STATISTICS, OPTIMIZATION AND INFORMATION COMPUTING
Stat., Optim. Inf. Comput., Vol. **16**, December 2026, pp 6361–6395.
Published online in International Academic Press (www.IAPress.org)

Toward Secure and Scalable IoT Authentication: A Survey of Protocols, Challenges, and Emerging Technologies

Mohamed Ech-chebaby, Hicham Zougagh, Hamid Garmani, Zouhair Elhadari

Faculty of Sciences and Techniques, Sultan Moulay Slimane University, Beni Mellal, Morocco

Abstract The Internet of Things (IoT) comprises a wide range of heterogeneous devices, including sensors, radio-frequency identification (RFID) systems, and actuators, interconnected through large-scale networks to enable intelligent services such as smart homes, smart cities, smart transportation, and industrial automation. While this connectivity offers significant benefits, it also introduces serious security and privacy challenges. Among the various security requirements of IoT systems such as access control, data confidentiality, network protection, and authorization authentication remains a fundamental component, as it governs the initial interaction between entities before any data exchange takes place. Conventional network security mechanisms cannot be directly applied to IoT environments due to the limited computational power, memory, and energy resources of IoT devices. As a result, the design of secure and lightweight authentication mechanisms is essential to protect IoT infrastructures against diverse attacks. In this survey, we focus on IoT authentication mechanisms by analyzing prevalent attack models and reviewing state-of-the-art authentication protocols. Furthermore, we examine existing security verification and evaluation techniques used to assess the robustness of these protocols. A comparative analysis of current solutions is provided, highlighting their strengths, limitations, and unresolved challenges. Finally, this study aims to support future research by identifying open issues and outlining promising directions for the development of more secure and efficient IoT authentication schemes.

Keywords Internet of Things, authentication protocols, IoT security, network attacks, wireless sensor networks.

DOI: 10.19139/soic-2310-5070-4009

1. Introduction

The Internet of Things (IoT) has grown exponentially in recent years, connecting billions of devices in smart homes, industries, and cities. The number of connected IoT devices is projected to surpass 20 billion by 2025 and approach 40 billion by 2030, underscoring the vast scale of this ecosystem. Ensuring secure authentication in IoT is critically important authentication protocols verify the identity of devices and users, establishing trust for subsequent communication and data exchange. Unlike traditional computing, IoT devices are often resource-constrained and deployed in diverse, sometimes hostile environments. Many devices have limited computational capabilities and cannot perform heavy cryptographic algorithms. This makes them susceptible to a wide range of attacks (e.g. impersonation, man-in-the-middle, cloning, and denial-of-service) if robust but lightweight authentication measures are not in place. Moreover, preserving privacy is a key concern: IoT deployments frequently handle sensitive personal or sensor data, and authentication schemes must prevent adversaries from tracing device identities or eavesdropping on credentials. Recent studies highlight that some IoT authentication protocols remain vulnerable to deanonymization and privacy attacks, motivating stronger privacy-preserving designs.

These challenges drive the need for a comprehensive survey of IoT authentication protocols. While several surveys have examined general IoT security threats and countermeasures, the rapid evolution of authentication

*Correspondence to: Mohamed Ech-chebaby (Email: mohamed.ech-chebaby@usms.ma). Faculty of Sciences and Techniques, Sultan Moulay Slimane University, Beni Mellal, Morocco

ISSN 2310-5070 (online) ISSN 2311-004X (print)
Copyright © 2026 International Academic Press

techniques – from hardware-based keys to AI-driven methods – warrants a focused review. Table 1 compares this survey with representative recent works on IoT authentication security (2020–2025), highlighting the unique combination of contributions offered by this paper.

Table 1. Comparison with recent related surveys on IoT authentication (2020–2025). ✓ = fully covered; P = partial; – = not covered.

Survey	Attack taxonomy	Auth. techniques	PUF / PQ	Perf. evaluation	Formal verification	NMS focus	6G / AI	Open issues
Singh et al. 2024 [1]	P	✓	–	–	–	–	–	✓
Szymoniak 2023 [2]	–	P	–	P	–	–	–	P
Bekri et al. 2024 [3]	P	P	–	–	–	–	–	✓
Butun et al. 2020 [4]	✓	P	–	–	–	–	–	P
He et al. 2024 [5]	–	–	–	P	–	–	–	✓
Kaur & Gupta 2025 [6]	P	P	–	–	–	–	P	P
Braeken 2025 [7]	–	P	✓	P	–	–	P	–
Malele 2025 [8]	–	P	–	–	P	–	–	P
Tawfik et al. 2025 [9]	P	–	–	P	–	–	✓	✓
This Survey	✓	✓	✓	✓	✓	✓	✓	✓

This survey article is motivated by the goal of summarizing and analyzing state-of-the-art IoT authentication mechanisms, identifying their limitations, and highlighting emerging solutions. In particular, the article covers the following topics and contributions:

- **Threat Taxonomy:** The survey begins by identifying the major security threats affecting IoT authentication mechanisms, including masquerade attacks, replay attacks, man-in-the-middle attacks, denial-of-service attacks, and physical tampering. It explains how these attacks exploit intrinsic IoT vulnerabilities such as open wireless communication channels, limited computational resources, and unattended deployment environments. This taxonomy highlights the need for specialized authentication protocols capable of addressing IoT-specific attack vectors and operational constraints.
- **Authentication Schemes Overview:** A wide range of IoT authentication protocols is reviewed and categorized based on their design principles and underlying technologies. The survey covers conventional cryptographic approaches, including symmetric-key and public-key schemes such as elliptic-curve cryptography, as well as lightweight variants tailored for low-power and resource-constrained devices. It further examines multi-factor and biometric-based authentication schemes, hardware-assisted security primitives such as Physically Unclonable Functions (PUFs) for device fingerprinting, and emerging techniques including chaotic-map-based and blockchain-enabled authentication protocols. Representative schemes from recent literature are analyzed, emphasizing how they achieve security objectives such as mutual authentication, secure key agreement, and entity anonymity.
- **Performance and Constraints Analysis:** The survey analyzes how authentication protocols balance security and efficiency in resource-constrained IoT environments. Key performance metrics, including computational complexity, communication overhead, average authentication latency, and energy consumption, are compared across different schemes. This analysis underlines the importance of lightweight authentication, as many IoT devices cannot support computationally intensive cryptographic operations. Optimization strategies, such as pre-computation techniques and the use of lightweight cryptographic primitives, are discussed alongside the associated trade-offs between security strength and efficiency.

- **Privacy and Anonymity Considerations:** Special attention is given to privacy preservation in IoT authentication protocols. The survey reviews anonymity-enhancing mechanisms such as pseudonym-based identification, hash-based identity protection, and zero-knowledge proof techniques, while highlighting existing limitations. Although several recent schemes incorporate anonymity or untraceability features to mitigate device tracking, prior studies indicate that some protocols remain vulnerable to identity disclosure and linkability attacks. This comparison highlights best practices for privacy-preserving authentication and the need for stronger safeguards to protect sensitive IoT data.
- **Open Challenges and Emerging Directions:** Finally, the survey identifies open research challenges and future directions in IoT authentication. Key limitations, including incomplete resistance to advanced attacks, scalability issues in large-scale and heterogeneous IoT deployments, and insufficient formal security validation, are critically discussed. The article highlights promising future techniques such as cloud-, fog-, and edge-assisted authentication frameworks, AI- and machine-learning-driven adaptive authentication mechanisms, blockchain-based decentralized trust management, and post-quantum and hybrid authentication schemes that combine lightweight cryptography with PUF-based hardware security to enhance resilience against future threats.

Overall, the introduction of strong, efficient authentication protocols is pivotal to realizing the potential of the IoT. By surveying the landscape of existing methods and emerging innovations, this article sets the stage for understanding how IoT devices can be authenticated reliably despite stringent resource constraints and evolving security threats.

From a network and systems management perspective, IoT authentication is not merely a device-level security primitive but a critical service management concern. Authentication failures directly translate into service disruptions, unauthorized data access, and policy violations that affect the operation of managed networks. Research published in network management venues including the IEEE/IFIP International Symposium on Integrated Network Management (IM) [10], the IEEE Conference on Network and Service Management (CNSM), and the IEEE Transactions on Network and Service Management (TNSM) has addressed related challenges such as anomaly-based intrusion detection in managed IoT infrastructures [11], policy-driven authentication enforcement at network edges [6], and the operational overhead of authentication protocol deployment in heterogeneous managed environments. This survey aligns with that tradition by providing network administrators and service managers with a structured assessment of authentication protocol capabilities, their associated management overhead, and their fitness for deployment in large-scale, policy-governed IoT infrastructures.

2. Research methodology

Every survey should rest on an explicit and reproducible research methodology. This section outlines the procedure that guided our review, describing how the relevant literature was identified, filtered, and analysed. By restricting the corpus to indexed peer-reviewed venues and by applying a documented sequence of selection criteria, we ensure that the study is both replicable and credible. Table 1 indicates the distinction between the current survey and previous studies conducted on IoT authentication, highlighting the dimensions that remain insufficiently covered in the existing literature.

2.1. Research questions

The review is guided by six research questions covering the full lifecycle of an IoT authentication scheme, from the threats it must withstand to the evidence supporting its security claims.

RQ1. Which attack categories specifically target authentication mechanisms in IoT environments, and which intrinsic properties of IoT deployments do they exploit?

RQ2. What cryptographic and hardware-assisted techniques underpin existing IoT authentication protocols, and what trade-offs does each family impose?

RQ3. To what extent do current protocols achieve resistance across the full spectrum of attacks rather than against isolated threats?

RQ4. How is the security of proposed protocols validated, and how rigorous is that validation?

RQ5. Which performance metrics govern the deployability of authentication protocols on constrained devices, and how are they quantified?

RQ6. What open problems remain unresolved, and which emerging technologies offer credible paths towards addressing them?

Table 2. Research questions and the sections addressing them

ID	Research question	Section
RQ1	Which attack categories target IoT authentication?	3
RQ2	Which techniques underpin existing protocols?	4
RQ3	Is attack resistance comprehensive or partial?	3, 6
RQ4	How rigorously are security claims validated?	5
RQ5	Which performance metrics govern deployability?	6
RQ6	Which open problems and directions remain?	7

2.2. Search strategy

The literature search was conducted across five scientific databases: ScienceDirect (Elsevier), IEEE Xplore, Springer Link, MDPI, and ACM Digital Library. Queries combined the core concept with its principal variants and application domains, using the following string:

> (“IoT” OR “Internet of Things”) AND (“authentication” OR “mutual authentication” OR “key agreement”) AND (“lightweight” OR “protocol” OR “security”)

Complementary searches were performed for specific technique families “PUF”, “elliptic curve cryptography”, “chaotic map”, “three-factor”, “post-quantum” in order to capture schemes that do not use the generic terminology in their titles. Searches were restricted to the period 2016–2025 and applied to titles, abstracts, and keywords. The databases were last queried in 2025.

2.3. Inclusion and exclusion criteria

Retrieved records were filtered through a sequence of criteria applied in a fixed order, as illustrated in Figure 1. A record was retained only if it satisfied all of the following conditions:

1. it addressed authentication or key agreement in IoT or a closely related constrained-device setting;
2. it was published in a peer-reviewed journal or conference between 2016 and 2025;
3. it appeared in an indexed venue (Scopus, SCI, IEEE, or ACM);
4. it was not a duplicate of a record already retrieved from another database;
5. it remained relevant after examination of its abstract, results, and conclusion.

Records failing any criterion were excluded at that point and not carried forward. Books, magazines, technical white papers, and non-peer-reviewed material were excluded. Two exceptions were deliberately retained for definitional purposes only, and are not counted among the analysed studies: an encyclopedia entry on the elliptic curve discrete logarithm problem, and background taxonomies of IoT attacks.

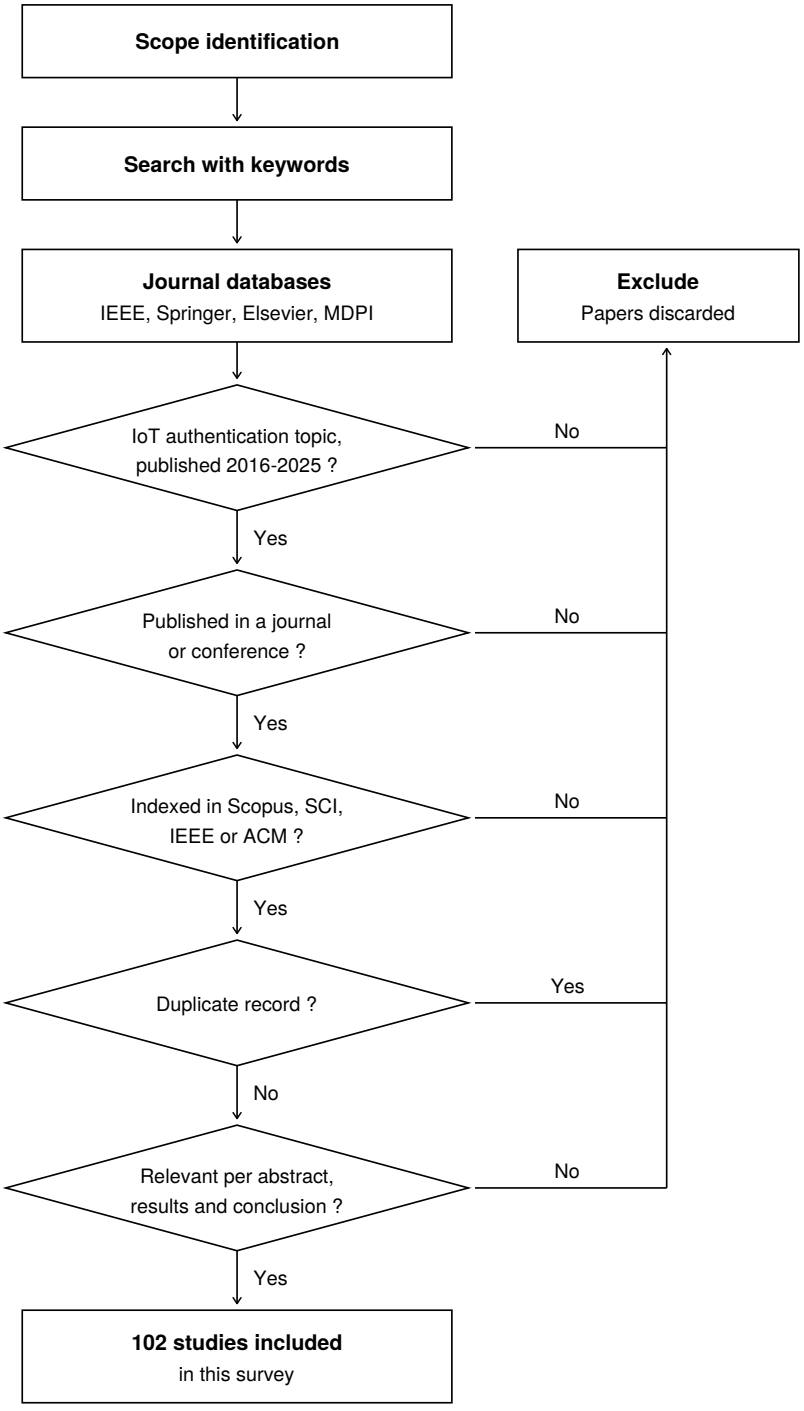


Figure 1. Inclusion and exclusion criteria

2.4. Study selection and reporting

The selection process is reported following the PRISMA 2020 flow diagram [12], which structures study selection into three successive stages identification, screening, and inclusion and requires the number of records entering and leaving each stage to be stated explicitly, together with the reasons for exclusion.

