Open Access and Peer Reviewed Journal ISSN 2394-2231 https://www.ijctjournal.org/

RESEARCH ARTICLE OPEN ACCESS

Lightweight IoT Authentication Protocols: A Comparative Review

Jamal M. Al-Abdi[1,*], Adnan H. Al-Helali[2]

[1] *Department of Cybersecurity, College of Science and Information Technology, Irbid National University, Irbid, Jordan*
[2] *Department of Cybersecurity, College of Science and Information Technology, Irbid National University, Irbid, Jordan*
Corresponding author email: 202430159@inu.edu.jo

Abstract — The Internet of Things (IoT) is expected to interconnect more than 75 billion devices worldwide, yet device authenticity remains one of the most pressing unsolved security challenges in the IoT space. Typical IoT nodes have limited computing power, memory, and battery capacity, making traditional public-key-based authentication difficult to implement without compromising either security or resource conservation. This paper presents a structured narrative review and quantitative comparison of lightweight authentication protocols for IoT environments published between 2024 and 2026, spanning seven families: Elliptic Curve Cryptography (ECC)-based, ECC for Radio Frequency Identification (RFID), hash-based, Physical Unclonable Function (PUF)-based, biometric and behavioural, blockchain-assisted, and machine-learning-augmented protocols. The review adds message-level protocol-flow comparisons for representative ECC- and PUF-based schemes, a benchmarking table of published latency, message-size, and energy indicators, and five sector-specific case studies. Reported findings include dynamic-credential ECC schemes reducing communication and computational overhead by more than 37% over prior ECC schemes; PUF-based techniques using machine learning to improve modelling-attack resistance by more than 35% over earlier techniques; blockchain-assisted authentication for fog-enabled IoT; and multi-sector schemes such as SELAP, reducing computation and communication cost to 422 ms and 960 bits respectively, against 548 ms and 2048 bits for the earlier ELWSCAS protocol. Protocols are also examined against ephemeral information leakage, modelling attacks on PUFs, node cloning, and physical tampering. No protocol category is universally optimal; selection depends on a deployment's constraints, threat model, and sector. Research is converging on hybrid designs combining hardware-rooted trust, efficient public-key primitives, decentralised trust, and intelligent anomaly detection.

Keywords — blockchain-assisted authentication; elliptic curve cryptography; Internet of Things (IoT); lightweight authentication protocols; physical unclonable function (PUF); resource-constrained devices

I. INTRODUCTION

IoT is no longer a niche idea — it is embedded throughout today's digital infrastructure, spanning sensors and actuators, wearables and vehicles, and industrial controllers that generate and exchange vast amounts of data. Many of these devices communicate over open, often wireless links and are physically accessible in ways a traditional server is not, making authentication the primary line of defence against unauthorised devices, impersonation, and large-scale data leaks.

Industry estimates already place the number of connected IoT devices in the tens of billions, with smart-home devices, connected medical equipment, agricultural sensors, and critical-infrastructure controllers joining the mix, and forecasts projecting more than 75 billion connected devices within the decade. Each deployment context carries its own threat profile and constraints, and a single authentication scheme rarely transfers cleanly from one — say, a battery-powered soil-moisture sensor — to another, such as an implantable medical device or a programmable logic controller (PLC) on a factory floor. Many IoT devices are also deployed in physically unattended or adversarial environments, where an attacker may gain direct physical access, capture and replay wireless transmissions, or clone a device's identity outright.

The limited CPU cycles, kilobyte-scale memory, and battery or energy-harvesting power budgets typical of IoT nodes are not compatible with authentication mechanisms designed for desktop or cloud environments; those mechanisms cannot simply be ported into the IoT domain without substantial redesign.

This gap between security requirements and hardware capability has driven the emergence of lightweight authentication protocols: schemes that preserve the core security properties required of any authentication protocol — mutual authentication, confidentiality, integrity, and forward secrecy — while reducing computational and communication load to what a microcontroller-class device can support.

Existing survey literature on this subject falls into two broad groups: (1) surveys that catalogue dozens of schemes without evaluating their comparative performance under

practical constraints, and (2) surveys that examine only a single cryptographic primitive — typically elliptic-curve or physically-unclonable-function-based schemes — without considering the rest of the protocol landscape. Very few studies connect protocol-level features to sector-specific deployment needs, and fewer still account for current AI-assisted attack tooling or 2026 regulatory developments. That gap in the literature is the primary motivation for this work.

