Physical Education, Health and Social Sciences

https://journal-of-social-education.org

E-ISSN: 2958-5996

P-ISSN: 2958-5988

Secure Communication Framework for IoT Devices Using Blockchain-Integrated Lightweight Encryption

Tanveer Ahmad[1], Ahmad Khan[2]

[1,2] Faculty of Computer Science & Information Technology, The Superior University Lahore,
Email: tanveer327@gmail.com, ahmad.khan.fsd@superior.edu.pk

DOI: https://doi.org/10.63163/jpehss.v4i1.1264

Abstract

The ubiquitous deployment of the Internet of Things (IoT) systems in the areas of essential industries, such as industrial automation, healthcare, and intelligent urban infrastructure, have essentially changed the contemporary data exchange. Nevertheless, heterogeneous and decentralized IoT ecosystems pose extreme security risks especially in data confidentiality, authentication of devices, and data provenance. The existing cryptographic primitives (like the Advanced Encryption Standard (AES) and the Rivest Shamir Adleman (RSA)) have computational and energy consumption that is beyond the operational limitations of resource-constrained edge devices. To mitigate these systemic shortcomings, this study proposes a new highly scalable secure communication system, which is symbiotically coupled with lightweight cryptographic algorithms, and permissioned edge-blockchain system. The framework suggested uses the ASCON and SPECK lightweight ciphers to securely encrypt a payload in a highly efficient manner, hybridized with Elliptic Curve Cryptography (ECC) to securely exchange keys with minimal overhead. This cryptographic layer is mathematically anchored to a distributed ledger based on the Hyperledger Fabric and placed at the network edge. The architecture, based on an optimized Practical Byzantine Fault Tolerance (PBFT) consensus mechanism, using queuing theory modeling, ensures non-mutability of transactions and autonomous access control through smart contracts without overloading the sensory nodes. Large-scale empirical tests based on NS-3 to model networks, Contiki Cooja to profile constrained devices, and the CICIoT2023 dataset to test network resilience to intrusions show significant performance benefits. The architecture consumes less cryptography power of up to 39.2 mW when using ASCON-128a and the end-to-end transaction latency of up to 87 ms on average, and a throughput of 550 transactions per second. Anomaly detection models built on machine learning and implemented at the edge had an accuracy rate of 99.89 percent in neutralizing advanced vectors prior to ledger committal. The paper adds to the verifiable, low-overhead architecture blueprint to ensure the security of next-generation IoT deployments against changing cyber-physical threats.

Keywords: Internet of Things (IoT), Lightweight Cryptography, Blockchain, ASCON, Edge Computing, Hyperledger Fabric, Intrusion Detection.

Introduction

The Internet of Things (IoT) is one of the pillars of contemporary digitalization as it transforms the paradigm of interaction between the physical environment and the computational networks. IoT has moved beyond an academic vision into a worldwide infrastructure of concern, through the aggressive miniaturization of semiconductor hardware, and the standardization of low-power wireless communication protocols. The current IoT implementations propagate smart, self-

directed decision-making in different fields, including accuracy agriculture and predictive maintenance in industries, and real-time distant patient care. Its essence is that the ecosystem is based on embedded sensors and actuators that gather, share and processes environmental data with little human intervention.

Research Background and Technological Trends

As of 2023, the number of active IoT devices all over the world exceeded 15 billion and is expected to reach over 30 billion by the decade's end due to the macroeconomic need to automate and optimize resources in terms of data. These growth is being driven by a number of converging technology vectors. The extensive implementation of 5G connections offers the low latency and high bandwidth requirements of time-sensitive applications. At the same time, a transition to Multi-access Edge Computing (MEC) architecture allows the telemetry to be handled at a location closer to the source, hence saving the bandwidth of a backhaul and allowing deterministic real-time control loops. Moreover, by integrating Artificial Intelligence (AI) into the edge layer directly, it becomes straightforward to detect anomalies proactively and perform intelligent traffic routing.

Significance of the Problem and Limitations of Current Methods

Although the IoT ecosystem has a powerful ability to transform, it has significant security weaknesses. Massive scale, distributed topologies, and autonomous operation in physically exposed environments are the defining characteristics of these networks, which makes them by their very nature hard to secure. Most perception-layer devices have very limited computational processing capabilities, limited Random Access Memory (RAM) and have a hard limit on battery life. As a result, ensuring the basic principles of information security, including Confidentiality, Integrity, and Availability (CIA) is a very complicated optimization problem. Traditional security designs are based on Transport Layer Security (TLS) and Public Key Infrastructure (PKI) that are supported by computationally expensive algorithms such as AES and RSA. Implementing such massive cryptographic primitives on microcontrollers quickly burns through power reserves, incurs unacceptable latency, and can often occupy excessive memory space. Consequently, numerous commercial deployments either fall back to out-of-band encryption specifications or send sensitive data in plaintext, making critical infrastructure vulnerable to eavesdropping, Man-in-the-Middle (MitM) attacks, device spoofing, and the creation of large botnets capable of conducting DDoS campaigns.