In the identification stage, records were retrieved from the five databases listed in Section 2.2. Duplicate records appearing in more than one database, and records whose subject fell outside the scope of IoT authentication, were removed before screening. In the screening stage, the remaining records were assessed on the basis of their titles and abstracts; reports were then sought for retrieval for those that passed. In the eligibility assessment, retrieved reports were examined in full against the criteria of Section 2.3. Reports were excluded when authentication was mentioned only incidentally rather than being the contribution, when no security evaluation was reported, when the contribution duplicated an already retained study, or when the venue was not indexed. The resulting flow, with the number of records at each stage, is presented in Figure 2.

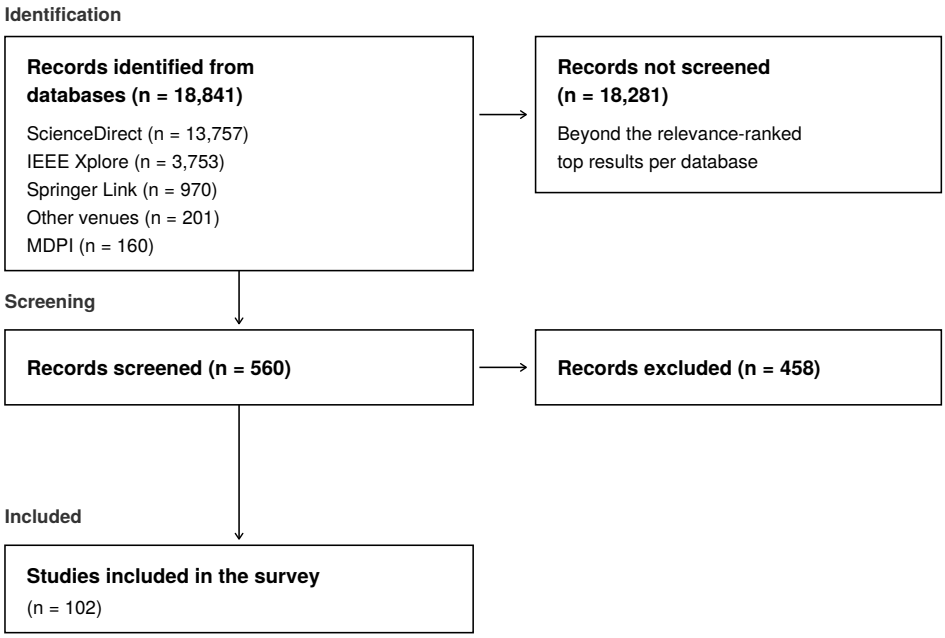


Figure 2. PRISMA 2020 flow diagram of the study selection process

2.5. Distribution of the selected literature

The selection process yielded 102 distinct studies. Their distribution across the source databases is reported in Table 3. Elsevier and IEEE venues account for more than half of the corpus, reflecting the concentration of IoT security research in those outlets, while MDPI contributes a substantial share of the most recent work.

Of the selected studies, 88 are journal articles and 13 are conference papers, with one encyclopedia entry retained for definitional purposes as noted in Section 2.3.

Returning to the research questions stated in Section 2.1, this survey has shown that IoT authentication is threatened by six distinct families of attack whose exploitation depends on the open, unattended, and resource-constrained nature of IoT deployments (RQ1), and that the protocols proposed to counter them draw on a limited set of primitives symmetric and asymmetric cryptography, chaotic maps, biometrics, and physical unclonable functions each imposing its own trade-off between security strength and computational cost (RQ2). The comparative tables show that no reviewed scheme achieves resistance across all attack categories, with coverage concentrating

Table 3. Distribution of the reviewed literature by publisher

Library	Number of studies
ScienceDirect (Elsevier)	32
IEEE Xplore	26
Springer Link	19
MDPI	18
Other venues	7
Total	**102**

on the threats that are cheapest to mitigate (RQ3). Validation practice remains uneven: symbolic verification under bounded adversary models is common, but a substantial fraction of schemes rely on informal argument alone (RQ4). Performance is characterised through a stable set of metrics response time, handshake duration, communication and computation cost, memory footprint, and energy consumption though these are rarely reported consistently enough to permit direct comparison (RQ5). Finally, post-quantum readiness, PUF reliability under aging, scalability to massive deployments, and the absence of a unified verification methodology emerge as the principal open problems (RQ6).

3. Attack Taxonomy for IoT Authentication

In this section, we present a comprehensive taxonomy of attacks on IoT authentication in accordance with existing research in the literature. As security threats against IoT authentication mechanisms increase, various research efforts have classified these attacks into different classes based on their nature, impact, and exploitation techniques.[13, 14, 4, 15] For better understanding of these threats, we have developed an organized diagram (Figure 3) that graphically represents the different types of attacks cited in literature. The taxonomy categorizes attacks into six general classes: Masquerade Attacks, Man-in-the-Middle Attacks, Denial-of-Service (DoS) Attacks, Forging Attacks, Physical Attacks, and Routing Attacks, with a number of specific attack types under each.By classifying these attacks, we want to bring to light the most extreme vulnerabilities in IoT authentication and emphasize the need for robust security mechanisms. A detailed description of all classes is provided in the following sections, which self-describe, their attack vectors, and potential mitigation techniques

3.1. Physical Attacks

In the Internet of Things (IoT) environment, physical attacks are a real security issue since are widely deployed and often left unmonitored. Unlike standard computing systems, which enjoy the luxury of remaining in secure environments, IoT devices have the tendency of being placed in exposed or uncontrolled environments in most instances, thus being highly susceptible to nefarious individuals physically touching them.[16] These attacks may occur in many forms, including theft or loss of mobile phone handsets, smart cards, or embedded nodes, which may hold confidential credentials or cryptographic material. It is possible to reverse-engineer its components when in possession of one such device, conduct side-channel attacks like power or timing analysis, or pick locally stored sensitive data. Furthermore, USB attacks using malicious USB devices like keyboards, USB flash drives, or data cables to inject malware present a growing threat, especially when users unknowingly connect them to trusted systems. Yet another new threat is the ”same-type device attack,” wherein an attacker acquires a device of the same make and model as the legitimate device and clones it to impersonate the original. This is particularly problematic in networks where the protocol does not validate the unique physical identity of the transmitting device. In addition, since authentication is performed most often using mobile devices in IoT networks, their theft may become an immediate entry point for third parties if the protocols applied do not account for such incidents. To counter these attacks, newer research has been focused on the development of robust authentication schemes that can resist physical compromise, e.g., device fingerprinting, tamper detection, and privacy-preserving methods.

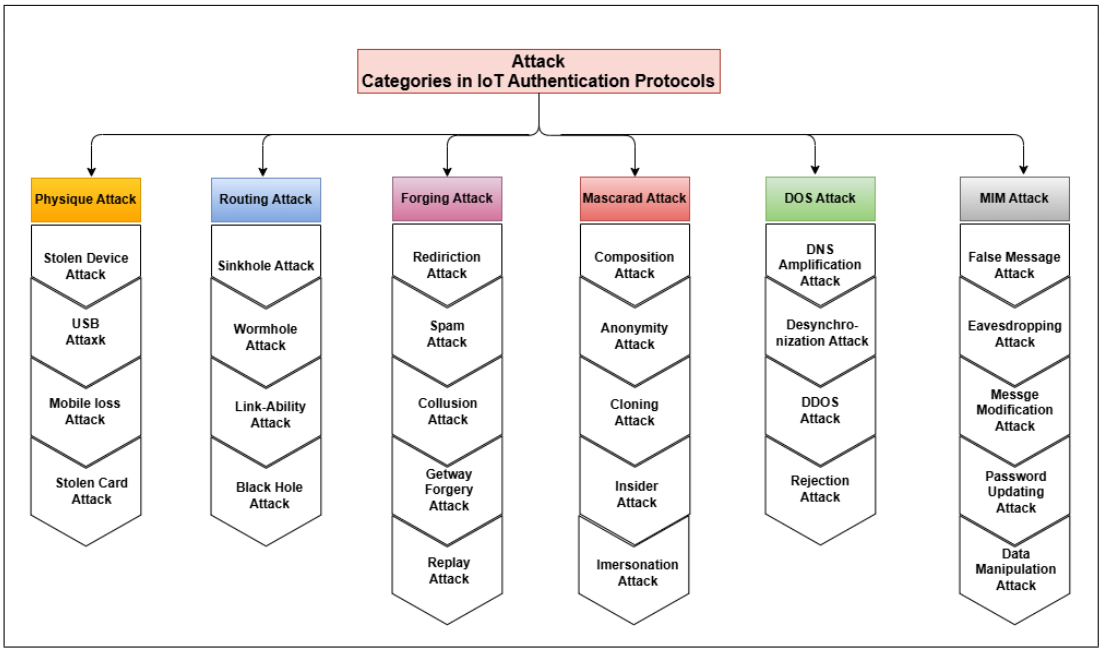


Figure 3. Mechanisms used by authentication protocols

This article [17] presents two lightweight and secure protocols, specifically against physical attacks, T2S-MAKEP (Thing-to-Server) and T2T-MAKEP (Thing-to-Thing), to provide mutual authentication and key exchange for IoT devices using Physical Unclonable Functions (PUF). The protocols are constructed in such a way as to thwart a range of attacks physical tampering aimed at extracting stored secrets, replay, denial of service, man-in-the-middle, modeling, and helper data manipulation by avoiding the storage of secret information on devices and using techniques such as fuzzy extractors, hashing, and encryption. Formal verification using Verifpal guarantees the protocols' robustness, and they are thus suited for security-critical and resource-constrained IoT environments. In this paper[18], the authors introduce an efficient and adaptable end-to-end anonymous authentication protocol for IoT based on Physical Unclonable Functions (PUF) as a hardware security primitive. The proposed protocol supports direct mutual authentication between IoT devices without the need for a real-time trusted third-party intervention, solving the issues of flexibility and efficiency in current solutions. By taking advantage of the new physical properties of PUFs, the protocol stores no secret information on the devices, which the authors argue provides strong resistance to secret extraction and side-channel analysis. In this paper [19], the authors present a new authentication and key agreement (AKA) protocol suitable for Internet of Things (IoT) devices using Chebyshev chaotic maps. They begin by thoroughly analyzing the shortcomings of existing ECC-based and chaotic map-based protocols, such as those presented by He et al[20]. and Qiu et al[21], demonstrating that these schemes are vulnerable to several protocol-level attacks including server key compromise impersonation (KCI), lack of perfect forward secrecy (PFS), ephemeral secret leakage (ESL), and desynchronization attacks. To address these issues, the authors design a lightweight and robust protocol that provides mutual authentication, user anonymity, and resistance to these main attacks. Notably, the protocol takes into account the possibility that an attacker could gain physical access to a smart card and extract stored data. In [22], the authors present SELAP, a secure and efficient lightweight authentication protocol for multi-sector IoT applications in this article. SELAP is presented to address serious vulnerabilities discovered in the well-known ELWSCAS [23] protocol, including its vulnerability to impersonation, forgery, absence of forward secrecy, and traceability attacks. Solid mutual authentication and immunity to a wide range of attacks: man-in-the-middle, replay, message tampering, and identity tracing derive from SELAP's use of EC-Schnorr signatures and the extremely lightweight ASCON algorithm. However, like

any software cryptographic protocol for IoT, SELAP remains exposed to side-channel analysis, which requires hardware-level countermeasures beyond the protocol itself and falls outside the vectors considered in Table 4.

Table 4. IoT authentication schemes against physical attacks

Protocol	Stolen device Attack	USB Attack	Mobile loss Attack	Stolen card Attack
Zerrouki et al [17]	No	Yes	No	No
Li et al [18]	No	Yes	No	No
Zahednejad et al [19]	No	No	No	Yes
Qiu et al[21]	No	Yes	No	Yes
He et al[20]	No	Yes	Yes	Yes
Javadi et al [22]	Yes	No	Yes	Yes
Wu et al [24]	No	No	No	Yes
Niu et al [25]	No	No	Yes	Yes
Peng et al [26]	No	No	Yes	No
Nissim et al [27]	No	Yes	No	No
Lin et al [28]	Yes	No	No	Yes
Amsaad et al [29]	No	No	Yes	Yes
Akber et al [30]	Yes	No	No	No
Ali et al [31]	Yes	No	No	No
Lee et al [32]	Yes	No	No	Yes

Table 4 provides a comparative overview of various IoT authentication protocols, based on their ability to thwart physical attacks. The data presented are either copied directly from the original work that specifies the protocols or derived from survey papers that have comprehensively analyzed them. The table indicates whether each protocol has specific mechanisms to thwart such threats, where *Yes* denotes an explicit countermeasure and *No* an unaddressed vector. As the comparison shows, no protocol addresses all four vectors: He et al. [20] and Javadi et al. [22] offer the broadest coverage with three vectors each, while the majority of the surveyed schemes address one or two at most. These findings highlight the need for more secure and strong authentication mechanisms tailored to the physical security requirements of IoT environments.

Analysis. A critical examination of the protocols in Table 4 reveals three recurring design limitations. First, most schemes prioritise smart-card or stolen-credential threats (9 of 15) over hardware-oriented vectors such as USB and same-type device attacks, which exploit hardware-level vulnerabilities rather than credential weaknesses; same-type device attacks in particular remain entirely unreported across the surveyed protocols. Second, PUF-based solutions (e.g., Zerrouki et al., Li et al.) achieve strong resistance to secret extraction, since no credential is stored in memory, but do not address mobile-device loss or device-capture scenarios, since PUF responses are bound to fixed hardware and cannot be revoked or migrated. Third, purely software-based ECC schemes are inherently unable to resist side-channel analysis without additional hardware countermeasures, a vector that falls outside the scope of Table 4 and is therefore rarely evaluated. These gaps collectively indicate that physical security requires a hybrid approach combining hardware fingerprinting, tamper-detection mechanisms, and protocol-level contingency handling for device loss or theft.

