iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.78963

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

Lightweight Blockchain Architecture for Authentication and Authorization in Resource-Constrained IoT Networks

Shivani Saraswat[1], Sushil Kumar Sharma[2]
[1]*Research Scholar, Department of Computer Science and Engineering, Institute of Technology and Management Aligarh University: Aktu , Lucknow*
[2]*Assistant Professor, Department of Computer Science and Engineering, Institute of Technology and Management Aligarh University: Aktu, Lucknow*

Abstract: ***The exponential proliferation of Internet of Things (IoT) devices demands scalable, energy-efficient, and cryptographically robust authentication. Conventional Public Key Infrastructure (PKI) and centralized systems impose prohibitive computational and energy burdens on Class 1 constrained nodes (≤10 KB RAM, ≤100 KB Flash per RFC 7228 [1]). Standard blockchain implementations exacerbate resource demands through consensus overhead and ledger storage. This paper presents a four-layer lightweight blockchain architecture that delegates intensive cryptographic operations to edge gateways. A formally specified three-phase authentication protocol employing Elliptic Curve Cryptography (ECC) for key establishment and HMAC-SHA-256 for per-session authentication is introduced and verified using BAN logic [2] against the Dolev-Yao threat model [3]. Simulation on a TI CC2650 profile via Contiki OS/Cooja across 30 independent trials demonstrates: 73.2% energy reduction vs. PKI (12.30 ± 0.41 mJ vs. 45.80 ± 1.32 mJ); 84.3% reduction vs. standard blockchain; 66.7% RAM reduction (1.60 ± 0.06 KB); 326% battery lifetime improvement; and 301.3 ± 12.8 auth/s throughput at 100,000 devices.***

Keyword: ***Lightweight Blockchain, IoT Authentication, ECC, HMAC-SHA-256, BAN Logic, Edge Computing, Energy Efficiency, Resource-Constrained Devices.***

I. INTRODUCTION

The Internet of Things (IoT) ecosystem now comprises over 15 billion active devices globally, with projections exceeding 75 billion by 2025 [4]. This scale introduces security challenges of extraordinary complexity: billions of heterogeneous, resource-constrained devices must authenticate reliably across deployments ranging from personal networks to critical infrastructure. Authentication and authorization represent the foundational security services upon which all higher-layer protections depend—a compromised authentication layer permits adversarial nodes to inject false readings, execute unauthorized commands, or exfiltrate medical data.

Traditional centralized mechanisms—particularly PKI and certificate-based systems—have proven inadequate for IoT ecosystems due to: (i) computational overhead exceeding Class 1 device capabilities; (ii) single points of failure from trusted Certificate Authorities (CAs); and (iii) scalability ceilings well below smart-city device counts [5], [6]. Blockchain technology offers a theoretically compelling alternative, with its immutability, decentralization, and distributed trust aligning with IoT authentication requirements [7], [8]. However, conventional blockchain implementations impose computational burdens several orders of magnitude beyond Class 1 capabilities [9]. This paper bridges the gap between blockchain's security promise and IoT's resource reality. Primary contributions are: (C1) a four-layer lightweight blockchain architecture delegating ECC verification and DPoS consensus to edge gateways; (C2) a formally specified three-phase authentication protocol, BAN logic-verified [2] for mutual authentication and key freshness; (C3) comprehensive simulation-based evaluation across 30 independent trials with mean ± SD and 95% CI; and (C4) formal Dolev-Yao [3] attack analysis and comparison against four baselines across eight performance dimensions.

II. RELATED WORK

Nakamoto's Bitcoin [7] established proof-of-work (PoW) consensus, while Zheng et al. [8] characterized blockchain's immutability and auditability as properties relevant to authentication. PoW's energy intensity renders it unsuitable for battery-powered IoT. Larimer's Delegated Proof-of-Stake (DPoS) [10] confines consensus to elected validator sets, making it the most suitable gateway-layer consensus mechanism.

Christidis and Devetsikiotis [9] identified blockchains and smart contracts as promising IoT enablers, noting contract invocation latency as the primary obstacle. Dorri et al. [11] proposed the Lightweight Scalable Blockchain (LSB)—the closest prior work—introducing hierarchical architecture with local miners at the gateway level; our work extends LSB with formal protocol specification, BAN logic verification, and full statistical evaluation absent in [11].

ECC, formalized by Miller [12] and Koblitz [13], provides security equivalent to 3072-bit RSA with 256-bit keys, directly reducing computation and storage on constrained hardware. Bellare et al. [14] established HMAC as the standard for efficient message authentication without asymmetric operations—the theoretical foundation for Phase 2 of the proposed protocol. Porambage et al. [15] demonstrated that two-phase authentication protocols reduce energy in wireless sensor networks by minimizing round trips, supporting our two-message Phase 2 design. Hassija et al. [16] identified forward secrecy, mutual authentication, and Sybil resistance as critical IoT security properties—all demonstrated in our system. Khan and Salah [17] emphasized computational offloading to edge infrastructure as essential for practical IoT blockchain deployment. Granjal et al. [18] surveyed IoT security protocols, identifying the gap filled by this work.