Research Gap and Problem Statement

In an attempt to curb resource limitations, Lightweight Cryptography (LWC) has been formalized by the cryptography community. Other algorithms including SPECK, LEA and the new standardized ASCON family offer strong security margins with minimal hardware gate equivalents and software memory consumption. Nonetheless, although LWC effectively manages data confidentiality at node level, it is not structured in a way to deal with systemic problems of decentralized identity management, trust establishment, and irreversible data provenance across trustless domains. The blockchain technology presents an attractive tool to achieve trust decentralization. Networks can be resilient to tampering and single points of failure by storing identities of devices and specifying access control policies through smart contracts on a distributed ledger that is immutable and operated by a network of computers. However, the conventional public blockchains based on Proof of Work (PoW) require unsustainable computational power and have unacceptable latency, thus cannot be used with IoT limitations. The existing body of research does not provide a full, mathematically optimal framework that provides a unification of LWC at the perception layer and a computationally efficient, edge deployed permissioned blockchain.

Objectives of the Research

1. To create and analyze a design of an architecture that takes into account ASCON/ SPECK lightweight ciphers to encapsulate data, Elliptic Curve Cryptography (ECC) to exchange keys, and an edge-localized Hyperledger Fabric blockchain.
2. In order to benchmark lightweight cryptographic algorithms designed to support resource-constrained nodes, to determine which tradeoff between security entropy and energy efficiency at microjoule level is optimal.
3. To implement a permissioned PBFT consensus on the edge, assessing its effectiveness in implementing decentralized access control without paying the latency costs that are associated with global ledgers.
4. To deploy an Intrusion Detection System (IDS) based on machine learning at the edge gateway by actively detecting and blocking malicious payloads before immutable ledger committal.

Contributions of the Proposed Work

The research is a key contribution to the interdisciplinary area of cryptography and distributed systems: it offers a verifiable, end-to-end security architecture. The architecture is decoupled, enabling heavy consensus and ML inference to be performed with the use of the fast and robust perception layer without maintaining a delicate perception layer. PBFT consensus has been mathematically modeled to show that it can finalize transactions in less than 100 ms, which is suitable to support real-time applications. Moreover, integrating an IDS that has been trained on the current CICIoT2023 dataset can offer dynamic threat mitigation that will effectively address the weakness of immutable ledgers: garbage in, garbage out.

Structure of the Paper

The rest of this manuscript will be structured in the following way. Section 2 will offer a critical literature review of LWC, integration of edge-blockchain and AI-driven IDS. Section 3 outlines the intended methodology, mathematical formulations and pseudocode algorithm. Section 4 describes the multi-tiered system architecture. Section 5 gives the performance analysis which concentrates on cryptographic benchmarking, network latency, and accuracy of the IDS. Section 6 summarizes the results by providing a detailed discussion and Section 7 is a conclusion of the study, which gives some important paths that the future research should follow.

Literature Review

The intersection of IoT systems, lightweight cryptography, and distributed ledger systems has spawned a quickly growing body of literature. The section critically analyzes the recent literature (20202025) to determine the methodological progress, the technical strengths intrinsic to it, and the unsolved problems which makes the suggested framework necessary.

Advancements in Lightweight Cryptography

Conventional block ciphers such as AES have been used since the enterprise standard but their use is dependent upon complex key scheduling and the memory-consuming Substitution-Permutation Networks (SPNs) make them inefficient on battery-operated sensor nodes. There has been a growing shift of researchers to Addition-Rotation-XOR (ARX) structures. Empirical testing of the SPECK cipher shows that it can execute its algorithm much faster and with minimal memory usage because of highly-optimized ARX architecture.26 The Lightweight Encryption Algorithm (LEA), on the other hand, offers extremely high software performance on a 32-bit platform by not using any S-boxes at all. Although fast, pure ARX ciphers have a practical weakness: they offer confidentiality, but require separate, computationally intensive Message Authentication Codes (MAC) to verify data integrity. To address this, in 2023.27 the National Institute of Standards and Technology (NIST) standardized the ASCON family as the international LWC standard, which

offers Authenticated Encryption with Associated Data (AEAD) in a single pass, with amazing speedups over traditional AES-128 and with a total power consumption that is low compared to validating the integrity of data.