3.2. Routing Attack

Routing attacks directly target the integrity of data delivery in IoT networks. Instead of targeting the central infrastructure., such as gateways or cloud servers, these routing attacks aim at compromising intermediate nodes, typically sensors or other low-power devices,nodes to forward traffic towards the base station (or sink). With the compromise of a single node, an attacker can modify the routing logic and reroute packets from their intended path. Figure 4 illustrates this threat: a strategically placed sinkhole node captures network traffic and redirects it to a counterfeit sink, thereby disrupting normal communication. Such activity can lead to data leakage, service unavailability, or outright communication failure. Because IoT devices are physically exposed and heavily resource-constrained, they are especially susceptible to these attacks. Consequently, deploying robust, lightweight, and context-aware routing-security mechanisms is essential for today's IoT environments.

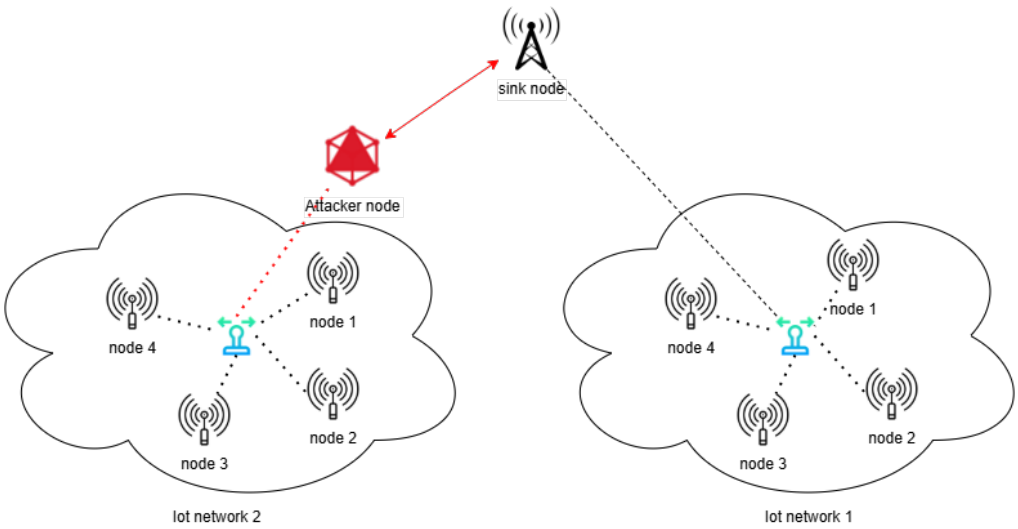


Figure 4. Routing Attack

Several forms of routing attacks have been documented, many of which involve intentionally dropping or altering network packets to degrade performance and reduce the Packet Delivery Ratio (PDR). Raza et al. [33] introduced the blackhole attack, in which an attacked node simply discards all packets that it is supposed to forward. This attack effectively isolates a node or set of nodes from the network, which results in a significant loss of the Packet Delivery Ratio (PDR). On this basis, Chen et al. [34] proposed the induced blackhole attack in which malicious nodes repeatedly loss all router packets meant for the target continuously without altering the inner logic of the original router. The attack prefers to employ a jammer to avoid outgoing routing updates to neighborhood nodes, but incoming packets and MAC-layer ACK frames are left unscathed.

To further improve the threat model, Essaadi et al. [35] introduced the coordinated blackhole attack, a variation of the binary blackhole attack [36], in which more than one colluding attackers conspire to deploy an enormous packet dropping. They also explained a mitigation scheme using Hop-Count Reachability (HCR) for the detection and neutralization of coordinated attacks.

Sheibani et al. [37] identified the Dropped DAO attack, wherein an attacking node drops Destination Advertisement Object (DAO) messages of legitimate nodes and sends forged DAO Acknowledgments (DAO-ACKs). This action prevents the establishment of new downward routes and results in the loss of all downward packets.

In another well-known threat, Wallgren et al. [38] examined the sinkhole attack, where a malicious node manipulates its rank to attract network traffic, which is then either modified or dropped after the node becomes the preferred parent in the routing topology. The same authors also discussed the grayhole or selective forwarding

attack, in which an adversary selectively forwards only certain RPL control packets while discarding others, thereby distorting routing paths and degrading overall network performance. Table 5 compares some proposed

Table 5. IoT authentication schemes against routing attacks

Protocol	Sinkhole Attack	Wormhole Attack	Link-Ability Attack	Black Hole Attack
Malina et al [10]	Yes	No	No	No
Remya et al [39]	No	Yes	No	No
Kamel and Elhamayed [40]	No	Yes	No	Yes
Ferrag et al [41]	Yes	Yes	No	No
Amish et al[42]	No	Yes	Yes	Yes

authentication protocols in the literature on the basis of how resistant these protocols are to certain routing attacks, that is, Sinkhole, Wormhole, Link-Ability, and Black Hole attacks. From the results, each scheme has certain advantages but also certain weaknesses. For example, the Malina et al. protocol resists just the Sinkhole attack, whereas Remya et al. have resistance only for the Wormhole attack. In the case of the protocol by Kamel and Elhamayed, it has resistance to the Wormhole and Black Hole attacks, but for the protocol by Ferrag et al., resistance is for the Sinkhole and the Wormhole attacks. Finally, for the protocol by Amish et al., resistance is for the broader set of the Wormhole, Link-Ability, and the Black Hole attacks. This comparison reveals the nonexistence of just one protocol resistant to all these attacks, thereby stressing the requirement for fuller and stronger authentication solutions in the context of IoT settings.

Analysis. The routing-attack results expose a fundamental tension in IoT network security design. Sinkhole and wormhole attacks operate at different protocol layers rank manipulation versus tunnel insertion and therefore require orthogonal countermeasures. Schemes that handle one class (e.g., Malina et al. addressing sinkhole via rank validation) typically offer no protection against the other. Moreover, link-ability attacks are addressed by only a single protocol in the table (Amish et al.), despite being a critical concern for privacy-sensitive deployments. A key design insight is that routing-security mechanisms must be co-designed with the authentication protocol rather than treated as a separate network layer concern, particularly in resource-constrained RPL-based IoT networks.

3.3. Forging Attack

Forgery attacks are a significant threat in UAV-based and IoT networks as they involve the use of forgery mechanisms to bypass authentication and breach system trust. There are several types of such attacks. In a redirection attack, communication is diverted maliciously from its legitimate destination to an attacker, thereby subjecting data to tampering. Spam attacks flood the network with false requests, draining the limited resources of IoT devices and impairing authentication performance. Collusion attacks are driven by collusion between penetrated nodes to avoid security processes in concert, presenting a particular challenge in their detection. Gateway forgery attacks involve attackers impersonating a legitimate gateway for traffic intercept, modification, or blocking, which disqualifies the network as a whole from reliability. Finally, replay attacks exploit capture and retransmission of valid authentication messages to deceive the system and gain unauthorized access. All these variations put together reflect the sophistication and scope of forgery-based attacks, justifying the need for lightweight, secure, and context-dependent authentication protocols that may be able to withstand such sophisticated attacks in IoT applications.

Replay attacks, as illustrated in Figure 5 under forgery attacks, exploit the forwarding and intercepting of authenticating messages to deceive the system. By replaying genuine credentials or session data, an attacker gains unauthorized access without generating new credentials or breaking encryption. Besides undermining

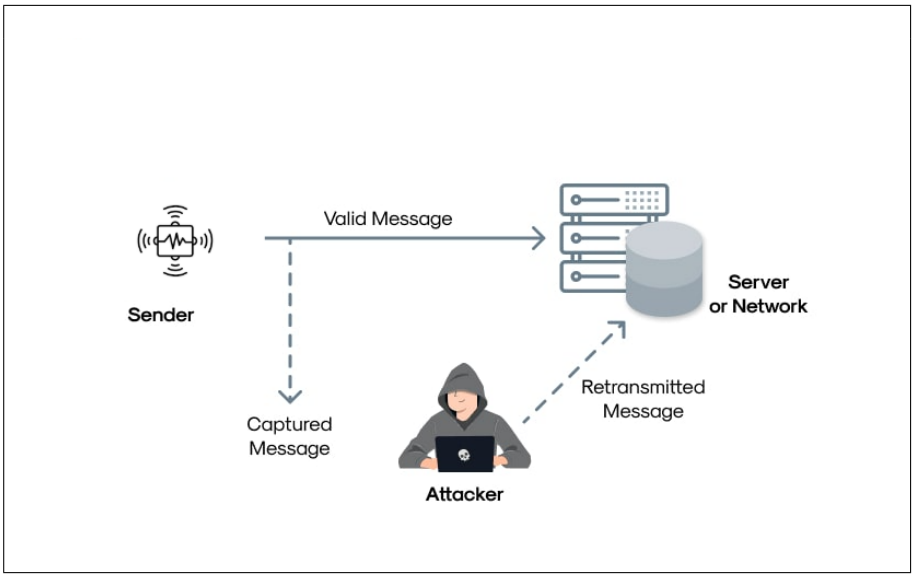


Figure 5. Replay Attack

the authenticity of the authenticating process, IoT networks become susceptible to impersonation and service disruption.

In their work, Ech-chebaby et al. [43] proposed a low-cost ECC-based mutual authentication scheme for IoT devices, an improvement of the earlier scheme by Fatma et al. [44]. While Fatma's scheme was computation saving, it had some major shortcomings, notably allowing an attacker to extract a device's hashed identity and session key. These weaknesses exposed the system to preimage and eavesdropping attacks, which were extendable to forgery-based attacks such as replay attacks. A malicious attacker can eavesdrop authentication messages and use existing valid credentials to deceive the server, masquerade valid devices, and achieve unauthorized access.

The PSLAP protocol introduced by Shariq et al. [45] was designed to offer authentication protection to autonomous vehicles in IoT environments. Compared to existing schemes that remained vulnerable, it employs light mechanisms such as timestamps and nonces, by which it is capable of resisting replay attacks effectively. By avoiding the reuse of messages after being intercepted, PSLAP improves the authenticity of the authentication process and offers immunity against key forms of forgery-based attacks.

Wu et al. [24] proposed a protocol that safeguards IoT networks against gateway forgery attacks by distributing critical information across multiple messages, thereby reducing the risk of interception and manipulation.

Table 6 compares the IoT authentication protocols against resistance to different forgery-based attacks, including redirection, spam, collusion, gateway forgery, and replay attacks. From the results, it is clear that no protocol offers far-reaching protection against these attacks. For example, the Wu et al. [24] protocol demonstrates strength only regarding gateway forgery attack resistance but is vulnerable to the others. Similarly, Paavolainen et al. [46] can resist spam attacks but is not secure against redirection, collusion, gateway forgery, and replay. Ech-Chebaby et al.'s [43] protocol, although secure against replay, is not secure against the other types of attacks. Merabet et al.'s [44] solution offers broader coverage, with resistance to redirection and replay attacks, yet remains vulnerable to spam, collusion, and gateway forgery. Within the referenced literature, Wong et al. [48] provides the widest coverage by addressing redirection, collusion, and replay, while Wang et al. [47] and Roy et al. [49] each combine collusion and replay resistance. Replay is by far the most widely covered threat (9 of 11 protocols), whereas spam and gateway forgery are each addressed by a single scheme. These results highlight the main gap: while all protocols provide protection against certain forgery threats, none provide full-spectrum security, revealing the urgent need to develop lightweight and complete authentication solutions with the potential to thwart all major forgery attack kinds in IoT environments.

Table 6. IoT authentication schemes against forging attack

Protocol	Redirection Attack	Spam Attack	Collusion Attack	Gateway Forgery Attack	Replay Attack
Wu et al [24]	No	No	No	Yes	No
Paavolainen et al [46]	No	Yes	No	No	No
Ech-Chebaby et al [43]	No	No	No	No	Yes
Merabet et al [44]	Yes	No	No	No	Yes
Wang et al[47]	No	No	Yes	No	Yes
Wong et al[48]	Yes	No	Yes	No	Yes
Roy et al[49]	No	No	Yes	No	Yes
Lu et al[50]	No	No	No	No	Yes
Nishant et al [51]	No	No	No	No	Yes
Wang et al [52]	No	No	No	No	Yes
Das et al [53]	No	No	No	No	Yes

Analysis. The forging-attack comparison exposes two critical design trade-offs. First, replay attack resistance is the most commonly addressed forgery threat (9 of 11 protocols) because it can be mitigated with relatively inexpensive mechanisms such as timestamps or nonces; however, these techniques introduce synchronization dependencies that create new vulnerabilities (desynchronization attacks). Second, spam and gateway forgery attacks remain almost entirely unaddressed, each covered by a single scheme, because they require trust-management and gateway-verification mechanisms that are expensive to implement on resource-constrained devices; collusion resistance is only marginally better represented, with three protocols out of eleven. Notably, protocols that distribute authentication information across multiple messages (e.g., Wu et al.) provide better gateway forgery resistance but at the cost of increased communication overhead, a trade-off that must be carefully evaluated against the deployment's energy budget.

3.4. Masquerade Attack

IoT authentication is primarily device or user identity-based, and thus the network becomes highly vulnerable if the identity is compromised. A masquerade attack occurs when an attacker uses forged credentials to impersonate a legitimate entity of the system. Without adequate countermeasures, IoT networks are easily vulnerable to such threats, which are usually backed up with stolen identifiers (i.e., usernames or passwords) or by profiling user behavior to mimic authentication patterns. Although common in IoT systems, the severity of such forms of attack is contextual depending on the privileges offered by them. When attackers manage to gain high-level authorization, they are given ample opportunities for executing malicious activities. Figure 6 illustrates various scenarios of masquerade attacks in IoT networks, pointing out the vulnerabilities created as a result of inadequate authentication security.

Impersonation attack as shown in Figure 6 is a sophisticated threat in IoT networks, in which an attacker exploits the authentication process to masquerade as a legitimate user. The attacker typically intercepts the authentication request or session information of a previous communication and replays it to trick the system into granting access. Chen et al [54] proposed a novel technique to handle impersonation attacks in IoT by introducing the FSMFA protocol, which integrates PUF-based hardware authentication with firmware integrity verification. This lightweight multi-factor scheme ensures mutual authentication and secure key exchange. *User impersonation* enables an adversary to appropriate a legitimate user's credentials or information to access the system and carry out malicious actions. Such impersonation can be executed through multiple vectors: for instance, the attacker may

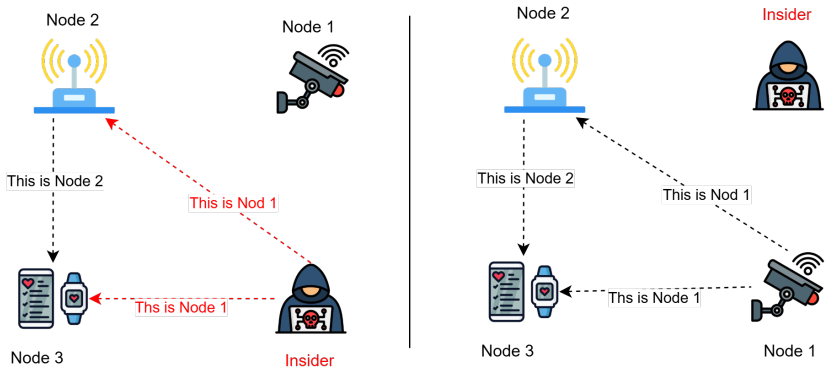


Figure 6. (Before and After) Impersonation Attack

obtain private server data leaked by a genuine user, or a legitimate user may willingly or unknowingly behave maliciously. Amin et al. [55] discuss countermeasures to prevent user-impersonation during authentication.