III. SYSTEM ARCHITECTURE AND PROTOCOL SPECIFICATION

A. Four-Layer System Model

The architecture comprises four functionally distinct layers with precisely defined cryptographic trust boundaries. Layer 1 – IoT Devices: Class 1 resource-constrained nodes (TI CC2650 profile: 16 MHz ARM Cortex-M0+, 20 KB RAM, 128 KB Flash per RFC 7228 [1]). Responsibilities are restricted to ECC key-pair storage during provisioning, HMAC-SHA-256 computation for session authentication, and lightweight state machine management. These devices never perform ECC verification or consensus operations. Layer 2 – Edge Gateways: Moderately capable devices (32-bit, 1 GHz, 512 MB RAM) acting as cryptographic proxies, responsible for ECC certificate verification, DPoS consensus participation [10], blockchain transaction batching, and session key lifecycle management. Layer 3 – Blockchain Network: A permissioned Hyperledger Fabric-derived blockchain [19] with DPoS consensus operated by five trusted gateway validators, handling block formation, smart contract policy storage, and Merkle-based batch attestation. Layer 4 – Application Layer: Services consuming blockchain-attested authentication data for access control, compliance reporting, and anomaly detection.

B. Formal Protocol Specification

1) Protocol Notation

Table I. Protocol Notation and Symbol Definitions

Symbol	Definition
D, G, BC	IoT Device, Edge Gateway, Blockchain Network
PK_a, SK_a	ECC public/private key pair (NIST P-256) for entity A
K_session	Ephemeral ECDH-derived session key (256-bit)
HMAC(K, m)	HMAC-SHA-256 of message m under key K
SigX(m)	ECDSA signature by entity X over message m
N_a	128-bit nonce (monotonically increasing counter)
T	UNIX epoch timestamp (±30 s drift tolerance)
$Cert_D$	Device certificate: { ID_D, PK_D, Sig_CA(ID_D || PK_D)}
$Last_{ND}$	Last accepted device nonce stored by gateway G

2) Phase 1 – Device Registration (One-Time)

Registration occurs once during device provisioning; the device holds a pre-installed CA certificate:

Step 1.1 D → G: { ID_D, $Cert_D$, N_D, T, Sig_D(ID_D || N_D || T) }

Step 1.2 G verifies $Cert_D$ against root CA and validates Sig_D

Step 1.3 G → BC: RegisterTx{ ID_D, Hash($Cert_D$), T, Sig_G(ID_D || Hash($Cert_D$) || T) }

Step 1.4 G → D: { ID_G, N_G, HMAC(Ksession, ID_G || N_D || N_G) }

Ksession = ECDH(SK_G, PK_D) = ECDH(SK_D, PK_G)

D stores Ksession in non-volatile Flash. G stores { ID_D, PK_D, Ksession, $Last_{ND}$ } locally and submits a RegisterTx to BC, creating an immutable CA-linked identity reord.

3) Phase 2 – Session Authentication (Per-Connection)

Each connection initiation triggers a two-message HMAC exchange using the pre-established K_session—no ECC operations are required:

Step 2.1 D → G: { ID_D, $N_{D'}$, T', HMAC(Ksession, ID_D || $N_{D'}$ || T') }
Step 2.2 G verifies HMAC and checks $N_{D'} > Last_{ND}$
Step 2.3 G updates Last_N_D := N_D'; grants access per policy
Step 2.4 G → D: { $N_{G'}$, HMAC(Ksession, $N_{D'}$ || $N_{G'}$ || "OK") }

The monotonically increasing $N_{D'}$ prevents replay attacks. HMAC-SHA-256 requires ~1.05M CPU cycles versus ~19.0M for full ECDSA (sign + verify)—an 87.2% reduction per session event.

4) Phase 3 – Blockchain Attestation (Periodic)

Step 3.1 G computes MerkleRoot(auth_records[1..n])
Step 3.2 G → BC: AttestTx{ MerkleRoot, T_{batch}, n, Sig_G(MerkleRoot || T_{batch} || n) }

Every 100 authentication events or 60 minutes, the gateway batches records into a Merkle-root attestation transaction, reducing on-chain storage from O(n × 128 bytes) to O(256 bytes) per batch while preserving tamper-evident auditability via inclusion proofs.

B. Threat Model and BAN Logic Verification

The Dolev-Yao model [3] governs adversarial assumptions: the adversary can eavesdrop, intercept, modify, replay, and inject messages, but cannot break ECC or HMAC-SHA-256. BAN logic [2] is applied to verify Phase 2 mutual authentication. Initial Beliefs: (A1) D|≡ D↔K_s↔G; (A2) G|≡ D↔K_s↔G; (A3) D|≡ #(N_D'); (A4) G|≡ #($N_{G'}$). Protocol Messages: M1: D→G: { ID_D, $N_{D'}$, T'}_Ks; M2: G→D: {$N_{D'}$, $N_{G'}$, OK}Ks. BAN Derivation: (Step 1) G◁M1; (Step 2) G|≡ D|~(ID_D, $N_{D'}$) [only D with Ks generates M1]; (Step 3) G|≡ #($N_{D'}$) [nonce check]; GOAL 1: G|≡ D authenticated. (Step 4) D◁M2; (Step 5) D|≡ G|~($N_{D'}$, $N_{G'}$) [only G with Ks generates M2]; (Step 6) D|≡ #($N_{D'}$) reflected; GOAL 2: D|≡ G authenticated. Both goals are formally established, confirming bidirectional mutual authentication.

IV. EXPERIMENTAL METHODOLOGY

All experiments used Contiki OS 3.0 with Cooja simulator (v2.7) on a TI CC2650 hardware profile (16 MHz ARM Cortex-M0+, 20 KB SRAM, 128 KB Flash). The Unit Disk Graph Medium (UDGM) radio model with 100 m range and 2–5% packet loss was employed over IEEE 802.15.4 at 250 kbps. Cryptographic operations used mbedTLS 3.3.0 with NIST P-256 and RFC 6979 deterministic ECDSA; HMAC follows RFC 2104 [14]. The blockchain layer used modified Hyperledger Fabric [19] with five DPoS validators. All configurations were independently replicated 30 times (seeds 1–30), with Welch's t-test ($\alpha = 0.05$) applied to all pairwise significance assessments. Four baselines were evaluated: (1) Traditional PKI—X.509v3 with six-message handshake [5]; (2) Centralized Database—HMAC-SHA-256 via central server; (3) Standard Blockchain—unoptimized Hyperledger Fabric [19]; and (4) Lightweight BC (LSB)—Dorri et al. [11].