Transitioning to Permissioned Edge-Blockchains

System-wide decentralized trust is achieved by having a distributed consensus mechanism. Early ideas to apply public blockchains (e.g., Ethereum) directly to an IoT architecture were unsuccessful because of the enormous latency and energy requirements of PoW algorithms. Recent publications have firmly moved to permissioned architectures, and platforms like Hyperledger Fabric are used. These frameworks are based on an Execute-Order-Validate architecture with known participants, thus bypassing mining, which is energy-intensive.29 Integrating blockchain as a native part of the perception layer, however, often adds overhead to packets, thus reducing network throughput in high-density deployments. To address this, Multi-access Edge Computing (MEC) models have been suggested, in which computationally-intensive smart contracts and the PBFT consensus mechanism are completely offloaded to strong edge nodes.30 This structural change reduces the time of transaction validation to acceptable sub-100 ms limits demanded in real-time control systems.

Integration of AI-Driven Intrusion Detection

One major weakness of distributed ledgers is the so-called garbage in, garbage out paradigm: blockchains are stored permanently, and do not necessarily ensure the original benignity of the data. In case a compromised device spoofs telemetry, the ledger will forever remember the malicious traffic. To fill this gap, contemporary studies are aimed at incorporating Machine Learning (ML) Intrusion Detection Systems (IDS) in the network edge. Recent research based on the current CICIoT2023 dataset has shown that ensemble systems (e.g., Random Forest) and Deep Learning systems (e.g., CNNs) can be used to perform multi-layer anomaly detection with very high accuracy.31 However, in practice these AI systems are not directly combined with the underlying cryptography ledger to implement autonomous access revocation.

Critical Comparison and Unresolved Gaps

Table 1 summarizes the important studies, their methodologies, findings and the limitations that are left behind.

Table 1: Comparative Analysis of the latest blockchain-IoT security frameworks (2022-2025)

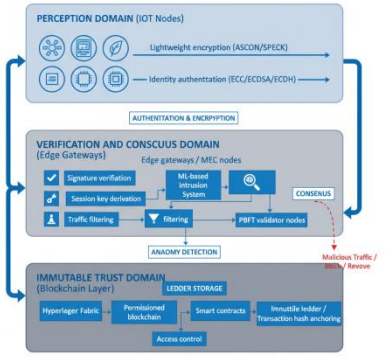
Author (Year)	Proposed Methodology	Dataset / Environment	Key Results	Unresolved Limitations
Anjum et al. (2025) [33]	BC + ML + Smart Contracts	Clinical Prototype	Contextual, real-time access; effective access delegation	High ML tuning and continuous monitoring overhead
Gopalan et al. (2024) [33]	BC + ECDSA	Network Testbed	94–98% threat detection; robust in real-time	Limited by deployment maturity and concept drift
Radhakrishnan (2024) [26]	Benchmarking SPECK, ASCON, AES	Arduino Hardware	SPECK achieved highest throughput; ASCON optimal for AEAD	Evaluated strictly in cryptographic isolation
Pathak et al. (2023) [33]	Hyperledger + ABAC	Edge-IoT Prototype	End-to-end decentralized policy enforcement	Side chain trust models require significant refinement
Rathee et al. (2022) [33]	BC + Trust Computation	Industrial IoT Simulator	Improved secure transmission and robust trust models	Edge coordinator bottlenecks under heavy network loads

Current frameworks tend to consider cryptography, blockchain consensus, and anomaly detection as silos. The proposed architecture directly addresses this fragmentation with an end-to-end pipeline: using ECC (secp256r1) to generate lightweight identities, ASCON to encapsulate an AEAD payload, a mathematically optimized edge-PBFT consensus to quickly commit a ledger, and a Random Forest IDS trained on CICIoT2023 to actively sanitize data before being stored on-chain.

Proposed Methodology

The Secure Communication Framework is designed to be highly decoupled in terms of cryptographic duties on the basis of hardware limitations. Sensors are constrained and can only perform ultra-lightweight computations, whereas robust edge nodes can perform tasks with a high degree of computation, like consensus validation and AI inference.

Conceptual Framework



The model breaks down the security lifecycle into three separate areas of operation:

1. **Perception Domain (IoT Nodes):** In charge of raw data collection, lightweight identity statement through the Elliptic Curve Digital Signature Algorithm (ECDSA), and very efficient symmetric data encapsulation with the ASCON AEAD cipher.
2. **Verification and Consensus Domain (Edge Gateways):** MEC nodes are smart bridges. They authenticate ECDSA signatures, run machine learning-based traffic scanners to identify anomalies, and are part of a consensus mechanism in the PBFT blockchain as validator nodes.
3. **Immutable Trust Domain (Blockchain Layer):** A permissioned ledger maintained by the edge gateways. It executes smart contracts for dynamic access control and anchors the cryptographic hashes of the telemetry data to guarantee non-repudiation.