An anonymity attack violates the user/device's or device's privacy by attempting to deanonymize them linking pseudonymous identifiers or traffic patterns to real-world identities. In IoT scenarios, attackers utilize metadata (traffic volume, timing, routing pathways) or inadequate pseudonym-management to trace devices, reassemble activity profiles, or match sessions across services. Deanonymization can open the door to follow-up attacks (surveillance, profiling, targeted impersonation) and significantly violate user privacy. Moreover, as highlighted in [31], privacy preservation has become an explicit design objective in recent IoT authentication protocols, several of which incorporate dedicated countermeasures against anonymity attacks.

Table 7. IoT authentication schemes against masquerade attack

Protocol	Composition Attack	Anonymity Attack	Cloning Attack	Insider Forgery Attack	Impersonation Attack
Khan et al [31]	No	Yes	No	No	No
Amintoosi et al [56]	No	Yes	No	No	No
Ghafouri et al [57]	No	Yes	No	No	No
Yang et al [58]	No	Yes	No	No	No
Ju et al [59]	Yes	No	No	Yes	No
Li et al [60]	No	Yes	No	No	No

Table 7 compares the surveyed authentication schemes with respect to their resistance to masquerade-related threats, where *Yes* denotes an explicit countermeasure and *No* an unaddressed vector. The distribution is markedly uneven: anonymity attacks are addressed by five of the six protocols, whereas composition and insider forgery attacks are each covered by a single scheme [59]. Cloning and impersonation attacks, by contrast, are not explicitly

countered by any of the reviewed protocols, even though impersonation constitutes the defining mechanism of this attack class. No scheme addresses more than two of the five vectors considered.

Analysis. This imbalance suggests that privacy preservation and identity verification are pursued as separate objectives rather than complementary ones. Anonymity mechanisms such as pseudonym rotation conceal *who* is communicating, but they do not establish that a claimed identity is genuine. Conversely, the hardware-bound approaches required to defeat cloning and impersonation, such as the PUF-based FSMFA protocol of Chen et al. [54], are typically evaluated against physical rather than masquerade threat models and therefore rarely appear in comparisons of this kind. Bridging these two lines of work, by combining pseudonymity with hardware-rooted identity binding, remains an open direction for IoT authentication design.

3.5. Dos Attack

Denial of Service (DoS) attacks are especially damaging to IoT authentication protocols because the devices and wireless sensor nodes involved are resource constrained. Surveys on IoT key agreement protocols note that sensors have limited computing power and that protocol computations should not drain their energy; hence lightweight algorithms must be used [2]. FlowGuard researchers similarly point out that IoT devices have limited CPU and storage and therefore rely on simplified protocols, leaving them vulnerable to being co-opted into botnets[11]. In distributed DoS (DDoS) attacks, adversaries compromise many IoT devices and flood authentication servers with handshake messages, exhausting computation and memory and causing legitimate authentication attempts to fail [11]. Edge based schemes such as FlowGuard employ traffic variation detection and machine-learning models (LSTM and CNN) to identify and classify IoT DDoS traffic with 98.9 [11], while TCN-based approaches in 5G healthcare IoT dynamically monitor message frequencies and blacklist malicious nodes [61].



Figure 7. DDoS attack schema

DNS amplification attacks are a form of reflection: attackers spoof the victim's IP and send small queries (often ANY type) to open DNS resolvers; the resolvers reply with responses that are much larger (amplification ratios of 264–499), overwhelming the victim and draining the energy of authentication devices[62]. Desynchronization attacks disrupt the state between tag and server; an adversary blocks update messages so that tag and server store different values [63]. Such attacks can break synchronization in ultralightweight protocols [64], leaving devices unable to authenticate and thus unavailable. Reflection attacks use innocent IoT devices as reflectors; a case study shows that smart light bulbs, IP cameras and Raspberry Pi devices can be abused to send attack traffic to a victim without compromising the devices [65]. Collectively, these attacks cause availability loss, energy depletion and service disruption in IoT authentication.

Table 8 presents a comparative analysis of existing IoT authentication schemes with respect to their resistance to different categories of Denial-of-Service (DoS) attacks, including DNS amplification, desynchronization, distributed DoS (DDoS), and rejection attacks. As shown in the table, most surveyed schemes focus primarily on mitigating desynchronization-based DoS attacks (7 of 10), which typically arise from blocking or tampering with authentication or update messages and can render legitimate devices unable to re-authenticate. A smaller subset of protocols explicitly addresses DDoS attacks (4 of 10), often through rate-limiting mechanisms or lightweight verification techniques, while DNS amplification is considered by a single scheme only. Notably, rejection attacks are addressed by none of the reviewed protocols, indicating a common assumption that authentication endpoints are not exploited as traffic reflectors. Overall, the comparison highlights that although partial DoS resistance is

Table 8. IoT authentication schemes against DOS attacks

Protocol	DNS Amplification Attack	Desynchro-nization Attack	DDOS Attack	Rejection Attack
Braeken et al [66]	Yes	No	No	No
Nishant et al [51]	No	No	Yes	No
Kim et al [67]	No	Yes	No	No
Riaz et al [68]	No	Yes	Yes	No
Morteza et al [69]	No	Yes	Yes	No
Li et al [60]	No	Yes	No	No
Chatterjee et al [70]	No	Yes	No	No
Lee et al [71]	No	Yes	No	No
Qiu et al [21]	No	Yes	No	No
Wang et al [72]	No	No	Yes	No

achieved in several proposals, comprehensive protection against all major DoS attack vectors remains an open challenge in IoT authentication design.

Analysis. The DoS results reveal an important asymmetry in the IoT threat landscape: desynchronization is treated as a first-class concern because it directly breaks the authentication state machine, while volumetric DDoS and reflection-based vectors are considered secondary because they are often viewed as network-layer rather than protocol-layer problems. This is a dangerous assumption in large-scale IoT deployments where millions of devices can be simultaneously compromised and weaponized as reflectors. Future protocol designs should incorporate rate-limiting tokens or lightweight proof-of-work challenges at the authentication layer itself, rather than relying solely on network-level defenses.

3.6. MIM Attack

Man-in-the-middle (MITM) attacks in IoT authentication occur when an adversary covertly inserts itself between an IoT device and the gateway or cloud server to intercept, relay or alter authentication messages, as illustrated in Figure 8. IoT authentication protocols are particularly vulnerable because they often operate over open wireless channels; adversaries can eavesdrop on communications and even replay signals due to limited encryption and resource constraints[73]. Many IoT devices use lightweight handshakes without strong mutual authentication, leaving them susceptible to relay message attacks in which a malicious relay forwards messages between the device and server without modification, tricking both ends into believing they communicate directly[74]. Attackers can also passively eavesdrop to capture credentials or session keys [75] or actively modify messages altering, replaying or injecting fraudulent data to forge authentication or command execution[73]. Protocols that rely on synchronized counters or password update values are exposed to de-synchronization attacks: by blocking or altering update messages, an attacker can desynchronize the device and server, causing subsequent authentication failures [76]. Impersonation attacks occur when adversaries masquerade as a legitimate device or gateway by exploiting weak key management or predictable identifiers [77]. The impact of these attacks includes exposure of sensitive credentials, session hijacking, forged authentication decisions, and persistent disruptions that compromise data integrity and confidentiality[78]. Mitigating these threats requires robust mutual authentication, fresh nonce-based handshakes, integrity-protected messages and careful synchronization mechanisms to ensure that devices and servers maintain consistent state while resisting relay, eavesdropping, message modification and impersonation attacks.

Table 9 provides a comparative evaluation of existing IoT authentication schemes with respect to their resilience against various Man-in-the-Middle (MITM) attack vectors, including false message attacks, eavesdropping attacks, message modification attacks, password update attacks, and data manipulation attacks. The comparison reveals

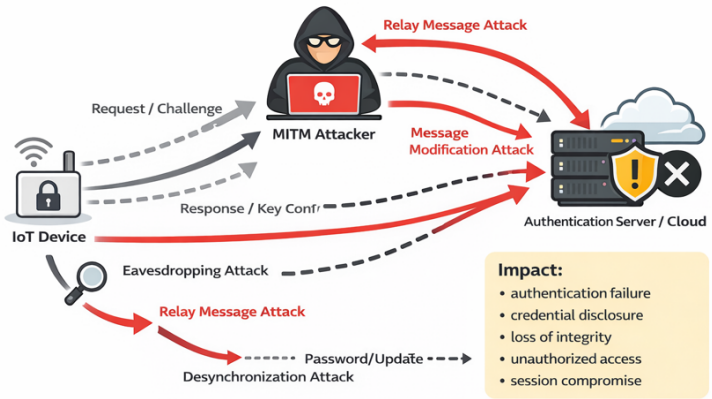


Figure 8. MITM attack schema

Table 9. IoT authentication schemes against MITM attack

Protocol	False Message Attack	Eaveadropping Attack	Message Modification Attack	Password Updating Data Manipulation Attack	Data Manipulation Attack
Abdi et al [79]	No	Yes	No	No	No
Merabet et al [44]	No	Yes	No	No	No
Alzahrani et al [80]	No	Yes	No	No	No
Banerjee et al [81]	No	Yes	No	No	No
Dammak et al [82]	No	Yes	No	No	No
Khan et al [83]	Yes	No	No	No	No
Kim et al [84]	Yes	No	No	No	No
Das et al [53]	No	No	Yes	No	No
Rostampour et al [85]	No	No	No	No	Yes
Kaveh et al [86]	Yes	No	No	No	No
Su et al [87]	Yes	Yes	No	No	Yes
Li et al [88]	Yes	No	No	No	Yes
Alharthi et al [89]	No	Yes	No	No	Yes
Mahapatra et al [90]	No	No	Yes	No	Yes
Tun et al [91]	No	No	Yes	No	Yes
Lee et al [92]	Yes	No	Yes	No	Yes

that eavesdropping is the most widely covered threat, addressed by half of the surveyed schemes, typically through encryption of authentication exchanges and the use of fresh nonces or timestamps. Data manipulation and false message attacks follow, with seven and six schemes respectively, while message modification is explicitly countered by only four protocols, often relying on cryptographic binding between identities, messages, and session keys. Su et al. [87] and Lee et al. [92] offer the broadest coverage, each addressing three of the five vectors, yet no scheme covers more than three. Most strikingly, password update attacks are addressed by none of the surveyed protocols, suggesting that update and re-registration phases are left unprotected in current designs. Overall, the

table highlights that while partial MITM resistance is commonly achieved, comprehensive protection against both passive and active MITM attack variants remains inconsistent across existing IoT authentication schemes, underscoring the need for more holistic security designs.

Analysis. Three design gaps emerge from Table 9. First, passive eavesdropping resistance is achieved cheaply via encryption and is therefore the most commonly addressed MITM vector; however, encryption alone does not prevent relay attacks, where a legitimate ciphertext is forwarded without modification. Second, active attacks such as message modification require integrity-protected channels (e.g., MACs or digital signatures), which impose additional computation and are therefore avoided in the lightest-weight schemes. Third, password update and re-registration phases are entirely neglected across the surveyed literature: these phases are temporally distant from the initial authentication and are therefore less studied, yet they represent a significant window of vulnerability in long-lived IoT deployments. Comprehensive MITM resistance thus requires protocol designs that give equal security attention to all protocol phases, not just the initial handshake.

4. IoT Authentication Techniques

Authentication protocols for IoT leverage a set of specific cryptographic and hardware-based techniques aiming at overcoming the extreme constraints linked to connected nodes, such as low computation, energy supply, high heterogeneity, and openness to potential attacks due to unsecured and open channels. This is a stark contrast from the traditional network environment, which demands scalability and the capability of resisting threats from an impersonation attack, replay attack, MITM, and DoS attacks with lightweight authentication mechanisms. The literature has presented different IoT authentication approaches leveraging different primitives and architectures, such as symmetric and asymmetric cryptography, hash-based techniques, chaotic-map-based constructions, biometric information, Physical Unclonable Functions, and cloud-, fog-, and blockchain-enabled authentication frameworks [1].

Figure 9 illustrates a classification of the principal authentication methods used in IoT systems, highlighting the diversity of underlying techniques and their roles within different architectural models. Each of these techniques offers specific trade-offs in terms of security strength, computational and communication overhead, preservation of privacy, and deployment complexity. For this reason, recent IoT authentication protocols combine several techniques with the aim of striking an appropriate tradeoff between security robustness and operational efficiency under resource constrained conditions.

4.1. Password-Based Authentication

Password-based authentication represents one of the earliest and simplest mechanisms for validating the identity of a user or device in networked systems. In this approach, authentication relies on a knowledge factor, where a legitimate entity proves its identity by submitting a unique identifier (user or device ID) together with a secret password, typically composed of alphanumeric characters and symbols. During the registration phase, the credentials often stored as hashed or salted values are maintained in a centralized authentication database. Subsequently, during the authentication phase, the user or IoT node transmits its credentials to the authentication server, which verifies the received information against the stored records and grants access only if a match is found, as illustrated in Figure 10, which depicts the complete registration and authentication workflow of password-based schemes. Despite its conceptual simplicity and low computational overhead, this mechanism is rarely adopted in pure IoT environments, as most IoT nodes operate autonomously without human interaction and lack secure interfaces for password input. Moreover, the low entropy of user-chosen passwords exposes such schemes to dictionary and password-guessing attacks, while transmission over open wireless channels renders them vulnerable to replay and man-in-the-middle attacks if challenge–response or nonce-based protections are not incorporated. Consequently, password-only authentication is considered insufficient for large-scale IoT deployments, particularly in sensor-centric networks such as WSNs and smart environments. To mitigate these limitations, recent research has explored enhanced variants, including password-based authentication protocols integrated with quantum key distribution for next-generation communication systems. In particular, quantum-assisted password authentication

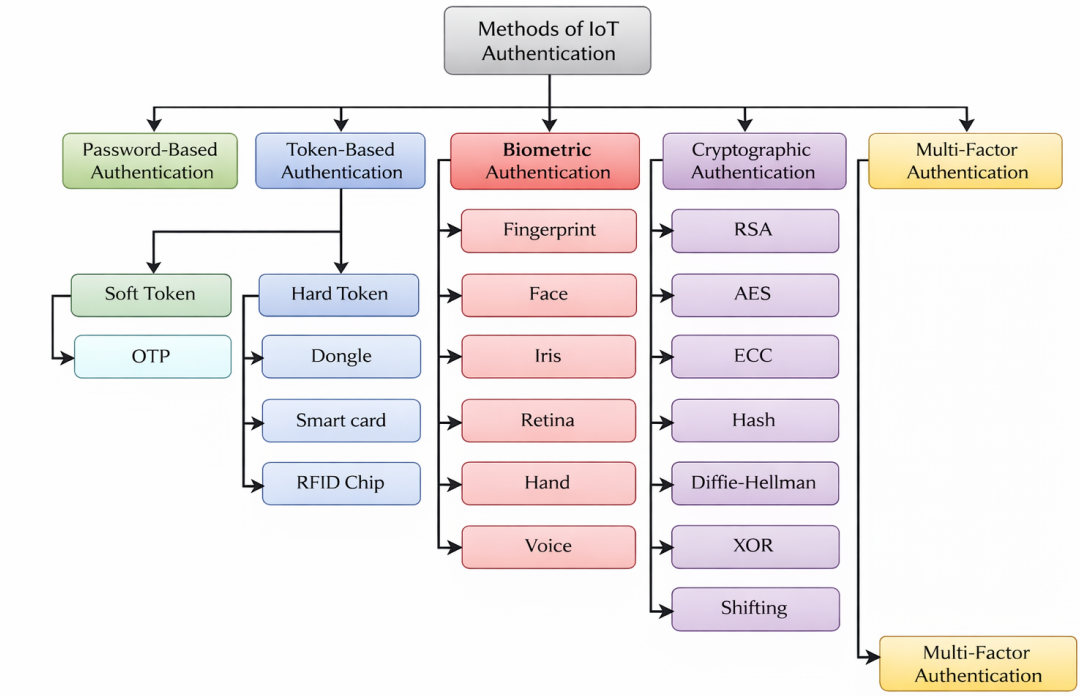


Figure 9. Authentication methods

schemes have been proposed for emerging 6G-enabled smart grids and vehicular ad hoc networks, demonstrating improved resistance against eavesdropping and impersonation attacks through quantum security primitives [93, 94, 95]. Nevertheless, even with such enhancements, password-based authentication is generally regarded as a baseline solution that must be combined with additional authentication factors to satisfy the stringent security requirements of modern IoT systems.

