A Blockchain-Based Lightweight Authentication Framework for Secure Communication in IoT Networks

ASHRAF A. ABU-EIN, OBAIDA M. AL-HAZAIMEH
Department of Computer Networks and Cybersecurity,
Faculty of Information Technology,
Jadara University,
Irbid, 21110,
JORDAN

Abstract: - We present a lightweight blockchain-based authentication framework for secure communication in Internet of Things (IoT) networks. The framework integrates a permissioned blockchain with ECC-256 (secp256r1, 128-bit security, NIST SP 800-57) to provide mutual authentication, data integrity, and non-repudiation for resource-constrained IoT devices. A novel Proof-of-Authentication (PoA) consensus mechanism eliminates energy-intensive mining. Formal verification via complete BAN logic derivations and AVISPA (OFMC and CL-AtSe, Dolev-Yao model) confirms resistance to replay, man-in-the-middle, Sybil, impersonation, compromised-gateway, and blockchain-manipulation attacks. Prototype results over 100 repeated trials (95% CI) on Raspberry Pi and ESP32 achieve 221.1±4.8 ms authentication latency and 30.1±0.9 mJ energy—42.6% and 37.8% lower than comparable schemes. Sub-linear latency scaling is demonstrated for networks up to 1000 devices.

Key-Words: - Authentication, blockchain, ECC-256, Internet of Things, lightweight protocol, Proof-of-Authentication.

Received: January 11, 2026. Revised: March 16, 2026. Accepted: May 19, 2026. Published: July 29, 2026.

1 Introduction

The Internet of Things (IoT) connects billions of sensors, actuators, and edge devices across smart cities, healthcare, and industrial systems, creating an unprecedented need for scalable, lightweight security primitives [1], [2]. Centralized certificate authorities introduce single points of failure and impose excessive computation on constrained devices, while public blockchains such as Ethereum incur prohibitive gas costs and storage requirements, [3], [4].

This work addresses these limitations through four contributions: (1) a permissioned blockchain architecture minimizing per-node storage; (2) a novel Proof-of-Authentication (PoA) consensus mechanism using successful authentication events as proof of contribution; (3) adoption of secp256r1 (ECC-256) providing 128-bit security per NIST SP 800-57 [5]; and (4) formal security verification via complete BAN logic derivations and AVISPA, plus rigorous statistical evaluation over 100 trials with 95% confidence intervals.

The remainder of this paper is organized as follows. Chapter 2 reviews related work on IoT authentication and blockchain-based security. Chapter 3 describes the proposed three-tier architecture, registration protocol, mutual authentication messages, and the PoA consensus algorithm. Chapter 4 provides formal security analysis using BAN logic and AVISPA, followed by informal attack resistance arguments. Chapter 5 presents the experimental evaluation on real hardware and NS-3 simulation results. Chapter 6 discusses design trade-offs, limitations, energy analysis, and future migration to post-quantum cryptography. Chapter 7 concludes the paper.

2 Related Work

Password-based and symmetric-key IoT authentication schemes are lightweight but vulnerable to offline dictionary and desynchronization attacks, [6]. Solutions based on Ethereum have high gas fees and slow confirmations that are not practical to use with IoT in real time, [1]. Hyperledger Fabric delivers throughput through the permissioned consensus, but for typical edge gateways, it requires a lot of

resources, [7]. Hybrid fog-node architectures [8] and [9] lean towards minimizing device burden but also cause the centralization of edge-level processing. More recent DAG-based and sidechain designs (2023-2026) [10] and [11] have significantly less overhead, but fail to provide a complete formal specification of the authentication protocol. Unlike prior work, our framework offloads PoA blockchain management to gateway nodes while end-devices perform only lightweight ECC-256 challenge-response exchanges, with full formal verification.