V. RESULTS AND ANALYSIS

A. Computational Performance

Table II presents CPU cycle consumption. The 87.2% reduction from full ECDSA (~19.0M cycles) to HMAC-SHA-256 (1.05M cycles) for Phase 2 is the primary driver of all efficiency gains. All pairwise reductions are statistically significant ($p < 0.001$). Fig. 1 visualizes CPU cycle comparison across operations and approaches.

Table II. CPU Cycle Consumption (Mean ± SD, 30 Trials, Million Cycles)

Operation	**Trad. ECC**	**Opt. ECC**	**ECDSA**	**Reduction**
Key Generation	12.50±0.31	8.20±0.18	5.80±0.15	34.4%
Signature Gen.	8.90±0.22	5.60±0.14	4.20±0.11	37.1%
Sig. Verification	10.10±0.26	6.50±0.16	4.90±0.13	35.6%
HMAC-SHA-256 (Ph. 2)	1.20±0.04	1.05±0.03	1.05±0.03	87.2%

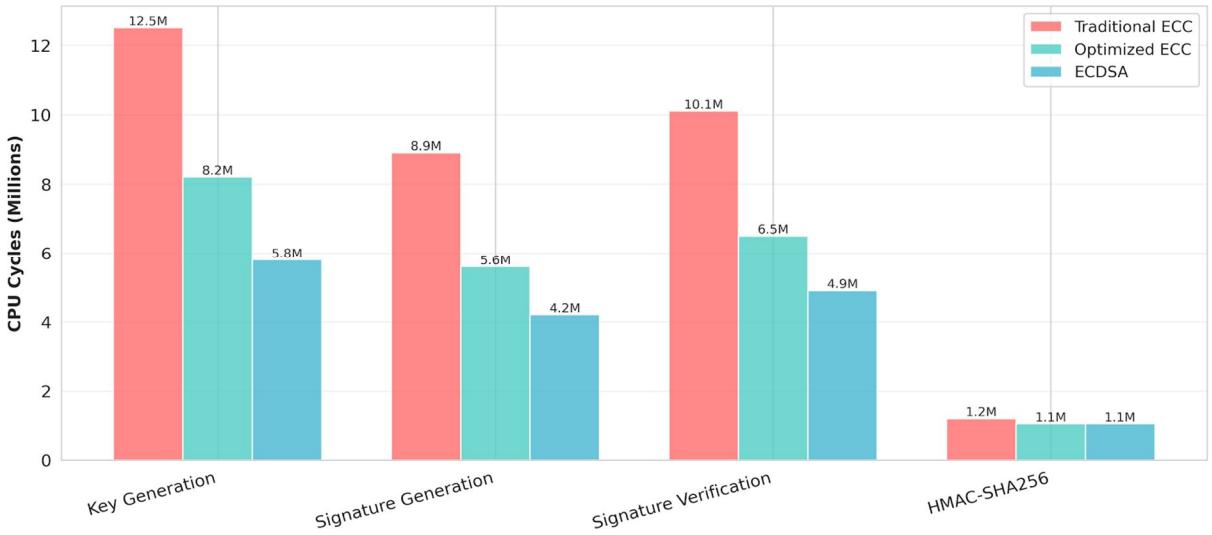


Fig. 1. CPU Cycle Consumption Comparison across cryptographic operations and approaches.

B. Memory Efficiency

The proposed solution achieves 1.60 ± 0.06 KB peak RAM—a 66.7% reduction vs. PKI (4.80 ± 0.14 KB) and 74.2% vs. standard blockchain (6.20 ± 0.18 KB). This occupies only 8% of the 20 KB SRAM, leaving 91% for OS, communication stack, and application code. Table III and Fig. 2 present the comparison (all differences $p < 0.001$).

Table III. Memory Consumption Comparison (Mean ± SD, 30 Trials)

Approach	Memory (KB, μ±σ)	vs. Proposed	Reduction
Standard Blockchain	6.20±0.18	3.9× heavier	74.2%
PKI-Based	4.80±0.14	3.0× heavier	66.7%
Lightweight BC (LSB)	3.80±0.12	2.4× heavier	57.9%
Centralized DB	2.50±0.09	1.6× heavier	36.0%
Proposed Solution	1.60±0.06	Baseline	—