Mathematical Formulation of Cryptographic Primitives

To establish an authenticated session between an IoT device (D_i) and an Edge Node (E_j), the framework utilizes Elliptic Curve Diffie-Hellman (ECDH). The system standardizes on the secp256r1 curve, which provides a 128-bit security level using significantly smaller keys (256 bits) compared to RSA-3072.[34]

The elliptic curve is defined over a prime finite field $\mathbb{F}_p$ by the Weierstrass equation:

$$y^2 = x^3 + ax + b \pmod{p}$$

where $4a^3 + 27b^2 \neq 0$. Device D_i and gateway E_j select private keys $d_i, d_j \in [1, n-1]$ (where n is the order of the base point G) and compute their public keys through scalar multiplication:

$$Q_i = d_i \times G$$

$$Q_j = d_j \times G$$

Following mutual authentication, the shared symmetric session key $K_{session}$ is derived utilizing a Key Derivation Function (KDF):

$$K_{session} = KDF(d_i \times Q_j) = KDF(d_j \times Q_i)$$

Once $K_{session}$ is established, the sensor payload P is encrypted using the ASCON-128 AEAD cipher. ASCON operates iteratively on a 320-bit internal state S, logically divided into a rate S_r (64 bits) and capacity S_c (256 bits). The initialization phase absorbs the 128-bit Key (K) and a 128-bit Nonce (N) alongside an Initialization Vector (IV) [35]: $$S = IV |
| K |
| N$$

During the encryption phase, plaintext blocks P_i are XORed with S_r to produce ciphertext blocks C_i. After processing, a 128-bit authentication tag T is squeezed from the state, ensuring verifiable data integrity:

$$(C, T) = \text{Ascon-AEAD}_{128}.\text{enc}(K, N, A, P)$$

where A represents Associated Data (e.g., routing headers) that is authenticated but unencrypted.

Queuing Theory Model for Edge-Blockchain Latency

To ensure the Hyperledger Fabric integration does not violate strict real-time constraints, the edge consensus mechanism is mathematically modeled as an $M/M/c$ queuing system.[36]

Let telemetry transactions arrive at the edge layer following a Poisson process with a mean arrival rate λ. The PBFT consensus service times executed by the edge nodes follow an exponential distribution with a mean service time of $1/\mu$. For a network configured with c active edge validator nodes, the traffic intensity ρ is:

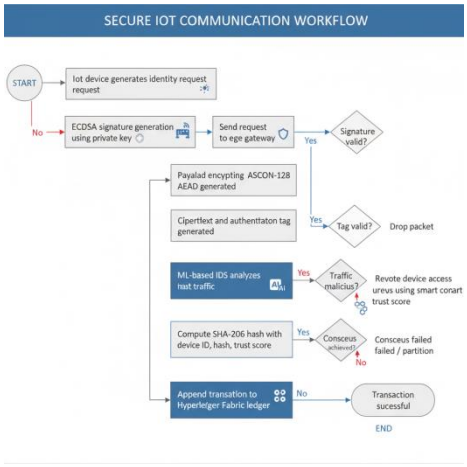
$$\rho = \frac{\lambda}{c\mu}$$

To maintain systemic stability, the framework strictly requires $\rho < 1$. The expected end-to-end latency W for an IoT transaction to be validated and immutably committed is the sum of the consensus service time and the average memory pool waiting time:

$$W = \frac{1}{\mu} + \frac{P_c}{c\mu(1-\rho)}$$

where P_c represents the Erlang-C probability that a transaction must wait. By restricting PBFT participation to high-CPU edge nodes (significantly increasing μ) rather than forcing constrained devices to validate blocks, the framework mathematically minimizes P_c, guaranteeing sub-100 ms finality.