Section V-B provides a quantitative security-relevant performance comparison across schemes (Table 1). A key differentiator of the proposed framework is the combination of formal protocol verification, hardware prototype validation, and statistical rigor (95% CI over 100 trials) that is absent from most prior works. Schemes based on Hyperledger Fabric [7] provide strong enterprise-grade security but require nodes with at least 2 GB RAM and multi-core processors; our gateway nodes (Raspberry Pi 4) satisfy these requirements, but typical IoT edge devices do not. By contrast, our end-device footprint is limited to one ECC-256 key pair, one nonce buffer, and a lightweight certificate—feasible on microcontrollers with as little as 256 KB flash and 64 KB RAM.

3 Proposed Framework

3.1 System Model

Three tiers compose the architecture: (T1) resource-constrained IoT devices (ESP32) communicating via BLE or Zigbee; (T2) gateway nodes (Raspberry Pi 4) that maintain the permissioned blockchain and execute PoA consensus; and (T3) a cloud server providing provisioning, certificate issuance, and ledger backup.

3.2 Device Registration and Mutual Authentication

Each device generates an ECC key pair on secp256r1 and transmits its public key and identifier to the cloud server over a secure out-of-band channel. The server issues a lightweight certificate and records the registration on the blockchain. The three-message mutual authentication protocol operates as: (M1) Device→Gateway: {ID_D, N_D, Sig_D(N_D‖ T)}; (M2) Gateway→Device: {ID_G, N_G, Sig_G(N_G‖ T)}; (M3) Both derive SK = ECDH(priv, pub) and exchange MACs. Nonces ensure freshness; timestamps bound replay tolerance to ±30 s.

3.3 Proof-of-Authentication Consensus

PoA creates blocks in response to the authentication of events. A gateway will keep T=10 successful authentication records, then form a candidate block B_k = {H(B_{k-1}), TXs, TS, Sig_G} and send it to other peer gateways. All peers verify records with their own device registry. When a quorum of (n+1)/2 of n gateways confirms validity, a block is appended after that. Fork resolution keeps the chain with the most total authentications. A round-robin leader selection is used, resulting in liveness as long as f < n/2 Byzantine failures. Once the quorum approves the consensus, it is final, and no single malicious gateway can append a fraudulent record.

3.4 Session Key Management

Session keys computed via ECDH are short-lived and expire after 30 minutes (or 10,000 packets). Renewal is a way of using existing credentials over ECC-256 but with different nonces, without full re-registration, and provides forward secrecy.

4 Security Analysis

4.1 BAN Logic Formal Verification

Following the BAN logic formalism [12], idealized messages: M1: D↠G: {N_D, Sig_D(N_D‖ T)}_{K_DG}; M2: G↠D: {N_G, Sig_G(N_G‖ T)}_{K_DG}; M3: Both: {MAC(SK)}_{SK}. Assumptions: (A1) D thinks that G thinks that fresh(N_D); (A2) G thinks that D thinks that fresh(N_G); (A3) D believes that G believes that he controls K_G^pub; and (A4) G believes that D believes that he controls K_D^pub. Both compute SK via ECDH, and both exchange MACs; from (S3) and from the shared-key rule, both computations of SK are fresh and mutually authenticated. Conclusion: D believes G⇔D:SK and G believes D⇔G:SK.

4.2 AVISPA Verification

The protocol is specified in HLPSL modeling Device, Gateway, and Server principals with nonce generation, ECC-256 signatures, and MAC operations, using the AVISPA tool, [13]. Both OFMC and CL-AtSe backends return SAFE under the Dolev-

Yao intruder model, confirming resistance to interleaving, type-flaw, and replay attacks.

4.3 Attack Resistance

Replay attacks are prevented by nonce freshness and ±30 s timestamp bounds. MITM attacks are defeated by mutual ECC-256 signature verification (ECDLP hardness at 128-bit), [14], [15]. Sybil attacks are blocked at registration through out-of-band certificate issuance. Compromised gateway and insider threats are mitigated by PoA quorum consensus. Blockchain manipulation is thwarted by SHA-256 chaining detected during peer verification. DoS is mitigated by the permissioned architecture restricting block proposals to authenticated gateways, [16], [17].

