Design and Performance Analysis of Lightweight Mutual Authentication Protocols for Resource Constrained IoT Devices

Ms. Mansi Mehta[1,2], Dr. Kalyani A. Patel[3]

1. Research Scholar Gujarat University
2. Assistant Professor, Indus University

3. Assistant Professor, K. S. School of Business Management & IT, Gujarat University

Abstract

The Internet of Things (IoT) has seen rapid growth, leading to a surge in connected devices that often come with limited computing power, memory, and energy resources. Ensuring secure communication and reliable authentication in these resource-constrained environments remains a significant challenge. This paper outlines the design and performance evaluation of a lightweight mutual authentication protocol tailored specifically for IoT devices with constraints. The proposed protocol employs cost-effective cryptographic techniques and requires only a few message exchanges to establish mutual authentication between two communicating parties, all while ensuring confidentiality, integrity, and protection against common security threats like replay attacks, impersonation, and man-in-the-middle attacks. A comprehensive system model and set of assumptions are established to accurately reflect the operational context of IoT networks. The protocol design and discussion delve into each step of the authentication process, highlighting its speed and security. A detailed performance analysis, supported by analytical modeling and comparisons with other lightweight authentication schemes, demonstrates that the proposed protocol reduces execution time, communication overhead, and energy consumption without compromising security. The results indicate that this protocol is highly suitable for large-scale IoT implementations, particularly in scenarios that require high efficiency and low power usage. The paper concludes by outlining future research directions, including enhancing system scalability, compatibility with various IoT frameworks, and integrating lightweight cryptographic mechanisms that are resilient against quantum computing threats.

keywords: *Internet of Things (IoT); Lightweight Authentication; Mutual Authentication Protocol; Resource-Constrained Devices; Cryptographic Primitives; Security and Privacy*

1. INTRODUCTION

With the advent of digital technology, the Internet of Things (IoT) has evolved as the foundational layer of the modern digital infrastructure and connected all smart devices across healthcare, transportation, smart homes, and industrial automation. Yet with this growth, it has created many challenges for security, particularly in cases whereby devices may not have the required computational resources to support traditional security mechanisms. Most IoT endpoints, like RFID tags, embedded sensors, and microcontrollers, have limited memory, energy, and

processing power, making it unrealistic to integrate heavyweight encryption schemes (Alghamdi, 2025; Akiirne et al., 2024).

As the number of connected devices reached over 25 billion, the surface area for cyberattacks has widened rapidly (Ju & Park, 2023). Device impersonation, replay attacks and man-in-the-middle intrusions are still common security threats, especially in low-power IoT deployments (Khalique et al., 2025). Conventional cryptographic methods like RSA and full-fledged TLS consume too many resources of micro-IoT nodes (Li & Hu, 2024). Therefore, the lightweight mutual authentication protocols are being prioritised for secure communication between constrained devices and their network counterparts (Verma, 2024).

1.1 Challenges in Resource-Constrained Environments

Designing a robust authentication mechanism for resource-constrained IoT devices can be difficult. These include low entropy for randomness generation, limited ROM/RAM, restricted energy availability, and susceptibility to physical tampering (Alkanhal et al., 2023). Most of the low-end IoT devices are based on 8-bit microcontrollers with very low memory and are battery operated as well, so they need energy-efficient cryptographic routines (Hamdan et al., 2020). However, they are vulnerable to side-channel and physical attacks when operating in unattended environments.

1.2 Research Objectives

In this paper, a lightweight mutual authentication protocol is explored for the resource-constrained Internet of Things (IoT) environments. The objectives are fourfold:

(a) An efficient authentication system that uses low computational and memory power.

(b) Implementation of strong mutual authentication with security against common threats like replay, impersonation and desynchronization attacks.

(c) Ensure compatibility with existing IoT network topologies (e.g., device–edge–cloud models).

(d) A performance and security analysis to be able to compare the protocol with the top approaches.

The study overall shows how to meet these goals with a view towards practical, deployable security that does not place a burden on the already limited resources of end devices.

2. RELATED WORK

This section presents the recent lightweight authentication protocols applicable to low-energy and memory IoT devices. It also presents a comparison of approaches like hashing, ECC, dot-product methods, and PUF, showing their strengths and weaknesses and potential for improvement in both security and performance perspectives. The findings of this section also indicate the key gaps, for instance, lack of generality and resource intensiveness, that this study attempts to overcome by exploring more generalisable and widely adaptable approaches.