4.2. Token-based authentication

Token-based authentication is a widely used mechanism in which the authentication server verifies the identity of the user or device based on the possession of a cryptographic token, which is obtained or produced in the registration phase. Contrary to password-based systems, this mechanism requires possession authentication and can be broadly categorized under soft token-based authentication and hard token-based authentication. In soft token-based authentication, the server will dynamically send a temporary password (T-P Password) or challenge, which is used for only one time and is applicable for a limited time duration, in order to prevent the threat of a replay attack. On the other hand, hard token-based authentication makes use of specialized hardware tokens, which include devices such as USB tokens, smart cards, and RFID, to store secrets and support cryptographic computations. These hardware tokens are beneficial in an IoT setup, wherein computational-intensive operations can be delegated to remote devices with large computational capacities, while providing mutual authentication.

4.3. Biometric authentication

Biometric authentication is an inherence-based mechanism that verifies the identity of a user by exploiting unique physiological or behavioral characteristics, such as fingerprints, facial features, iris or retina patterns, hand geometry, and voice traits. These biometric modalities are widely recognized for their distinctiveness and have

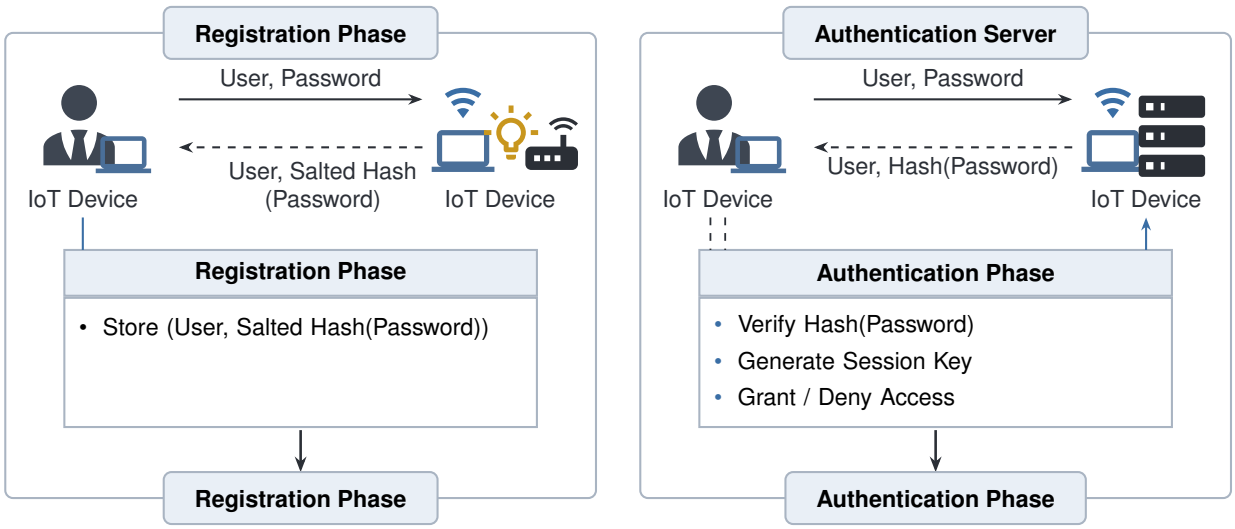


Figure 10. Authentication phases

been extensively studied in secure access control systems and IoT-enabled applications [82, 96, 97]. Among them, fingerprint-based authentication is the most commonly adopted due to its technological maturity, low sensing cost, and ease of integration with IoT gateways and smart devices. In a typical biometric authentication process, a user's biometric data are captured during a registration phase, processed to extract distinctive features, and stored often in encrypted or transformed form on an authentication server or trusted edge node. During subsequent authentication attempts, newly acquired biometric samples are matched against the stored templates, and access is granted only if the similarity threshold is satisfied. Despite offering stronger identity assurance than knowledge-based schemes, biometric authentication is rarely deployed as a standalone solution in IoT environments. This is primarily due to the autonomous operation of IoT nodes, the absence of biometric sensing capabilities on resource-constrained devices, and the irreversible nature of biometric traits once compromised. Furthermore, biometric systems may be exposed to replay and man-in-the-middle attacks if biometric templates or feature vectors are transmitted over insecure communication channels without freshness guarantees. As a result, biometric authentication in IoT systems is typically combined with cryptographic techniques or additional authentication factors to enhance resistance against impersonation, privacy leakage, and denial-of-service attacks.

4.4. Cryptographic Authentication

Cryptographic authentication is a basic cybersecurity mechanism used in the context of the Internet of Things to ensure the secure verification of identity and secure communication between devices without human interaction[3]. This type of authentication uses matured concepts of cryptography and can thus be mainly categorized into symmetric key-based authentication, asymmetric key-based authentication, and hardware-based authentications involving Physical Uncloneable Functions (PUFs). Another authentication method using elliptic curve cryptography (ECC) has emerged as a lightweight and efficient public-key authentication method for resource-limited devices in the Internet of Things.

4.4.1. Symmetric Key Based Authentication Symmetric Key Based Authentication is an authentication methods based on the utilization of secret keys shared by communicating parties. This includes methods using light cryptographic primitives like hash functions, message authentication codes (MAC), or XOR functions. This is commonly implemented in resource-constrained nodes like those used in the internet of things (IOT)[98].

4.4.2. Asymmetric Key–Based Authentication This subsection introduces authentication methods involving public-key cryptography, where every entity has its own public and private key. This section also covers traditional authentication methods as well as the problems associated with computation in IoT networks[98].

4.4.3. ECC-Based Authentication Protocol Design Elliptic curve cryptography based authentication has gained significant attention in IoT security due to its ability to provide a security level comparable to traditional public key schemes while requiring substantially smaller key sizes. By operating over elliptic curve groups defined on finite fields, ECC enables efficient public key operations with reduced computational complexity, memory usage, and energy consumption, making it particularly well suited for resource constrained IoT devices such as sensors, actuators, and embedded controllers. As a result, ECC is widely adopted in modern IoT authentication and key agreement protocols to achieve strong security guarantees, including mutual authentication and session key establishment, without imposing excessive overhead on low power devices.

4.4.4. ECC: Fundamentals and Mathematical Background over a finite field $\mathbb{F}_p$ is commonly defined by the following Weierstrass equation:

$$E: \quad y^2 \equiv x^3 + ax + b \pmod{p}, \tag{1}$$

where $a, b \in \mathbb{F}_p$ satisfy the non singularity condition

$$4a^3 + 27b^2 \not\equiv 0 \pmod{p}. \tag{2}$$

In ECC based authentication, a private key d is randomly selected from the interval $[1, n-1]$, and the corresponding public key Q is computed as

$$Q = d \cdot G, \tag{3}$$

where G is a publicly known base point on the elliptic curve of order n. The security of ECC relies on the computational hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP) [99], which makes it infeasible to derive d from Q, thereby ensuring strong resistance against impersonation and key recovery attacks in IoT authentication protocols.

4.4.5. Physical Uncloneable Functions PUF-based authentication has emerged as a robust hardware-assisted security solution for IoT environments, leveraging the inherent manufacturing variations of integrated circuits to generate device-unique and unclonable identities. Unlike conventional cryptographic schemes that rely on stored secret keys, Physical Unclonable Functions exploit intrinsic physical properties of hardware components to produce challenge–response pairs that are extremely difficult to replicate or predict. During authentication, a verifier issues a challenge to the IoT device, which generates a corresponding response derived from its unique physical structure; this response is then validated against a reference model stored at the authentication server. The absence of permanently stored secret keys significantly enhances resistance against physical capture, invasive attacks, and device cloning. Moreover, when combined with fuzzy extractors and lightweight cryptographic primitives, PUF-based authentication schemes can achieve reliable and repeatable responses despite environmental noise and aging effects. Owing to their low computational overhead and strong security properties, PUF-based mechanisms are particularly well suited for resource-constrained IoT devices deployed in hostile or unattended environments.

5. Security Verification Techniques and Simulation tools

A synthesis of the main tools, simulation platforms, and evaluation environments used in the analyzed research works is presented in Table 10. It highlights the various simulators, formal frameworks, and security analysis tools employed by the authors to validate the performance and robustness of the proposed authentication protocols. This overview helps identify the dominant methodological approaches adopted in the literature, as well as current trends in experimental and formal evaluation of security mechanisms in IoT environments.

Table 10. Security Verification Techniques and simulation tools

Protocol	Security Verification Techniques	simulation tools	Description
Zerrouki et al [17]	AVISPA	-	The authors proposed an authentication protocol for IoT devices based on PUFs.
Li et al [18]	Verifpal	-	The authors propose a PUF-based end-to-end anonymous authentication protocol for IoT devices.
Zahednejad et al [19]	ProVerif	-	The authors propose a robust AKA scheme for IoT and cloud environments.
Merabet et al [44]	AVISPA	Reel Implementation	The authors propose a robust ECC scheme for IoT and cloud environments.
Abdi et al [79]	ROR model, proVerif	OPNET	The authors propose a secure and efficient AKA protocol for IoT and cloud servers.
Alzahrani et al [80]	BAN logic, Dual CPU E2200	-	The authors propose a PUF-based end-to-end anonymous authentication protocol for IoT devices.
Banerjee et al [81]	BAN logic	-	The authors propose a biometric-based user authentication and key agreement scheme for WSN-based IoT using smart cards.
Kaveh et al [86]	AVISPA	Reel Implementation	The authors propose an OCECPUF-based lightweight authentication protocol for smart grid IoT.

Continued on next page

Table 10 – continued from previous page

Protocol	Security Verification Techniques	simulation tools	Description
Su et al [87]	ProVerif	NS-3	A three-factor (password, biometrics, smart card) cluster-based AKA protocol for IoMT. Ensures mutual authentication, anonymity, resistance to replay, impersonation, privilege escalation, and desynchronization attacks, while maintaining low computational and communication overhead for resource-constrained medical sensors.
Li et al [88]	BAN logic, Syther	C/C++ OPENSSL	The authors propose an ECC-based anonymous authentication and key agreement protocol for IIoT.
Alharthi et al [89]	AVISPA, BAN logic	-	The authors propose a lightweight PUF-based mutual authentication protocol for smart manufacturing IoT.
Mahapatra et al [90]	AVISPA, ProVerif	-	The authors propose a multilayer authentication and key agreement (ML-AKA) protocol for NSA-based 5G C-IoT networks, ensuring mutual authentication, resistance to MITM, spoofing, and DDoS attacks, with improved communication efficiency.

Continued on next page

Table 10 – continued from previous page

Protocol	Security Verification Techniques	simulation tools	Description
Tun et al [91]	AVISPA	Reel implementation	Authors propose a secure PUF-based authentication protocol for IoT devices using Paillier homomorphic encryption and plaintext equality testing to prevent CRP disclosure, resist modeling and impersonation attacks, and enable encrypted verification with low computational overhead.
Lee et al [92]	Scyther, Ban Logic	Reel implementation	The authors propose a lightweight anonymous authentication and key agreement protocol for IoT-enabled smart environments.
Kim et al [67]	Ban Logic, RoR Model, AVISPA	NS-3	The authors propose a biometric-based user authentication and key agreement scheme for WSN-based IoT using smart cards.
Malik et al [100]	No	Contiki-NG / Cooja simulator	The authors propose an ECC- and MD5-based lightweight authentication and key establishment protocol for IoT devices.
Zhang et al [101]	Syther	Reel implementatio	The authors propose a lightweight authentication and key agreement protocol for IoT networks, ensuring mutual authentication and resistance to common attacks.
Wan et al [102]	BAN logic	-	Authors propose a lightweight two-factor continuous authentication protocol for agricultural IoT devices based on PUF and location information.

6. Performance Evaluation Techniques

As the IoT ecosystem continues to face increasingly sophisticated security threats, the development of advanced authentication mechanisms has become essential. Equally important is the rigorous evaluation of these proposed schemes to assess their security strength and operational efficiency. Accordingly, this section presents a comprehensive discussion of various evaluation techniques, along with their associated parameters and the mathematical formulations used to support the analysis.

Table 11 provides a cross-cutting synthesis of all authentication protocols reviewed in this survey. Each protocol is characterised along five dimensions: the attack categories it resists, its underlying authentication technique, qualitative assessments of computation and communication cost, the formal verification tool(s) employed, and the degree of privacy/anonymity support. Taken together, these columns reveal a consistent pattern: no single protocol achieves comprehensive coverage across all dimensions. Most proposals excel in one or two areas typically either security breadth or efficiency while leaving others underserved. In particular, privacy and formal verification remain the most frequently neglected properties, and no reviewed scheme simultaneously achieves full-spectrum attack resistance with low computation/communication cost and rigorous formal proofs. This gap motivates the open challenges discussed in Section 7.