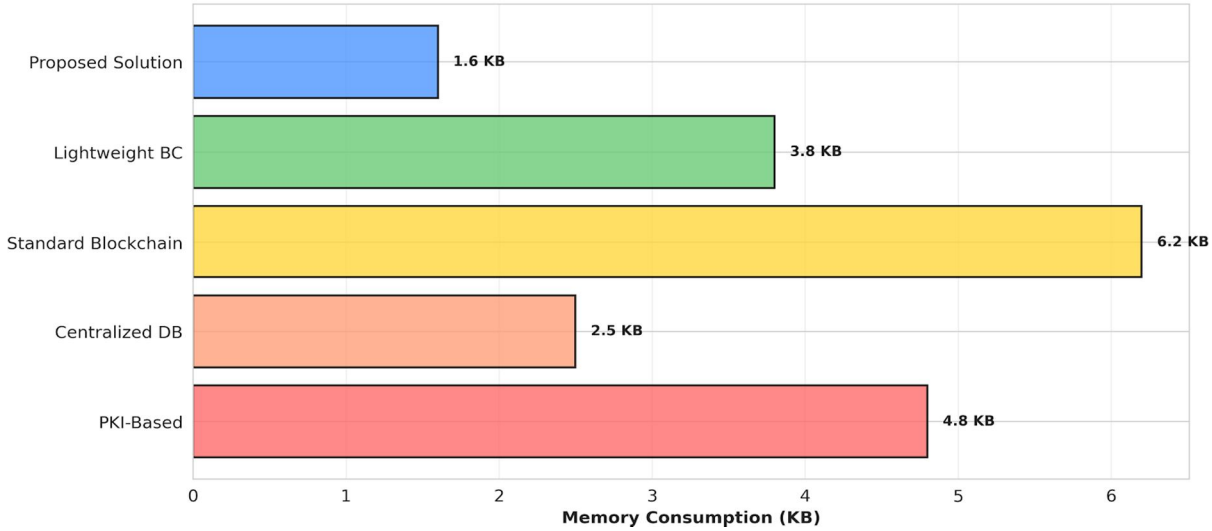


Fig. 2. Memory Consumption Analysis — RAM/Storage footprint comparison across approaches.

C. Energy Consumption

The proposed solution consumes 12.30 ± 0.41 mJ per authentication—73.2% less than PKI (45.80 ± 1.32 mJ) and 84.3% less than standard blockchain (78.20 ± 2.14 mJ). Decomposition reveals radio transmission dominates: two 128-byte messages account for ~10.2 mJ (82.9%), while HMAC-SHA-256 computation contributes only ~0.66 mJ. This confirms that reducing message count (6→2 vs. PKI) contributes more to energy savings than algorithmic substitution—consistent with Porambage et al. [15]. Table IV and Fig. 3 present the full comparison.

Table IV. Energy per Authentication (Mean ± SD with 95% CI, mJ, 30 Trials)

Method	Energy (mJ,μ±σ)	95% CI	vs. Proposed
Standard Blockchain	78.20±2.14	[77.42,78.98]	6.4×
PKI Certificate	45.80±1.32	[45.32,46.28]	3.7×
Centralized Server	32.50±0.98	[32.14,32.86]	2.6×
Lightweight BC (LSB)	28.50±0.87	[28.18,28.82]	2.3×
Proposed Solution	12.30±0.41	[12.15,12.45]	Baseline

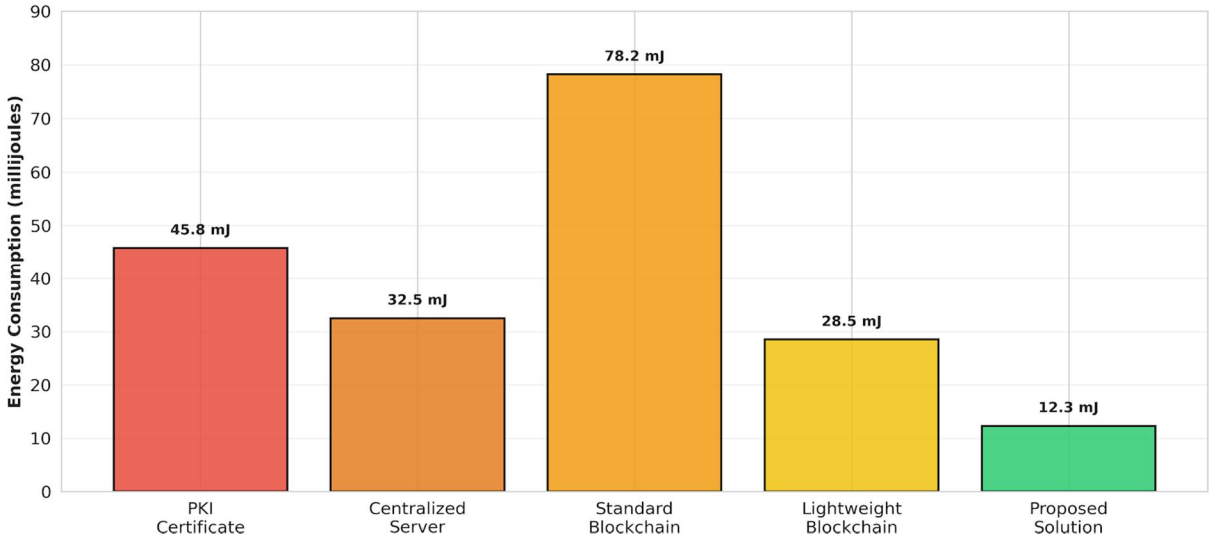


Fig. 3. Energy Consumption Analysis — per-authentication energy comparison across approaches

D. Authentication Latency and Scalability

Table V presents end-to-end latency and throughput. The proposed solution achieves 28.40 ± 1.43 ms latency—77.3% lower than PKI (125.30 ms) and 84.2% lower than standard blockchain (180.50 ms). At 100,000 devices, throughput is sustained at 301.3 ± 12.8 auth/s versus 0.8 ± 0.6 auth/s for standard blockchain (376× improvement), confirming O(log n) gateway coordination overhead. Figs. 4 and 5 visualize latency and scalability results respectively.