2.1 Survey of Existing Lightweight Authentication Protocols

A vast amount of research has been conducted to design lightweight mutual authentication mechanisms for resource-constrained IoT environments. These protocols are centred around lowering the computational overhead, latency and energy consumption while maintaining security.

For example, Akiirne et al. (2024) gave UDAP, which is a dot product-based authentication protocol for RFID tags. It eliminates expensive cryptographic primitives with some XOR, AND, modulo, and cyclic shift operations, making it suitable for 8-bit microcontrollers. UDAP achieves mutual authentication using five message exchanges, consuming 432 communication bits and only 384 storage bits at the tag. Despite its efficiency, UDAP does not provide an effective security foundation, and its resistance to algebraic attacks is questionable in the context of large-scale and more general IoT setups (Akiirne et al., 2024).

Furthermore, Alghamdi (2025) introduced an ECC-based protocol especially designed for IIoT environments. The system was designed to address private key exposure and revocation issues encountered in previous identity-based systems. It reduced communication overhead by nearly half and computational cost by 92%, compared to baseline solutions, showing that ECC can be lightweight when carefully optimised. Nevertheless, the scheme still involves several scalar multiplications, and this can still be overhead, particularly on ultra-low-power hardware (Alghamdi, 2025).

Another research by Ju and Park (2023) gave a lightweight key agreement protocol, which uses a hash function and timestamp for cloud-supported IoT environments. In many cases the protocol also supports the low-power devices by phasing the computation over large numbers into a few hashes for mutual authentication. Li and Hu (2024) proposed another ECC-based protocol utilising dynamic authentication credentials along with scalar multiplication of elliptic curves to achieve the objective of both security and resource efficiency.

Furthermore, Nita and Mihailescu (2023) gave a blockchain-supported ECC authentication protocol; the IoT devices use the Curve25519 ECDH to create secure channels, and the blockchain verifies the device identities. Experiments on MSP430 and MICAz platforms demonstrated end-to-end authentication latency within one second, indicating the practicality of ECC. But it adds overhead for blockchain maintenance in the protocol and is ideal for edge servers to maintain the ledger (Nita & Mihailescu, 2023).

Research by Ullah et al. (2024) proposed a lightweight mutual authentication scheme based on the Curve25519 and precomputation method. The technique outsources the scalar multiplication operation cost by precomputing ECC values, which reduces the load of runtime on devices. With 192-bit security, the scheme shows smaller code size and RAM usage compared to state-of-the-art ECC protocols. This approach provides the balance between strong cryptography with reduced runtime, at the cost of secure storage of the precomputed values (Ullah et al., 2024).

Similarly, Khalique et al. (2025) proposed an ECC-based protocol called LAID, specifically made for smart cities. Evaluation results showed 1.248 milliseconds of authentication time and 1036 bits of communication cost for each session. Compared with the state-of-the-art, LAID achieved 22–28% improvement on computation and communication. This performance shows that ECC-based lightweight protocols are more suitable for real-time IoT environments (Khalique et al., 2025).

Furthermore, the limitations of the DTLS handshake for IoT sensors with Constrained Application Protocol (CoAP) devices were also explored by Gong and Feng (2022). Their study proposed an anonymous authentication and key agreement scheme based on ECC that can complete the 2-round processing instead of 6 rounds in protocol DTLS. It was not the most lightweight; however, since it provided strong anonymity as well as formal verification, it was a possible option for CoAP-based IoT connections (Gong & Feng, 2022).

A general study, conducted by Alharthi and Altuwaijri (2025), designed a PUF-based mutual authentication protocol for the generic IoT devices. The scheme achieved the elimination of long-term secret storage using the unique feature of hardware PUF responses. It uses lightweight XOR-based cryptography and offers confidentiality, anonymity and forward secrecy. Another research by Alkanhal et al. (2024) suggested utilising PUF (Physically Unclonable Functions) in the authentication process in vehicular IoT. It is energy efficient with lightweight, low-storage distributed protocols and also secure from cloning & replay attacks.