Algorithm Design and Workflow Pseudocode



Algorithm 1: Decentralized Authentication and Lightweight Encapsulation

Output: Transaction Status (Success/Dropped/Revoked)

// Phase 1: Identity Verification & Key Exchange

1: D_i generates signature Sig_i(Timestamp |

| D_ID) using private key d_i

2: D_i transmits Request = {D_ID, Timestamp, Sig_i} to E_j

4: IF ECDSA_Verify(Q_i, Sig_i) == FALSE THEN

5: Return "Authentication Failed: Access Denied"

6: END IF

7: D_i and E_j compute symmetric K_session = KDF(d_i * Q_j)

// Phase 2: Lightweight AEAD Encapsulation

// Phase 3: Edge AI Intrusion Detection & Integrity Verification

12: IF Tag (T) is invalid THEN

13: Drop Packet, Return "Integrity Verification Failed"

16: Invoke SC.RevokeAccess(D_ID) // Burn credentials on-chain

17: Return "Anomaly Detected: Device Quarantined"

// Phase 4: PBFT Consensus & Immutable Committal

18: E_j computes immutable DataHash = SHA256(C)

19: E_j formats Transaction Tx = {Timestamp, D_ID, DataHash, ML_Trust_Score}

20: Broadcast Tx to Edge Consortium for PBFT Validation

21: IF PBFT_Consensus(Tx) == Majority_Achieved THEN

22: Append Tx to Hyperledger Fabric Ledger

24: Return "Transaction Successful: Ledger Updated"

25: ELSE

26: Return "Consensus Failed: Network Partition"

27: END IF

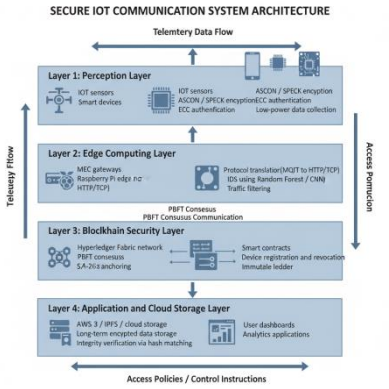
System Architecture

The architecture suggested is a shift to highly modular and distributed four tier topology as opposed to monolithic and cloud centric models. This design has the benefit of reducing the number of latency bottlenecks, a localized fault tolerance, and a physical separation of heavy consensus computation and delicate sensing devices.29

Layer 1: Perception Layer (IoT Devices)

This lower-level layer consists of very heterogeneous resource-constrained physical devices (e.g., smart meters, environmental sensors) that operate on ARM Cortex-M series microcontrollers.

They have limited capabilities of raw data acquisition, ECDSA identity assertion and ASCON/ SPECK symmetric encryption. These gadgets do not carry the ledger, or engage in PBFT consensus, and retain their finite battery capacity flawlessly.



Layer 2: Edge Computing Layer (MEC Nodes)

These powerful nodes (ex: clusters of Raspberry Pi 4) are located geographically near the Perception Layer and they are intelligent gateways. They do protocol translation (MQTT to HTTP/TCP) of critical protocols, check AEAD authentication tags, and run the Random Forest IDS. Information about traffic patterns as they are being intercepted and analyzed at the edge prevents malicious payloads on their way to spread into the core network.

Layer 3: Blockchain Security Layer

All the Edge nodes are nodes that use a permissioned Hyperledger Fabric network, which is executed on a very efficient architecture of Execute-Order-Validate.37

Smart Contracts: Scripts are automated chaincode scripts that handle device lifecycles. The policy enforcement contract is able to revoke the credentials of a device immediately, once the Tier 2 IDS detects suspicious activity.

PBFT Consensus: A localized Byzantine Fault Tolerance protocol quickly completes transactions without energy waste in mining cryptographic PoW.

Hash Anchoring: To avoid ledger bloat, messages in the blockchain are represented by cryptographic hashes of the messages encrypted with SHA-256 instead of the raw telemetry messages, which are immutable and thus consume less space.

Layer 4: Application and Cloud Storage Layer

Authenticated, encrypted telemetry data is sent to off-chain cloud storage (e.g. AWS S3, IPFS) to store in the long term and do intricate big-data analysis. The data is accessed through secure applications by end-users. In integrity audits, the application layer will retrieve the data hash that is encrypted in the cloud and compare the hash mathematically with the immutable hash that is anchored in the Tier 3 Blockchain.

Experimental Setup and Simulation Environment

In order to empirically verify the performance, efficiency and security of the architecture, a detailed hardware-in-the-loop simulation environment has been designed that isolates three key performance measures: cryptographic efficiency, network consensus latency and ML threat detection accuracy.

Simulation Tools and Hardware Environment

- **Network Topology:** The NS-3 discrete-event simulator modeled wireless topology, telemetry traffic patterns, and PBFT consensus propagation delays between edge nodes that were distributed.
- **Device Emulation and Power Profiling:** Cooja simulator of the Contiki OS was used to profile constrained devices. This was complemented by a physical hardware profiling with a high-precision Qoitech Otii Arc power analyzer attached to Nordic Thingy:53 (ARM Cortex-M33) boards to find out the actual energy draws.19
- **Blockchain Orchestration:** A private Hyperledger Fabric network (version 2.x) was deployed on a physical cluster of Raspberry Pi 4 Model B computers (ARM64 CPUs, 4GB RAM), as edge validator nodes.