6.1. Average Response Time

The average response time represents the duration required by the server or gateway node (GWN) to generate and deliver a response to a client request. This metric is affected by several factors, including server configuration, the number of concurrent users, available network bandwidth, request arrival rate, request type, and processing (thinking) time. The response time for an individual request is defined as the difference between the instant at which the client submits the request and the moment the first response is received, as expressed in Equation (4):

$$T_{res} = t_{res} - t_{req} \tag{4}$$

where T_{res} denotes the response time, t_{req} is the time at which the client issues the request, and t_{res} corresponds to the time at which the response is received. The average response time is then computed as the mean of all response times over a given observation period, as shown in Equation (5):

$$T_{avg_res} = \frac{n}{r} - T_{think} \tag{5}$$

where T_{avg_res} represents the average response time, n is the number of concurrent users, r denotes the number of requests processed per second, and T_{think} is the average user thinking time (in seconds). For accurate performance evaluation, the thinking time should always be included in the response time calculation, as it significantly influences the perceived responsiveness of the system.

6.2. Handshake Duration

The handshake duration refers to the time required to complete the negotiation process between two communicating entities in an IoT environment, such as a user, sensor, actuator, server, or other network nodes. As illustrated in Figure 11, the authentication handshake typically involves a two-round message exchange, where the client initiates a discovery request, the server responds, and the client request is finally acknowledged by the server. The handshake duration is measured at the client side and includes both communication and processing delays.

The total handshake duration, denoted by T_{hs}, is computed using Equation (6):

$$T_{hs} = T_{ts} + T_{res} + T_p \tag{6}$$

where T_{hs} represents the handshake duration, T_{ts} denotes the time required to transmit the session request, T_{res} is the client response time, and T_p corresponds to the processing time at the server. To obtain accurate and reliable results, the handshake duration is evaluated over multiple authentication sessions between the client and the server. Additionally, statistical measures such as the standard deviation are used to analyze the variability and accuracy of

Table 11. Comprehensive comparative analysis of IoT authentication protocols across attack resistance, authentication technique, performance, formal verification, and privacy dimensions. Attack coverage reports only the vectors explicitly tabulated in Tables 4–9; a dash indicates that the protocol was not evaluated in the corresponding comparison. Comp. = Computation cost; Comm. = Communication cost; L = Low; M = Medium; H = High.

Protocol	**Attack Coverage**	**Auth. Tech.**	**Comp.**	**Comm.**	**Formal Verif.**	**Privacy**
Zerrouki [17]	Physical (USB)	PUF + Hash	L	M	Verifpal	Partial
Li [18]	Physical (USB)	PUF (E2E)	L	L	Verifpal	High
Zahednejad [19]	Physical (Card)	Chaotic Map	M	M	ProVerif	Partial
Ech-chebaby [43]	Forging (Replay)	ECC	M	L	None	Partial
Javadi [22]	Physical (Device, Mobile, Card)	ECC + ASCON	L	L	None	Partial
Wu [24]	Physical (Card); Forging (Gateway)	Symmetric	L	L	None	Partial
Su [87]	MITM (False msg., Eavesdrop., Data)	3-Factor+Bio	H	M	ProVerif	High
Kim [67]	DoS (Desync)	Blockchain+Bio	H	H	BAN+AVISPA	High
Lee [92]	Physical (Device, Card); MITM	Lightweight AKA	L	L	Scyther+BAN	High
Braeken [66]	DoS (DNS Amp.)	PUF	L	L	None	Partial
Das [53]	Forging (Replay); MITM (Msg. mod.)	ECC	M	L	None	Partial
Alharthi [89]	MITM (Eavesdrop., Data)	PUF	L	L	AVISPA+BAN	Partial
Abdi [79]	MITM (Eavesdrop.)	Symmetric+ECC	M	M	ROR+ProVerif	High
Khan [31]	Physical (Device); Masquerade (Anonymity)	ECC+Biometric	M	L	None	Partial
Riaz [68]	DoS (Desync, DDoS)	RFID Lightweight	L	L	None	Low
Tun [91]	MITM (Msg. mod., Data)	PUF+Homomorphic	M	M	AVISPA	High
Mahapatra [90]	MITM (Msg. mod., Data)	Multi-layer AKA	M	M	AVISPA+ProVerif	Partial

the handshake performance.

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \mu)^2} \tag{7}$$

where σ denotes the standard deviation, N is the total number of samples, x_i represents the handshake duration of the i-th iteration, and μ is the mean handshake duration.

6.3. Communication Cost

The communication overhead associated with IoT authentication varies significantly across different protocols, depending on their design and operational phases. Authentication procedures often involve the exchange of multiple messages with varying sizes across several stages of the protocol. Typically, establishing a secure authentication

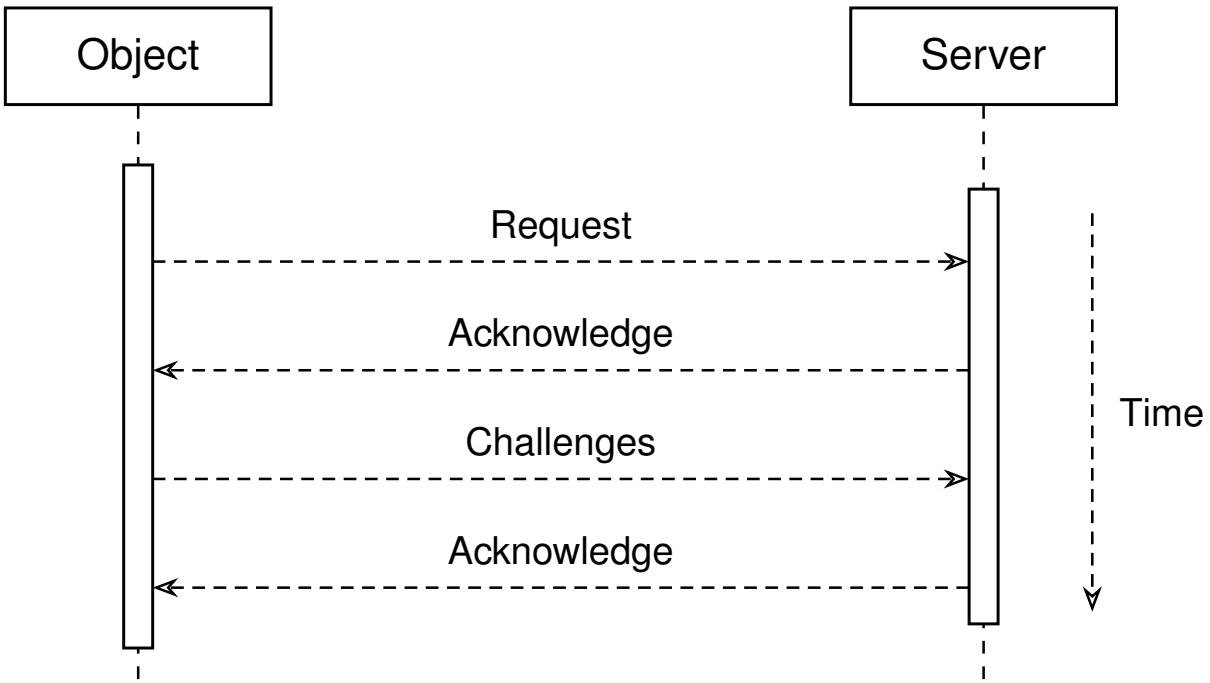


Figure 11. Handshake Duration

session requires at least four message exchanges among entities such as the user, sensor node, and gateway or authentication server. Since each message carries distinct authentication parameters, their lengths are not uniform, resulting in different transmission costs. In addition to protocol design, communication cost must also be evaluated with respect to the constraints imposed by underlying communication standards. Different IoT standards specify different maximum payload sizes; for example, IEEE 802.15.4 supports a maximum frame size of 127 bytes, whereas IEEE 802.15.6 allows frame lengths of up to 255 bytes. Therefore, authentication protocols must be carefully designed to ensure that their communication requirements remain compatible with the targeted IoT standards while minimizing overhead.

6.4. Computation Cost

In IoT networks, computational cost is highly dependent on the type of authentication protocol employed. Since most IoT devices operate under strict resource constraints, executing computationally intensive operations is often impractical. Consequently, protocol designers aim to develop lightweight authentication schemes that minimize processing overhead while maintaining adequate security. To achieve this balance, many existing protocols rely on simple and efficient cryptographic primitives such as hash functions, XOR operations, and concatenation techniques to protect transmitted messages. In addition, mechanisms based on elliptic curve cryptography, modular arithmetic, fuzzy commitments, and related lightweight cryptographic constructs have been incorporated to enhance security without imposing excessive computational burden. These approaches enable secure authentication while remaining suitable for resource-limited IoT environments

6.5. Storage Cost / Memory Cost

Storage cost is another important factor in the design of IoT authentication protocols, as devices typically have limited memory capacity. Authentication mechanisms may require the storage of various credentials

and parameters, such as secret keys, identities, sensor information, or gateway-related data. Smart card–based approaches are commonly adopted in IoT authentication due to their ability to securely store sensitive information required during the authentication process. Different protocols impose different storage requirements depending on the number and type of cryptographic elements maintained by the participating entities. As a result, minimizing memory usage while preserving strong security properties remains a key objective in the development of efficient IoT authentication schemes.

6.6. Energy Cost

IoT components typically operate under strict energy constraints, making energy consumption a critical performance metric for authentication protocols. Since energy usage is directly related to power consumption, protocols that require excessive computation or communication may significantly reduce device battery lifetime. Consequently, evaluating the energy cost associated with authentication procedures is essential alongside other performance metrics. The energy consumed during data transmission and reception can be estimated using well-established energy models, as defined in Equations (8) and (9).

The energy required to transmit data between two communicating entities is given by:

$$E_{Tx}(k,d) = E_{elec} \cdot k + E_{amp} \cdot k \cdot d^2 \tag{8}$$

where $E_{Tx}(k,d)$ denotes the energy consumption for transmitting data, k represents the data size in bits, d is the distance between the two entities, E_{elec} is the energy consumed by the electronic circuitry per bit, and E_{amp} is the energy consumption constant of the power amplifier used to maintain radio transmission over distance d.

Similarly, the energy consumed for receiving data is expressed as:

$$E_{Rx}(k) = E_{elec} \cdot k \tag{9}$$

where $E_{Rx}(k)$ denotes the energy required to receive k bits of data. These expressions indicate that the transmission energy depends on both the data size and the transmission distance, whereas the reception energy depends solely on the data volume. Therefore, minimizing communication overhead and transmission distance is essential for improving the energy efficiency of IoT authentication protocols.

7. Open Issues and Future Directions

Although significant progress has been made in designing lightweight authentication and key agreement protocols, our survey reveals several unsolved problems and emerging directions. Many proposals still focus narrowly on selected attack classes and exhibit trade-offs between security, computational cost and implementation complexity. This section discusses the major challenges and outlines promising research directions.

7.1. Full-Spectrum Attack Resistance

Most IoT authentication schemes target a limited set of threats such as replay or impersonation while overlooking other attacks such as modelling of hardware responses, side-channel leakage or sophisticated multi-stage intrusions. For example, studies on physical unclonable functions (PUFs) note that many PUF designs are susceptible to machine-learning modelling attacks and require additional error-correction to handle noisy responses[103]. In addition, research on 6G IoT highlights that legacy devices continue to employ weak or outdated authentication mechanisms and that low-latency immersive communications enlarge the attack surface for spoofing and man-in-the-middle attacks[6]. Future protocols must therefore provide comprehensive resistance against a broad range of network-layer, physical-layer and modelling attacks. One possible direction is to integrate cryptographic authentication with anomaly detection and behavioural profiling so that deviations in traffic patterns, timing or device states trigger verification of the session. Leveraging federated or edge-based intrusion detection to collaboratively identify emerging attack signatures could also enhance the resilience of resource-constrained devices.Hybrid deep-learning detectors designed under tight parameter budgets, such as the

moment-based EfficientNet framework of Al-Hazaimeh et al. [104], indicate that this coupling is computationally realistic for gateway-class devices. Furthermore, research should explore how side-channel countermeasures and privacy-preserving machine-learning models can be applied to authentication contexts without violating energy budgets.

7.2. Lightweight yet Post-Quantum Secure Authentication

The advent of quantum computing threatens classical public-key primitives. While post-quantum cryptography (PQC) offers alternatives, implementing PQC on constrained devices is non-trivial. Hybrid frameworks combining elliptic curve cryptography (ECC) with post-quantum key encapsulation mechanisms (KEMs) have been proposed to balance efficiency and security: the classical ECC component is used for low-overhead authentication, while the post-quantum KEM ensures long-term confidentiality[7]. However, such schemes require two key exchanges and careful coordination of cryptographic domains. A complementary line of work moves the privacy guarantee into the authentication exchange itself: Tawfik et al. [105] combine a lightweight post-quantum zero-knowledge proof protocol with blockchain-based device verification and homomorphic computation, reporting authentication latencies of approximately 350 ms and proof generation/verification costs of 300 ms and 120 ms respectively. Their results illustrate both the feasibility of quantum-resistant privacy-preserving authentication and its remaining cost, since the reported evaluation relies on a simulated sensor network rather than constrained hardware. There is a need for systematic exploration of hybrid architectures that integrate lightweight symmetric primitives, ECC and lattice-based or code-based KEMs under a unified key-agreement framework. Future research should evaluate how parameter selection, compression techniques and hardware acceleration can reduce the overhead of PQC while maintaining forward secrecy and mutual authentication. As quantum-safe hardware PUFs emerge, combining them with hash-based signatures or authenticated key-exchange protocols could enable post-quantum-secure yet lightweight authentication for IoT devices.

7.3. PUF Reliability, Modelling Attacks and Aging Effects

PUF-based authentication leverages the intrinsic manufacturing variations of hardware to generate device-unique responses. Nevertheless, many existing PUFs exhibit unstable responses under environmental changes and are vulnerable to modelling and statistical attacks. Studies have shown that arbiter PUFs can be approximated by linear models, making them susceptible to machine-learning attacks and poor statistical characteristics[103]. Response feedback and other enhanced PUF architectures offer improved avalanche characteristics and resistance to modelling, but their reliability across the device lifetime has not been thoroughly evaluated[103]. Aging effects and environmental noise can gradually degrade PUF reproducibility, undermining authentication reliability. Future work should therefore develop adaptive error-correction and response-stabilisation mechanisms that consider temperature, voltage and aging. Combining multiple weak PUFs or hybridising PUFs with lightweight hash functions could increase entropy and modelling resistance. Additionally, there is a need for systematic benchmarks and modelling-attack competitions to evaluate PUF designs under realistic IoT conditions.

7.4. Scalability and 6G IoT Environments

Emerging 6G networks will support massive machine-type communications (mMTC) with billions of devices and diverse quality-of-service requirements. Surveyed literature notes that massive connectivity, ultra-low latency and heterogeneous network conditions challenge existing authentication protocols, since many devices have limited computational capabilities and cannot participate in heavy cryptographic exchanges [6]. Furthermore, the lack of standardised security frameworks for 6G means that protocols must accommodate variable frame sizes, multiple access schemes and cross-domain service orchestration [6]. To scale securely, future schemes should support batch or group authentication that amortises computational cost across many devices, possibly using aggregate signatures or certificate-less mechanisms. Identity-based cryptography and trust delegation at edge/fog nodes could offload expensive operations from sensors and support seamless handovers. Lightweight key-update strategies and revocation mechanisms are also required to cope with device churn and dynamic topologies in 6G networks.

