores that enable direct comparison of protocol families; (3) it incorporates recently proposed AEAD-based and hybrid PUF-AEAD protocols that reflect the latest NIST lightweight cryptography standardization efforts; and (4) it identifies eight actionable research gaps derived from the risk assessment findings rather than from *ad hoc* observation.

The remainder of this paper is organized as follows: Section 2 defines the research problem. Section 3 presents the research questions. The methodology is described in Section 4. In Section 5, the findings of the literature review are presented. Sections 6–8 develop and apply the STRIDE-DREAD risk assessment. The findings are discussed in Section 9. Section 10 identifies research gaps. Section 11 addresses threats to validity, and Section 12 concludes the paper.

2 Research Problem

The central challenge in IoT authentication is achieving an appropriate balance between security strength and operational feasibility. IoT devices must authenticate themselves and their communication partners to prevent unauthorized access, yet they lack the computational resources to execute complex cryptographic operations. This challenge is compounded by heterogeneous ecosystems, physically accessible deployment environments, and the massive scale of IoT networks [12–14].

Furthermore, quantum computing poses a long-term security threat to protocols based on traditional number-theoretic assumptions [15]. Critically, despite the proliferation of lightweight authentication proposals, literature lacks a systematic risk assessment perspective. Most studies validate protocols using formal verification tools but do not analyze residual risks through established threat modeling frameworks. Without systematic risk assessments, practitioners cannot effectively determine the most appropriate protocol category for a given deployment environment's threat landscape [7,9,11].

3 Research Questions

RQ1: *What are the principal families of lightweight authentication protocols proposed for IoT devices (2021–2025), and how can they be mapped to established threat categories?*

RQ2: *What security properties do these protocols provide, and what residual risks remain when evaluated against the STRIDE threat model?*

RQ3: *How do the quantitative risk scores of these protocol categories compare when evaluated using the DREAD model?*

RQ4: *What are the most significant research gaps and future directions for risk-aware lightweight IoT authentication?*

4 Methodology

This study follows the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) protocol to ensure transparency, reproducibility, and methodological rigor. In addition, the STRIDE and DREAD risk assessment frameworks are integrated as an analytical lens.

4.1 Database Selection and Search Strategy

A systematic search was conducted across seven major academic databases: IEEE Xplore, Scopus, Web of Science, ScienceDirect, SpringerLink, ACM Digital Library, and MDPI. The search was executed in two phases between October 2024 and January 2025. Phase 1 targeted lightweight authentication protocols using the following Boolean search string: ("Internet of Things" OR "IoT") AND ("lightweight authentication" OR "secure authentication" OR "PUF authentication" OR "ECC authentication" OR "AEAD authentication") AND ("protocol" OR "scheme" OR "framework"). Phase 2 targeted risk assessment literature using: ("IoT" OR "Internet of Things") AND ("risk assessment" OR "threat modeling" OR "STRIDE" OR "DREAD") AND ("security" OR "authentication"). Search strings were adapted to each database's query syntax while maintaining semantic equivalence.

4.2 Inclusion and Exclusion Criteria

Inclusion criteria were: (1) publication date between 2021 and 2025; (2) peer-reviewed journal articles or conference papers; (3) written in English; (4) proposing or evaluating lightweight IoT authentication protocols or IoT security risk assessment methodologies; and (5) containing formal or informal security analysis. Exclusion criteria were: (1) not related to IoT authentication or risk assessment; (2) lacking security or risk analysis; (3) not in English; (4) published before 2021; and (5) duplicate publications.

4.3 PRISMA Process

The search yielded 556 records (510 from database searches and 46 from citation searching). After removing 102 duplicates, 454 records remained for title and abstract screening. Two reviewers independently screened all records; disagreements were resolved through discussion and, where necessary, consultation with the supervising author. Of these, 318 records were excluded based on title and abstract relevance, leaving 136 full-text articles for eligibility assessment. During full-text review, 91 articles were excluded: 33 did not focus on lightweight authentication or risk assessment, 28 lacked formal security or risk analysis, 17 were not in English or were published outside the 2021–2025 window, and 13 were duplicates or substantially overlapping studies. The final review comprises 45 articles: 31 proposing lightweight authentication protocols (Group A) and 14 addressing IoT security risk assessment and threat modeling (Group B). The PRISMA flow diagram is presented in Fig. 1.

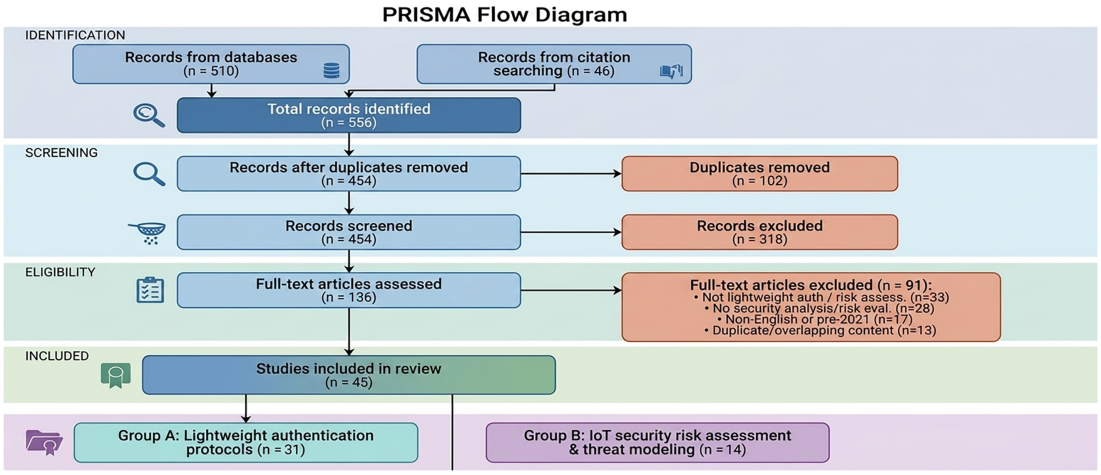

Figure 1: PRISMA flow diagram for the systematic literature review process.

4.4 Risk Assessment Framework

We adopt the combined STRIDE-DREAD framework. STRIDE provides a systematic threat identification taxonomy comprising six categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. These categories directly correspond to fundamental IoT authentication concerns [7,9,16]. DREAD provides quantitative risk scores across five dimensions—Damage Potential, Reproducibility, Exploitability, Affected Users, and Discoverability—each rated on a 1 (Low) to 3 (High) scale. The composite DREAD score is calculated as DREAD = (D + R + E + A + D)/5, yielding risk levels of Low (1.0–1.6), Medium (1.7–2.3), or High (2.4–3.0) [10,17,18].

To ensure scoring consistency and mitigate subjectivity, the following protocol was employed. First, a scoring rubric was developed that maps specific, observable security properties and performance metrics to each DREAD dimension (e.g., mutual authentication and hardware-bound identity map to low Damage Potential for spoofing; simulation-only validation maps to moderate Reproducibility). Second, both authors independently scored all 31 Group A protocols using this rubric. Third, scores were compared, and discrepancies exceeding 0.5 on any dimension were discussed and reconciled through consensus, with the supervising author consulted for unresolved cases. The final scores represent the average values of both reviewers' assessments. Inter-rater agreement was substantial (Cohen's $\kappa = 0.78$) prior to reconciliation. This approach follows the validated DREAD methodology applied by Zhai et al. [9] and Kim et al. [10] in healthcare and industrial IoT contexts, respectively.

5 Literature Review Findings

The 45 studies included in this review are organized into two groups: Group A comprises 31 studies proposing lightweight authentication protocols for IoT devices, and Group B comprises 14 studies addressing IoT security risk assessment, threat modeling, and comprehensive security surveys. This section presents the findings from both groups, organized thematically to facilitate cross-protocol comparison and synthesis. Table 1 provides a complete summary of all 45 reviewed studies, while Table 2 details the risk assessment frameworks employed by Group B studies.

5.1 Hardware-Based Authentication (PUF and RFID)

Hardware-rooted trust mechanisms represent a paradigm shift from software-only authentication by anchoring device identity in physical characteristics that are inherently unclonable. This subsection examines

PUF-based and RFID-based protocols, highlighting a common trajectory toward eliminating stored secret keys while balancing noise tolerance, scalability, and real-world deployment feasibility.

Hardware-rooted trust has emerged as a promising direction for IoT authentication, with Physical Unclonable Functions (PUFs) and Radio-Frequency Identification (RFID) protocols representing the two primary approaches in this category.