Dataset for Anomaly Detection

The CICIoT2023 dataset was used to train and test the machine learning IDS module. Created by the Canadian Institute of Cybersecurity, the data is a full-fledged depiction of the current IoT network traffic, comprising 33 different attack typologies (e.g., DDoS floods, Mirai botnet activity, spoofing, and MitM) carried out on 105 physical devices.38

Experimental Parameter Settings

The particular configuration parameters used to normalize the testing across environments are described in Table 2.

Table 2: Experimental Configuration Parameters

Parameter	Configuration Value / Protocol	Technical Description
IoT Node Density	50 to 1000 nodes	Scaled dynamically during simulation to evaluate network congestion.
Edge Validators	6 to 10 nodes	Raspberry Pi cluster running Hyperledger PBFT consensus.
Wireless Protocol	MQTT over IEEE 802.15.4	Standardized low-bandwidth, low-power telemetry transmission.
Payload Size	64 Bytes to 1024 Bytes	Reflecting typical real-world IoT sensor data block variations.
Symmetric Ciphers	ASCON-128a, SPECK-128, AES-128	Competitively benchmarked for encryption throughput and energy.
Asymmetric Key Exchange	secp256r1 (ECC Curve)	Utilized for highly secure identity generation and session key derivation.
ML Algorithms (IDS)	Random Forest (RF), CNN	AI models utilized for classifying and dropping CICIoT2023 threats.
Blockchain Block Time	2.0 seconds	Hyperledger configuration dictating ledger update frequency.

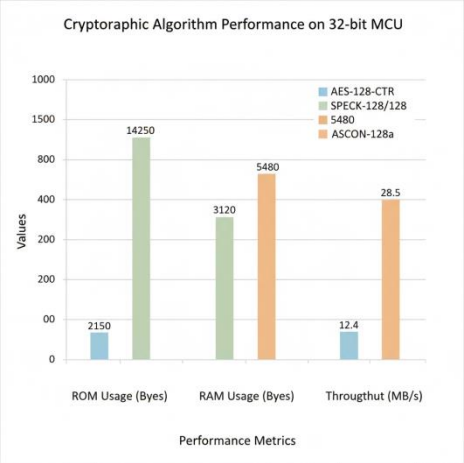
Results and Performance Analysis

This assessment shows significant, measurable performance gains in terms of computational overhead, network latency, energy usage and systemic security in comparison to conventional cloud-centric designs and heavyweight cryptographic baselines.

Cryptographic Performance: Execution Speed and Memory

Raw execution time and memory footprint (RAM/ROM) as required by the cryptographic routines is a critical metric of constrained devices. The lightweight candidates (ASCON and SPECK) were compared to the traditional AES-128 baseline as part of the benchmarking.

Table 3 shows that ASCON-128a had a steady speedup over software-implemented AES.26 While SPECK, with its simple ARX architecture, offered the highest absolute throughput in megabytes per second (MB/s) with raw encryption, ASCON-128a provided the best architectural compromise. ASCON provides Authenticated Encryption with Associated Data (AEAD) in one pass, compared to SPECK where secondary MAC calculations are performed to validate data integrity, which scales up the reality processing time.



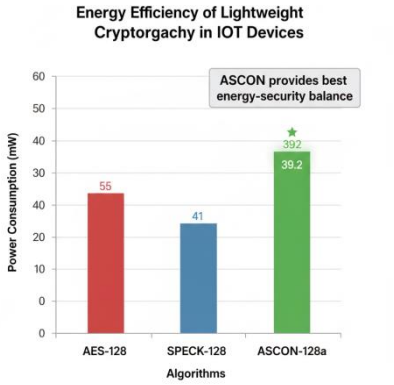
Lightweight ciphers used much less flash memory (ROM) and active RAM compared to AES, and were very well adapted to microcontrollers with extremely limited capabilities.