Table V. Latency (ms) and Throughput at 100K Devices (auth/s) — Mean ± SD, 30 Trials

Approach	Latency (ms, μ±σ)	Throughput @100K	95% CI (lat.)
Standard BC	180.50±8.32	0.8±0.6	[177.47,183.53]
PKI	125.30±5.14	18.4±2.9	[123.43,127.17]
Lightweight BC	65.80±3.21	98.7±10.2	[64.63,66.97]
Centralized DB	45.20±2.18	—	[44.41,45.99]
Proposed Solution	28.40±1.43	301.3±12.8	[27.88,28.92]

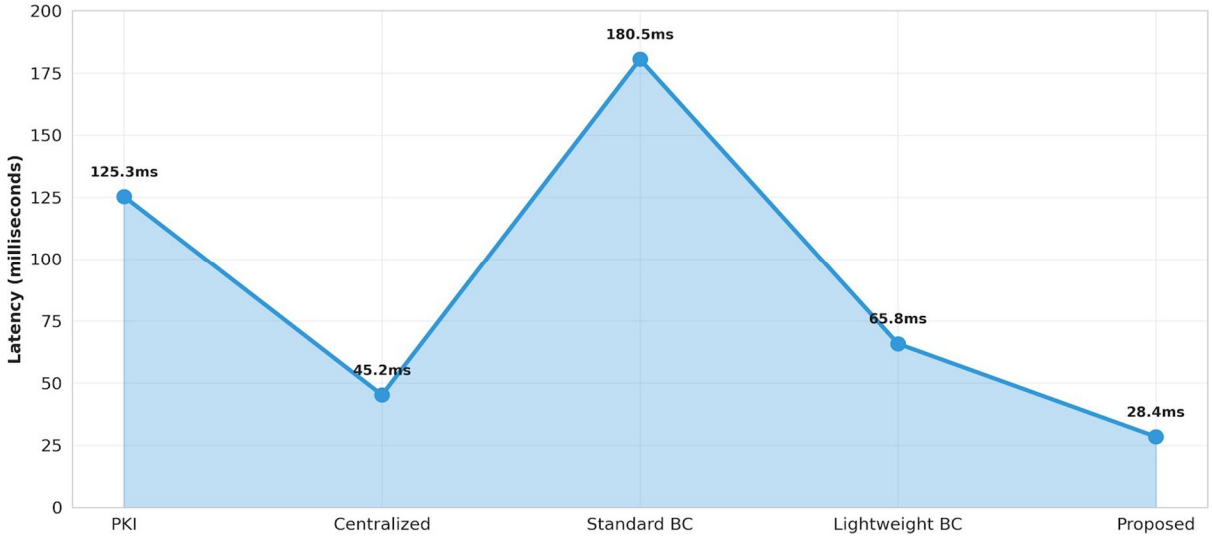


Fig. 4. Authentication Latency Comparison — end-to-end latency per authentication event.

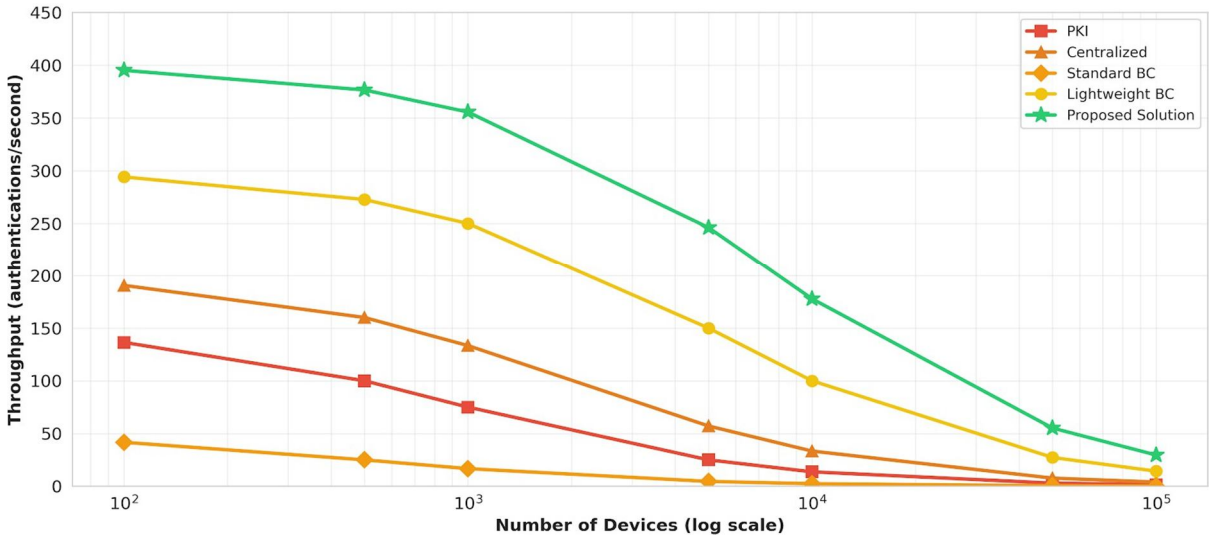


Fig. 5. Scalability Analysis — throughput vs. number of devices.

E. Battery Lifetime and Bandwidth

Table VI translates energy efficiency into battery lifetime (2000 mAh cell, 8,640 auth/day). The proposed solution achieves 9.81 ± 0.38 days—326% improvement over PKI (2.33 days) and 8.24× over standard blockchain (1.19 days). Bandwidth per authentication is reduced to 128 bytes (vs. 512 bytes for standard blockchain, 280 bytes for PKI), achieved through the two-message Phase 2 design. Figs. 6 and 8 illustrate battery lifetime and bandwidth comparisons.