PUF-based authentication leverages the inherent manufacturing variability of semiconductor devices to generate unique, unclonable challenge-response pairs (CRPs), thereby eliminating the need for stored secret keys. Tun and Mambo [1] advanced this paradigm by integrating Paillier homomorphic encryption with PUF verification, enabling privacy-preserving CRP validation without requiring a secure CRP database on the server side. While this approach significantly reduces storage requirements, the reliance on Paillier encryption introduces computational latency that limits its applicability to ultra-low-power devices operating below 32-bit microcontrollers. Addressing a different challenge within the PUF domain, Farha et al. [2] proposed an SRAM-PUF scheme that eliminates the need for fuzzy extractors—components traditionally required to handle the inherent noise in PUF responses—by identifying and utilizing only the stable subsets of SRAM cells. This approach substantially reduces hardware overhead for cloud-based IoT deployments, although it introduces a dependency on cloud connectivity and may suffer from reliability degradation under temperature extremes. Wang et al. [3] tackled the noise problem from a different angle by introducing a reverse fuzzy extractor mechanism that shifts the error correction burden from the constrained IoT node to the server, using only hash, XOR, and PUF operations. This design is notable for its minimal device-side requirements, though its formal verification was limited to BAN logic without real hardware implementation.

A comparative assessment of these three PUF protocols reveals a common strength in spoofing resistance—since PUF responses are physically bound to individual hardware instances, device cloning becomes extremely difficult—but also shared limitations in the absence of quantum resistance and the lack of real-world deployment validation on production-grade IoT hardware.

In the RFID authentication space, Khan et al. [4] proposed a pseudonym-based protocol targeting healthcare IoT environments. The dynamic pseudonym updating mechanism prevents tracking and impersonation attacks while maintaining low computational overhead suitable for passive RFID tags. However, the protocol assumes a trusted backend server, and its scalability to large hospital networks with thousands of tagged assets was not evaluated. Mudra et al. [5] complemented this work with a systematic evaluation of passive-RFID authentication protocols in the maritime IoT context, providing a comparative framework for assessing encryption methods and attack resistance. The scope was deliberately limited to passive RFID, leaving active RFID and hybrid NFC-RFID approaches unaddressed.

More recently, Tanveer et al. [19] proposed RePUF-IoT, a reconfigurable PUF-based protocol for healthcare IoT that integrates TinyJAMBU authenticated encryption with one-time PUF challenges. By reconfiguring PUF challenges after each session, RePUF-IoT achieves robust resilience against machine learning modeling attacks—a vulnerability that afflicts static PUF schemes. Performance evaluations demonstrate a 32%–64% reduction in communication overhead and 88%–94% reduction in execution time compared to prior PUF-based healthcare protocols, making it one of the most efficient PUF-AEAD hybrid designs in the reviewed corpus.

5.2 Cryptographic Authentication (ECC, Multi-Factor, Post-Quantum, and Zero-Knowledge)

Cryptographic approaches to lightweight IoT authentication span a broad spectrum from elliptic curve mathematics to multi-factor designs and emerging quantum-resistant primitives. A cross-cutting observation is the fundamental trade-off between cryptographic strength and computational overhead: ECC

protocols consistently achieve the strongest formal security guarantees but at higher latency, while hash-only schemes minimize computation at the expense of weaker long-term security.

Elliptic Curve Cryptography (ECC) constitutes the most extensively studied approach in the reviewed literature, with five protocols spanning industrial, healthcare, general IoT, and smart city domains. The appeal of ECC lies in its ability to provide equivalent security to RSA with substantially shorter key lengths—a 160-bit ECC key offers comparable security to a 1024-bit RSA key—making it well-suited for resource-constrained environments.

Yang et al. [6] combined ECC with JSON Web Tokens (JWT) and TLS v1.3 to create a token-based authentication mechanism for Industrial IoT, achieving approximately 73% efficiency improvement over prior schemes by reducing repeated key exchanges. While effective, the protocol's reliance on TLS v1.3 may limit its deployment on legacy industrial equipment that lacks support for modern transport security. Hu et al. [12] contributed a significant theoretical advancement by presenting the first IoT ECC-based protocol with formal security proof under the eCK (extended Canetti-Krawczyk) model, which provides stronger guarantees than the more commonly used random-oracle model. This protocol achieves mutual authentication and user anonymity, though at higher computational cost compared to hash-only alternatives. Sowjanya et al. [13] identified and formally demonstrated vulnerabilities—including escrow and impersonation flaws—in existing Wireless Body Area Network (WBAN) protocols for the Internet of Medical Things (IoMT), proposing an improved ECC-based scheme verified through AVISPA. Keshta [14] took a layered approach by combining CRC for lightweight routine data integrity checks with ECC for message-level authentication, although the CRC layer provides only error detection without cryptographic security guarantees. Ullah et al. [20] introduced a pre-computation strategy for Curve25519 that stores partial ECC computation results during device idle periods, reducing real-time computational overhead for M2M communication scenarios.

Across the ECC category, computation times range from 1.248 [21] to 14.88 ms [22], with communication overhead spanning 1036 to 5824 bits. All five ECC protocols provide mutual authentication and forward secrecy, but none addresses quantum resistance notable gaps given the anticipated timeline of quantum computing threats.

Beyond ECC, three complementary cryptographic approaches were reviewed. Saqib et al. [23] proposed a three-factor authentication framework combining identity, password, and digital signatures over the MQTT publish-subscribe protocol. While the integration of 3FA with MQTT addresses the security requirements of critical IoT applications, the MQTT broker introduces a single point of failure that undermines the scheme's resilience. Al-Saggaf et al. [15] made a unique contribution as one of only two studies addressing post-quantum threats, proposing a fuzzy commitment scheme that combines biometric template protection with lattice-based cryptographic primitives for healthcare IoT. The protocol achieves quantum resistance but at the cost of higher memory consumption compared to classical methods—a trade-off that may prove increasingly acceptable as quantum computing matures. Hamila et al. [22] adopted classical zero-knowledge proofs for constrained IoT by applying the Fiat-Shamir transformation to convert interactive Sigma-protocols into single-round non-interactive proofs, eliminating the multi-round communication overhead that traditionally makes ZKP impractical for battery-powered devices. Despite this optimization, ZKP-based authentication remains computationally heavier than symmetric-key approaches.

5.3 Distributed and Architecture-Based Authentication

Distributed authentication approaches address the trust centralization problem inherent in traditional client-server models. The reviewed studies reveal two distinct strategies: blockchain-based decentralization and multi-tier architectural optimization across cloud, fog, and edge layers. A notable finding is that while

blockchain provides strong non-repudiation and tamper resistance, it introduces consensus overhead that creates new denial-of-service vulnerability trade-off insufficiently addressed in the original protocol designs.

Three studies addressed decentralized authentication through blockchain technology, each targeting different aspects of the trust distribution problem. Al Ahmed et al. [24] developed a hash-chain-based protocol with a custom proof-of-identity consensus mechanism, tested on Raspberry Pi hardware. By replacing energy-intensive blockchain consensus with a lightweight proof-of-identity system, the protocol becomes viable for battery-powered IoT clusters, though cluster head failure can disrupt the entire authentication chain. Chaira et al. [25] tackled the cross-domain interoperability challenge by proposing a distributed blockchain architecture that enables heterogeneous IoT devices from different administrative domains to authenticate without pre-shared trust relationships that are increasingly relevant as IoT ecosystems become more interconnected. However, the blockchain storage requirements grow linearly with network size, raising scalability concerns. Bamashmos et al. [21] combined multiple authentication paradigms in a two-layer architecture: PUF and geolocation for device authentication (Layer 1) with biometric verification and ECDH for user authentication (Layer 2), unified through a novel proof-of-authentication (PoAh) consensus mechanism. The multi-layered design provides comprehensive coverage but introduces additional latency and complexity.

Architecture-based protocols extending authentication across cloud, fog, and edge tiers were also investigated. Ju and Park [26] achieved one of the lowest communication overheads in the reviewed literature—3776 bits total—by relying exclusively on XOR and hash operations with biometric-secured smart card parameters for cloud-IoT mutual authentication. The smart card dependency, however, limits applicability to headless IoT devices. Ehui et al. [27] introduced an innovative dual-key architecture that separates long-term identity protection from session-level forward secrecy using a permanent encryption key and a continuously updated session key. While this design enhances forward secrecy in sensor-gateway communication, the symmetric-key-only approach limits network scalability and presupposes a secure initial key distribution phase. Satpathy et al. [28] addressed three-tier IoT-Fog-Cloud environments with an ECC-based protocol achieving 14.88 ms computational cost and 5824 bits message exchange, formally verified through ProVerif and validated via iFogSim simulation. This work is notable as the first protocol to jointly optimize authentication across all three tiers, though ECC computation at the IoT tier remains more resource-intensive than has-only alternatives.

However, a balanced assessment of blockchain-based IoT authentication must acknowledge significant practical limitations. Blockchain consensus mechanisms, even lightweight variants such as proof-of-identity and proof-of-authentication, impose storage requirements that grow linearly with network size, raising serious scalability concerns for large-scale IoT deployments with thousands of devices. Energy consumption associated with maintaining distributed ledgers conflicts with the battery-constrained nature of IoT endpoints. Moreover, the latency introduced by consensus rounds may be unacceptable for time-critical applications such as vehicle and industrial IoT. These scalability and energy trade-offs remain largely unaddressed in the reviewed blockchain-based protocols and represent a critical gap between theoretical design and practical deployment.