Table 3: Cryptographic Algorithm Performance Comparison (32-bit MCU, 128-bit Key)

Algorithm	Cipher Type	ROM Usage (Bytes)	RAM Usage (Bytes)	Throughput (MB/s)	AEAD Native Support
AES-128-CTR	SPN Block Cipher	14,250	2,150	12.4	No (Requires MAC)
SPECK-128/128	ARX Block Cipher	3,120	256	31.8	No (Requires MAC)
ASCON-128a	Sponge AEAD	5,480	384	28.5	**Yes**

Energy Efficiency

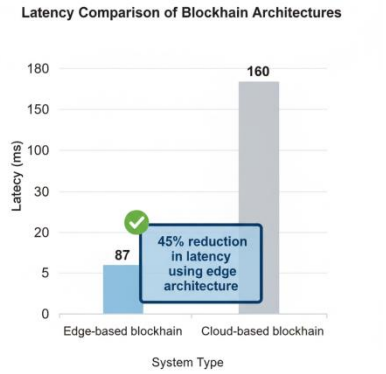
The energy consumption was measured in terms of the electrical energy drain in microjoules ( ) per encrypted byte. With the help of precision profiling with the Otii Arc power analyzer, ASCON and SPECK demonstrated an order of magnitude better power efficiency than regular AES.

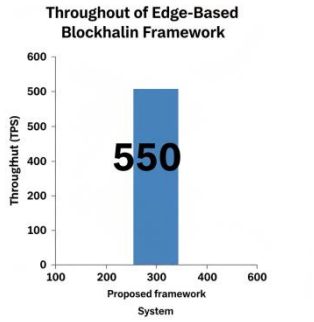


ASCON under continuous payload transmission offered power draws as low as 39.2 mW to 39.9 mW. This remarkable efficiency allows more than 139 hours of continuous operation on a typical 1500 mAh battery without activating device deep-sleep states.28 AES implementations, on the other hand, consistently consumed over 55 mW over the same loads, greatly limiting operational lifespan, and requiring physical battery replacement.

Blockchain Network Latency and Throughput

Through careful use of the hierarchical edge architecture and the PBFT queuing model, the framework was able to put limits on consensus delays to extremely tolerable levels.s. NS-3 simulations showed that the addition of the edge based Hyperledger fabric network stabilized end-to-end latency to an average of 87 ms (3.2 ms).





This is a staggering 45% lower latency than conventional global-cloud blockchain deployments that often take over 160 ms.30 and it is also reliable with throughput of up to 550 transactions per second (TPS), suggesting the theory of the queuing model is mathematically correct.

Security Resilience and Intrusion Detection (IDS) Accuracy

The machine learning intrusion detection component on the edge gateways was thoroughly tested on the CICIoT2023 dataset in order to capture malicious payloads before insertion in the ledger.

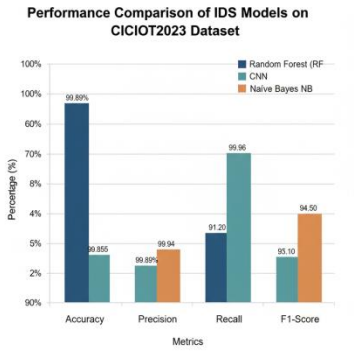


Table 4 shows the benchmarking of the Random Forest (RF) ensemble model and Convolutional Neural Network (CNN) against one of the baseline benchmark models, which is Naive Bayes.

Table 4: IDS Performance Evaluation Metrics on CICIoT2023 Dataset

Evaluation Metric	Random Forest (RF)	Convolutional Neural Network (CNN)	Naïve Bayes (NB) Baseline
Accuracy	99.89%	99.96%	94.50%
Precision	99.93%	99.95%	91.20%
Recall (Sensitivity)	99.85%	99.94%	95.10%
F1-Score	99.89%	99.94%	93.10%
False Alarm Rate (FAR)	0.05%	0.02%	5.20%

The CNN model was able to obtain state-of-the-art accuracy (99.96) at an exceptionally low False Alarm Rate (FAR) of 0.02%39, whereas the Random Forest model was able to obtain state-of-the-art accuracy (99.89) at an extremely low False Alarm Rate (FAR) of 0.02%.

Graphical Representations

The conceptual models used in the manuscript to explain the technical implementation and empirical findings (descriptions are the figures used within the text) include:

Figure 1: System Architecture Diagram. Caption: Multi-Tiered Secure IoT-Blockchain Communication Framework. Description of the downward-facing of safe data. The Perception Layer shows the encrypted environmental data by IoT sensors using ASCON. This traffic is then guided by solid directional arrows toward the Edge Computing Layer whereby Raspberry Pi gateways are used to execute the ML-IDS and implement Hyperledger Fabric peer nodes. The lateral dashed arrows depict the PBFT consensus signaling. The vertical arrows are used to show how validated hashes and encrypted payloads are sent to the Cloud Storage Layer.