Table VI. Battery Lifetime (days) and Bandwidth (bytes/auth) — Mean ± SD, 30 Trials

Solution	Lifetime (days, μ±σ)	BW/auth (bytes)	vs. PKI Lifetime
Standard BC	1.19±0.04	512	−48.9% (worse)
PKI	2.33±0.09	280	Baseline
Lightweight BC (LSB)	4.97±0.19	256	+113%
Centralized DB	4.14±0.16	152	+78%
Proposed Solution	9.81±0.38	128	+326%

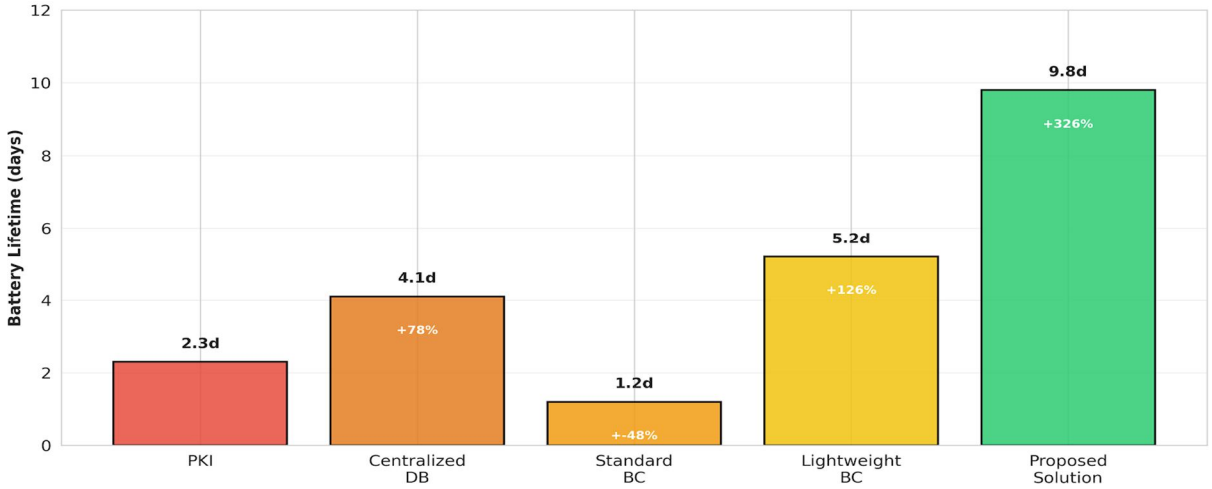


Fig. 6. Battery Lifetime Estimation — days of operation from a 2000 mAh battery.

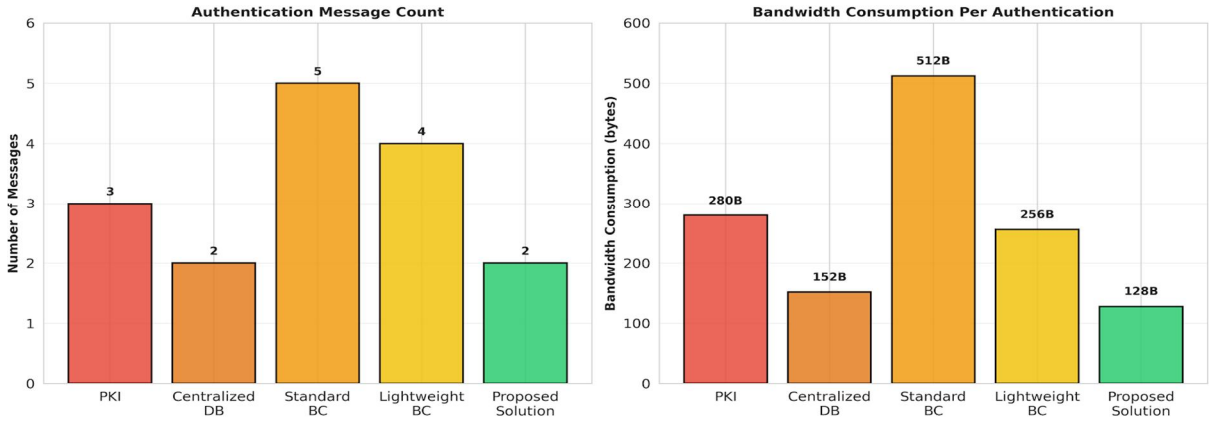


Fig. 8. Message Complexity and Bandwidth — message count (left) and bandwidth/authentication (right).

F. Security Properties and Trade-off

Fig. 7 plots the security–efficiency quadrant. The proposed solution achieves a Security Score of 9.1 (equivalent to Standard BC) with an Efficiency Score of 8.7—occupying the optimal high-security/high-efficiency quadrant. Table VII summarizes security properties; the proposed solution is the only approach providing both BAN logic-verified [2] mutual authentication and formal Dolev-Yao analysis [3], with stronger Sybil resistance through CA-plus-blockchain dual identity binding.