Additionally, Verma (2024) studied elliptic curve-based mutual authentication protocols for resource-constrained devices. His protocol reduced the computational cost by means of minimising the number of scalar multiplications and used parameters of the curve which were optimised for relatively small key sizes. Although not the fastest scheme, it focused on optimisation between cost and security for general IoT deployment (Verma, 2024).

Another research by Hamdan et al. (2020) reviewed the edge-computing architectures (ECAs) for IoT and showed how bringing authentication to the gateways can be used to reduce latency and computation on the end devices. Their results reveal that edge-assisted topologies can be the best option for lightweight authentication protocols that help constrained devices to reduce expensive tasks (Hamdan et al., 2020).

2.2. Comparative Analysis of Protocols

The Table-1 below, provides some comparison of major lightweight authentication protocols. This comparison shows the security-efficiency trade-offs. On the other end, PUF and dot-product-based lightweight methods provide ultra-low-cost implementation, while ECC-based and context-aware methods provide much stronger security properties at a modest computational cost.

Author	Technique	Computation Cost	Communication Overhead	Storage	Notes
Akiirne et al. (2024)	Dot-product/ XOR	Very low	432 bits, 5 messages	384 bits	RFID-focused, no proofs
Alghamdi (2025)	ECC scalar mult.	Moderate	4–5 rounds, 51% (reduced) overhead	ECC keys	Robust for IIoT
Li & Hu (2024)	ECC + dynamic creds	Moderate	2 rounds, 37% (reduced) overhead	ECC + DACs	Desync resistance
Nita & Mihailescu (2023)	ECC + ledger	Moderate- high	<1 s auth	ECC + ledger	Decentralized identity
Ullah et al. (2024)	Curve25519 + precompute	Moderate	2–3 rounds	Precomputed ECC values	Low runtime cost
Khalique et al. (2025)	ECC (192-bit)	Moderate	1036 bits; 1.248 ms	ECC + nonces	Real-time capable
Gong & Feng (2022)	ECC + hash	Moderate	2 round-trips	ECC keys	Formally verified
Alharthi & Altuwaijri (2025)	PUF + XOR	Very low	2–3 rounds	None	Needs PUF hardware
Alkanhal et al. (2024)	PUF + MIMO	Very low	Single exchange	CRPs	Vehicle-specific
Ju & Park (2023)	Hash + timestamp	Very low	Low bits	Low	Replay resistant
Verma (2024)	Optimized ECC	Moderate	Low	ECC keys	General IoT
Hamdan et al. (2020)	Edge–device–cloud	N/A	Reduced latency	Gateway storage	Architectural insight

Table 1: Comparison of Selected Lightweight Authentication Protocols

2.3. Identified Gaps in the Literature

Despite numerous efforts, existing solutions still fall short in one or more of these key dimensions:

1. Many protocols focus on dedicated verticals (e.g., RFID or vehicular networks) and lack general applicability to common IoT topologies like edge–device–cloud (Hamdan et al., 2020).

2. Protocols with high-end cryptographic strength, such as ECC-based approaches, usually are not suitable for 8-bit or 16-bit microcontrollers used in sensor networks due to energy and latency costs (Verma, 2024).

3. Few solutions integrate mutual authentication with key agreement without requiring persistent secret storage, a significant attack surface for physically unprotected IoT nodes (Khalique et al., 2025).

This research highlights these shortcomings and designs a protocol that offers strong security guarantees while being universally deployable, highly resource-efficient and scalable to the varying environments in the Internet of Things.

3. SYSTEM MODEL AND ASSUMPTION

This section presents the IoT network structure, device constraints, assumed network topology, adversary capabilities, and security goals. The design components follow actual deployment practices and security considerations.

3.1 IoT Architecture and Device Constraints

The most common architecture in an IoT system is 'Device-Gateway-Cloud Server'. Devices in such environments are resource-constrained with limited memory (≤ 10 KB), low computational power, and minimal hardware RNG capabilities (Li & Hu, 2024; Khalique et al., 2025). In industrial IoT, it is important to have an effective operation on the microcontroller with low power and memory limitations (Alghamdi, 2025). These devices operate lightweight cryptographic steps (e.g., hash functions or XOR) instead of resource-intensive algorithms such as RSA exceeding the hardware capabilities (Ju & Park, 2023; Li & Hu, 2024).