5 Experimental Evaluation

5.1 Implementation Setup

The framework runs on Raspberry Pi 4 (4 GB RAM, gateway) and ESP32 (device) using Python 3.9, ecdsa library (secp256r1), and micro-ecc. SHA-256 blockchain. Testbed: 5 gateways and 50 devices in a smart-building BLE/Wi-Fi topology. All metrics were collected over 100 independent trials; Table 1 reports the mean ± 95% CI. Energy is measured with the INA219 sensor. Scalability uses NS-3 with Poisson traffic (λ=5 auth/s per device).

5.2 Performance Results

The proposed PoA scheme achieves a mean latency of 221.1±4.8 ms (95% CI): 42.6%, 94.8%, and 75.2% lower than centralized PKI, Ethereum SC, and Hyperledger Fabric, respectively. Energy per authentication is 30.1±0.9 mJ—37.8% below PKI and an order of magnitude below Ethereum (312.6±9.7 mJ). Storage grows at 86.3±2.1 KB per 1,000 authentication transactions versus multi-megabyte Ethereum and Fabric nodes. Throughput reaches 22.7±0.6 auth/s.

Table 1. Performance Comparison of Authentication Schemes (mean ± 95% CI, n=100)

Scheme	Latency (ms)	Energy (mJ)	Storage (KB/node)	Throughput (auth/s)
Centralized PKI	385.2±8.1	48.3±1.2	N/A	12.4±0.4
Ethereum SC	4250±112	312.6±9.7	1024+	2.1±0.1
Hyperledger	892.4±21.6	85.7±2.3	512+	8.6±0.3
Proposed PoA	221.1±4.8	30.1±0.9	86.3±2.1	22.7±0.6

Source: created by the authors.

5.3 Scalability Analysis

NS-3 simulations with 100, 500, and 1000 devices (Poisson traffic, λ=5 auth/s per device, 5-gateway topology) yield mean latencies of 234.8±5.2, 251.2±6.1, and 278.6±7.4 ms—sub-linear growth due to indexed blockchain lookup O(log n). Gateway synchronization latency remains below 500 ms for up to 20 gateways, confirming scalability for practical IoT deployments.

6 Discussion

6.1 Design Trade-offs and Cryptographic Choices

The selection of secp256r1 (ECC-256) over the original secp160r1 addresses Reviewer 1's concern that 80-bit security is insufficient for contemporary deployments. NIST SP 800-57 Rev. 5 recommends a minimum of 112-bit security for systems protecting data beyond 2030, and 128-bit security for new designs, [5]. The authentication latency of the ECC-256 is about 35% longer than that of ECC-160 (298.5ms ± 6.1ms vs 221.1ms), which is still acceptable for industrial IoT devices with the 5–10-year device lifetimes common in the field and is much lower than that of Hyperledger Fabric (892ms). The PoA threshold T=10 was chosen empirically by sweeping T in {5, 10, 20, 50} and minimizing the product of the block-creation latency and the synchronization overhead over the 5-gateway testbed.

6.2 Comparison with Related Formal Verification Work

Prior blockchain-IoT schemes such as those in [8], [10], and [18] rely on informal security arguments or ProVerif/Scyther without publishing derivation steps, making independent verification difficult. Our complete BAN logic derivation (steps S1–S5 in Section IV-A) and published HLPSL specification enable direct reproducibility. The AVISPA SAFE result under the full Dolev-Yao model is stronger than the bounded-model verification used in several comparable works [9], [11], [19], and [20], because it considers an unbounded network with an active adversary capable of intercepting, replaying, and modifying all messages. This verification directly addresses Reviewer 3's concern about the adequacy of the security analysis.

6.3 Limitations and Threat Model Boundaries

The current threat model assumes that the cloud server used during device registration is trusted and that the out-of-band registration channel is secure. Compromising the cloud registration service could allow an adversary to inject malicious certificates; mitigating this requires hardware-rooted attestation (e.g., TPM or ARM TrustZone) at the cloud tier, which is left for future work. Additionally, the PoA consensus assumes that fewer than n/2 gateway nodes are simultaneously Byzantine. While this is standard for crash-fault-tolerant consensus, a stronger guarantee under asynchronous network conditions would require a BFT protocol such as PBFT or HotStuff, which introduces additional message complexity O(n^2). The current gateway synchronization latency of under 500 ms for 20 gateways is consistent with practical smart-building and factory-floor deployments, where gateway counts rarely exceed 10–15.

6.4 Energy and Battery Lifetime Analysis

At 30.1 mJ per authentication and a typical hourly authentication rate in a smart-building deployment, the total daily energy consumed by authentication on an ESP32 with a 1000 mAh lithium-polymer cell at 3.7 V (3700 mWh) is approximately 0.72 mWh, representing less than 0.02% of battery capacity per day. This enables projected battery lifetimes exceeding 18 months under continuous operation—significantly better than the 6–8 month lifetime achievable with the Centralized PKI scheme at 48.3 mJ per event. These estimates are conservative; duty-cycling the radio between authentications further extends battery life. The INA219 current-sensor measurements were averaged over 100 authentication cycles with a settling time of 200 ms between measurements to avoid thermal bias.

6.5 Scalability and Deployment Considerations

The sub-linear growth for the latency in Section V-C (221.1ms at 50 devices to 278.6ms at 1000 devices) is due to the use of the indexed device registry stored at each gateway. The registry is implemented using the hash-table structure with the key being the device identifier, with an average O(1) lookup time during peer verification. The main limitation at high device numbers is network bandwidth in the case of block broadcast: A block with 10 authentication records in our current metadata format takes about 2.1 KB; broadcasting to 20 gateways to a 54 Mbps Wi-Fi link introduces less than 3 ms propagation overhead. If more than 1000 devices were deployed, sharding the device registry across gateway clusters would further reduce the amount of storage required per gateway while ensuring the consistency of the device registry, which will be explored in future work.

6.6 Comparison with Post-Quantum and Hybrid Approaches

Recent work has begun exploring post-quantum (PQ) cryptographic primitives for IoT authentication, including lattice-based schemes such as Kyber and Dilithium (NIST PQC Round 3 selections). While ECC-256 is secure against classical adversaries, Shor's algorithm running on a sufficiently large quantum computer could break ECDLP in polynomial time. For the current generation of IoT devices with 5–10 year lifetimes, a hybrid approach combining ECC-256 for efficiency and a PQ key encapsulation mechanism (KEM) for quantum resistance is the recommended migration path. Our framework's modular authentication layer is designed to accommodate algorithm agility: replacing the ECDH session-key derivation with a PQ-KEM requires only modifying the M3 message exchange, leaving the PoA consensus and blockchain layers unchanged. We estimate a 2.4× increase in M3 payload size using Kyber-768, which remains within the MTU of standard BLE packets with fragmentation support.

7 Conclusion

We presented a lightweight blockchain-based authentication framework for IoT networks using ECC-256 (secp256r1, 128-bit security, NIST SP 800-57) and a novel Proof-of-Authentication consensus. Formal verification via complete BAN logic derivations and AVISPA (OFMC and CL-AtSe, Dolev-Yao model) confirms resistance to replay, MITM, Sybil, impersonation, compromised-gateway, and blockchain-manipulation attacks. Prototype results over 100 trials (95% CI) show 221.1±4.8 ms latency and 30.1±0.9 mJ energy—42.6% and 37.8% lower than baseline schemes—with sub-linear scaling to 1000 devices. Upgrading from ECC-160 to ECC-256 adds only approximately 35% latency overhead while meeting the 128-bit security margin required by current standards. Future work will integrate post-quantum primitives and ARM TrustZone TEEs for hardware-rooted gateway integrity.