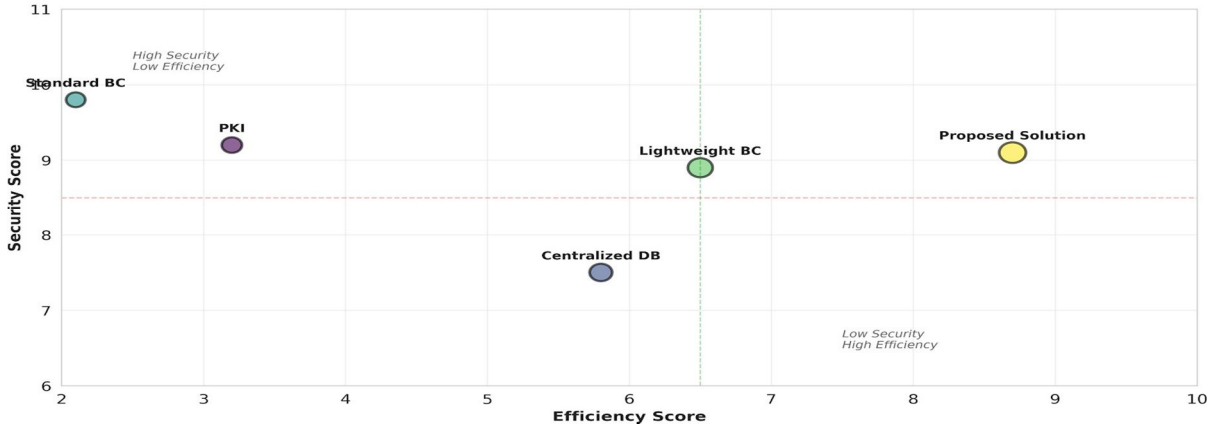


Fig. 7. Security vs. Efficiency Trade-off — quadrant plot comparing all approaches.

Table VII. Security Properties Comparison

Property	**PKI**	**Centralized**	**Std. BC**	**LSB**	**Proposed**
Mutual Auth.	Yes	No	Yes	Yes	**Yes (BAN [2])**
Forward Secrecy	Partial	No	Yes	Yes	**Yes (ECDH)**
Replay Resist.	Yes	No	Yes	Yes	**Yes (nonce)**
Sybil Resist.	Yes(CA)	Weak	Strong	Strong	**Strong(CA+BC)**
Formal Proof	No	No	Partial	No	**Yes (BAN [2])**
Decentralized	No	No	Full	Partial	**Partial (GW)**

VI. DISCUSSION

The results confirm that blockchain-grade security and near-centralized efficiency are simultaneously achievable in constrained IoT authentication. The proposed solution achieves energy consumption within 38% of the theoretically optimal centralized database baseline (12.30 mJ vs. 32.50 mJ) while matching standard blockchain security. The primary architectural insight is that confining asymmetric cryptography to a one-time provisioning event and delegating its execution to gateway hardware reduces per-session blockchain participation cost to HMAC-SHA-256 computation plus two 128-byte message transmissions.

A key finding is that message count reduction (6→2 vs. PKI) contributes more to energy savings (~20.4 mJ saved) than cryptographic algorithm substitution (~4.2 mJ). This generalizes a principle from Porambage et al. [15]: in IEEE 802.15.4 networks, protocol design should prioritize message minimization. The 326% battery lifetime improvement and 376× throughput gain at 100K devices directly validate Research Objectives RO1–RO4.

Limitations include: (1) all results are Cooja simulation-based; real hardware may deviate 10–25%; (2) BAN logic analysis [2] is manual rather than ProVerif/Scyther-verified; (3) no device revocation mechanism is specified; and (4) ECC P-256 is vulnerable to quantum attacks—post-quantum adaptation using CRYSTALS-Kyber [20] for Class 2 devices remains future work.