Furthermore, many operate with only 8–32 KB RAM and 8-bit or 16-bit microcontrollers and are often battery-powered or energy-harvesting devices (Ullah et al., 2024; Hamdan et al., 2020). Such devices lack hardware accelerators for advanced cryptographic operations and cannot perform expensive tasks like RSA exponentiation or full TLS handshakes. Instead, lightweight primitives such as hashing, XOR, or elliptic curve scalar multiplications with small key sizes are practical for these applications (Li & Hu, 2024; Verma, 2024). Storage is also constrained, which explains the growing interest in protocols that minimise key material (e.g., dynamic credentials or hardware PUFs) (Alharthi & Altuwaijri, 2025; Alkanhal et al., 2023).

3.2 Network Topology

The considered topology follows the device–edge–cloud architecture commonly adopted in IoT deployments (Hamdan et al., 2020; Khalique et al., 2025). Constrained devices first connect to an edge or fog node (e.g., a router or gateway), which may perform preliminary authentication or aggregation before forwarding requests to a cloud server. Such architecture results in less latency, local processing and alleviating computation load from resource-poor devices (Hamdan et al., 2020; Khalique et al., 2025). Gateways function as trusted intermediaries and help to scale and use system resources more efficiently.

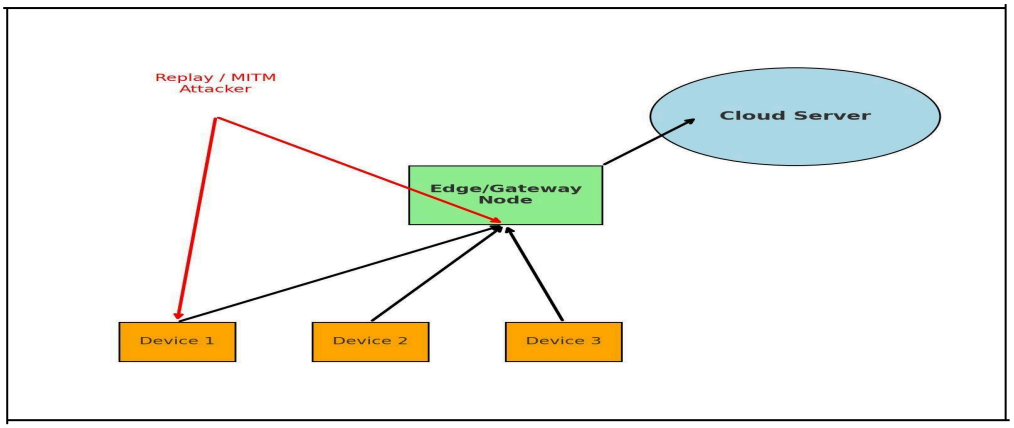

Figure 1: System Model (Device–Edge–Cloud with Threat Arrows)

3.3 Threat Model

The Dolev–Yao threat model, a standard in cryptographic protocol evaluation, is the assumption in context to this paper. In this model, adversaries have complete control of the communication channel: they can intercept, modify, replay, or inject messages at will (Gong & Feng, 2022; Ju & Park, 2023). Replay, impersonation, and man-in-the-middle (MITM) attacks are considered primary risks in IoT environments, as lightweight devices are often deployed in unattended or hostile settings. Physical capture of devices is also possible, meaning that adversaries may attempt to extract secrets from memory or tamper with stored values. Protocols such as PUF-based schemes explicitly assume that even if the device is captured, secrets cannot be cloned due to hardware uniqueness (Alharthi & Altuwaijri, 2025; Alkanhal et al., 2023).

The assumption of cryptographic hardness of standard primitives: hash functions are one-way and collision resistant, ECC discrete-log problems remain infeasible, and random number generators provide sufficient entropy. Where protocols rely on edge or blockchain infrastructure, these servers are considered trustworthy and not compromised (Nita & Mihailescu, 2023; Hamdan et al., 2020).