This area of research has grown more critical as attacks against IoT devices have increased. The 2026 threat landscape indicates that IoT botnets exploiting weak or absent authentication remain among the most prevalent attack vectors, with attackers increasingly relying on automated and AI-assisted tools to find poorly authenticated devices at scale [1]. Regulatory pressure is increasing in parallel, with new requirements pushing manufacturers toward stronger default authentication and hardware-rooted cryptographic strength [2].

Although most lightweight authentication protocols in the literature share the same underlying goal, they differ significantly in the guarantees they provide and the resources they consume. This paper first introduces the seven major families of lightweight authentication protocols, then addresses six research questions: (RQ1) How do the major protocol families differ in security guarantees and resource consumption? (RQ2) What attack classes has the 2024–2026 literature focused on, and how are they addressed? (RQ3) What deployment-sector and threat-model conditions should drive protocol choice? (RQ4) What quantitative performance data is available, and how comparable is it across studies? (RQ5) Where, at the message level, is computational cost concentrated in representative protocols? (RQ6) What directions has the field not yet pursued thoroughly?

The remainder of the paper is organised as follows. Section II describes the review methodology. Section III introduces the seven protocol families and their guaranteed properties, and discusses the resource-constrained authentication problem in more depth. Section IV traces the message-level flow of two representative protocols. Section V presents the quantitative comparative analysis, reviews the 2024–2026 literature on attack classes and mitigations, presents five sector-specific mini case studies, discusses design implications, and states the review's limitations. Section VI concludes and outlines future research directions.

II. REVIEW METHODOLOGY

This paper does not propose or test a new lightweight authentication protocol; accordingly, the review follows a structured narrative-review process rather than a complete systematic review such as PRISMA. A narrative approach was chosen deliberately: the literature spans a rapidly developing and heterogeneous set of protocol types — ECC-based, hash-based, PUF-based, biometric, and blockchain-assisted — for which a single fixed systematic protocol would be a poor fit.

Sources were identified through combined searches of IEEE Xplore, ScienceDirect, MDPI (Sensors, Electronics), SpringerLink, Nature/Scientific Reports, and open-access preprint repositories, using the keywords *lightweight IoT authentication, PUF authentication protocol, ECC IoT authentication, RFID mutual authentication, biometric IoT authentication, blockchain IoT authentication*, and *IoT authentication survey*. Two general classification and trends surveys [3], [4] were added to help position the field, and industry threat-intelligence sources [1], [2] were used for general threat-landscape statistics only, not for protocol-level security claims.

Inclusion criteria were: (a) the protocol proposed or surveyed is an authentication or authenticated key-agreement protocol specifically designed for resource-constrained devices — IoT, RFID/ID, industrial IoT, agricultural, or IoT-adjacent devices; and (b) the source provides at least an informal security analysis, or a computational/communication cost evaluation via formal verification or simulation. This process produced six primary/secondary source families: ECC, RFID-ECC, hash-based, PUF-based, biometric, and blockchain-assisted.

One conference source could not be independently confirmed through indexed databases, as its author list was unavailable; it is therefore cited by title and venue rather than by author, and its findings are treated with correspondingly lower confidence throughout. Where formal verification tools (ProVerif or AVISPA) were used, that is noted explicitly, since formally verified claims warrant more confidence than informal security discussion.

The seven categories of lightweight authentication protocols surveyed in this review are described in Section III.

III. RELATED WORK: FAMILIES OF LIGHTWEIGHT AUTHENTICATION PROTOCOLS

A. Elliptic Curve Cryptography (ECC)-Based Protocols

ECC extends the "security at low cost" argument to resource-constrained IoT devices: it offers RSA-equivalent security at much smaller key lengths and operand sizes, directly reducing the storage and bandwidth demands placed on constrained hardware. This matters especially for battery-powered sensors, where every bit of key material corresponds to a measurable amount of energy — which is why ECC is the default public-key primitive across nearly all the protocols surveyed here.

Using dynamic authenticated credentials (DACs) in place of temporary public keys, Li and Hu [5] designed an authentication and key-agreement (AKA) protocol formally proven secure under the Real-or-Random model, reporting improvements of more than 37% in message count and computational overhead relative to prior protocols aimed at preventing ephemeral-key information-leakage attacks. Khalique [6] proposed the Lightweight Authentication algorithm for IoT Devices (LAID), a four-phase, elliptic-curve-based scheme built around smart-city deployment. Li [7] presented an identity-authentication protocol based on the Schnorr signature mechanism, adapted to the ECC attribute structure to avoid the high overhead of conventional signature verification while preserving unforgeability.