7.5. Continuous and Context-Aware Authentication

Most protocols adopt one-time authentication, after which the session remains valid indefinitely. However, continuous authentication is necessary to detect session hijacking, stolen devices and dynamic risk conditions. Recent work has advocated combining biometric cues with environmental sensing to provide ongoing verification; for example, a lightweight system fusing facial recognition with ambient sensors can authenticate users continuously and includes formal analysis with Scyther[106]. Nevertheless, continuous methods must account for energy consumption and adversarial manipulation. Many current schemes are susceptible to face spoofing or can be easily disabled by draining the device battery[106]. Future research should explore multimodal context-aware authentication that adapts to user behaviour, device state and environmental factors while minimising sensing overhead. Machine-learning models can detect anomalies in sensor patterns, but they must be designed to resist adversarial examples and preserve user privacy. Integration of continuous authentication with session-key update mechanisms could automatically re-negotiate keys when context changes.

7.6. Formal Verification and Real-World Deployment Gaps

A recurring issue in IoT authentication literature is the reliance on informal reasoning or simulation-based evaluation. Numerous protocols claim resistance to various attacks, yet later analyses reveal flaws due to desynchronisation, key compromise or man-in-the-middle attacks. A recent study emphasises that many IoT authentication schemes undergo only informal or simulation-based validation, which fails to detect subtle logical flaws and leaves systems vulnerable[8]. Formal verification tools such as ProVerif and AVISPA typically support bounded sessions and simplified adversary models, while advanced frameworks like Tamarin can handle unbounded sessions and complex equational theories[8]. However, there is no unified methodology for applying these tools to resource-constrained environments, and performance under varying network conditions is rarely examined. Future work should integrate formal verification into the design process and complement symbolic analysis with real-world experiments on heterogeneous testbeds. Establishing open benchmark suites that combine formal proofs, emulated environments and field deployments could promote reproducible research and accelerate the maturation of IoT authentication protocols.

7.7. Energy-Aware and Sustainability-Driven Security Design

With billions of devices expected to operate unattended, energy consumption is a major constraint. Achieving high security and low energy usage simultaneously remains an open challenge. A recent survey on energy-aware security mechanisms outlines several research trends such as energy harvesting, context-aware security, blockchain-based protection and standardisation aimed at balancing energy efficiency with robustness. Energy-harvesting technologies can extend device lifetimes by powering cryptographic operations from ambient sources, but they introduce variability and require careful scheduling of computation and communication. Context-aware security policies can adjust authentication strength based on risk levels, reducing overhead in benign environments. Blockchain technology offers tamper-proof data management with minimal energy overhead when consensus algorithms are optimised for IoT. Standardisation and interoperability are also essential to ensure that devices from different vendors can implement consistent and efficient security mechanisms. Future research should develop adaptive protocols that leverage energy harvesting, dynamically adjust cryptographic operations based on residual energy and integrate sustainability metrics into security evaluation.[5]

7.8. Directions Leveraging Emerging Technologies

To address the above challenges, several technological trends offer promising avenues:

7.8.1. Edge/Fog/Cloud-Assisted Authentication Offloading heavy cryptographic computations and trust management to edge or fog nodes can reduce latency and energy usage.[107] Hierarchical authentication frameworks can support group keys and mutual trust across devices while relying on cloud resources for policy enforcement and revocation. Integration with explainable AI can provide transparency in authentication decisions.

7.8.2. AI/ML-Assisted Intrusion-Aware Authentication Machine-learning models deployed at the network edge can detect anomalies in authentication attempts and dynamically adjust security policies. Federated learning allows collaborative model training without sharing raw data, enhancing privacy. Combining AI with homomorphic encryption and lightweight cryptographic primitives can enable real-time intrusion-aware authentication in mission-critical applications.A recent systematic review of large language models applied to IoT security [9] reports detection accuracies above 98% for transformer-based frameworks, but also identifies persistent gaps in resource optimisation, energy reporting and cross-platform compatibility, constraints that mirror the deployability limits discussed in Section 6.

7.8.3. Blockchain-Enabled Trust Management Distributed ledgers can manage device identities, credentials and revocation lists in a tamper-proof manner. Proof-of-authority or delegated proof-of-stake consensus mechanisms reduce energy consumption compared with proof-of-work. Smart contracts can automate key-agreement workflows and enforce access policies.

7.8.4. Hybrid ECC–PUF–Hash Constructions To achieve strong security with low overhead, hybrid schemes can combine ECC for key exchange, PUFs for device authentication and hash chains for lightweight message authentication. For instance, an ECC-based mutual authentication protocol could derive session keys from PUF responses hashed with lightweight functions, providing resilience to both quantum attacks and physical cloning.

By tackling the open issues identified above and exploring these emerging directions, future research can pave the way for secure, energy-efficient and scalable authentication in next-generation IoT and 6G ecosystems.

8. Conclusion

The concepts of networking and connectivity are expected to undergo significant transformation in the coming years due to the rapid increase in the number of connected devices worldwide. This growth is largely driven by the continuous expansion of the Internet of Things (IoT), which enables large-scale interconnection of heterogeneous systems. Despite these advancements, IoT security remains a critical concern, as existing solutions still struggle to provide adequate reliability and protection against evolving security threats.

Authentication plays a central role in securing IoT environments, as it represents the primary gateway through which users or devices gain access to the network. Weak or poorly designed authentication mechanisms can undermine the entire system, leaving it vulnerable to various attacks. Consequently, it is essential to identify potential threats targeting IoT authentication and to evaluate existing protocols designed to mitigate these risks.

To the best of our knowledge, comprehensive studies that jointly analyze IoT authentication threats, attack models, and protection mechanisms remain limited. Most existing research focuses either on general IoT security or on specific authentication schemes in isolation. This survey aims to address this gap by providing a systematic overview of authentication-related attacks and corresponding defense strategies. The insights presented in this paper can assist researchers in understanding current limitations and guide future efforts toward the design of more secure, efficient, and user-oriented IoT authentication protocols.

REFERENCES

1. R. Singh, K. P. Sharma, and L. K. Awasthi, “A decade review of authentication and communication methods in iot environment,” *Wireless Personal Communications*, vol. 139, pp. 595–623, Nov. 2024.
2. S. Szymoniak and S. Kesar, “Key agreement and authentication protocols in the internet of things: A survey,” *Applied Sciences*, vol. 13, no. 1, 2023.
3. W. Bekri, R. Jmal, and L. C. Fourati, “Secure and trustworthiness iot systems: investigations and literature review,” *Telecommunication Systems*, vol. 85, pp. 503–538, 2024.
4. I. Butun, P. Österberg, and H. Song, “Security of the internet of things: Vulnerabilities, attacks, and countermeasures,” *IEEE Communications Surveys Tutorials*, vol. 22, no. 1, pp. 616–644, 2020.
5. P. He, Y. Zhou, and X. Qin, “A survey on energy-aware security mechanisms for the internet of things,” *Future Internet*, vol. 16, no. 4, 2024.

6. N. Kaur and L. Gupta, "Securing the 6g–iot environment: A framework for enhancing transparency in artificial intelligence decision-making through explainable artificial intelligence," *Sensors*, vol. 25, no. 3, 2025.
7. A. Braeken, "Flexible hybrid post-quantum bidirectional multi-factor authentication and key agreement framework using ecc and kem," *Future Generation Computer Systems*, vol. 166, p. 107634, 2025.
8. V. Malele and G. Mandinyenya, "Tamarin-based verification of authentication protocols in smart city iot," *IJIRSS*, vol. 8, no. 12, p. 11065, 2025. Open Access.
9. M. Tawfik, A. H. Abdelhaliem, and I. S. Fathi, "Transforming IoT security through large language models: A comprehensive systematic review and future directions," *Statistics, Optimization & Information Computing*, vol. 14, pp. 1018–1044, 2025.
10. L. Malina, J. Hajny, R. Fujdiak, and J. Hosek, "On perspective of security and privacy-preserving solutions in the internet of things," *Computer Networks*, vol. 102, pp. 83–95, 2016.
11. Y. Jia, F. Zhong, A. Alrawais, B. Gong, and X. Cheng, "Flowguard: An intelligent edge defense mechanism against iot ddos attacks," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 9552–9562, 2020.
12. M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, *et al.*, "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *BMJ*, vol. 372, p. n71, Mar. 2021.
13. J. Deogirikar and A. Vidhate, "Security attacks in iot: A survey," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, pp. 32–37, 2017.
14. M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of things (iot): Taxonomy of security attacks," in *2016 3rd International Conference on Electronic Design (ICED)*, pp. 321–326, 2016.
15. I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Communications Surveys Tutorials*, vol. 20, no. 4, pp. 3453–3495, 2018.
16. F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017.
17. F. Zerrouki, S. Ouchani, and H. Bouarfa, "T2s-makep and t2t-makep: A puf-based mutual authentication and key exchange protocol for iot devices," *Internet of Things*, vol. 24, p. 100953, 2023.
18. S. Li, Y. Huang, and B. Yu, "A practical and flexible puf-based end-to-end anonymous authentication protocol for iot," *Computer Networks*, vol. 247, p. 110426, 2024.
19. B. Zahednejad and C. zhi Gao, "Mitigating server key compromise impersonation: A secure and efficient authentication and key agreement protocol for iot devices using chaotic maps," *Journal of Information Security and Applications*, vol. 92, p. 104083, 2025.
20. D. He, Y. Cai, S. Zhu, Z. Zhao, S. Chan, and M. Guizani, "A lightweight authentication and key exchange protocol with anonymity for iot," *IEEE Transactions on Wireless Communications*, vol. 22, pp. 7862–7872, Nov. 2023.
21. S. Qiu, D. Wang, G. Xu, and S. Kumari, "Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 1338–1351, 2022.
22. A. Javadi, S. Sadeghi, P. Pahlevani, N. Bagheri, S. Rostampour, and Y. Bendavid, "Secure and efficient lightweight authentication protocol (selap) for multi-sector iot applications," *Internet of Things*, vol. 30, p. 101499, 2025.
23. U. Ali, M. Y. I. B. Idris, J. Frnda, M. N. B. Ayub, M. A. Khan, N. Khan, R. Beegum T, A. A. Jasim, I. Ullah, and M. Babar, "Enhanced lightweight and secure certificateless authentication scheme (elwscas) for internet of things environment," *Internet of Things*, vol. 24, p. 100923, 2023.
24. F. Wu, L. Xu, S. Kumari, X. Li, J. Shen, K.-K. R. Choo, M. Wazid, and A. K. Das, "An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in iot deployment," *Journal of Network and Computer Applications*, vol. 89, pp. 72–85, 2017. Emerging Services for Internet of Things (IoT).
25. X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ecc-based provable secure authentication protocol with privacy preserving for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3599–3609, 2020.
26. X. Li, J. Peng, J. Niu, F. Wu, J. Liao, and K.-K. R. Choo, "A robust and energy efficient authentication protocol for industrial internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1606–1615, 2020.
27. N. Nissim, R. Yahalom, and Y. Elovici, "Usb-based attacks," *Computers Security*, vol. 70, pp. 675–688, 2021.
28. T. H. Lin, C. C. Lee, and C. H. Chang, "WSN integrated authentication schemes based on Internet of Things," *Journal of Internet Technology*, vol. 19, pp. 1043–1053, July 2022.
29. F. Amsaad, A. Oun, M. Y. Niamat, A. Razaque, S. Kose, M. Mahmoud, W. Alasmary, and F. Alsolami, "Enhancing the performance of lightweight configurable puf for robust iot hardware-assisted security," *IEEE Access*, vol. 9, pp. 136792–136810, 2021.
30. A. A. Khan, V. Kumar, and M. Ahmad, "An elliptic curve cryptography based mutual authentication scheme for smart grid communications using biometric approach," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 3, pp. 698–705, 2022.
31. A. A. Khan, V. Kumar, M. Ahmad, and S. Rana, "Lakaf: Lightweight authentication and key agreement framework for smart grid network," *Journal of Systems Architecture*, vol. 116, p. 102053, 2021.
32. H. Lee, D. Kang, J. Ryu, D. Won, H. Kim, and Y. Lee, "A three-factor anonymous user authentication scheme for internet of things environments," *Journal of Information Security and Applications*, vol. 52, p. 102494, 2020.
33. S. Raza, L. Wallgren, and T. Voigt, "Svelte: Real-time intrusion detection in the internet of things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2661–2674, 2013.
34. B. Chen, Y. Li, and D. Mashima, "Analysis and enhancement of rpl under packet drop attacks," in *2018 10th International Conference on Communication Systems Networks (COMSNETS)*, pp. 167–174, 2018.
35. D. Essaadi, "Detection and mitigation technique against collusion attack in rpl-based iot networks," 2021. Bachelor thesis.
36. T. Zhang, T. Zhang, X. Ji, and W. Xu, "Cuckoo-rpl: Cuckoo filter based rpl for defending ami network from blackhole attacks," in *2019 Chinese Control Conference (CCC)*, pp. 8920–8925, 2019.
37. M. Sheibani, B. Barekatain, and E. Arvan, "A lightweight distributed detection algorithm for ddao attack on rpl routing protocol in internet of things," *Pervasive and Mobile Computing*, vol. 80, p. 101525, 2022.