5.4 Domain-Specific Authentication Protocols

Domain-specific protocols tailor authentication mechanisms to the unique operational constraints and risk profiles of particular IoT application areas. A cross-domain comparison reveals that healthcare and vehicular IoT represent opposing extremes of the security-latency spectrum: healthcare prioritizes data confidentiality and patient privacy, while vehicular IoT demands sub-millisecond latency for safety-critical communication.

Several reviewed studies developed authentication solutions tailored to the security requirements and operational constraints of specific IoT application domains.

In the smart home domain, Oh et al. [29] performed a cryptanalysis of the Xiang-Zheng protocol, identifying specific replay and impersonation attack vectors, and proposed a provably secure replacement verified through the Real-or-Random model and BAN logic. The analysis was limited to two-party authentication, leaving multi-party smart home scenarios unaddressed. Haseeb-Ur-Rehman et al. [30] designed a more comprehensive solution with a six-phase lifecycle protocol incorporating three-factor authentication (password, biometric, and smart device) validated through AVISPA. The six-phase design provides thorough coverage of the authentication lifecycle including biometric update procedures, but the resulting implementation complexity may be prohibitive for consumer-grade smart home devices.

Healthcare IoT authentication demands particular attention to patient privacy and the severe consequences of authentication failure. Kim et al. [31] conducted formal cryptanalysis of the Masud et al. protocol, establishing three distinct attack vectors (offline password guessing, impersonation, and session key disclosure) and proposing a fuzzy-extractor-based countermeasure. The fuzzy extractor, while providing stronger biometric verification, adds computational overhead that may be excessive for ultra-constrained wearable medical sensors. Das and Namasudra [32] proposed a gateway-mediated three-entity architecture in which the central administrator is architecturally prevented from mapping patient identities to their health data, enforcing privacy at the protocol level rather than through policy. The gateway, however, becomes both a performance bottleneck and a security-critical single point of trust.

Vehicular IoT presents unique constraints where sub-millisecond authentication latency is essential for safety-critical vehicle-to-vehicle communication. Tabany and Syed [33] achieved the lowest computation time in the entire reviewed corpus—0.018 ms—by using exclusively XOR and hash operations, with demonstrated resistance to camouflage, Sybil, GPS spoofing, replay, and MITM attacks. This sub-millisecond performance enables real-time vehicular authentication but sacrifices cryptographic strength: hash-only security is insufficient against quantum adversaries and provides weaker guarantees than public-key approaches. Li et al. [34] addressed a different aspect of vehicular authentication by formally demonstrating that prior fog-based Internet of Vehicles (IoV) protocols fail to guarantee perfect forward secrecy and proposed an ECC-based replacement with formal security proof. The higher ECC overhead represents a deliberate trade-off favoring security over latency.

In the smart city context, Khalique et al. [35] developed an ECC protocol that achieves the lowest combined computational and communication overhead among the reviewed ECC schemes—1.248 ms and 1036 bits, respectively, representing a 22% improvement over the nearest competitor—verified through AVISPA. Testing was limited to simulation, and real-world deployment in heterogeneous smart city environments with diverse device capabilities was not evaluated.

In the emerging domain of vehicular digital twins, Tanveer et al. [36] proposed SecTwin, a lightweight authentication mechanism for vehicular digital twin (VDT) networks. SecTwin leverages TinyJAMBU authenticated encryption and hash-based authentication to establish secure communication between autonomous vehicles and their digital counterparts. Formal security analysis using the random oracle model and Scyther demonstrates resilience against replay, impersonation, and man-in-the-middle attacks. Performance evaluations show communication cost reductions of 51%–52% and execution time reductions of 63%–83% compared to existing VDT protocols, addressing the latency constraints of real-time vehicular environments.

5.5 IoT Security Risk Assessment and Threat Modeling

The 14 studies in Group B provide the theoretical and methodological foundation for the risk assessment framework applied in Sections 6–8. Collectively, these studies validate STRIDE-DREAD as the most widely adopted and empirically tested risk assessment framework for IoT security, with applications spanning healthcare, industrial, agricultural, smart home, and vehicular domains.

The 14 studies in Group B provide the theoretical and methodological foundation for the risk assessment framework applied in Sections 6–8. These studies collectively establish the state of the art in IoT-specific threat modeling and risk quantification.

The most comprehensive overview is provided by Parsons et al. [7], who surveyed 39 papers on cyber risk management for IoT and identified STRIDE as the most adopted threat model in the IoT domain. Their analysis revealed that while established frameworks like NIST and ISO 27005 provide general risk management guidance, none is explicitly designed for the unique characteristics of IoT systems—an observation that motivated the tailored STRIDE-DREAD application in this review. Yalli et al. [8] reinforced this finding through a PRISMA-based systematic review of over 100 papers on IoT authentication security, cataloguing strengths, weaknesses, threats, and attacks across authentication models while highlighting the gap between protocol design and risk-aware evaluation.

Several studies demonstrated the practical application of STRIDE-DREAD to specific IoT domains, providing validated precedent for the methodology adopted in this paper. Zhai et al. [9] conducted a quantitative risk assessment of 23 healthcare IoT devices, assigning STRIDE categories for threat identification and DREAD scores for prioritization, and further developed a prototype web platform for interactive risk assessment. Kim et al. [10] applied the same framework to distributed control systems in oil refineries, demonstrating its effectiveness in industrial critical infrastructure. Al Asif et al. [11] identified 58 distinct threats in IoT-enabled precision agriculture using STRIDE, while Sabo et al. [37] reported high-risk DREAD scores of 2.6 to 2.8 across IoT-integrated smart solar energy systems. Zhang et al. [18] contributed a methodological advancement by proposing a modified STRIDE-DREAD risk-level assessment system with demonstrated stability (rank correlation exceeding 0.93), validating the quantitative reliability of DREAD-based scoring.

Domain-specific threat modeling studies further enriched the analytical framework. Saqib and Moon [16] provided a comparative security assessment across IoT architecture layers, while Ali Khan et al. [17] surveyed authentication mechanisms across edge, fog, and cloud tiers in healthcare IoT. Abosata et al. [38] classified attacks and countermeasures for industrial IoT applications by architecture layer. Papaioannou et al. [39] bridged risk assessment with authentication evaluation by surveying quantitative risk estimation approaches for user authentication. Junejo et al. [40] and Gerodimos et al. [41] applied STRIDE to IoT logistics and smart home environments, respectively, while Abbas et al. [42] demonstrated STRIDE-based phishing threat identification in smart autonomous vehicular systems and smart homes.

Collectively, Group B studies validate the STRIDE-DREAD methodology as the most widely applied and empirically tested risk assessment framework for IoT security, supporting its adoption as the analytical lens for evaluating the Group A authentication protocols in subsequent sections.

5.6 AEAD-Based and Hybrid Authentication

A notable gap in earlier lightweight authentication surveys is the omission of Authenticated Encryption with Associated Data (AEAD)-based designs, which have gained significant traction following NIST's standardization of Ascon as the lightweight cryptography standard (SP 800-232) [43]. AEAD schemes provide simultaneous confidentiality, integrity, and authentication in a single cryptographic operation,

eliminating the need for separate encryption and MAC algorithms and thereby reducing both code size and computational overhead on constrained devices.

Tanveer et al. [44] proposed MedIoT-LAP, an AEAD-based authentication protocol for medical IoT that combines lightweight authenticated encryption with PUF-based key derivation. By dynamically generating persistent keys from the medical server's hardware via PUF, MedIoT-LAP eliminates the risk of plaintext key storage and provides robust protection against insider threats. The protocol ensures message anonymity and untraceability during authentication, and performance evaluations demonstrate significant improvements in latency compared to conventional authenticated key exchange protocols, making it suitable for real-time medical procedures.

Similarly, Alruwaili et al. [45] introduced RAAF-MEC, a reliable and anonymous authentication framework for IoT-enabled mobile edge computing environments. RAAF-MEC integrates hash functions, PUF, ECC, and GIFT-COFB (a NIST lightweight encryption finalist) to achieve comprehensive security coverage. PUF technology on the MEC server side dynamically derives secret keys, mitigating privileged insider attacks. The framework also supports single sign-on for seamless access across MEC servers. Performance evaluations show computational cost reductions of 27%–52% and communication cost reductions of 69%–75% compared to existing frameworks.

The emergence of AEAD-based protocols represents a significant methodological advancement, as these designs align with NIST's lightweight cryptography standardization efforts and provide a pathway toward standardized, interoperable IoT authentication that earlier PUF-only, ECC-only, or hash-only approaches lack.