Javadi et al. [8] identified security weaknesses in the earlier ELWSCAS protocol and proposed SELAP in response, reducing computation and communication cost to 422 milliseconds and 960 bits respectively — compared with 548 milliseconds and 2048 bits for ELWSCAS, reductions of roughly 23% and 53%. This is among the more directly comparable quantitative results in the literature reviewed here.

B. Radio Frequency Identification (RFID)-Based Protocols

Passive RFID tags represent a basic and particularly constrained class of IoT device: they typically have no onboard battery and draw both computation and energy from the reader's signal. Despite substantial research on ECC-based RFID mutual authentication, most proposed RFID protocols still contain identifiable vulnerabilities to tracking or desynchronisation attacks [9], making RFID a useful test bed for how far lightweight ECC authentication can be pushed. These persistent, unaddressed vulnerabilities suggest a near-fundamental ceiling on the security achievable in passive RFID designs, imposed by their extreme resource limitations.

C. Hash-Based Protocols

For the most constrained end nodes, hash-based schemes are attractive because authentication relies on cryptographic hash functions rather than the comparatively heavy computation of public-key schemes. Elaoudi et al. [10] examined the evolution of IoT device authentication from hash-based to blockchain-based schemes, and discussed integrating hash functions with time-stamping and clock synchronisation based on the Precision Time Protocol (PTP), highlighting time-stamping's role in improving replay-attack resistance across remote, distributed IoT systems. Their survey points to a broader shift: hash-based schemes are increasingly treated as lightweight building blocks folded into more complex PUF- or blockchain-based designs, rather than as independent solutions.

D. Physical Unclonable Function (PUF)-Based Protocols

PUF-based protocols exploit the inherent physical variation between hardware components. That variation can serve as a source of cryptographic key material and, by extension, a low-cost hardware root of trust for silicon authentication and verification — without requiring secure key storage in non-volatile memory. To counter machine-learning modelling attacks on conventional PUFs, Mefgouda et al. [11] proposed LPUF-AuthNet, combining PUFs with split learning (SL) and a tandem neural network (TNN) architecture. Because real-time authentication is critical in industrial control loops with strict latency budgets, Alharthi [12] proposed a lightweight PUF-based authentication approach for smart-manufacturing systems.

For deployments where the third-party server does not require real-time communication, Li, Huang, and Yu [13] proposed an anonymous, certificateless PUF-based authentication scheme that avoids any real-time exchange between the PUF and other parties or the third-party server. The protocol requires only three handshake exchanges and stores neither raw challenge-response pairs (CRPs) nor other state data, giving it stronger anonymity and forward-secrecy properties than comparable schemes while resisting modelling attacks. Dargaoui et al. [14] proposed a PUF authentication scheme tailored to smart-agriculture applications in outdoor, unattended deployments.

E. Biometric and Behavioural Authentication

Between 2025 and 2026, publications on biometric and behavioural traits as IoT authentication methods increased. The 2026 ICSC proceedings on AI-enabled smart interfaces explored embedding AI-driven interaction modalities into advanced biometric authentication — including behavioural and multimodal fusion — while also addressing privacy questions such as edge-based processing and cancellable biometrics [15]. A shift from purely digital to physical IoT deployments is visible in embedded biometric applications for remotely controlled physical environments, such as the fingerprint- and GSM-based door-access system of Kanagamalliga [16]. A central open problem is that, unlike passwords, biometric templates cannot easily be re-keyed once lost or stolen; cancellable biometric transforms remain a promising but still-emerging mitigation.

F. Blockchain-Assisted Authentication

Blockchain-assisted authentication protocols aim to remove the single point of failure inherent in centralised authentication servers by distributing trust across a decentralised ledger. Ponnuru et al. [17] proposed BAAP-FIoT, a fog-enabled IoT authentication model combining blockchain, elliptic curve cryptography, and hash functions to support authentication decisions at the fog layer and reduce dependence on constant cloud connectivity. A separate

blockchain-based IoT device authentication and key-management system, published in the 2024 IHCSP proceedings, reported success on 99% of measured security metrics — including user anonymity — though the individual author list for that source could not be independently verified (see Section II) [18].

G. Machine-Learning-Augmented Authentication

Machine learning plays a dual role in PUF security: ML-based modelling attacks are among the most significant threats to conventional PUFs, while ML-based defences such as LPUF-AuthNet are designed specifically to counter those same attacks [11], [13]. Alsheavi et al. [3] similarly identify machine learning and blockchain as the two dominant trends currently shaping IoT authentication design. Across all seven categories surveyed here, the field shows a consistent trend away from single-primitive designs and toward hybrid mechanisms combining two or more of the primitives reviewed above.

H. The Authentication Problem in Resource-Constrained Environments

IoT devices differ from conventional computing endpoints in ways that directly shape authentication design choices. Many sensor nodes and embedded controllers run processors clocked far below desktop- or mobile-class chips, with memory measured in kilobytes rather than gigabytes, and power budgets set by small batteries or energy harvesting — constraints that rule out the computationally expensive public-key operations used at scale in traditional PKI systems. These devices are also frequently deployed in physically unsecured or remote locations, increasing exposure to physical tampering, node cloning, and side-channel attacks.

The result is a fundamental security-efficiency trade-off: stronger cryptographic primitives generally demand more computation and energy, while lighter primitives can expose the protocol to a broader range of attacks if not carefully designed. The literature generally divides IoT authentication schemes into two categories: those built on lightweight cryptographic primitives, and those built on authentication elements such as biometrics, tokens, and physical unclonable functions.

Alsheavi et al. [3] note that a newer class of protocols integrates blockchain technology for decentralised trust alongside machine learning for adaptive, behaviour-based authentication — evidence of a broader move toward hybrid architectures. A further constraint specific to many IoT deployments is device heterogeneity: a single network may combine ultra-constrained 8-bit sensor nodes with far more capable gateway or fog nodes, requiring authentication architectures that can operate asymmetrically across tiers of computational capability.

IV. PROTOCOL-FLOW ANALYSIS

To make the comparative claims in Section III-H concrete, this section traces the message-level authentication sequence of two representative protocols: the ECC dynamic-credential scheme of Li and Hu [5] and the PUF-plus-neural-network scheme of Mefgouda et al. [11]. Table I summarises both flows side by side.

In the ECC flow, the device first transmits a request containing its identifier; the server responds with a challenge and its ECC public parameters; the device returns a dynamically generated authenticated credential together with its ECDH key share, which the server verifies before both sides derive a shared session key confirmed via a message authentication code. Computational cost concentrates in the elliptic-curve point multiplications needed to compute the ECDH share and verify the dynamic credential — precisely the step the dynamic-credential design targets for reduction relative to static public-key exchange.

In the PUF-based flow, the device transmits only its identifier; the server retrieves a stored challenge from its CRP database and returns it; the device computes a response by physically evaluating its PUF circuit, processed through the tandem neural network to produce a response resistant to modelling; the server verifies this response against its expected model output before both sides establish a mutual session key. Here, computational cost concentrates in server-side neural-network inference rather than public-key arithmetic, while device-side cost is limited to a single physical PUF evaluation — which explains the markedly lower device-side computational burden reported for PUF-based schemes relative to ECC-based schemes (Section V-A).

TABLE I. Message-Level Authentication Flow: ECC Dynamic-Credential vs. PUF + Neural-Network Schemes

Step	ECC Dynamic-Credential Flow (Li & Hu [5])	PUF + Neural-Network Flow (Mefgouda et al. [11])
1. Device → Server	Auth request + device identifier	Device identifier only
2. Server → Device	Challenge + server ECC public parameters	Challenge C retrieved from the CRP database
3. Device → Server	Dynamic authenticated credential (DAC) + ECDH key share	Response R = PUF(C), processed through the tandem neural network

Step	ECC Dynamic-Credential Flow (Li & Hu [5])	PUF + Neural-Network Flow (Mefgouda et al. [11])
4. Server (local)	Verifies the DAC and computes the shared session key	Verifies R against the expected model output
5. Mutual confirmation	MAC-confirmed session key	Mutual session key established
Where the cost sits	Elliptic-curve point multiplication for the ECDH share and DAC verification — the exact step the dynamic-credential design reduces relative to static public-key exchange	Neural-network inference at the server; the device performs a single physical PUF evaluation, which explains its markedly lower device-side computational load

V. RESULTS AND DISCUSSION

A. Comparative Analysis of Protocol Categories

Table II synthesises the trade-offs across the major protocol categories, distinguishing quantitative figures explicitly reported in the source studies from qualitative characterisations where no comparable number was published.

TABLE II. Comparative Summary of Lightweight IoT Authentication Protocol Categories

Protocol Category	Reported Latency	Reported Message/Key Size	Energy Efficiency (qualitative)	Key Security Strength	Best-Fit Sector
ECC, dynamic credentials (Li & Hu [5])	Not separately reported	N/A (37% overhead reduction vs. baseline)	Moderate–High	Formally verified mutual auth; resists ephemeral leakage	Smart city, general IoT
ECC, Schnorr signature (Li [7])	N/A (qualitative only)	N/A (qualitative only)	Moderate	Efficient signature verification; unforgeability	Identity-centric IoT
RFID-ECC (Timouhin et al. [9])	N/A (survey, no single figure)	N/A (survey, no single figure)	High (passive tags)	Mutual auth under passive power budget	Supply chain, retail RFID
Hash + blockchain timestamp (Elaoudi et al. [10])	N/A (survey, no single figure)	N/A (survey, no single figure)	High	Replay resistance via PTP-synchronised timestamps	Distributed sensor networks
PUF + neural network (Mefgouda et al. [11])	Not separately reported	Reduced CRP dataset size (qualitative)	High	ML-attack resistance, 6G-ready mutual auth	Smart manufacturing, 6G IoT
PUF, anonymous, certificateless (Li, Huang & Yu [13])	3 handshake exchanges (round count only)	No raw CRP storage required	High	Perfect forward secrecy, no CRP storage	Smart agriculture, remote sensors
SELAP, multi-sector (Javadi et al. [8])	422 ms (vs. 548 ms, ELWSCAS)	960 bits (vs. 2048 bits, ELWSCAS)	High	Validated via NS-3 simulation and formal analysis	Cross-sector IoT
Biometric/behavioural + AI (Kanagamalliga [16])	N/A (hardware demo, no latency reported)	N/A	Moderate (edge-dependent)	Continuous, unobtrusive identification	Wearables, personal IoT
Blockchain-assisted (Ponnuru et al. [17])	N/A (qualitative only)	N/A (qualitative only)	Moderate	Decentralised trust, fog-layer resilience	Fog computing, smart grid

Marking most latency and message-size cells as N/A is a deliberate methodological choice: only Javadi et al. [8] and, to a lesser extent, Li, Huang, and Yu [13] report the kind of head-to-head numeric benchmark that permits direct cross-protocol comparison, while most other sources report either percentage improvements over an internal baseline or purely qualitative security claims. That asymmetry is itself a finding of this review, reinforcing the case made in Section VI for standardised benchmarking. Where quantitative data exists, PUF-based and SELAP-style hybrid schemes show the clearest evidence of genuine efficiency gains, while ECC-based schemes report strong relative improvements without providing absolute figures that could be benchmarked directly against the PUF-based results.

B. Security Threats Addressed by Lightweight Authentication

Lightweight authentication protocols are evaluated primarily against a recurring set of IoT-specific attack vectors that have evolved alongside protocol design. Ephemeral information-leakage attacks — in which temporary session data is exposed and used to compromise long-term keys — were a specific motivation for the dynamic-credential ECC scheme validated under the Real-or-Random model [5].

Machine-learning modelling attacks against PUFs have become a central concern, directly motivating both the neural-network defence in LPUF-AuthNet [11] and the certificateless PUF scheme that avoids storing raw CRPs altogether [13]. Hash-based and blockchain-integrated schemes must consistently contend with replay attacks, which timestamp-

synchronisation mechanisms help mitigate [10]. RFID-specific literature also identifies tracking and desynchronisation attacks as ongoing vulnerabilities, even in RFID schemes hardened with ECC [9].

At the network level, Nozomi Networks [1] found that 68% of surveyed industrial wireless networks had not adopted management frame protection, meaning devices can be spoofed regardless of whatever higher-layer authentication is in place.

Source note (to be removed before final submission): the original manuscript also cited "The World Economic Forum & IoT Insider (2026)" for a claim that transportation and manufacturing are the most-targeted IoT sectors, with government infrastructure third. That report could not be independently located or verified during this revision (the same caveat the original authors applied to the unattributed 2024 IHCSP conference paper in Section III-F). Rather than repeat an unverifiable statistic, this revision omits the claim; the authors should confirm the source and either restore it with a verifiable citation or replace it before submission.

C. Sector-Specific Mini Case Studies

1) Smart Manufacturing and Industrial IoT: In a robotic assembly cell, each component must authenticate to a local programmable logic controller within a control-loop cycle measured in milliseconds; the cell may contain dozens of actuators and vision sensors, and an authentication delay can disrupt synchronised motion. Recommended protocol: PUF-based schemes such as the smart-manufacturing protocol of Alharthi [12], whose low post-enrolment computational cost fits within tight control-loop budgets. Core trade-off: PUF enrolment carries a one-time per-device deployment cost, and a scheme configured without ML-hardening — as in the base LPUF-AuthNet design [11] — remains more susceptible to well-resourced adversaries performing modelling attacks on factory-floor devices over time.

2) Smart Cities and Urban Sensor Networks: A city deployment spanning multiple districts and municipal departments, with no single trusted authority, and environmental and traffic sensors owned by different agencies. Recommended protocol: the four-phase LAID protocol of Khalique [6] for scalability, augmented with blockchain-based identity management [17] to avoid concentrating trust in any one department. Key trade-off: decentralisation introduces consensus latency, which may be perceived as a disadvantage, and growing on-chain storage overhead that must be weighed against the number of devices in the network.

3) Fog-Enabled and Vehicular Networks: Connected vehicles authenticating to roadside units while moving at highway speed, where the handshake must complete before the vehicle exits the roadside unit's communication range. Suggested approach: lightweight ECC or hash-based schemes [5], [10] rather than heavier blockchain consensus, given the sub-second time budget. Key trade-off: the decentralised-trust advantages of BAAP-FIoT [17] are best exploited at the fog-aggregation layer rather than the vehicle-to-roadside-unit hop itself, implying a layered design with fast local authentication periodically reconciled against a slower fog-level blockchain ledger.

4) Smart Agriculture and Remote Sensing: Outdoor, unattended sensor deployments where hardware-rooted trust must survive years of environmental exposure without key redistribution. Recommended protocol: PUF-based schemes for smart agriculture such as that of Dargaoui et al. [14]. Core trade-off: PUF response drift under extreme temperature or humidity variation may degrade matching accuracy over years of outdoor exposure — a durability question the current literature has not yet quantified longitudinally.

5) Healthcare and Wearable IoT: A continuous glucose monitor or cardiac wearable that must authenticate to a paired smartphone application throughout the day without requiring repeated manual login, while handling data subject to strict health-privacy regulation. Recommended protocol: biometric/behavioural fusion approaches such as those discussed in the 2026 ICSC research on AI-enhanced intelligent interfaces [15], combined with cancellable biometric transforms to limit the impact of template compromise. Core trade-off: continuous biometric sensing increases battery drain relative to a one-time cryptographic handshake, and the irrevocability of raw biometric compromise makes template-protection design a higher-stakes decision in this sector than in most others.

D. Design Implications

The comparative findings across Sections V-A through V-C suggest that protocol selection cannot be reduced to a single best choice; it depends on a deployment's specific constraints, sector, and threat profile. For ultra-low-power sensor networks and smart-manufacturing environments where battery replacement is impractical and latency is tightly bounded, PUF-based schemes — particularly those hardened against machine-learning modelling attacks — offer the most favourable energy-security balance. For applications requiring interoperability with existing public-key infrastructure, ECC-based mutual authentication using dynamic credentials or Schnorr-based signatures remains the more established choice.

SELAP and other multi-sector protocols reflect a growing recognition that authentication schemes must be validated not only theoretically but across varied real deployment scenarios. The emergence of blockchain-assisted and biometric/behavioural authentication as distinct, actively researched categories signals that the field is moving beyond narrow cryptographic-primitive efficiency toward broader

systemic questions of decentralised trust and continuous, human-centric identification. The protocol-flow analysis in Section IV further clarifies that ECC-based and PUF-based schemes concentrate computational cost at structurally different points in the authentication exchange — a distinction that matters when matching a protocol family to a specific hardware profile.

E. Limitations of This Review

Several limitations should be considered when interpreting these findings. The search process was targeted rather than systematic — it did not follow a PRISMA flow diagram, dual-reviewer screening, or database-wide replication — so the review should be read as representative rather than exhaustive of the 2024–2026 literature. Several protocols are described from abstracts and secondary citations rather than a full independent read of each paper's proofs and experimental appendices; reported figures, such as the 37% overhead reduction and the 422 ms SELAP latency, are taken at face value from the original authors and were not independently reproduced.

Cross-study comparability is further limited because the studies summarised in Section V-A use different testbeds, threat models, and formal-verification tools — including ProVerif, AVISPA, BAN logic, and the Real-or-Random model — and the extensive N/A entries in Table II are themselves evidence that the field currently lacks a shared benchmarking standard. Most importantly, this review contains no independent experimental validation, simulation, or re-implementation of any surveyed protocol: it is a narrative synthesis of published claims rather than an original empirical contribution, and all numeric figures presented should be attributed entirely to the cited original authors. Individual author names could not be independently verified for two conference sources; these are cited by title and venue only (Sections II and III-F), and one industry-report claim from the original manuscript could not be verified at all and has been removed rather than repeated (Section V-B). Finally, quantum-resistance considerations for post-quantum IoT authentication remain only lightly addressed in the current literature base.

VI. CONCLUSION AND FUTURE WORK

Lightweight authentication protocols address a foundational security requirement for IoT ecosystems: verifying device and user identity without exceeding the processing, memory, and energy budgets of constrained hardware. The 2024–2026 literature reflects a maturing and diversifying landscape spanning dynamic-credential ECC schemes, RFID-specific ECC protocols, timestamp-synchronised hash-based methods, neural-network-hardened PUF protocols, biometric and behavioural authentication, blockchain-assisted decentralised-trust architectures, and multi-sector validated frameworks such as SELAP.

The protocol-flow analysis and quantitative benchmarking added in this revision show that computational cost concentrates at structurally different points across protocol families, and that only a minority of published studies report figures that are directly comparable across schemes. As IoT deployments continue to expand into smart cities, industrial manufacturing, agriculture, healthcare, and critical infrastructure — and as attackers increasingly weaponise automated and AI-assisted tools against poorly authenticated devices — continued refinement of lightweight authentication protocols, validated through formal security analysis, standardised real-world benchmarking, and independent replication across comparable testbeds, will remain essential to securing the expanding IoT attack surface through 2027 and beyond.

Several open research gaps emerge from this review. First, cross-study benchmarking remains a significant unmet need: the field would benefit substantially from standardised testbeds and shared evaluation criteria enabling direct, controlled comparison of computational cost, energy consumption, and security strength across ECC, PUF, hash-based, biometric, and blockchain-assisted schemes. Second, post-quantum resistance is only beginning to be addressed in lightweight IoT authentication; ECC-based schemes in particular will need migration paths toward lattice-based or hash-based post-quantum primitives that remain compatible with constrained hardware.

Third, the integration of machine learning into authentication carries a dual-use risk that warrants further study, pointing to a need for adversarial robustness testing as a standard component of ML-augmented protocol evaluation. Fourth, human-centric and usability-focused authentication design remains underexplored relative to the purely technical performance metrics that dominate the current literature. Fifth, and directly motivated by the gap this review identifies, future work adapting one of the surveyed protocol families into an independently implemented and benchmarked simulation — for example, an NS-3 or hardware-testbed replication of a PUF-based scheme under a common threat model — would convert this narrative synthesis into a foundation for original empirical contribution. Finally, longitudinal field studies evaluating how lightweight authentication protocols perform under sustained real-world deployment conditions, rather than laboratory or simulated testbeds alone, would substantially strengthen the evidentiary basis for protocol-selection guidance.

VII. DECLARATIONS

A. Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors. [Authors to confirm.]

B. Conflict of Interest

The authors declare no conflict of interest. [Authors to confirm.]

C. Data Availability

This study is a narrative review of previously published literature; no new data were generated or analysed. All sources analysed are listed in the reference list and are available from their respective publishers. [Authors to confirm.]

D. Ethics Statement

This study did not involve human or animal subjects. [Authors to confirm.]

E. Author Contributions

[To be completed by the authors using the CRediT taxonomy — this information was not present in the source manuscript. Example format: "Conceptualization, J.M.A.; Methodology, J.M.A.; Investigation, A.H.A.; Writing — original draft, J.M.A.; Writing — review and editing, A.H.A.; Supervision, A.H.A. All authors have read and agreed to the published version of the manuscript."]

VIII. ACKNOWLEDGMENTS

[To be completed or deleted by the authors — no acknowledgments were present in the source manuscript.]

IX. REFERENCES

[1] Nozomi Networks Labs, "OT/IoT cybersecurity trends and insights, February 2026," Feb. 2026. [Online]. Available: https://www.nozominetworks.com/ot-iot-cybersecurity-trends-insights-february-2026

[2] GlobalSign, "The future of IoT security is regulation, standards and trust," Feb. 25, 2026. [Online]. Available: https://www.globalsign.com/en/blog/will-iot-security-finally-grow-up-in-2026

[3] A. N. Alsheavi, A. Hawbani, X. Wang, W. Othman, L. Zhao, Z. Liu, S. H. Alsamhi, and M. A. A. Al-Qaness, "Internet of Things (IoT) authentication protocols: Classification, trend and opportunities," IEEE Trans. Sustainable Comput., vol. 10, no. 3, pp. 515–533, 2025, doi: 10.1109/TSUSC.2024.3492152.

[4] I. Cetintav, "Lightweight IoT authentication protocols — review from the cryptographic engineering perspective," IEEE Access, 2025. [Online]. Available: https://ieeexplore.ieee.org/iel8/6287639/10820123/10904450.pdf

[5] M. Li and S. Hu, "An IoT lightweight authentication and key agreement protocol using dynamic authentication credentials based on ECC," Sensors, vol. 24, no. 24, art. no. 7967, 2024, doi: 10.3390/s24247967.

[6] A. Khalique, "Lightweight authentication for Internet of Things (IoT) devices in sustainable smart city," Sci. Rep., vol. 15, 2025. [Online]. Available: https://www.nature.com/articles/s41598-025-10181-0

[7] M. Li, "An efficient identity authentication protocol for IoT devices employing Schnorr signature," Procedia Comput. Sci., 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050925011226

[8] A. Javadi, S. Sadeghi, P. Pahlevani, N. Bagheri, S. Rostampour, and Y. Bendavid, "Secure and efficient lightweight authentication protocol for multi-sector IoT applications," Internet of Things, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S2542660525000125

[9] H. Timouhin et al., "Survey of RFID mutual authentication protocols based on ECC in resource-constrained environments in IoT," in Lecture Notes in Networks and Systems. Berlin, Germany: Springer, 2024, pp. 195–200, doi: 10.1007/978-3-031-48573-2_28.

[10] Elaoudi et al., "[Full author list, title, and venue as cited in the source manuscript — incomplete; to be completed by the authors before submission]," 2025.

[11] B. Mefgouda, R. Khan, O. Alhussein, H. Saleh, H. B. Eldeeb, A. Pandey, and S. Muhaidat, "LPUF-AuthNet: Low-power and lightweight authentication for IoT using split learning and tandem neural network based PUFs," in Proc. IEEE Global Communications Conf. (GLOBECOM), 2024. [Online]. Available: https://arxiv.org/abs/2410.12190

[12] A. M. Alharthi, "Authentications for Internet of Things (IoT) in smart manufacturing with lightweight protocol based on PUFs," Electronics, vol. 14, no. 9, art. no. 1788, 2025. [Online]. Available: https://www.mdpi.com/2079-9292/14/9/1788

[13] S. Li, Y. Huang, and B. Yu, "Flexible and practical anonymous end-to-end authentication protocol to the PUF," Comput. Netw., vol. 247, art. no. 110426, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1389128624002585

[14] S. Dargaoui, M. Azrour, A. El Allaoui, A. Guezzaz, and M. A. A. Hammoudeh, "Novel efficient PUF-based authentication protocol for IoT-based smart agriculture applications," J. Adv. Inf. Technol., vol. 16, no. 4, pp. 582–593, 2025, doi: 10.12720/jait.16.4.582-593.

[15] "State-of-the-art and future research directions of AI-enabled smart interfaces for secure biometric authentication in IoT ecosystems," in Proc. Int. Conf. on Smart Computing (ICSC), 2026, pp. 312–319, doi: 10.1109/ICSC67292.2026.00052.

[16] S. Kanagamalliga, "Integration of biometrics and IoT for door access control and security in the distant future," in E3S Web of Conferences (ICSGET 2025), 2025. [Online]. Available:

https://www.e3s-conferences.org/articles/e3sconf/pdf/2025/19/e3sconf_icsget2025_03013.pdf

[17] Ponnuru et al., "BAAP-FIoT: Blockchain-assisted authentication protocol for fog-enabled IoT," 2025. [Reference details absent from the source manuscript — full author list, venue, volume, pages, and DOI to be completed by the authors before submission.]

[18] "Authenticating and cost-saving IoT device authentication key management system," in Proc. IHCSP 2024, 2024, doi: 10.1109/ihcsp63227.2024.10960153. [Individual author list not independently verifiable.]