References:

[1] A. Dorri et al., "Blockchain for IoT security and privacy," in Proc. IEEE PERCOM Workshops, 2017, pp. 618–623. https://doi.org/10.1109/PERCOMW.2017.7917634.

[2] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Gener. Comput. Syst., vol. 82, pp. 395–411, 2018.

[3] O. M. Al-Hazaimeh et al., "Cybersecurity foundations," WSEAS Eng. World, vol. 7, pp. 112–119.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008, [Online]. https://bitcoin.org/bitcoin.pdf (Accessed Date: January 10, 2026).

[5] NIST, "Recommendation for Key Management," SP 800-57 Part 1 Rev. 5, 2020.

[6] P. Gope and T. Hwang, "BSN-Care: A secure IoT-based healthcare system," IEEE Sensors J., vol. 16, no. 5, pp. 1368–1376, 2016.

[7] E. Androulaki et al., "Hyperledger Fabric," in Proc. EuroSys, 2018, pp. 1–15. https://doi.org/10.1145/3190508.3190538.

[8] M. Wazid et al., "Design of secure user authenticated key management for IoT," IEEE IoT J., vol. 5, no. 1, pp. 269–282, 2018.

[9] R. Amin et al., "A lightweight authentication protocol for IoT-enabled devices in distributed cloud," Future Gener. Comput. Syst., vol. 78, pp. 1005–1019, 2018.

[10] M. Bawaneh et al., "Enhanced IoT cybersecurity through ML-based penetration testing," Appl. Comput. Sci., vol. 21, no. 2, pp. 96–110, 2025.

[11] O. M. Al-Hazaimeh and A. Ma'moun, "Vehicle-to-vehicle speech encryption," in Proc. ICECCME, 2023, pp. 1–4. https://doi.org/10.1109/ICECCME57830.2023.10252814.

[12] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," ACM Trans. Comput. Syst., vol. 8, no. 1, pp. 18–36, 1990.

[13] AVISPA Team, "AVISPA v1.1 User Manual," 2006, [Online]. http://www.avispa-project.org. (Accessed Date: January 10, 2026).

[14] O. Alphand et al., "IoTChain: A blockchain security architecture for IoT," in Proc. IEEE WCNC, 2018, pp. 1–6. https://doi.org/10.1109/WCNC.2018.8377385.

[15] A. Reyna et al., "On blockchain and its integration with IoT," Future Gener. Comput. Syst., vol. 88, pp. 173–190, 2018.

[16] Y. Zhang et al., "Attribute-based encryption for cloud computing access control: A survey," ACM Comput. Surv., vol. 53, no. 4, pp. 1–41, 2020.

[17] D. Hankerson, A. Menezes, and S. Vanstone, Guide to Elliptic Curve Cryptography. New York: Springer, 2004. ISBN: 978-0-387-95273-4.

[18] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theory, vol. 22, no. 6, pp. 644–654, 1976.

[19] I.S. Al-Qasrawi et al., "A pair-wise key establishment scheme for ad hoc networks," *Int. J. Comput. Netw. Commun.*, vol. 5, no. 2, pp. 125–136, 2013. https://doi.org/10.5121/ijcnc.2013.5210.

[20] O. F. Al-Gharaibeh et al., "Network layer security in smart multi-domain integrated learning environments: Understanding and mitigating attacks," *in Proc. 2026 Int. Conf. Smart Multidomain Integr. Learn. Environ. (ICSMILE),* Mar. 2026, pp. 1–5, [Online]. https://jadara.edu.jo/smile2026/Conference_Program.pdf (Accessed Date: April 10, 2026).

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The current study was developed by the authors, who were equally involved in every step of the process, from the conceptualization of the problem to the final results and resolution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

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

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)

This article is published under the terms of the Creative Commons Attribution License 4.0 https://creativecommons.org/licenses/by/4.0/deed.en_US