38. L. Wallgren, S. Raza, and T. Voigt, "Routing attacks and countermeasures in the rpl-based internet of things," *International Journal of Distributed Sensor Networks*, vol. 9, no. 8, p. 794326, 2013.
39. S. Remya, M. J. Pillai, C. Arjun, S. Ramasubbareddy, and Y. Cho, "Enhancing security in llns using a hybrid trust-based intrusion detection system for rpl," *IEEE Access*, vol. 12, pp. 58836–58850, 2024.
40. K. SOM and S. A. Elhamayed, "Mitigating the impact of iot routing attacks on power consumption in iot healthcare environment using convolutional neural network," *International Journal of Computer Networks and Information Security*, vol. 12, no. 4, pp. 11–29, 2020.
41. M. A. Ferrag and A. Ahmim, "ESSPR: an efficient secure routing scheme based on searchable encryption with vehicle proxy re-encryption for vehicular peer-to-peer social network," vol. 66, no. 3, pp. 481–503.
42. P. Amish and V. Vaghela, "Detection and prevention of wormhole attack in wireless sensor network using aomdv protocol," *Procedia Computer Science*, vol. 79, pp. 700–707, 2016. Proceedings of International Conference on Communication, Computing and Virtualization (ICCCV) 2016.
43. M. Ech-Chebaby, H. Zougagh, H. Garmani, and Z. Elhadari, "A secure authentication protocol for iot devices," *International Journal of Advanced Computer Science and Applications*, vol. 16, no. 8, 2025.
44. F. Merabet, A. Cherif, M. Belkadi, O. Blazy, E. Conchon, and D. Sauveron, "New efficient m2c and m2m mutual authentication protocols for IoT-based healthcare applications," vol. 13, pp. 439–474, 03 2020.
45. M. Shariq, I. T. Ahmed, M. Masud, A. D. E. Berini, and N. Jamil, "Design of a provable secure lightweight privacy-preserving authentication protocol for autonomous vehicles in iot systems," *Computer Networks*, vol. 261, p. 111155, 2025.
46. S. Paavolainen, T. Elo, and P. Nikander, "Risks from spam attacks on blockchains for intemet-of-things devices," in *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 314–320, 2018.
47. C. Wang, X. Zhao, Q. Liu, T. Chen, and T. Liu, "A security authentication scheme for mobile industrial iot supply chains based on blockchain and group key management," *Digital Communications and Networks*, 2025.
48. K. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authentication scheme for wireless sensor networks," in *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06)*, vol. 1, pp. 8 pp.–, 2006.
49. K. S. Roy, S. Deb, and H. K. Kalita, "A novel hybrid authentication protocol utilizing lattice-based cryptography for iot devices in fog networks," *Digital Communications and Networks*, vol. 10, no. 4, pp. 989–1000, 2024.
50. R. Lu, X. Lin, X. Liang, and X. Shen, "Flip: An efficient privacy-preserving protocol for finding like-minded vehicles on the road," in *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, pp. 1–5, 2010.
51. N. Doshi and P. Chaudhari, "Cryptanalysis of authentication protocol for cloud assisted iot environment," *Procedia Computer Science*, vol. 220, pp. 886–891, 2023. The 14th International Conference on Ambient Systems, Networks and Technologies Networks (ANT) and The 6th International Conference on Emerging Data and Industry 4.0 (EDI40).
52. F. Wang and J. Song, "Cryptanalysis of two lightweight authentication protocols for iot environments," in *2024 10th International Conference on Computer and Communications (ICCC)*, pp. 405–409, 2024.
53. A. K. Das, M. Wazid, A. R. Yannam, J. J. P. C. Rodrigues, and Y. Park, "Provably secure ecc-based device access control and key agreement protocol for iot environment," *IEEE Access*, vol. 7, pp. 55382–55397, 2019.
54. Z. Chen, Z. Cheng, W. Luo, J. Ao, Y. Liu, K. Sheng, and L. Chen, "Fsmfa: Efficient firmware-secure multi-factor authentication protocol for iot devices," *Internet of Things*, vol. 21, p. 100685, 2023.
55. R. Amin, N. Kumar, G. Biswas, R. Iqbal, and V. Chang, "A light weight authentication protocol for iot-enabled devices in distributed cloud computing environment," *Future Generation Computer Systems*, vol. 78, pp. 1005–1019, 2018.
56. H. Amintoosi, M. Nikooghadam, S. Kumari, S. Kumar, and C.-M. Chen, "Tama: Three-factor authentication for multi-server architecture," *Human-centric Computing and Information Sciences*, vol. 11, no. 39, 2021. Article number: 11:39.
57. A. Ghafouri Mirsaraei, A. Barati, and H. Barati, "A secure three-factor authentication scheme for iot environments," *Journal of Parallel and Distributed Computing*, vol. 169, pp. 87–105, 2022.
58. J. Yang, J. Park, H. Lee, K. Ren, and K. Kim, "Mutual authentication protocol for low-cost rfid," in *Workshop on RFID and lightweight crypto*, pp. 17–24, WRLC, 2005.
59. S. Ju and Y. Park, "Provably secure lightweight mutual authentication and key agreement scheme for cloud-based iot environments," *Sensors*, vol. 23, no. 24, 2023.
60. S. Li, T. Zhang, B. Yu, and K. He, "A provably secure and practical puf-based end-to-end mutual authentication and key exchange protocol for iot," *IEEE Sensors Journal*, vol. 21, no. 4, pp. 5487–5501, 2021.
61. M. Akhi, C. Eising, and L. Luxmi Dhirani, "Tcn-based ddos detection and mitigation in 5g healthcare-iot: A frequency monitoring and dynamic threshold approach," *IEEE Access*, vol. 13, pp. 12709–12733, 2025.
62. H. Shin, J. Jeong, K. Cho, J. Lee, O. Kwon, and D. Shin, "Detection of domain name server amplification distributed reflection denial of service attacks using convolutional neural network-based image deep learning," *Electronics*, vol. 14, no. 1, 2025.
63. R. Baashirah and A. Abuzneid, "Survey on prominent rfid authentication protocols for passive tags," *Sensors*, vol. 18, no. 10, 2018.
64. X. Zhuang, Y. Zhu, C.-C. Chang, and Q. Peng, "Security issues in ultralightweight rfid authentication protocols," *Wireless Personal Communications*, vol. 98, no. 1, pp. 779–814, 2018.
65. M. Šimon, L. Huraj, and T. Horák, "Ddos reflection attack based on iot: A case study," in *Cybernetics and Algorithms in Intelligent Systems* (R. Silhavy, ed.), (Cham), pp. 44–52, Springer International Publishing, 2019.
66. A. Braeken, "Puf based authentication protocol for iot," *Symmetry*, vol. 10, no. 8, 2018.
67. T. Kim, D. Kwon, Y. Park, and Y. Park, "Blockchain-based secure authentication protocol for fog-enabled iot environments," *Mathematics*, vol. 13, no. 13, 2025.
68. P. Riaz, M. Khalid, M. Hussain, N. Riaz, U. Mujahid, and M. Najam-ul Islam, "Breaking the ultralightweight rfid mutual authentication protocol: Confidentiality under threat," *International Journal of Information Security*, vol. 24, no. 5, p. 202, 2025.
69. M. Adeli, N. Bagheri, H. Martín, and P. Peris-Lopez, "Challenging the security of "a puf-based hardware mutual authentication protocol"," *Journal of Parallel and Distributed Computing*, vol. 169, pp. 199–210, 2022.
70. S. Chatterjee, S. Roy, A. K. Das, S. Chattopadhyay, N. Kumar, and A. V. Vasilakos, "Secure biometric-based authentication scheme using chebyshev chaotic map for multi-server environment," *IEEE Transactions on Dependable and Secure Computing*, vol. 15,

no. 5, pp. 824–839, 2018.
71. T.-F. Lee, Y.-Y. Diao, and Y.-P. Hsieh, "A ticket-based multi-server biometric authentication scheme using extended chaotic maps for telecare medical information systems," *Multimedia Tools and Applications*, vol. 78, no. 22, pp. 31649–31672, 2019.
72. D. Wang, J. Ming, T. Chen, X. Zhang, and C. Wang, "Cracking iot device user account via brute-force attack to sms authentication code," in *Proceedings of the First Workshop on Radical and Experiential Security*, pp. 57–60, 2018.
73. C. Pu, I. Ahmed, and S. Chakravarty, "Resource-efficient and data type-aware authentication protocol for internet of things systems," in *2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, pp. 101–110, 2023.
74. Y.-J. Tu and S. Piramuthu, "On addressing rfid/nfc-based relay attacks: An overview," *Decision Support Systems*, vol. 129, p. 113194, 2020.
75. N. Sivasankari and S. Kamalakkannan, "Detection and prevention of man-in-the-middle attack in iot network using regression modeling," *Advances in Engineering Software*, vol. 169, p. 103126, 2022.
76. T. Li and G. Wang, "Security analysis of two ultra-lightweight rfid authentication protocols," in *New Approaches for Security, Privacy and Trust in Complex Environments* (H. Venter, M. Eloff, L. Labuschagne, J. Eloff, and R. von Solms, eds.), (Boston, MA), pp. 109–120, Springer US, 2007.
77. A. Merchant, V. Panchami, S. Justine, and S. Eswaran, "An efficient lightweight authentication scheme for smart healthcare in iomt applications," *Discover Computing*, vol. 28, no. 1, p. 261, 2025.
78. M. A. Ali and S. A. H. Al-Sharafi, "Intrusion detection in iot networks using machine learning and deep learning approaches for mitm attack mitigation," *Discover Internet of Things*, vol. 5, no. 1, p. 48, 2025.
79. H. Abdi Nasib Far, M. Bayat, A. Kumar Das, M. Fotouhi, S. M. Pournaghi, and M. A. Doostari, "Laptas: Lightweight anonymous privacy-preserving three-factor authentication scheme for wsn-based iiot," *Wireless Networks*, vol. 27, no. 2, pp. 1389–1412, 2021.
80. B. A. Alzahrani, S. A. Chaudhry, A. Barnawi, A. Al-Barakati, and T. Shon, "An anonymous device to device authentication protocol using ecc and self certified public keys usable in internet of things based autonomous devices," *Electronics*, vol. 9, no. 3, 2020.
81. S. Banerjee, C. Chunka, S. Sen, and R. S. Goswami, "An enhanced and secure biometric based user authentication scheme in wireless sensor networks using smart cards," *Wireless Personal Communications*, vol. 107, no. 1, pp. 243–270, 2019.
82. M. Dammak, O. R. M. Boudia, M. A. Messous, S. M. Senouci, and C. Gransart, "Token-based lightweight authentication to secure iot networks," in *2019 16th IEEE Annual Consumer Communications Networking Conference (CCNC)*, pp. 1–4, 2019.
83. R. Khan, K. McLaughlin, J. H. D. Laverty, H. David, and S. Sezer, "Demonstrating cyber-physical attacks and defense for synchrophasor technology in smart grid," in *2018 16th Annual Conference on Privacy, Security and Trust (PST)*, pp. 1–10, 2018.
84. H. Kim and T. Kim, "Vehicle-to-vehicle (v2v) message content plausibility check for platoons through low-power beaconing," *Sensors*, vol. 19, no. 24, 2019.
85. S. Rostampour, M. Safkhani, Y. Bendavid, and N. Bagheri, "Eccbap: A secure ecc-based authentication protocol for iot edge devices," *Pervasive and Mobile Computing*, vol. 67, p. 101194, 2020.
86. M. Kaveh, M. R. Mosavi, D. Martín, and S. Aghapour, "An efficient authentication protocol for smart grid communication based on on-chip-error-correcting physical unclonable function," *Sustainable Energy, Grids and Networks*, vol. 36, p. 101228, 2023.
87. X. Su and Y. Xu, "Secure and lightweight cluster-based user authentication protocol for iomt deployment," *Sensors*, vol. 24, no. 22, 2024.
88. N. Li, M. Ma, and H. Wang, "Asap-iiot: An anonymous secure authentication protocol for industrial internet of things," *Sensors*, vol. 24, no. 4, p. 1243, 2024.
89. A. M. Alharthi and F. S. Altuwaijri, "Lightweight iot authentication protocol using pufs in smart manufacturing industry," *Electronics*, vol. 14, no. 9, 2025.
90. B. Mahapatra, V. Singh, R. Bhattacharjee, and C. Srinivasan, "Ml-aka: An authentication protocol for non-standalone 5g-based c-iot networks," *Designs*, vol. 8, Dec. 2024. Publisher Copyright: © 2024 by the authors.
91. N. W. Tun and M. Mambo, "Secure puf-based authentication systems," *Sensors*, vol. 24, no. 16, 2024.
92. S. Lee, K. A. Kang, S. Lee, and J. Kim, "Exploring authentication protocols for secure and efficient internet of medical things systems," *Electronics*, vol. 14, no. 21, 2025.
93. K. Prateek, N. K. Ojha, F. Altaf, and S. Maity, "Quantum secured 6g technology-based applications in internet of everything," *Telecommunication Systems*, vol. 82, no. 2, pp. 315–344, 2023.
94. K. Prateek, S. Maity, and R. Amin, "An unconditionally secured privacy-preserving authentication scheme for smart metering infrastructure in smart grid," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 2, pp. 1085–1095, 2023.
95. K. Prateek, S. Maity, and N. Saxena, "A quantum communication based secure road condition monitoring application in intelligent internet of vehicular things," in *2022 IEEE 19th India Council International Conference (INDICON)*, pp. 1–6, 2022.
96. X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K. R. Choo, "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments," *Journal of Network and Computer Applications*, vol. 103, pp. 194–204, 2018.
97. J. Srinivas, S. Mukhopadhyay, and D. Mishra, "Secure and efficient user authentication scheme for multi-gateway wireless sensor networks," *Ad Hoc Networks*, vol. 54, pp. 147–169, 2017.
98. M. Ech-chebaby, H. Zougagh, H. Garmani, Z. El-hadari, and N. Idboufker, "Enhanced ecc-based authentication protocol for iot devices m2c," in *Proceedings of the 4th International Conference on Advances in Communication Technology and Computer Engineering (ICACTCE'24)* (C. Iwendi, Z. Boulouard, and N. Kryvinska, eds.), (Cham), pp. 154–169, Springer Nature Switzerland, 2025.
99. D. Hankerson and A. Menezes, *Elliptic Curve Discrete Logarithm Problem*, pp. 397–400. Boston, MA: Springer US, 2011.
100. A. Malik and R. Kushwah, "A secure authentication and key establishment protocol for iot devices using eccmd," *SN Computer Science*, vol. 6, no. 7, p. 803, 2025.
101. Q. Zhang, Y. Liu, N. Wu, C. Chen, and Z. Du, "Spuf-kg and ssl-trng enhanced lightweight iot authentication and key exchange protocol," *Journal of King Saud University – Computer and Information Sciences*, vol. 37, no. 9, p. 279, 2025.
102. T. Wan, J. Ge, W. Liao, and H. Zhao, "A lightweight two-factor continuous authentication protocol for agricultural iot devices," *Wireless Personal Communications*, vol. 136, no. 2, pp. 921–945, 2024.

103. B. Zhu, X. Jiang, K. Huang, and M. Yu, "A response-feedback-based strong puf with improved strict avalanche criterion and reliability," *Sensors*, vol. 24, no. 1, p. 93, 2023.
104. O. M. Al-Hazaimeh, A. A. Abu-Ein, I. S. Fathi, and M. Tawfik, "Securing IoT systems using artificial intelligence-driven approaches," *Statistics, Optimization & Information Computing*, vol. 15, no. 3, pp. 1899–1912, 2026.
105. M. Tawfik, A. H. Abdelhaliem, and I. Fathi, "Quantum-resistant privacy-preserving IoT authentication via zero-knowledge proofs and blockchain integration," *Statistics, Optimization & Information Computing*, vol. 14, no. 3, pp. 1374–1402, 2025.
106. N. Zeeshan, M. Bakyt, N. Moradpoor, and L. La Spada, "Continuous authentication in resource-constrained devices via biometric and environmental fusion," *Sensors*, vol. 25, no. 18, p. 5711, 2025.
107. I. S. Fathi and M. Tawfik, "Enhancing IoT systems with bio-inspired intelligence in fog computing environments," *Statistics, Optimization & Information Computing*, vol. 13, no. 5, pp. 1916–1932, 2025.