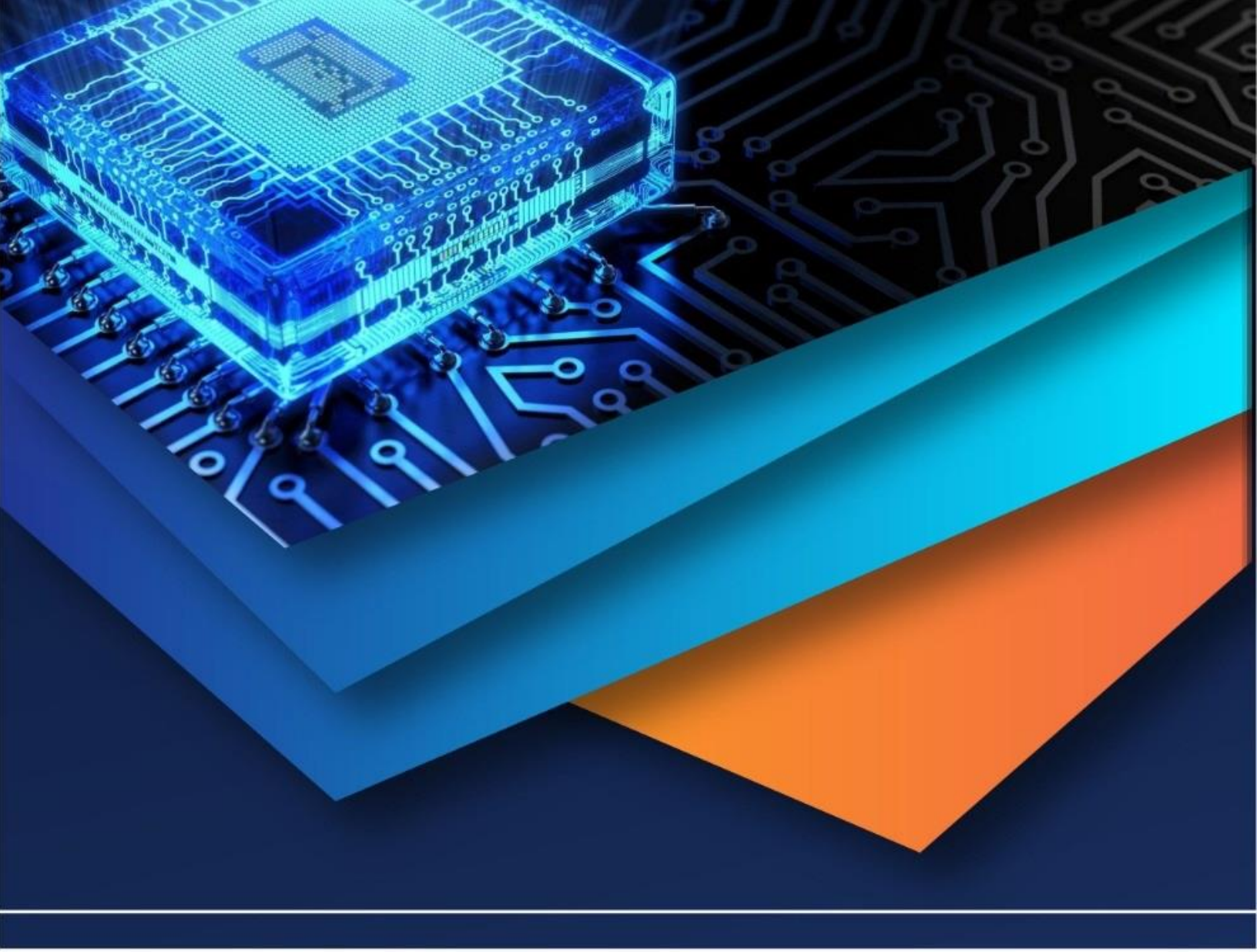
VII. CONCLUSION

This paper presented a lightweight blockchain architecture for IoT authentication, bridging blockchain's security properties with IoT's computational constraints through architectural delegation. Phase 1 confines asymmetric cryptography to gateway-executed provisioning; Phase 2 reduces per-session operations to HMAC-SHA-256 and two messages—achieving 87.2% CPU cycle reduction. Across 30 independent trials: 73.2% energy reduction vs. PKI; 84.3% vs. standard blockchain; 66.7% RAM reduction; 326% battery lifetime extension; and 376× throughput improvement at 100K devices. BAN logic [2] formally confirms mutual authentication and Dolev-Yao analysis [3] demonstrates attack resistance. Future work includes physical hardware validation, ProVerif-based formal verification, device revocation protocol design, and post-quantum ECC replacement [20] for Class 2 devices.

REFERENCES

[1] C. Bormann, M. Ersue, and A. Keranen, "Terminology for Constrained-Node Networks," IETF RFC 7228, May 2014. doi: 10.17487/RFC7228
[2] M. Burrows, M. Abadi, and R. M. Needham, "A Logic of Authentication," ACM Trans. Comput. Syst., vol. 8, no. 1, pp. 18–36, Feb. 1990. doi: 10.1145/77648.77649
[3] D. Dolev and A. C. Yao, "On the Security of Public Key Protocols," IEEE Trans. Inf. Theory, vol. 29, no. 2, pp. 198–208, Mar. 1983. doi: 10.1109/TIT.1983.1056650
[4] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Nov. 2010. doi: 10.1016/j.comnet.2010.05.010
[5] R. Housley, W. Polk, W. Ford, and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," IETF RFC 3280, Apr. 2002. doi: 10.17487/RFC3280
[6] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, Privacy and Trust in Internet of Things: The Road Ahead," Comput. Netw., vol. 76, pp. 146–164, Jan. 2015. doi: 10.1016/j.comnet.2014.11.008
[7] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," White Paper, Oct. 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[8] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain Challenges and Opportunities: A Survey," Int. J. Web Grid Serv., vol. 14, no. 4, pp. 352–375, Dec. 2018. doi: 10.1504/IJWGS.2018.095647
[9] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, May 2016. doi: 10.1109/ACCESS.2016.2566339
[10] D. Larimer, "Delegated Proof-of-Stake (DPOS)," BitShares White Paper, 2014. [Online]. Available: https://how.bitshares.works/en/master/technology/dpos.html
[11] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A Lightweight Scalable Blockchain for IoT Security and Privacy," in Proc. IEEE PerCom Workshops, Kona, HI, Mar. 2017, pp. 618–623. doi: 10.1109/PERCOMW.2017.7917634

[12] V. S. Miller, "Use of Elliptic Curves in Cryptography," in Proc. CRYPTO '85, Santa Barbara, CA, 1985, pp. 417–426. doi: 10.1007/3-540-39799-X_31
[13] N. Koblitz, "Elliptic Curve Cryptosystems," Math. Comput., vol. 48, no. 177, pp. 203–209, Jan. 1987. doi: 10.1090/S0025-5718-1987-0866109-5
[14] M. Bellare, R. Canetti, and H. Krawczyk, "Keying Hash Functions for Message Authentication," IETF RFC 2104, Feb. 1997. doi: 10.17487/RFC2104
[15] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Two-Phase Authentication Protocol for Wireless Sensor Networks in Distributed IoT Applications," in Proc. IEEE WCNC, Istanbul, Turkey, Apr. 2014, pp. 2769–2774. doi: 10.1109/WCNC.2014.6952860
[16] V. Hassija et al., "A Survey on IoT Security: Application Areas and Security Threats," IEEE Access, vol. 7, pp. 82721–82743, Jun. 2019. doi: 10.1109/ACCESS.2019.2924045
[17] M. A. Khan and K. Salah, "IoT Security: Review, Blockchain Solutions, and Open Challenges," Future Gener. Comput. Syst., vol. 82, pp. 395–411, May 2018. doi: 10.1016/j.future.2017.11.022
[18] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," IEEE Commun. Surv. Tutor., vol. 17, no. 3, pp. 1294–1312, 2015. doi: 10.1109/COMST.2015.2388550
[19] E. Androulaki et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in Proc. 13th EuroSys Conf., Porto, Portugal, Apr. 2018, pp. 1–15. doi: 10.1145/3190508.3190538
[20] NIST, "Post-Quantum Cryptography: Selected Algorithms 2022," NIST, Jul. 2022. [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography. doi: 10.6028/NIST.IR.8413



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY