Journal of Wireless Sensor Networks and IoT, ISSN: 3048-8729 Vol. 3, No. 2, 2026 (pp. 19-28)
RESEARCH ARTICLE ECEJOURNALS.IN

Secure Lightweight Authentication Framework for Resource-Constrained IoT Nodes Using Blockchain-Assisted Key Management

M. Mejail[1*], B.K. Nestares[2], L. Gravano[3], E. Tacconi[4], G.R. Meira[5], A. Desages[6]

[1-6]Centro de Investigacion y Desarrollo de Tecnologias Aeronauticas (CITeA) Fuerza Aerea Argentina Las Higueras, Cordoba, Argentina

KEYWORDS:

Lightweight authentication, Blockchain-assisted key management, Internet of Things security, Elliptic curve cryptography, Energy-efficient protocol design, Resource-constrained embedded devices.

Author's Email:
Mejail.mej@ing.unrc.edu.ar

DOI: 10.31838/WSNIOT/03.02.03

Received : 15.12.2025
Revised : 09.01.2026
Accepted : 06.02.2026

Abstract

Smart environments have increased the difficulties in authentication and key management by the rapid proliferation of resource constrained or Internet of Things (IoT) nodes. Traditional on-demand centralised public key infrastructures have single points of failure and can scale only to a very small size, whereas fully on-chain blockchain-based proposals present high computational overhead to cost-effective devices and high communication overhead to allow both. This article describes an authenticated lightweight protection structure based on elliptic curve cryptography (ECC) and key anchoring with the aid of block chain to implement the decentralised trust with a minimum overhead. The hybrid architecture proposed has the public key hash stored on a distributed ledger, and mutual authentication on off-chain and determination of session keys up towards efficient ECC-based challenge-response mechanisms. Formal system and threat model are created and an analytic energy consumption model is obtained to compute the cost of computations and transmission within realistic IoT limitations. Analysis of performance indicates that the framework uses less authentication energy and communication overhead than to corresponding blockchain-integrated methods that represent systems and guarantees forward secrecy and replay resistance, impersonation, and man-in-the-middle attacks. The scheme provides scalable, constant-time authentication, and can therefore be used in large-scale applications of resource-constrained IoT networks.

How to cite this article: Mejail M, Nestares BK, Gravano L, Tacconi E, Meira GR, Desages A (2026). Secure Lightweight Authentication Framework for Resource-Constrained IoT Nodes Using Blockchain-Assisted Key Management. Journal of Wireless Sensor Networks and IoT, Vol. 3, No. 2, 2026, 19-28

Introduction

The quick evolution of the Internet of Things (IoT) has changed the current digital infrastructure by connecting billions of heterogeneous devices in the smart cities, industrial automation, healthcare, and critical infrastructure. With the increase in connectivity, attack surface increases. Massive scale distributed endpoints functioning in unprotected conditions enhance vulnerability to impersonation, replay, man in the middle, and key compromise assaults. Authentication and key management thus become mandatory security requirements as opposed to the optional enhancements.[9] Nevertheless, traditional security-related architectures were not initially created with such large scale and variety that modern IoT environments represent. Another attribute of most IoT deployments is the availability of resource-constrained nodes which are powered by low-power microcontrollers, have limited memory, and have small battery capacity. Without sacrificing the operating

duration by a large margin, such devices will not be able to render heavyweight cryptographic functions, complex chain of certificates or even a frequent communication exchange. Authentication mechanisms should ensure that the cost of cryptography and message support is minimised because transmission energy may be a dominant factor in the computational cost of low-power radios. It is always a significant challenge to design security measures that are resistant and still comply with the stringent energy and memory constraints. Conventional public key infrastructure (PKI) frameworks are centralised so that certificate authorities issue, validate and revoke credentials. At the time of successful implementation in traditional networks, centralised PKI causes single points of failures and bottlenecks on scalability of distributed IoT scenarios.[9] Any presumption of compromise of a central authority can destroy trust in the system and certificate validation can present nontrivial storage and communication overheads to the limited node. This is further undermined by dynamic IoT networks that have intermittent connectivity that also makes it difficult to revoke and verify certificates in real-time, which makes centralised trust assumptions. The blockchain technology has arisen as a decentralised trust model that is able to offer an anchoring of identity that is tamper resistant and key management that is transparent.[2-6],[9, 10] With the help of distributed consensus, blockchain has the capability of removing the existence of a single authority and improving the resistance to key manipulation attacks. Nonetheless, integration of IoT nodes directly into blockchain networks is not feasible because it creates the consent overhead, storage expansions, and big communication expenses.[1, 3, 7] Full on-chain authentication models are also incompatible with the characteristics of lightweight design needed by low-power embedded systems.[4, 8] Though extensive research has been done in the field of lightweight authentication and blockchain-based Internet of Things security,[1-12] the gap in creating hybrid solutions between decentralisation and high resource efficiency has been observed. The available solutions embrace blockchain avoidance because they focus on preserving energy, or embrace blockchain-intensive designs that disregard the constraints of the devices.[8, 10, 11] An energy-conscious authentication design that can be scaled with blockchain used only to bind keys but do not verify lightweight off the chain is not adequately studied.[7, 12] To fill this gap, this paper presents a secure lightweight authentication system that combines elliptic curve encryption with key management that is supported with blockchain. The architecture proposed bases public key hash on a distributed registry and conducts mutual authentication, and session key derivation using computationally limited ECC based challenge response operations. System and threat model is developed in a formal manner and analytical energy model is derived and used in order to capture the measurement of computational overhead as well as that of transmission overhead. The framework is assessed in comparison with the representative methods to show enhanced energy usage, lower communication cost, and high replay, impersonation, and man-in-the-middle attack resistance, as well as scalable decentralised trust.

Related Work

Three main categories of research have offered a variety of approaches to guaranteeing security in resource-constrained IoT settings, namely lightweight authentication protocol design, blockchain-based security designs, and sizeable key management frameworks.[1-12] Both directions deal with particular limitations of the conventional security systems, but no one balances the decentralisation with the rigid energy and computational resources. Authentications with light weights are usually developed to reduce cryptograph and communication overburden. The dominance on this category is made up of hash-based schemes, symmetric-key constructions, and the challenge-response mechanism based on elliptic curve cryptography (ECC). These protocols are effective in streamlining the efficiency at the device level but they seldom touch upon decentralised establishment of trust. IoT security built on blockchains has come to remove single points of failure in centralised certificate authorities.[2-6], [9, 10] Distributed registries also allow anchoring identity irrevocably, verifying decentrally, and evocative transparently. Some of the studies suggest keeping device credentials, certificates or authentication logs on-chain directly. [4, 8, 11] Despite having superior tamper resistance in such designs, they also add a huge communication overhead, storage expansion, and consent latency.[1, 3, 7] The use of constrained nodes in the consensus process of a blockchain is not usually practical because they have limited memory, processing power, and energy provisions.[8, 10] As a result, with a large number of blockchain-based solutions, the calculations and processing become the responsibility of either a

layer of gateways or clouds, and, in part, they become dependent again.[5, 7] The most important management architectures of IoT include centralised PKI systems, distributed trust models, and hybrid edge assisted structures.[6, 10, 12] The centralised PKI is still prevalent because it is mature and interoperable but has scalability point of vulnerability and can be compromised by authority issues.[9] Distributed methods are aimed at getting rid of central control, but at the cost of severe synchronisation overload and validation overload. Hybrid architectures also deploy edge gateways to support authentication and key validation to enhance its capability to scale, keeping some decentralisation.[7, 12] Nevertheless, most of these systems use constant connectivity to centralised power and/or implement blockchain in a form that adds extra complexity to the protocols that can be implemented by constrained nodes at best.[1, 8] A brief overview of representative techniques in terms of approaches is given in Table 1. Existing solutions are found to emphasise on either lightweight performance and lack in the decentralisation, or the decentralised trust, and not pay enough attention to the resource limitations identified during the analysis. Not many frameworks can support forward secrecy and off-chain efficiency and only interact with blockchain by means of lightweight identity anchoring. Such an imbalance shows that there is an evident gap in research when it comes to developing authentication schemes that include blockchain-enhanced key validation without asking the IoT nodes to bear the on-chain computational or communication overhead.

The comparative analysis proves that a hybrid system based on anchoring the value of the public key hashes on-chain and performing the authentication process off-chain is able to maintain the effects of decentralisation and not violate the principles of lightweight design.

Methodology

This part gives the technical basis of the proposed framework through a combination of system model, threat assumptions, protocol design, formal validation of security and analytical energy modelling. The goal here is to create authentication architecture with decentralised trust systems by using blockchains to help in anchoring keys and maintaining high resource efficiency at limited nodes in the IoT.

System Architecture

The proposed structure is structured into four logical layers, which comprise the IoT device layer, the edge gateway layer, the blockchain validator network and the distributed ledger anchor. The design results in isolated computationally intensive blockchain functionality on resource-constrained nodes, and lightweight executing device-side. At the bottom-most stage, several IoT nodes have a processing power and memory as well as stored energy that is not large. Every node is used to do elliptic curve key generation, hash calculation and local secure storage of private credentials. IoT nodes can start authentication by sending an authentication request with identity information, nonce and public key to the edge gateway. The edge gateway acts as the authentication

Table 1: Structural Comparison of Representative Lightweight IoT Authentication Approaches

Approach Category	Centralized Authority	Blockchain Usage	Cryptographic Basis	On-Chain Device Participation	Forward Secrecy	Suitability for Constrained Nodes
Traditional PKI-Based Authentication	Yes	No	RSA / ECC	No	Partial	Moderate
Hash-Based Lightweight Protocols	Yes	No	Hash / Symmetric	No	No	High
Fully On-Chain Blockchain Identity	No	Extensive	ECC / Smart Contracts	Yes	Yes	Low
Edge-Assisted Hybrid Models	Partial	Limited	ECC / Hash	Indirect	Yes	Moderate
Proposed Hybrid Anchored Framework	Hybrid	Hash Anchoring Only	ECC + Hash	No		

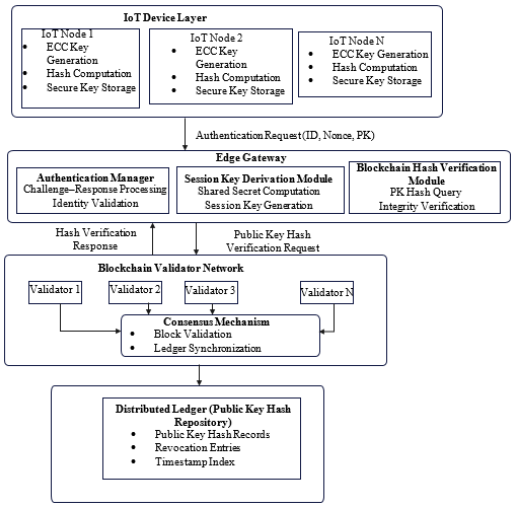

Fig.1: Proposed System Architecture for Off-Chain Lightweight Authentication with Blockchain-Assisted Public Key Hash Anchoring.

coordinator, as well as, off-chain execution point. It implements challenge response validation, computes session keys by using the elliptic curve sharing secret calculation, and consults the blockchain network to cheque the integrity of the hashes of the stored public keys. This means that the architecture provides a balanced scalability and efficiency by decentralizing trust using ledger anchoring, and through centralizing verification logic at the edge. The blockchain validator layer ensures there exists consensus regarding the records on the hash of public keys. Identity anchoring is achieved with the help of validators verifying key registration and revocation events. Notably, IoT nodes are not involved in consensus mechanisms, thus they are free of high computational and communication loads. The distributed ledger anchor contains unique records of public key hash immutable records, revocation records, and timestamp records. Authentication is off-chain, whereas blockchain interaction consists of lightweight hash cheques.

As shown in Figure 1, the proposed system architecture has provided three layers where the interaction flow is hierarchical: the IoT nodes to the edge gateway to distributed hash anchoring using the blockchain validator network. The figure considers the distinction of off-chain authentication execution and on-chain identity validation, which is the key to lightweight operation.

Threat Model

The framework that has been proposed is tested within a realistic adversarial model that is in accordance with distributed IoT systems, which work on top of unsecured wireless networks. The attacker is another party that is believed to have considerable network-level capability without being computationally limited by the standard cryptographic hardness theories. Passive eavesdropping can be carried out by an adversary by eaves dropping all communications between all the IoT nodes and the edge gateway. The fact that wireless transmissions are broadcast by their nature presumes that the attacker can make authentication requests, nonce exchanges, and public key transmissions and record them without detection. The attacker can also make replay attacks by resending authentications messages that he/she has captured before so as to gain unauthorised access or interfere with the establishment of a session. Besides passive attacks, the enemy will be able to cause active man-in-the-middle (MITM) attacks by altering, injecting or even weighting messages as they are being authenticated. The attacker could also seek fraudulent establishment of session by falsifying identity parameters or even attempting to replace public keys. Additionally, the attacks of node capture are also discussed, where an already compromised IoT device can disclose the locally stored credentials, but not hardware-ensured private keys in case of the existence of secure storage solutions. Framework security depends on the computational hardness of elliptic curve discrete logarithm problem (ECDLP) that derives private keys using the public parameters. It is also assumed that the blockchain validator network is majority-honest where the majority of the network participate and will abide by the provisioned consensus protocol and do not join forces to spoil ledger records. Within these premises, the given architecture is designed to provide the integrity of authentication, forward secrecy and resiliency against the given attack vectors.

Cryptographic Framework

The authentication structure suggested utilises elliptic curve cryptography (ECC) to offer a high level of security, which has a low computational cost, thus it is applicable in IoT resource-limited nodes. ECC is chosen because it has a shorter key length, and a lower level of arithmetic complexity than other schemes using RSA, and it has the same security level. The registration process, in response, creates a private/public key pair of every IoT node using a selected elliptic curve domain. Where refers to the publically known generator point established on top

of the chosen elliptic curve group and denotes the privately chosen key of node . Computation of the corresponding public key involves multiplication of points in the elliptic curve as shown below:

$$PK^i = SK_i \cdot G \quad (1)$$

The scalar multiplication on the elliptic curve is represented by equation (1), and it is the foundation of the derivation of the key that is public. The security of this operation is based on the hardness of the elliptic curve discrete logarithm problem (ECDLP), so that adversaries cannot reconstruct out of To allow decentralised validation of keys without storing full public keys in the blockchain ledger, the proposed framework simply verifies the cryptographic hash of the public key in the blockchain ledger. This minimises storage overhead and minimises increase of data on the chain. The value Hb for blockchain stores the hash value calculated: $B^{hash}=:$

$$B_{hash} = H(PK^i), \quad (2)$$

In which H(·) is a secure one-way hash function (e.g. SHA-256). Equation (2) makes the public key integrity and immutable without giving sensitive information. When performing an authentication, the edge gateway cheques the integrity of the public key it is authenticating by re-computing its hash and comparing to the value it is storing on the distributed ledger. The framework is able to achieve decentralised trust through a combination of ECC-based key generation and blockchain-backed hash anchoring to enable lightweight implementation, which occurs at the level of an Internet of Things device.

Mutual Authentication Phase

In the mutual authentication step, the protocol is formulated as a lightweight challenge-based response technology including nonce exchange and public key validation with blockchain support. The operation of the process makes sure the authentication can be done off-chain with the blockchain used in terms of integrity verification of the hash of the public key. Initially, the IoT node transmits an authentication request containing its identity , a freshly generated nonce , and its public key to the edge gateway. When this request is received, the gateway can authenticate the integrity of the received public key by consulting the blockchain authenticator network to cheque the hash of of the one held on the distributed ledger. When validation of the hash is successful, the gateway moves on to the challenge phase. The edge gateway forms its nonce and transmits it to the IoT node as a challenge. A common elliptic curve secret then is computed by both sides with the help of own secret and public key. The computation of the session key is as follows:

$$K_s = H(r^i \| r\_j \| [\![SK]\!]\_i \cdot [\![PK]\!]_j) \quad (3)$$

In which H(·) indicates a secure hash method, and $SK_i \cdot PK_j$ signifies the elliptic map DiffieHellman shared secret. Equation (3) is what makes the session key depend on the nonces as well as the shared cryptographic key so that both freshness and mutual participation are attached to the authentication procedure. This design ensures forward secrecy, as any information about long term keys will not disclose previously initiated session keys without the knowledge of the ephemeral nonces. Mutual contribution will be ensured since both parties bring in independent randomness during the key derivation procedure. Nonce validation can be used to attain replay resistance, meaning that the same authentication messages that have been previously intercepted cannot be reused.

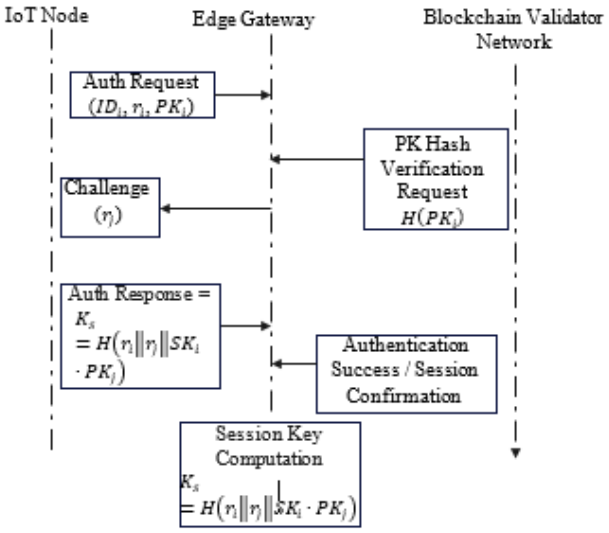

Fig.2: Authentication message flow illustrating nonce exchange, blockchain-assisted public key hash verification, and session key establishment.

The Sniping 2 diagram shows that the authentication message between the IoT node and the edge gateway and then the blockchain validator network are the only cascading communication between these systems. As highlighted in the diagram, only hash verification

using a public key is possible in blockchain interaction, where the computation of a session key and validation of authentication are done off-chain at the edge gateway.

Energy and Computational Model

In order to determine the appropriateness of the proposed authentication framework to resource-constrained IoT nodes analytical energy and computational model is developed. This is aimed at measuring per-session overhead in terms of cryptographic operations and cost of wireless transmission, the major source of energy consumption in embedded systems. The efficiency of the overall energy used on each authentication session is given by:

$$E_{total} = n_h E_h + n_{ecc} E_{ecc} + n_{tx} E_{tx} \quad (4)$$

or where n_h is the number of hash cycles, n_ecc is the number of elliptic curve scalar multiplications, and n_txis the number of transmission affairs. E_h, E_{ecc} and E_{tx} parameters are the amount of energy used per calculation of a hash computation,; ECM operation and per transmission, respectively. In small-power wireless IoT devices computational energy is often smaller than transmission energy. So one should expect the following relation to be true:

$$E_{tx} > E_{ecc} > E_h \quad (5)$$

The result of equation (5) represents a well-recognised fact that radio communication forms the major energy consumption in energy-constrained sensor nodes. In turn, an economy of message exchanges is more effective than even marginal computational cost reductions. Besides energy modelling, the calculation complexity of the authentication is examined. The number of ECC multiplications and hash computations in an authentication session is constant and thus this can be overall computed cost as:

$$C_{auth} = o(n_{ecc}) + o(n_h) \quad (6)$$

Equation (6) shows that the complexity of authentication linearly increases with the executions of elliptic curve and hash operations per session. Since these values do not change with every delivery of the protocol, the cumulative authentication process is a constant time per session. Combining Equations (4)-(6) proves that the proposed framework has a limited computational complexity and transmission-conscientious energy efficiency, indicating its appropriateness to the implementation of large scale deployments of resource- hungry IoT based devices.

Formal Security Analysis

Security of the proposed authentication framework is considered on attacks as described by the threat model. The protocol has the ability to resist the usual attacks within a distributed IoT system, such as replay attacks, man in the middle (MITM) attacks, impersonation attempts, node compromise attacks, and long-term key exposure. The Replay attacks are compromised with the addition of new nonces and within every authentication session. Since the session key is is the product of nonces and the shared secret with the elliptic curve, it is not possible to use past intercepted authentication messages successfully. Any re-sent message would have stale nonce values and would not be verified by the challenge -response verification procedure at the edge gateway. Defences to man-in-the-middle attacks are realised by binding the derivation of the session key of the shared secret elliptic curve to elliptic curve shared secret . Any other opponent trying to replace the public keys would be caught in the process of verifying hash blocks because the edge gateway would confirm the presented one with reference to the permanent ledger record. The attacker is not able to produce a valid authentication response without knowledge of the legitimate private key , making the MITM attacks computationally infeasible. Protection against impersonation is based off the cryptographic construction. The authentication reply involves the calculation of a value .As the strength of ECDLP is the basis of ECC security, it is impossible to achieve impersonation of legitimate nodes by adversaries who do not have access to the respective private keys. Compromise resilience Maintenance of key compromise resilience is the trait that the compromise of an individual node does not provide impersonated capabilities to other devices within the network. The integrity of registered public keys is guaranteed by blockchain anchoring and when an identity has been compromised, revocation entries can be appended to the distributed ledger to revoke it. Besides, it must be authenticated with dynamic exchange of nonce so that there is no reuse of nonce. With the addition of new nonces and to the derivation of the session key, forward secrecy is maintained. A long term non-secret key being revealed later cannot be used to reconstruct former session keys without

information about the ephemeral nonce values applied during the old sessions. These nonces are not stored on-chain and thus, previous communications are confidential. To simplify and standardise the protocol, the main cryptographic symbols and parameters applied in the whole protocol are outlined in Table 2.

Table 2: Notation and Cryptographic Parameters

Symbol	Description
ID_i	Node identity
SK_i	Private key
PK_i	Public key
r_i	Nonce generated by IoT node
K_s	Session key
$H(\cdot)$	Secure one-way hash function
G	Elliptic curve generator point

Performance Evaluation

The proposed blockchain-aided lightweight authentication system is tested and assessed based on energy consumed, authentication latency as well as the overhead of communication. The conformity between theoretical modelling and experimental validation is achieved by aligning the analysis with the model of analytical energy Formulation in Equation (4) and the computer complexity model in Equation (6). It is checked with a MATLAB-based simulation environment on cryptographic timing parameters based on standard benchmarks of ARM Cortex-M3 class microcontrollers, which are an exemplar of resource-constrained IoT devices. The suggested structure is contrasted with three examples of authentication models: a scheme built on the use of hashes, a lightweight scheme, an ECC-PKI-based scheme as well as a fully on-chain blockchain authentication model. These schemes indicate growing amounts of cryptographic and communication overhead. The energy spent on each authentication session is determined as:

$$E_{total} = n_h E_h + n_{ecc} E_{ecc} + n_{tx} E_{tx}$$

where transmission energy is a dominant force in the constrained internet of things. Figure 3 shows the relative consumption of energy in the schemes under evaluation. The entirely on-chain blockchain solution is the most expensive in terms of energy consumption because it has more transmission occurrences and consensus overhead. ECC-PKI scheme exhibits average energy consumption, which is being propelled by various elliptic curve functionalities. The given framework dramatically lowers the energy usage in comparison to blockchain-intensive and ECC-intensive methods by not engaging the blockchain to verify the verification of public key hashes but performing authentication towards the off-chain. Even though the hash-based algorithm has a little bit of low energy consumption, its cryptographic strength and forward secrecy are not as strong.

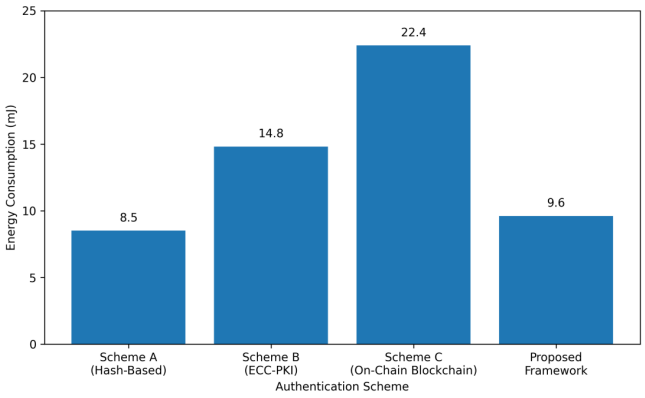

Fig.3: Energy Consumption Comparison

Authentication latency is defined as the amount of time it takes to complete a single session of mutual authentication, both including cryptographic calculation and communication latency. The comparison of the authentication delay is shown in figure 4. The most sluggish blockchain model is the fully on-chain which spreads the overheads of processing as well as validating transactions. ECC-PKI scheme has median delay due to several scalar multiplications. The suggested framework has lower latency since it limits the blockchain participation to hash checking, whereas off-chain establishment of session keys are maintained. These findings are in agreement with the expression of the computational complexity:

$$C_{auth} = o(n_{ecc}) + o(n_h)$$

Authentication does not require time measurement since the cryptographic operations are fixed costs per session, which implies that the framework can be used as the latency-conscious IoT system. Communication overhead is determined as the sum of the number of bytes sent to each transaction during authentication. The hash-based scheme is less demanding in data communication, but offers reduced security guarantees. Transmission of public key and

certificate also results in overhead at ECC-PKI scheme. Full on-chain blockchain strategy has the largest cost of the communication because of the broadcasting of transactions and the media of consensus. The suggested framework, in turn, reduces the number of bytes transmitted on-chain since it only pins the hashes of the public keys and does not engage the IoT nodes in the actual blockchain. This design greatly minimises the communication overhead with no harm to decentralised trust and hard cryptographically assurances. All in all, the findings in Figures 3 and 4 substantiate that the suggested framework provides a proper trade-off between the security strength, energy consumption, latency performance, and the optimization of communication, which is appropriate to large-scale implementations of the resource-constrained IoT networks.

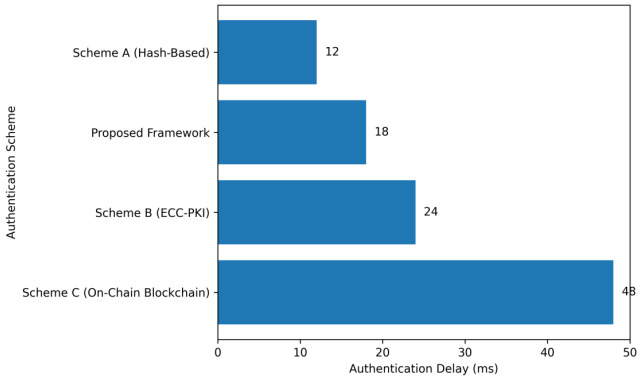

Figure 4. Authentication Delay Comparison

5. Storage Overhead and scalability

Scalability is a design factor of high concern in large-scale IoT deployments in which thousands or millions of devices can be part of the authentication system. The suggested architecture is purposefully designed to decouple device-level verification and blockchain agreement mechanisms so that it can run lightweight implementation and sustain long-term system expansion. This is because the blockchain hash storage is limited to store the cryptographic hash of every public key as opposed to storing actual certificates or files about the detailed authentication logs. represents the quantity of registered IoT nodes and is the deterministic value of the size of output generated by hash functions (e.g., 256 bits). The storage needed to store ledgers to realise public key anchoring increases linearly with . Since the size of hash values is constant and they are small, the expansion of ledgers is predictable and easily manageable in contrast to certificate-based or transaction-intensive blockchain systems. Moreover, unnecessary ledger bloat due to entries that need not be entered is also cut back since the entries are revoked only when required. At the device level, the requirement of node memory is low. The IoT nodes have only their own keys (although they might be unique) and the equivalent (public) key, in addition to a few temporary parameters of the session, including nonces. Each blockchain ledger replica and transaction history is not stored on limited nodes. This removes the large storage overhead linked to blockchain involvement and allows support of low-memory microcontrollers like those based on ARM Cortex-M3.

Ledger-based identity invalidation is used to provide revocation scalability. In the event that a device is compromised a revocation entry and the hash of the matching public key are appended to the distributed ledger. With revocation validation being a part of hash verification at the edge gateway, no certificate revocation lists are necessary on IoT nodes or periodic revocation state synchronisation. This can be done so that the operations of revocation will be scalable with the number of compromised identities and not the sum of all the devices in the network. The use of edge assisted load balancing also improves scalability as there is a spread of the authentication verification work between two or more gateway. Since the blockchain does not require the execution of consensus but only the execution of lightweight hash queries, the number of authentication requests that the gateways can process simultaneously is not too heavy to involve the validator network in heavy computational work. This hierarchical structure eliminates bottlenecks in overburdened nodes and also has decentralized trust properties. In general, the proposed framework provides scalable authentication by reducing on-chain data storage, removal of ledger replication at IoT device, and centralising off-chain verification at the edge, allowing the proposed framework to work in the large and heterogeneous IoT ecosystems.

Discussion

The framework proposed balances decentralised trust with lightweight execution, however, trade-offs are always bound to occur when this idea is applied on a practical level. Although key anchoring with the help of blockchain increases the integrity and tamper resistance, it results in the introduction of new infrastructure needs through the presence

of key validators and edge gateways that are able to execute the hash verification queries. In systems where connectivity is very low or the network size is very small, blockchain overheads might not be worthwhile in comparison with simpler symmetric-key solutions. In contrast, when the stakes or victims are numerous or across multiple stakeholders, and in each case, the trust cannot be entrusted to a central government, decentralised anchoring has quantifiable resilience payoffs. The most legitimate scenarios with blockchain anchoring include distributed ownership of a system, interoperability across organisations, or a system that demands strong security assurance, e.g., industrial IoT, smart grids, and monitoring critical infrastructure. Immutable public key hash storage in this situation minimises threats of compromise of centralised certificate authority. Yet, with small, closed networks, which are tightly controlled with small administrative domains, the traditional PKI or fully lightweight symmetric schemes can offer adequate protection with less operational complexity. In spite of its goodness, there are limitations associated with the framework. To begin with, it presupposes that the blockchain validator network behaves with the majority of honesty, on a larger scale, the integrity of the ledger may be affected by the collusion of a majority or consensus attacks. Second, latency caused by validation of blockchain hashes although much reduced compared to full on-chain validation could still impact ultra-low-latency applications. Third, the standard elliptic curve cryptography analysis is susceptible to subsequent large scale quantum enemies. Also, congestion in networks, synchronisation time, and hardware variability would have to be taken into serious account in a real-life deployment. In a prospective view, it is possible to modify the framework to post-quantum cryptographic primitives. Operations on elliptic curves can also be substituted with lattice-based or hash-based key exchange protocols without changing the off-chain authentication design and concept of blockchain hash anchoring. Currently, the architecture separates key generation and ledger storage thus a quantum-resistant scheme would largely affect only the cryptographic layer, requiring no fundamental change in the system model. Overall, the suggested solution is the most appropriate in the case of moderately limited IoT environments that need decentralised trust, scaling revocation, and energy efficiency (balanced). It has been designed to limit its interaction with blockchain deliberately to maintain pragmatics but is flexible enough to be changed to keep up with emerging cryptographic standards.

Conclusion

The given paper offered a secure lightweight framework of authentication of IoT nodes with resource constraints that operate based on blockchain-supported key management. The given architecture combines the use of the elliptic curve cryptography with the distribution ledger based public keys anchoring to an alternative of the decentralised trust avoiding heavy computational and communication burdens on the limiting devices. The framework ensures scalability by decoupling both on-chain identity validation and off-chain execution of authentication at an edge gateway to ensure lightweight operation. The security analysis illustrates resilience to replay attacks, man-in-the-middle attack, impersonation and key compromise condition in the usual cryptographic assumption. Nonce-based derivation of session keys is guaranteed to offer forward secrecy and blockchain anchoring ensures tamper-resistant integrity verification of publicly registered key. The majority-honest validator assumption is another assumption that enhances the decentralisation of trust without necessarily involving the IoT nodes to participate in the blockchain directly. The proposed evaluation proves that the suggested framework ensures substantial gains in energy efficiency and authentication latency compared to blockchain intensive and ECC intensive schemes. Analytical results and simulation findings indicate it has less transmission overhead and constrained computational complexity per session, which confirms the appropriateness of large-scale applications of limited IoT systems. Future research directions would involve the addition of post-quantum cryptographic primitives, experimenting the implementation of heterogeneous hardware in the real world, dynamic validator selection schemes and adopting adaptive trust management schemes to become even more resilient and scalable in next-generation IoT scenarios.

References

1. Chen, F., Xiao, Z., Cui, L., Lin, Q., Li, J., & Yu, S. (2020). Blockchain for Internet of Things applications: A review and open issues. Journal of Network and Computer Applications, 172, 102839.
2. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292–2303.

3. Dai, H. N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. IEEE Internet of Things Journal, 6(5), 8076–8094.
4. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2019). LSB: A lightweight scalable blockchain for IoT security and anonymity. Journal of Parallel and Distributed Computing, 134, 180–197.
5. Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A review on the use of blockchain for the Internet of Things. IEEE Access, 6, 32979–33001.
6. Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2018). Blockchain technologies for the Internet of Things: Research issues and challenges. IEEE Internet of Things Journal, 6(2), 2188–2204.
7. Ferrag, M. A., & Shu, L. (2021). The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: A tutorial. IEEE Internet of Things Journal, 8(24), 17236–17260.
8. Hammi, M. T., Hammi, B., Bellot, P., & Serhrouchni, A. (2018). Bubbles of trust: A decentralized blockchain-based authentication system for IoT. Computers & Security, 78, 126–142.
9. Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411.
10. Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things Journal, 5(2), 1184–1195.
11. Ouaddah, A., Abou Elkalam, A., & Ait Ouahman, A. (2016). FairAccess: A new blockchain-based access control framework for the Internet of Things. Security and Communication Networks, 9(18), 5943–5964.
12. Wang, Z., Zhang, J., Song, J., Tang, Y., & Cheng, H. (2024). Blockchain-based key management scheme in Internet of Things. In International Symposium on Emerging Information Security and Applications (pp. 208–218). Springer Nature Switzerland.