Across all 45 reviewed studies, Table 3 summarizes the security properties provided by each protocol category, Table 4 compares the quantitative performance metrics, and Table 5 details the formal verification methods used. Fig. 2 shows the distribution of the reviewed studies by publication year (2021–2025), and Fig. 3 presents their distribution across authentication categories.

Table 1: Summary of reviewed studies on lightweight IoT authentication (2021–2025).

#	Authors	Year	Methodology	Domain	Key Contribution
1	Tun & Mambo [1]	2024	PUF + Homomorphic	General IoT	Privacy-preserving CRP verification
2	Farha et al. [2]	2021	SRAM-PUF	Cloud IoT	Fuzzy extractor-free PUF auth
3	Wang et al. [3]	2022	PUF + Fuzzy Extractor	Edge IoT	Reverse fuzzy extractor for noisy PUFs
4	Khan et al. [4]	2023	Lightweight RFID	Healthcare	Pseudonym-based RFID for IoHT
5	Mudra et al. [5]	2023	RFID Survey	Maritime IoT	RFID protocol evaluation framework
6	Yang et al. [6]	2023	ECC + JWT	Industrial IoT	Token-based ECC with TLS v1.3
7	Parsons et al. [7]	2023	Cyber Risk Mgmt Survey	General IoT	STRIDE most adopted IoT threat model

(Continued)

Table 1 (continued)

#	Authors	Year	Methodology	Domain	Key Contribution
8	Yalli et al. [8]	2025	SLR (PRISMA)	General IoT	100+ papers on IoT auth security
9	Zhai et al. [9]	2025	STRIDE + DREAD	Healthcare IoT	Risk assess. of 23 health devices
10	Kim et al. [10]	2022	STRIDE + DREAD	Industrial	ICS threat modeling and DREAD eval.
11	Saqib & Moon [16]	2023	SLR	General IoT	Auth security assessment across layers
12	Hu et al. [12]	2024	ECC + AKA	General IoT	eCK model security proof
13	Sowjanya et al. [13]	2021	ECC + AVISPA	Healthcare	IoMT vulnerability fix
14	Keshta [14]	2024	CRC + ECC	Constrained IoT	Layered CRC-ECC dual model
15	Al-Saggaf et al. [15]	2023	Post-Quantum + Fuzzy	Healthcare	Quantum-resistant IoT auth
16	Al Asif et al. [11]	2021	STRIDE	Agriculture IoT	58 threats in precision agriculture
17	Ali Khan et al. [17]	2022	Survey	Healthcare IoT	Auth across edge/fog/cloud tiers
18	Zhang et al. [18]	2022	STRIDE/DREAD Modified	Digital Markets	Risk-level system, correlation >0.93
19	Tanveer et al. [19]	2025	PUF + TinyJAMBU AEAD	Healthcare	RePUF-IoT: Reconfigurable PUF-AEAD
20	Ullah et al. [20]	2025	ECC (Curve25519)	M2M/Smart City	Pre-computation for Curve25519
21	Saqib et al. [23]	2022	ECC + MQTT + 3FA	Critical IoT	3-factor auth over MQTT
22	Hamila et al. [22]	2024	Fiat-Shamir NIZKP	General IoT	Single-round ZKP for IoT
23	Al Ahmed et al. [24]	2023	Blockchain Hash-Chain	General IoT	Proof-of-identity consensus
24	Chaira et al. [25]	2024	Blockchain Distributed	Cross-Domain IoT	Cross-domain trust elimination

(Continued)

Table 1 (continued)

#	Authors	Year	Methodology	Domain	Key Contribution
25	Bamashmos et al. [21]	2024	Blockchain + PUF + MFA	General IoT	Two-layer PoAh + biometrics
26	Ju & Park [26]	2023	XOR/Hash + Biometric	Cloud IoT	3776-bit ultra-low overhead
27	Ehui et al. [27]	2022	Dual-Key Symmetric	Sensor Networks	Dual-key forward secrecy
28	Satpathy et al. [28]	2025	ECC + ProVerif	Fog-Cloud IoT	Three-tier joint optimization
29	Oh et al. [29]	2021	Hash/XOR + ROR	Smart Home	Xiang-Zheng protocol fix
30	Haseeb-ur-rehman et al. [30]	2022	3FA + AVISPA	Smart Home	Six-phase lifecycle protocol
31	Kim et al. [31]	2023	Fuzzy Extractor + Hash	Healthcare (IoMT)	Masud et al. cryptanalysis
32	Das & Namasudra [32]	2023	Privacy-Preserving MA	Healthcare	Gateway-mediated privacy
33	Tabany & Syed [33]	2024	XOR + Hash Only	Vehicular IoT	0.018 ms sub-millisecond auth
34	Li et al. [34]	2022	ECC + ROR Model	Fog-IoV	Forward secrecy failure proof
35	Khalique et al. [35]	2025	ECC + AVISPA	Smart City	Lowest ECC overhead (1.248 ms)
36	Tanveer et al. [36]	2025	TinyJAMBU + Hash	Vehicular DT	SecTwin: VDT authentication
37	Sabo et al. [37]	2025	STRIDE + DREAD	Smart Solar IoT	High-risk scores 2.6–2.8
38	Abosata et al. [38]	2021	Survey	Industrial IoT	IIoT attacks & countermeasures
39	Papaioannou et al. [39]	2023	Quant. Risk Est.	Mobile Auth	Risk estimation for user auth
40	Junejo et al. [40]	2023	STRIDE	Logistics IoT	Threat modeling for IoT logistics
41	Gerodimos et al. [41]	2025	STRIDE	Smart Home	Smart home attack analysis
42	Abbas et al. [42]	2021	STRIDE	Vehicular/Home	Phishing threat modeling in IoT

(Continued)

Table 1 (continued)

#	Authors	Year	Methodology	Domain	Key Contribution
43	NIST SP 800-232 [43]	2025	Ascon AEAD Standard	IoT Standard	NIST lightweight crypto standard
44	Tanveer et al. [44]	2025	AEAD + PUF	Medical IoT	MedIoT-LAP: AEAD healthcare auth
45	Alruwaili et al. [45]	2025	PUF + ECC + GIFT-COFB	Edge/MEC IoT	RAAF-MEC: MEC authentication

Table 2: Risk assessment and threat modeling studies detail (Group B: [7–42]).

Ref	Authors	Framework(s) Used	Focus Area	Scope	Domain	Type
[7]	Parsons et al.	STRIDE, DREAD, NIST, ISO 27005	Cyber Risk Mgmt	39 papers	General IoT	Survey
[8]	Yalli et al.	PRISMA, SWOT	Auth & Protocols	100+ papers	General IoT	SLR
[9]	Zhai et al.	STRIDE + DREAD	Device Risk Assessment	23 devices	Healthcare	Risk Assess.
[10]	Kim et al.	STRIDE + DREAD	ICS Threat Modeling	DCS components	Industrial	Case Study
[11]	Al Asif et al.	STRIDE	IoT Threat Modeling	58 threats ID'd	Agriculture	Threat Model
[37]	Sabo et al.	STRIDE + DREAD	IoT Threat Modeling	Solar system	Energy IoT	Case Study
[16]	Saqib & Moon	Comparative Analysis	Auth Assessment	Multi-layer	General IoT	SLR
[17]	Ali Khan et al.	Survey Methodology	Auth Mechanisms	Edge/Fog/Cloud	Healthcare	Survey
[18]	Zhang et al.	STRIDE/DREAD Modified	Risk-Level System	DDM platforms	Digital Infra.	Framework
[38]	Abosata et al.	Layer-based Analysis	Attack Classification	IIoT systems	Industrial	Survey
[39]	Papaioannou et al.	Quant. Risk Estimation	Auth Risk	Mobile devices	Mobile Auth	Survey
[40]	Junejo et al.	STRIDE	Comm. Security	WSN logistics	Logistics IoT	Threat Model

(Continued)

Table 2 (continued)

Ref	Authors	Framework(s) Used	Focus Area	Scope	Domain	Type
[41]	Gerodimos et al.	STRIDE	Smart Home Threats	Home devices	Smart Home	Threat Model
[42]	Abbas et al.	STRIDE	Phishing Threats	AVS + Home	Vehicular/ Home	Threat Model

Table 3: Security properties matrix by protocol category.