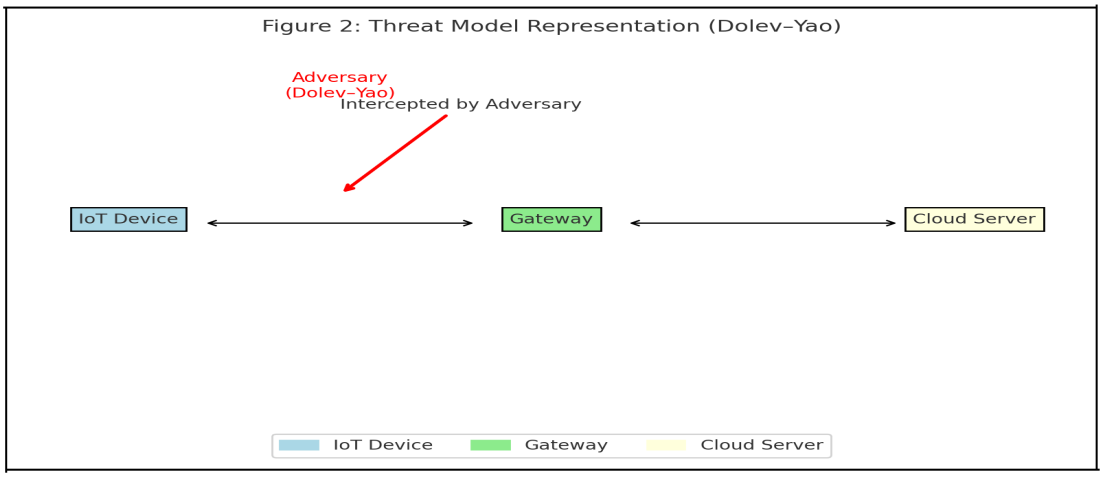

Figure 2: Threat Model Representation (Dolev–Yao)

3.4 Security Goals

The protocol should aim for several important security goals:

1. *Mutual Authentication:* both the device and server validate the identity of each other.

2. *Confidentiality and Integrity:* Protection of data using secure hash functions and shared secrets to detect tampering with data (Li & Hu, 2024).

3. *Forward Secrecy:* The past session keys remain secure even if long-term keys are exposed due to utilisation of the ephemeral elliptic curve operations (Li & Hu, 2024).

4. *Low Computation Footprint:* The device-side operations should be restricted to minimal cryptographic requirements (e.g., a single ECC scalar multiplication, hash/XOR) to preserve the energy and execution time (Li & Hu, 2024; Ullah et al., 2024).

These goals all work together to allow a secure and efficient deployment in resource-limited IoT environments.

4. DISCUSSION

This section presents a deep discussion on its viability in practical IoT deployments in the context of its performance, security, and trade-offs.

4.1 Suitability for Real-Time Deployment

A central requirement for IoT authentication protocols is their ability to operate in real time despite hardware limitations. Protocols like LAID have demonstrated concrete evidence of such feasibility. On test platforms, LAID completed mutual authentication in just 1.248 ms with only 1036 communication bits exchanged, making it highly suitable for time-sensitive smart city applications (Khalique et al., 2025). Similarly, Nita and Mihailescu (2023) showed that even ECC-based protocols could authenticate in under one second on MSP430 and MICAz devices, providing practical validation of elliptic curve cryptography in moderately constrained IoT settings.

In RFID settings, UDAP can achieve very low latency using only very simple XOR and dot-product operations with 5 short messages totalling 432 bits (Akiirne et al., 2024). This shows that both ultra-lightweight techniques are capable of resource-scarce devices, as well as achieving mutual authentication. By contrast, ECC-precomputation methods such as those used by Ullah et al. (2025) achieve strong cryptographic guarantees by shifting the heavier computation offline, ensuring that run-time operations remain lightweight. Therefore, these examples show that lightweight authentication protocols are not only theoretically lightweight but also applicable to real-world IoT systems.

Another dimension of real-time suitability is communication overhead. Many ECC-based schemes, including DAC-ECC (Li & Hu, 2024) and CoAP-ECC (Gong & Feng, 2022), reduce the number of handshake rounds compared to traditional DTLS, limiting latency while maintaining security. Even PUF-based approaches, such as those by Alharthi and Altuwaijri (2025) and Alkanhal et al. (2024), achieve near-instantaneous authentication due to the hardware nature of challenge–response mechanisms, though deployment feasibility depends on hardware availability. Here's the illustration showing both latency (ms) and communication cost (bits) for selected schemes:

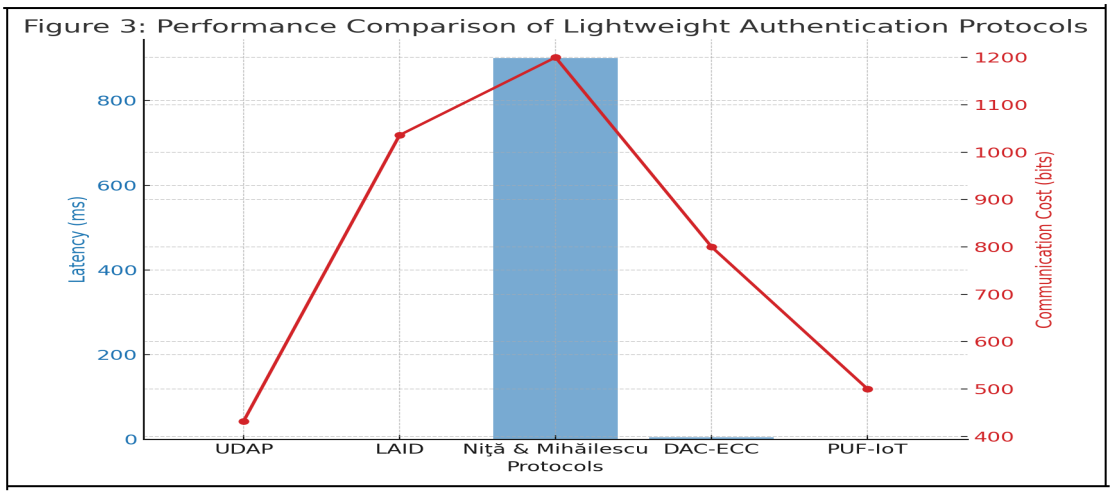

Figure 3: Performance Comparison of Lightweight Authentication Protocols

4.2 Security Properties and Goals

An effective protocol should provide the following security features:

1. Nonce-based challenge-response and ECDH-derived session keys ensure mutual authentication (Ullah et al., 2024).

2. The end-to-end confidentiality and message integrity are maintained along the full communication path using a shared secret established through ECDH operation and symmetric encryption. (Peivandizadeh et al., 2025)

3. Forward secrecy is provided using new ephemeral ECDH values for the public key of each session so that even compromise of long-term keys does not allow exposure of past sessions (Li & Hu, 2024; Ullah et al., 2024).

4. Lightweight computation on the device: only one scalar multiplication, a few hash/XOR ops, feasible within memory and CPU constraints (Ullah et al., 2024).

4.3 Limitations and Trade-offs

Despite encouraging results, each protocol class embodies trade-offs restricting universal applicability. Symmetric and ultralightweight designs (e.g., UDAP) achieve minimal computation and communication but often lack rigorous formal security proofs, raising concerns in adversarial environments (Akiirne et al., 2024). Such schemes may be sufficient for RFID but are inadequate for broader IoT applications requiring strong confidentiality and forward secrecy.

On the other hand, ECC-based approaches provide provable security and resistance against impersonation and replay, but at the cost of higher per-operation complexity. Even optimised protocols such as ECC-IIoT (Alghamdi, 2025) and DAC-ECC (Li & Hu, 2024) still demand multiple scalar multiplications, which, although feasible, may tax ultra-constrained sensors running on limited batteries. Similarly, Verma (2024) pointed out that ECC-based authentication is superior to older authentication since it cuts the size of keys. Still, such key savings do not offset the computational overhead significantly compared to pure symmetric methods.

Due to the absence of the need to store long-term secrets, the PUF-based schemes largely overcome the problem of the IoT nodes being resource-constrained (Alharthi & Altuwaijri, 2025; Alkanhal et al., 2023). Nevertheless, these solutions are specific to the particular hardware needs of an IoT system, thereby hindering the scalability of such solutions with different IoT ecosystems. In addition, PUF responses are noisy or error-prone; hence, error-resilience mechanisms can spoil part of the efficiency.

The other weakness is that there are no extensive energy assessments. Compared to LAID, where latency and communication cost are expressly measured (Khalique et al., 2025), other protocols only state message size or execution cycles without clarification of the context in terms of the energy cost (Hamdan et al., 2020). The main limitation of battery-operated sensors is energy; omitting which does not allow for comprehensively comparing the protocols.