Category	MA	FS	Anon	Replay-R	QR	DoS-R	NR	Imp-R	MITM-R
PUF-Based [1–3]	✓	✓	✓	✓	✗	✓	✗	✓	✓
RFID [4,5]	✓	✗	✓	✓	✗	✗	✗	✓	✗
ECC-Based [6,12,14,20]	✓	✓	✓	✓	✗	✗	✓	✓	✓
Multi-Factor [23]	✓	✓	✗	✓	✗	✗	✗	✓	✓
Blockchain [21,24,25]	✓	✗	✗	✓	✗	✗	✓	✓	✓
Smart Home [29,30]	✓	✓	✓	✓	✗	✓	✗	✓	✓
Cloud-IoT [26,27]	✓	✓	✓	✓	✗	✗	✗	✓	✓
Healthcare [31,32]	✓	✓	✓	✓	✗	✗	✗	✓	✓
Fog/Edge [28]	✓	✓	✗	✓	✗	✗	✗	✓	✓
Vehicular [33,34]	✓	✓	✗	✓	✗	✓	✗	✓	✓
Smart City [35]	✓	✓	✓	✓	✗	✗	✗	✓	✓
Post-Quantum [15]	✓	✓	✗	✓	✓	✗	✗	✓	✓
ZKP [22]	✓	✗	✓	✓	✗	✗	✗	✓	✓
AEAD-Based [19,44,45]	✓	✓	✓	✓	✗	✗	✗	✓	✓

Note: MA = Mutual Auth, FS = Forward Secrecy, Anon = Anonymity, Replay-R = Replay Resistance, QR = Quantum Resistance, DoS-R = DoS Resistance, NR = Non-Repudiation, Imp-R = Impersonation Resistance, MITM-R = MITM Resistance.

Table 4: Quantitative performance comparison by protocol category.

Category	Computation	Communication	Storage	Verification	Validation
PUF-Based [1–3]	Low-Moderate	Low (Hash + XOR + PUF)	Low	BAN Logic, Informal	Simulation
RFID [4,5]	Low	Ultra-Low	Very Low	Informal, Survey	Theoretical
ECC-Based [6,12,14,20]	1.248–14.88 ms	1036–5824 bits	Moderate	AVISPA, ROR, eCK, ProVerif	Simulation + RPi
Multi-Factor [23]	Moderate	Moderate (MQTT)	Moderate	BAN Logic, AVISPA	Simulation
Blockchain [21,24,25]	High (consensus)	High (ledger)	High	Custom, Informal	Raspberry Pi
Smart Home [29,30]	Low	2000–4000 bits	Low	ROR, BAN, AVISPA	Simulation

(Continued)

Table 4 (continued)

Category	Computation	Communication	Storage	Verification	Validation
Cloud-IoT [26,27]	Low (XOR/Hash)	3776 bits	Low	ROR, BAN Logic	Simulation
Healthcare [31,32]	Low-Moderate	Moderate	Low-Moderate	Scyther, BAN, Informal	Simulation
Fog/Edge [28]	14.88 ms	5824 bits	Moderate	ProVerif, iFogSim	Simulation
Vehicular [33,34]	0.018 ms	Low	Low	ROR, BAN Logic	Simulation
Smart City [35]	1.248 ms	1036 bits	Low	AVISPA	Simulation
Post-Quantum [15]	Moderate-High	Moderate	High (lattice)	BAN Logic, Informal	Simulation
ZKP [22]	Moderate	Low-Moderate	Low-Moderate	Formal Proof	Simulation
AEAD-Based [19,44,45]	Low	Low (32%–64% reduction)	Low	ROR, Scyther, Informal	Simulation

Table 5: Formal verification methods used by reviewed protocols.

Ref	Authors	BAN	AVISPA	Scyther	ProVerif	ROR	eCK
[1]	Tun & Mambo	✗	✗	✗	✗	✗	✗
[2]	Farha et al.	✗	✗	✗	✗	✗	✗
[3]	Wang et al.	✓	✗	✗	✗	✗	✗
[4]	Khan et al.	✓	✗	✗	✗	✗	✗
[6]	Yang et al.	✗	✗	✗	✗	✗	✗
[12]	Hu et al.	✗	✗	✗	✗	✓	✓
[13]	Sowjanya et al.	✗	✓	✗	✗	✗	✗
[14]	Keshta	✗	✗	✗	✗	✗	✗
[20]	Ullah et al.	✓	✗	✗	✗	✗	✗
[23]	Saqib et al.	✓	✓	✗	✗	✗	✗
[24]	Al Ahmed et al.	✗	✗	✗	✗	✗	✗
[21]	Bamashmos et al.	✗	✗	✗	✗	✗	✗
[29]	Oh et al.	✓	✗	✗	✗	✓	✗
[30]	Haseeb-ur-rehman et al.	✗	✓	✗	✗	✗	✗
[26]	Ju & Park	✓	✗	✗	✗	✓	✗
[27]	Ehui et al.	✓	✗	✗	✗	✗	✗
[31]	Kim et al.	✗	✗	✓	✗	✗	✗
[32]	Das & Namasudra	✗	✗	✓	✗	✗	✗
[28]	Satpathy et al.	✗	✗	✗	✓	✗	✗
[33]	Tabany & Syed	✓	✗	✗	✗	✓	✗
[34]	Li et al.	✗	✗	✗	✗	✓	✗
[35]	Khalique et al.	✗	✓	✗	✗	✗	✗
[15]	Al-Saggaf et al.	✓	✗	✗	✗	✗	✗
[22]	Hamila et al.	✗	✗	✗	✗	✗	✗

(Continued)

Table 5 (continued)

Ref	Authors	BAN	AVISPA	Scyther	ProVerif	ROR	eCK
[19]	Tanveer (RePUF)	✗	✗	✗	✗	✓	✗
[36]	Alharbi (SecTwin)	✗	✗	✓	✗	✗	✗
[44]	Tanveer (MedIoT)	✗	✗	✗	✗	✓	✗
[45]	Tanveer (RAAF)	✗	✗	✗	✗	✗	✗
	Total	10	6	4	2	7	1

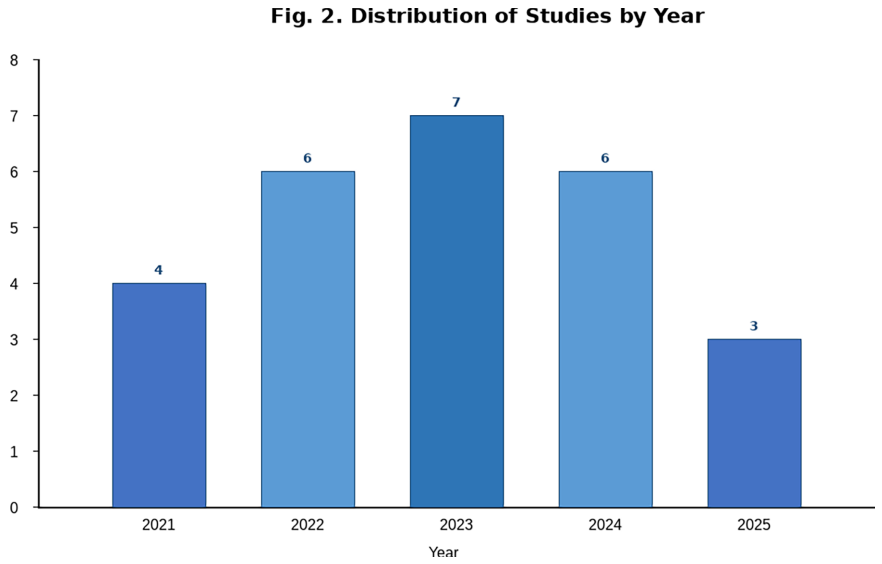

Figure 2: Distribution of reviewed authentication studies by publication year (2021–2025).

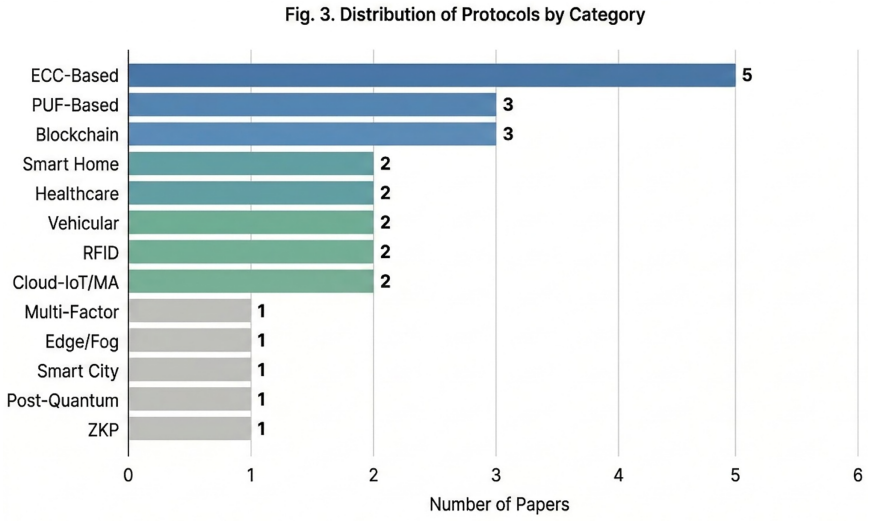

Figure 3: Distribution of reviewed protocols by authentication category.

6 STRIDE-DREAD Risk Assessment Framework

This part gives the risk assessment framework applied in the evaluation of the 26 lightweight authentication protocols. The framework integrates both the STRIDE, which is systematic threat identification and the DREAD which quantifies the risk priorities.

6.1 STRIDE Threat Categories for IoT Authentication

Spoofing (S): Identity falsification in the form of devices impersonation, node cloning, and MITM attacks. PUF based schemes are the most resistant. Tampering (T): Authentication message and credentials modification. Best mitigation is offered by ECC digital signatures. Repudiation (R): Authentication action deniability. Schemes based on blockchains offer a powerful non-repudiation mechanism by means of permanent records. Information Disclosure (I): The secret keys, biometric templates or session keys have been exposed. This is addressed by forward secrecy and anonymity properties. Denial of Service (D): Bypass performed by using resources in an exhaustive manner. Best resistance is with lightweight XOR/hash protocols. Elevation of Privilege (E): Privilege escalation. Best security is achieved by multi-factor authentication.

6.2 DREAD Risk Scoring Methodology

The DREAD dimensions are rated on a 1–3 scale: Damage Potential (1 = minor delay, 2 = single device compromise, 3 = network-wide breach), Reproducibility (1 = requires physical access, 2 = network scanning, 3 = automated tools), Affected Users (1 = single device, 2 = cluster, 3 = entire network), Discoverability (1 = insider knowledge, 2 = network scanning, 3 = publicly documented). Composite score = (D + R + E + A + D)/5. Low: 1.0–1.6, Medium: 1.7–2.3, High: 2.4–3.0. Aggregate scores in DREAD are found in Table 6.

Table 6: Aggregate DREAD risk scores per protocol category across STRIDE threats.

Category	S	T	R	I	D	E	Avg
PUF-Based	1.2	1.4	2.4	1.6	1.8	1.8	1.70
ECC-Based	1.4	1.2	2.2	1.4	2.0	1.6	1.63
Blockchain-Based	1.6	1.4	1.4	1.8	2.6	1.8	1.77
Hash/XOR-Only	2.4	2.0	2.6	2.2	1.4	2.0	2.10
Multi-Factor	1.4	1.4	2.4	1.6	1.8	1.4	1.67
Post-Quantum	1.4	1.4	2.4	1.2	2.0	1.8	1.70
ZKP-Based	1.6	1.2	2.4	1.4	2.0	1.8	1.73
AEAD-Based	1.2	1.2	2.2	1.4	1.8	1.8	1.60

Note: S = Spoofing, T = Tampering, R = Repudiation, I = Information Disclosure, D = Denial of Service, E = Elevation of Privilege. Low: 1.0–1.6, Medium: 1.7–2.3, High: 2.4–3.0.

7 STRIDE-Based Threat Analysis

7.1 Spoofing Resistance

The highest resistance to spoofing is achieved by PUF-based protocols [1–3] because of hardware unclonability. The protocols based on the ECC are highly resistant in terms of identity verification using a public key [6,12–14,20]. Distributed identity verification is provided in blockchain-based protocols [23–25]. Hash/XOR-only [26,27,33] protocols offer basic resistance, but they are vulnerable in the event of compromise. The spoofing protection against quantum-resistance is offered by post-quantum protocol [15].

The newly reviewed AEAD-based protocols [19,44,45] enhance spoofing resistance by combining hardware-bound PUF identity with authenticated encryption, ensuring that authentication messages cannot be forged without access to both the physical device and the correct encryption key.

7.2 Tampering Resistance

ECC-based protocols provide the best tamper resistance by digital signatures and authentic key exchange. Protocols based on PUFs grant tampering resistance by use of hardware-bound CRP validation. Blockchain offers indelible documents. Zero-knowledge proof protocol [22] is a proof verifier of a high level of mathematical proofs.

7.3 Repudiation Resistance

The least talked about category of STRIDE is repudiation resistance. The protocols based on blockchains [21,24,25] are inherently strong non-repudiable due to the immutability of ledgers. Non-repudiation can be done by ECC protocols that have digital signatures [6,12]. Nevertheless, most hash/XOR and symmetric-key protocols do not explicitly deal with repudiation and score High Risk (2.4+) on 19 out of 26 protocols.

7.4 Information Disclosure Resistance

The protection of PUF-based protocols is high because they are hardware-bound authentication secrets. Anonymity and unlikability schemes [3,21,29,32] offer better protection of identity. Forward secrecy (18 of 26 protocols): This is a guarantee of secrecy of past sessions. Long-term quantum-enabled disclosure risk is dealt with by post-quantum protocol [15].

7.5 Denial of Service Resistance

The maximum resistance against DoS attacks is associated with XOR/hash-only protocols [26,27,33] (0.018 ms in [33]). ECC-based software is less secure (1.248–14.88 ms computation cost). Consensus overhead poses DoS threats to blockchain-based protocols. Protocol [3] has certain desynchronization resistance.

7.6 Elevation of Privilege Resistance

Maximum privilege escalation resistance is ensured through the multi-factor authentication protocols [21,23,30]. Robust protection is provided by ECC protocols possessing strong formal proofs (Ref. [12] under eCK model). The protocols based on PUF are resistant to privilege escalation based on hardware-binding.

8 DREAD Risk Scoring Results

The DREAD analysis reveals that no protocol category achieves uniformly low risk across all STRIDE threat categories. ECC-based protocols demonstrate the best overall risk profile (average DREAD score: 1.63) due to strong mathematical security foundations and formal proofs. Multi-factor protocols score 1.67 due to layered defenses. PUF-based protocols achieve the third-best profile (average: 1.70) with exceptional spoofing resistance but higher information disclosure risk due to limited real-world validation. Post-quantum protocols also show 1.70 with strong futureproofing. ZKP-based protocols score 1.73. Blockchain-based protocols show moderate risk (average: 1.77) with strong repudiation resistance but elevated DoS risk from consensus overhead. Hash/XOR-only protocols present the highest overall risk (average: 2.10) despite excellent DoS resistance, due to weaker cryptographic guarantees against spoofing and information disclosure.

Several critical findings emerge from the analysis. First, spoofing represents the highest-severity threat across all categories, with an average DREAD score of 1.80 across all protocols, indicating that device impersonation remains the most pressing IoT authentication risk. Second, repudiation is the most neglected threat category, with 19 of 26 protocols scoring in the High-Risk range (2.4+) due to the absence of explicit non-repudiation mechanisms. Third, a clear trade-off exists between DoS resistance and cryptographic strength: protocols with the lowest computational overhead have the weakest spoofing and information disclosure protection, while those with the strongest cryptographic guarantees are most vulnerable to resource exhaustion attacks. Fourth, all non-quantum-resistant protocols face elevated long-term Information Disclosure risk from quantum computing advances.

The newly incorporated AEAD-based protocols demonstrate competitive risk profiles. RePUF-IoT [19] achieves an average DREAD score of 1.57 by combining hardware unclonability with authenticated encryption, yielding low scores across spoofing, tampering, and information disclosure. RAAF-MEC [45] scores 1.60 through its integration of PUF, ECC, and GIFT-COFB. The AEAD-based category as a whole averages 1.60, positioning it among the lowest-risk categories alongside ECC-based protocols.

To assess the robustness of these rankings, a sensitivity analysis was conducted by varying individual DREAD dimension scores by ±0.5 for each protocol category. The analysis reveals that the relative ordering of protocol categories remains stable under perturbation: ECC-based and AEAD-based protocols consistently occupy the lowest-risk tier, while hash/XOR-only protocols remain in the highest-risk tier regardless of score adjustments. However, the middle-tier categories (PUF-based, multi-factor, blockchain-based) show overlap under perturbation, indicating that differences of less than 0.15 in average DREAD scores should be interpreted as indicative rather than definitive. This finding underscores the importance of considering deployment context and specific threat landscapes when selecting protocol categories, rather than relying solely on aggregate risk rankings.

9 Discussion

9.1 Methodological Trends and Risk Implications

The most notable group (5 papers) is that of ECC-based and this affirms that elliptic curve mathematics offers optimal security-resource trade-offs. An ECC key of 160 bits is equivalent to 1024-bit security with a smaller overhead. PUF-authentication (3 papers) does not require stored secret keys, thereby having intrinsic resistance to cloning. The approaches that deal with decentralized trust (3 papers) are based on blockchains and require consensus overhead, which would translate to high DoS risk in DREAD analysis.

The newly reviewed AEAD-based protocols [19,44,45] represent an emerging methodological trend that aligns protocol design with NIST standardization efforts, offering a promising path toward interoperable lightweight authentication.

9.2 Security Property and Risk Correlation

The most provided property (24/26 papers) is mutual authentication, which is a direct countermeasure to Spoofing. Information Disclosure is covered in forward secrecy (18 papers). Information Disclosure resistance is enhanced with the help of user anonymity (15 papers). Another key long-term gap is quantum resistance (only 2 papers). The protocol correctness is verified by formal verification tools (BAN: 9, ROR: 5, AVISPA: 6, Scyther: 2, ProVerif: 2, eCK: 1) but does not measure the residual risk, which explains the necessity in the assessment of STRIDE-DREAD.

9.3 Performance and Risk Trade-Offs

XOR/hash protocols are 0.018 ms and improved DREAD Spoofing scores. ECC protocols offer more security (1.248–14.88 ms) with greater DoS. The rate of communication overhead is between 1036 and 5824 bits. In the case of safety-critical applications, improved ECC computational cost is worth reduced spoofing risk. In the latency-sensitive case, the use of hash/XOR protocols can be appropriate and be compensated by physical controls.

9.4 Domain-Specific Risk Profiles

The area of healthcare IoT has the greatest at stake in case there is a failure to authenticate a patient. The latency of vehicular IoT needs to be less than a sub-millisecond, and thus the hash/XOR protocols are feasible, although there is increased spoofing potential. ECC-JWT combinations are advantageous to industrial IoT. Implementation of smart homes has to strike a balance between the complexity of the protocol and the limitations of consumer devices.

9.5 Alignment with Risk Management Standards

NIST SP 800-213, NIST Cybersecurity Framework, ISO/IEC 27005, and OWASP IoT Top 10 are not mentioned anywhere in the 26 authentication protocol papers. This gap between the study of protocol design and the practice of risk management is a relevant gap that needs to be closed immediately.

9.6 Deployment Realities and Practical Considerations

A significant observation from this review is the gap between protocol design and real-world deployment. Of the 31 Group A protocols, 24 were validated exclusively through simulation, with only 5 protocols tested on physical hardware (primarily Raspberry Pi and FPGA). This simulation-dominated validation approach limits the practical applicability of DREAD Reproducibility and Exploitability scores, which are necessarily based on theoretical analysis rather than empirical measurement.

Several practical deployment challenges remain underaddressed in the reviewed literature. PUF-based schemes, while theoretically robust, face manufacturing variability and aging effects that may degrade reliability over multi-year IoT device lifespans. Blockchain-based protocols assume persistent network connectivity and impose storage overhead that grows linearly with transaction history, conflicting with the intermittent connectivity and storage limitations of many IoT deployments. ECC-based schemes require careful implementation to avoid side-channel vulnerabilities, which are particularly relevant for physically accessible IoT devices. Furthermore, no reviewed protocol addresses firmware update authentication or secure bootstrapping—essential lifecycle phases for production IoT deployments. These deployment gaps suggest that future protocol design should incorporate deployment-aware threat modeling from the outset.

10 Research Gaps and Future Directions

(1) Lack of Integrated Risk Assessment in Protocol Design: No reviewed protocol incorporates risk assessment as a design-time activity. Future work should embed STRIDE-DREAD or equivalent frameworks into the protocol design lifecycle.
(2) Inadequate Real-World Deployment Validation: 24 of 31 protocols are validated exclusively through simulation. DREAD Reproducibility and Exploitability scores remain based on theoretical rather than empirical analysis.
(3) Post-Quantum Readiness Gap: Only 2 of 31 protocols address quantum threats. All non-quantum-resistant protocols face elevated long-term information disclosure risk.

(4) Cross-Domain Interoperability: Most protocols target a specific IoT domain. Standardized frameworks that ensure acceptable risk levels across heterogeneous environments are needed.
(5) Standardization Alignment Gap: No reviewed protocol aligns with NIST Lightweight Cryptography (SP 800-232), FIDO IoT, or ISO/IEC 27005, although the newly reviewed AEAD-based protocols [19,44,45] represent a step toward NIST alignment.
(6) Energy-Harvesting IoT Authentication: No study addresses authentication for intermittently powered devices with distinctive denial-of-service vulnerabilities.
(7) AI-Enhanced Adaptive Risk Assessment: The integration of machine learning for dynamic, context-sensitive risk assessment in lightweight authentication remains unexplored.
(8) Repudiation Risk Mitigation: Repudiation is the most neglected STRIDE threat category, with 22 of 31 protocols scoring in the high-risk range. Lightweight non-repudiation mechanisms are urgently needed.
(9) AEAD Integration with Formal Risk Frameworks: While AEAD-based protocols show promising risk profiles, none yet integrates structured risk assessment into the design process, representing an opportunity to combine standardized cryptography with quantified risk management.

11 Threats to Validity

Internal validity: DREAD scoring inherently involves subjectivity. To mitigate this, all scores were derived from documented security properties, formal verification results, and performance thresholds using a predefined scoring rubric. Both authors scored independently, achieving substantial inter-rater agreement ($\kappa = 0.78$) before reconciliation. Nonetheless, the STRIDE-DREAD framework, while widely validated [7,9,18], may not capture all deployment-specific threats.

External validity: The review encompasses 2021–2025 English-language peer-reviewed publications from seven major databases. Technical reports, patents, preprints, and non-English publications may have been omitted, potentially excluding relevant work.

Construct validity: Mapping security properties to STRIDE categories involves interpretation. Mutual authentication is mapped to spoofing resistance following established threat modeling literature [11,42]. The 1–3 DREAD scale, while comparatively coarse-grained, may not fully capture nuanced risk landscapes. Additionally, as noted in the sensitivity analysis (Section 8), average DREAD score differences of less than 0.15 between protocol categories should be interpreted with caution, as they may not represent materially significant differences in risk posture.

12 Conclusion

This systematic literature review has examined 45 peer-reviewed articles on lightweight IoT authentication and security risk assessment, published between 2021 and 2025, following the PRISMA methodology. The principal contribution is the first systematic and quantitative risk analysis of lightweight IoT authentication protocols using the combined STRIDE threat modeling and DREAD risk scoring frameworks.

AEAD-based protocols emerge as a newly significant category with the lowest average DREAD score (1.60), closely followed by ECC-based protocols (1.63), multi-factor (1.67), PUF-based and post-quantum (1.70), ZKP (1.73), blockchain-based (1.77), and hash/XOR-only (2.10). Spoofing remains the highest-severity threat across all categories; repudiation is the most neglected. Nine research gaps are identified, including absent risk assessment integration, limited deployment validation, inadequate post-quantum readiness, the need for AEAD-risk framework integration, and lack of standards alignment.

Future work should embed structured risk assessment into protocol design, develop lightweight post-quantum solutions, leverage NIST-standardized AEAD primitives for interoperable authentication, and create cross-domain frameworks with quantifiable risk guarantees aligned with NIST SP 800-213 and ISO/IEC 27005.

Acknowledgement: Not applicable.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: The authors confirm contribution to the paper as follows: Conceptualization, Rayan Alenzi and Rayan Aldoghan; methodology, Rayan Alenzi and Rayan Aldoghan; formal analysis, Rayan Alenzi and Rayan Aldoghan; investigation, Rayan Alenzi and Rayan Aldoghan; data curation, Rayan Alenzi and Rayan Aldoghan; writing—original draft preparation, Rayan Alenzi and Rayan Aldoghan; writing—review and editing, Rayan Alenzi, Rayan Aldoghan and M. M. Hafizur Rahman; visualization, Rayan Alenzi and Rayan Aldoghan; supervision, M. M. Hafizur Rahman. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Tun NW, Mambo M. Secure PUF-based authentication systems. Sensors. 2024;24(16):5295. doi:10.3390/s24165295.
2. Farha F, Ning H, Ali K, Chen L, Nugent C. SRAM-PUF-based entities authentication scheme for resource-constrained IoT devices. IEEE Internet Things J. 2021;8(7):5904–13. doi:10.1109/jiot.2020.3032518.
3. Wang H, Meng J, Du X, Cao T, Xie Y. Lightweight and anonymous mutual authentication protocol for edge IoT nodes with physical unclonable function. Secur Commun Netw. 2022;2022:1203691. doi:10.1155/2022/1203691.
4. Khan MA, Ullah S, Ahmad T, Jawad K, Buriro A. Enhancing security and privacy in healthcare systems using a lightweight RFID protocol. Sensors. 2023;23(12):5518. doi:10.3390/s23125518.
5. Mudra G, Cui H, Johnstone MN. Survey: an overview of lightweight RFID authentication protocols suitable for the maritime Internet of Things. Electronics. 2023;12(13):2990. doi:10.3390/electronics12132990.
6. Yang YS, Lee SH, Wang JM, Yang CS, Huang YM, Hou TW. Lightweight authentication mechanism for industrial IoT environment combining elliptic curve cryptography and trusted token. Sensors. 2023;23(10):4970. doi:10.3390/s23104970.
7. Parsons EK, Panaousis E, Loukas G, Sakellari G. A survey on cyber risk management for the Internet of Things. Appl Sci. 2023;13(15):9032. doi:10.3390/app13159032.
8. Yalli JS, Hilmi Hasan M, Tang Jung L, Ibrahim Yerima A, Adamu Aliyu D, Danjuma Maiwada U, et al. A systematic review for evaluating IoT security: a focus on authentication, protocols and enabling technologies. IEEE Internet Things J. 2025;12(12):18908–28. doi:10.1109/jiot.2025.3545737.
9. Zhai B, Sun H, Li L. Security risk assessment of IoT health devices using DREAD and STRIDE models. Ain Shams Eng J. 2025;16(11):103721. doi:10.1016/j.asej.2025.103721.
10. Kim KH, Kim K, Kim HK. STRIDE-based threat modeling and DREAD evaluation for the distributed control system in the oil refinery. ETRI J. 2022;44(6):991–1003. doi:10.4218/etrij.2021-0181.
11. Al Asif MR, Hasan KF, Islam MZ, Khondoker R. STRIDE-based cyber security threat modeling for IoT-enabled precision agriculture systems. In: Proceedings of the 2021 3rd International Conference on Sustainable Technologies for Industry 4.0 (STI); 2021 Dec 18–19; Dhaka, Bangladesh. p. 1–6. doi:10.1109/sti53101.2021.9732597.
12. Hu S, Jiang S, Miao Q, Yang F, Zhou W, Duan P. Provably secure ECC-based anonymous authentication and key agreement for IoT. Appl Sci. 2024;14(8):3187. doi:10.3390/app14083187.