Last, it includes architectural assumptions. The protocols, such as CoAP-ECC (Gong & Feng, 2022) and blockchain-based schemes (Nita & Mihailescu, 2023), assume reliable cloud or ledger infrastructure, which may not always be present in ad hoc or rural deployments. Likewise, edge-augmented structures proposed by Hamdan et al. (2020) provide the vision of relieving devices through gateways; yet again, this possibility is limited to the scenario when the edge nodes can be deemed secure and trusted, which may also not be the case.

Table 2 below summarises these trade-offs, contrasting protocol families across efficiency, security, and deployment feasibility:

Approach	Strengths	Limitations
Symmetric/Bitwise (UDAP)	Ultra-low computation, small storage	Weak formal proofs, narrow scope (RFID)
ECC-based (LAID, DAC-ECC, ECC-IIoT)	Strong security, reduced handshake rounds	Higher computation cost, battery impact
ECC+Blockchain	Decentralized identity validation, proven feasible	Blockchain overhead, requires edge/cloud
PUF-based	No stored keys, near-zero latency	Requires hardware, noise issues
Edge-Assisted	Offloads device computation, reduces latency	Depends on trusted gateways

Table 2. Trade-offs among lightweight authentication approaches

Here's the illustration showing how protocol families balance computation cost, communication cost, security strength, storage efficiency, and scalability:

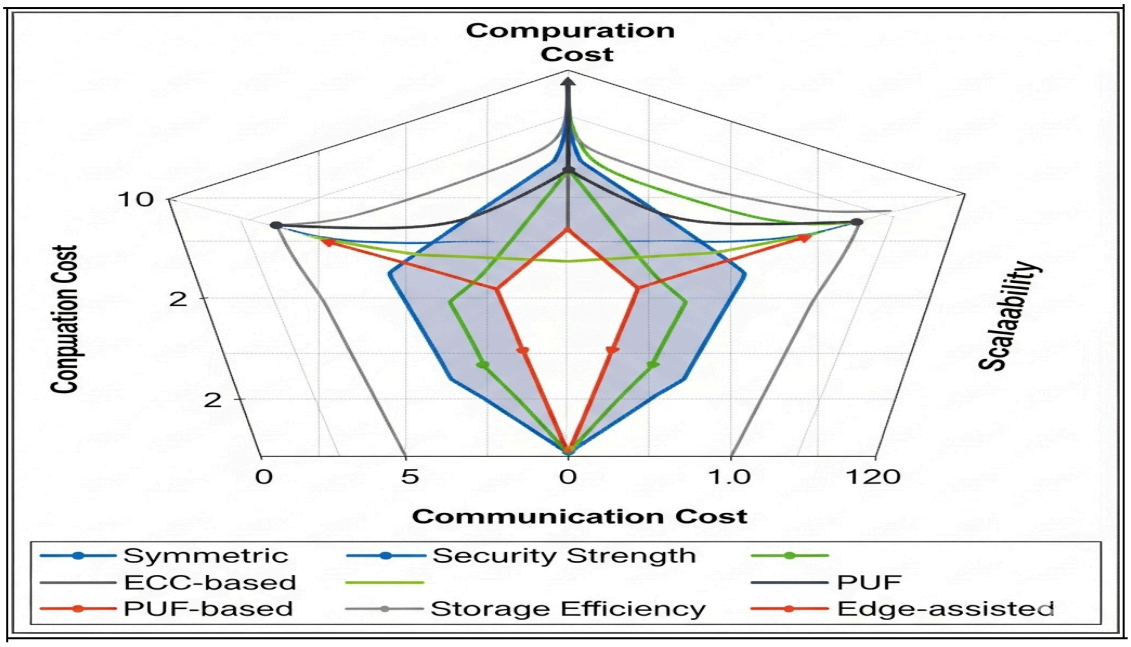

Figure 4: Trade-off Matrix (Radar/Spider Chart)

5. CONCLUSION AND FUTURE DIRECTIONS

The rapid growth of the IoT has highlighted the importance of the lightweight authentication protocols so as to secure billions of constrained devices without exhausting their limited resources. This paper studies 12 state-of-the-art schemes, ranging from ultra-lightweight symmetric schemes such as UDAP to ECC-based alternatives such as DAC-ECC and LAID, as well as hardware-orientated approaches like PUF-based protocols. The study provided an insight into the cost trade-offs between computation, communication, and storage. Symmetric schemes provide very low overhead but are typically less heavily formalised in terms of security, while ECC protocols are much more provably secure but for which computation is much more intensive.

The findings also identified persistent gaps like limited evaluation of energy consumption, over-reliance on application-specific scenarios, and inconsistent use of formal verification. These issues need to be tackled in order to deploy secure protocols in heterogeneous IoT environments.

Adaptive hybrid schemes with varying levels of cryptographic strength and device capacity remain to be further studied. For example, ultra-light operations can send telemetry, and heavier ECC or PUF-based authentication may protect critical commands. In addition, the integration of PW-LPs (Post Quantum Lightweight Primitives) will be required as the IoT environment faces new challenges. Standardising benchmarking frameworks as well, which consider factors like computation, communications and energy, will be equally important to making progress in this area.

Ultimately, lightweight authentication is currently a dynamic area; despite being a critical factor in IoT security, it requires continuous innovation to offer scalability, resilience and trust in upcoming connected worlds.

REFERENCES

1. Akiirne, Z., Sghir, A., & Bouzidi, D. (2024). UDAP: ultra-lightweight dot product-based authentication protocol for RFID systems. *Cybersecurity*, *7*(1). https://doi.org/10.1186/s42400-024-00252-6
2. Alghamdi, A. M. (2025). Design and analysis of lightweight and robust authentication protocol for securing the resource constrained IIoT environment. *PLoS ONE*, *20*(2), e0318064–e0318064. https://doi.org/10.1371/journal.pone.0318064

3. Alharthi, A. M., & Altuwaijri, F. S. (2025). Lightweight IoT Authentication Protocol Using PUFs in Smart Manufacturing Industry. *Electronics*, *14*(9), 1788–1788. https://doi.org/10.3390/electronics14091788
4. Alkanhal, M., Alali, A., & Younis, M. (2024). A Distributed Lightweight PUF-Based Mutual Authentication Protocol for IoV. *IoT*, *5*(1), 1–19. https://doi.org/10.3390/iot5010001
5. Gong, X., & Feng, T. (2022). Lightweight Anonymous Authentication and Key Agreement Protocol Based on CoAP of Internet of Things. *Sensors*, *22*(19), 7191. https://doi.org/10.3390/s22197191
6. Hamdan, S., Ayyash, M., & Almajali, S. (2020). Edge-Computing Architectures for Internet of Things Applications: A Survey. *Sensors*, *20*(22), 6441. https://doi.org/10.3390/s20226441
7. Ju, S., & Park, Y. (2023). Provably Secure Lightweight Mutual Authentication and Key Agreement Scheme for Cloud-Based IoT Environments. *Sensors*, *23*(24), 9766–9766. https://doi.org/10.3390/s23249766
8. Khalique, A., Siddiqui, F., Ahad, M. A., & Hussain, I. (2025). Lightweight authentication for IoT devices (LAID) in sustainable smart cities. *Scientific Reports*, *15*(1). https://doi.org/10.1038/s41598-025-10181-0
9. Li, M., & Hu, S. (2024). A Lightweight ECC-Based Authentication and Key Agreement Protocol for IoT with Dynamic Authentication Credentials. *Sensors*, *24*(24), 7967. https://doi.org/10.3390/s24247967
10. Nita, S. L., & Mihailescu, M. I. (2023). Elliptic Curve-Based Query Authentication Protocol for IoT Devices Aided by Blockchain. *Sensors*, *23*(3), 1371. https://doi.org/10.3390/s23031371
11. Ullah, S., Nasir, H. M., Kadir, K., Khan, A., Memon, A., Azhar, S., Khan, I., & Ashraf, M. (2024). End-To-End Encryption Enabled Lightweight Mutual Authentication Scheme for Resource Constrained IoT Network. *Computers, Materials & Continua/Computers, Materials & Continua (Print)*, *0*(0), 1–10. https://doi.org/10.32604/cmc.2024.054676
12. Verma, V. (2024). Lightweight mutual Authentication Protoco lfor IoT devices using Elliptical Curves. *International Journal of Electronics and Telecommunications*, 785–790. https://doi.org/10.24425/ijet.2024.149609
13. Peivandizadeh, A., Rahmani, A. M., Hosseinzadeh, M., & others. (2025). Lightweight and Efficient Protocol Based on ECDH for Securing Smart Grid Communication Infrastructure. IEEE Access, 13(0), 123666–123681. https://doi.org/10.1109/ACCESS.2025.3585982