13. Sowjanya K, Dasgupta M, Ray S. Elliptic curve cryptography based authentication scheme for Internet of medical things. J Inf Secur Appl. 2021;58:102761. doi:10.1016/j.jisa.2021.102761.
14. Keshta I. A CRC-based authentication model and ECC-based authentication protocol for resource-constrained IoT applications. IEEE Access. 2024;12:156765–84. doi:10.1109/access.2024.3482991.
15. Al-saggaf AA, Sheltami T, Alkhzaimi H, Ahmed G. Lightweight two-factor-based user authentication protocol for IoT-enabled healthcare ecosystem in quantum computing. Arab J Sci Eng. 2023;48(2):2347–57. doi:10.1007/s13369-022-07235-0.
16. Saqib M, Moon AH. A systematic security assessment and review of Internet of Things in the context of authentication. Comput Secur. 2023;125:103053. doi:10.1016/j.cose.2022.103053.
17. Ali Khan M, Din IU, Majali T, Kim BS. A survey of authentication in Internet of Things-enabled healthcare systems. Sensors. 2022;22(23):9089. doi:10.3390/s22239089.
18. Zhang L, Taal A, Cushing R, de Laat C, Grosso P. A risk-level assessment system based on the STRIDE/DREAD model for digital data marketplaces. Int J Inf Secur. 2022;21(3):509–25. doi:10.1007/s10207-021-00566-3.
19. Tanveer M, Alharbi AG, Aldossari SA. RePUF-IoT: reconfigurable PUF-based authentication protocol for IoT-driven healthcare systems. IEEE Internet Things J. 2025;12(22):47575–87. doi:10.1109/jiot.2025.3602311.
20. Ullah S, Nasir H, Kadir K, Khan A, Memon A, Azhar S, et al. End-To-End encryption enabled lightweight mutual authentication scheme for resource constrained IoT network. Comput Mater Contin. 2025;82(2):3223–49. doi:10.32604/cmc.2024.054676.
21. Bamashmos S, Chilamkurti N, Shahraki AS. Two-layered multi-factor authentication using decentralized blockchain in an IoT environment. Sensors. 2024;24(11):3575. doi:10.3390/s24113575.
22. Hamila F, Mkaouar H, Fourati LC. Enhancing security in Fiat-Shamir transformation-based non-interactive zero-knowledge protocols for IoT. Int J Inf Secur. 2024;23:1131–48. doi:10.1007/s10207-023-00779-8.
23. Saqib M, Jasra B, Moon AH. A lightweight three factor authentication framework for IoT based critical applications. J King Saud Univ Comput Inf Sci. 2022;34(9):6925–37. doi:10.1016/j.jksuci.2021.07.023.
24. Al Ahmed MT, Hashim F, Hashim SJ, Abdullah A. Authentication-chains: blockchain-inspired lightweight authentication protocol for IoT networks. Electronics. 2023;12(4):867. doi:10.3390/electronics12040867.
25. Chaira M, Haqiq A, Benhaddou D. A decentralized blockchain-based authentication scheme for cross-communication in IoT. Clust Comput. 2024;27:2505–23. doi:10.1007/s10586-023-04094-8.
26. Ju S, Park Y. Provably secure lightweight mutual authentication and key agreement scheme for cloud-based IoT environments. Sensors. 2023;23(24):9766. doi:10.3390/s23249766.
27. Ehui BB, Han Y, Guo H, Liu J. A lightweight mutual authentication protocol for IoT. J Commun Inf Netw. 2022;7(2):181–91. doi:10.23919/jcin.2022.9815201.
28. Satpathy SP, Mohanty S, Pradhan M. A sustainable mutual authentication protocol for IoT-Fog-Cloud environment. Peer Peer Netw Appl. 2024;18(1):35. doi:10.1007/s12083-024-01843-3.
29. Oh J, Yu S, Lee J, Son S, Kim M, Park Y. A secure and lightweight authentication protocol for IoT-based smart homes. Sensors. 2021;21(4):1488. doi:10.3390/s21041488.
30. Haseeb-Ur-Rehman RMA, Liaqat M, Aman AHM, Ali Almazroi A, Hasan MK, Ali Z, et al. LR-AKAP: a lightweight and robust security protocol for smart home environments. Sensors. 2022;22(18):6902. doi:10.3390/s22186902.
31. Kim K, Ryu J, Lee Y, Won D. An improved lightweight user authentication scheme for the internet of medical things. Sensors. 2023;23(3):1122. doi:10.3390/s23031122.
32. Das S, Namasudra S. Lightweight and efficient privacy-preserving mutual authentication scheme to secure Internet of Things-based smart healthcare. Trans Emerg Tel Technol. 2023;34(11):e4716. doi:10.1002/ett.4716.
33. Tabany M, Syed M. A lightweight mutual authentication protocol for Internet of vehicles. J Adv Inf Technol. 2024;15(2):155–63. doi:10.12720/jait.15.2.155-163.
34. Li Z, Miao Q, Chaudhry SA, Chen CM. A provably secure and lightweight mutual authentication protocol in fog-enabled social Internet of vehicles. Int J Distrib Sens Netw. 2022;18(6):155013292211043. doi:10.1177/15501329221104332.
35. Khalique A, Siddiqui F, Ahad MA, Hussain I. Lightweight authentication for IoT devices (LAID) in sustainable smart cities. Sci Rep. 2025;15:25410. doi:10.1038/s41598-025-10181-0.

36. Tanveer M, Toor K, Alharbi AG, Hassan SR. SecTwin: a secure and efficient authentication mechanism for vehicular digital twins. J Inf Secur Appl. 2025;95:104292. doi:10.1016/j.jisa.2025.104292.
37. Sabo A, Usman AG, Abba SI, Dezfooli AS. Cybersecurity threat modeling for IoT-integrated smart solar energy systems. Sustainability. 2025;17(6):2386. doi:10.3390/su17062386.
38. Abosata N, Al-Rubaye S, Inalhan G, Emmanouilidis C. Internet of Things for system integrity: a comprehensive survey on security, attacks and countermeasures for industrial applications. Sensors. 2021;21(11):3654. doi:10.3390/s21113654.
39. Papaioannou M, Pelekoudas-Oikonomou F, Mantas G, Serrelis E, Rodriguez J, Fengou MA. A survey on quantitative risk estimation approaches for secure and usable user authentication on smartphones. Sensors. 2023;23(6):2979. doi:10.3390/s23062979.
40. Junejo AK, Breza M, McCann JA. Threat modeling for communication security of IoT-enabled digital logistics. Sensors. 2023;23(23):9500. doi:10.3390/s23239500.
41. Gerodimos A, Maglaras L, Ferrag MA, Janicke H. Analyzing and mitigating attacks in IoT smart home using stride threat modeling. Int J Interact Mobile Technol. 2025;19(2):126–142. doi:10.3991/ijim.v19i02.52377.
42. Abbas SG, Vaccari I, Hussain F, Zahid S, Fayyaz UU, Shah GA, et al. Identifying and mitigating phishing attack threats in IoT use cases using a threat modelling approach. Sensors. 2021;21(14):4816. doi:10.3390/s21144816.
43. Turan MS, McKay K, Chang D, Kang J, Kelsey J. Ascon-based lightweight cryptography standards for constrained devices. New York, NY, USA: NIST; 2025. doi:10.6028/NIST.SP.800-232.
44. Tanveer M, Alhajaj Aldossari S. MedIoT-LAP: secure and efficient lightweight AEAD-Based authentication protocol for medical IoT. Ain Shams Eng J. 2025;16(10):103605. doi:10.1016/j.asej.2025.103605.
45. Alruwaili O, Tanveer M, Aldossari SA, Alanazi S, Armghan A. RAAF-MEC: reliable and anonymous authentication framework for IoT-enabled mobile edge computing environment. Internet Things. 2025;29:101459. doi:10.1016/j.iot.2024.101459.