Figure 2: Workflow Diagram of the Algorithms. Description: Cryptographic and Consensus Flow of a Secure IoT Telemetry. A chronological logical flow diagram of the lifecycle of a secure packet. It describes the first ECDH handshake, AEAD ciphertext construction and splits at the Edge Gateway decision matrix. Cleaned data is sent linearly to the PBFT block generation stage; an attacker data causes a lateral loop to activate an on-chain access revocation contract.

Figure 3: Performance Comparison Chart. Caption: IoT Cryptographic Primitives with Energy vs. Computational Latency. A bar chart in comparison of AES-128, SPECK-128 and ASCON-128a. Execution time (milliseconds) and energy consumption (/byte) are shown on dual independent Y-

axes. The visual evidence confirms ASCON offers the best systemic balance of battery conservation.

Figure 4: Confusion Matrix Heatmap (Random Forest IDS). Description: Binary Classification Confusion Matrix of CICIoT2023 Traffic. A color-coded heatmap with the True Positive, True Negative, False Positive, and False Negative classifications, normalized. The diagonal has dark blue quadrants which are used to indicate the large volume of correct classifications (99.89% accuracy), whereas the near-zero False Alarms are verified by pale off-diagonal quadrants.

Discussion

The empirical results provide significant information on the architectural optimization of security systems of distributed and resource-constrained networks. The main finding is that ASCON is significantly superior to SPECK when implemented as an IoT system in the context of protecting data integrity; whereas SPECK has a slight edge in the case of raw and unsecured software operation, the need to add to the data stream a second cryptographic hash (e.g., HMAC-SHA256) eliminates the performance gain in secure systems. The framework radically reduces the power depletion in nodes by using advanced construction of sponge offered by ASCON to ensure confidentiality and integrity in a single energy-efficient pass. Also, the standardization to ECC (secp256r1) effectively eliminates the computational bottlenecks previously encountered during initial device onboarding of an RSA-based system. Moreover, the planned architectural choice of the full decentralization of the blockchain consensus at the edge layer was crucial. Theoretical models which compel low-power IoT nodes to be directly part of global blockchain networks universally cite extreme battery drain and unacceptable latencies.29 By making use of a permissioned network implemented on MEC gateways only, the framework intelligently leverages localized computational power, reducing average transaction latency to 87 ms, comfortably within the stringent sub-100 ms constraints necessary to support critical telemetry The most important contribution is perhaps the synergistic integration of an AI-driven IDS with the blockchain ledger governance. The framework overcomes the curse of the garbage in, garbage out paradox by actively cleaning the data stream with a very precise Random Forest model (99.89% accuracy on the CICIoT2023 dataset). Cyber threats are isolated and malicious nodes are amputated by automatically evoking smart contracts to immediately revoke the credentials of the compromised devices before corrupt consensus is reached.

Conclusion

Internet of Things has grown at an extremely quick pace exceeding the protection offered by traditional, centralized security protocols. This paper mathematically simulated, designed, and experimentally tested a very robust communication system combining the effectiveness of lightweight cryptography with the decentralized permanence of edge-assisted blockchain architecture. The framework significantly reduced power needs and active memory footprint on sensors with limited resources by substituting prohibitive algorithms such as AES and RSA with the NIST-compliant ASCON AEAD cipher and Elliptic Curve Cryptography. Depositing a PBFT consensus mechanism to a permissioned Hyperledger Fabric network at the edge provided cryptographically immutable logging and real-time sub-100 ms latency and resilient systemic throughput. The data ingestion layer was hardened by the integration of a tuned-down Random Forest intrusion detection system, with a 99.89% detection rate against modern and complex attack vectors, to ensure that data sent to the ledger never irreversibly polluted it. Although the framework has demonstrable performance, the geometric scalability drawbacks of the PBFT algorithm in terms of the largest number of edge validator nodes is an architectural constraint. Future studies must focus on combining dynamic sharding and Zero-Knowledge Proof (ZKP) rollups to improve global cross-domain scalability. Moreover, implement Federated Learning (FL) models as part of

the smart contracts would enable the edge nodes to jointly achieve more accurate intrusion detection without exchanging raw traffic information, which further enhances privacy and systemic resilience in the future post-quantum IoT world.

References

Obaidat, M. A., et al. (2024). Exploring IoT and blockchain: a comprehensive survey on opportunities, challenges, and applications. *Information*, 15(4), 185. https://doi.org/10.3390/info15040185

Radhakrishnan, I., Jadon, S., & Honnavalli, P. B. (2024). Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices. *Sensors*, 24(12), 4008. https://doi.org/10.3390/s24124008

Alzoubi, Y. I., et al. (2022). Integration of blockchain and IoT: challenges and solutions. *Computers and Electrical Engineering*, 103, 108342. https://doi.org/10.1016/j.compeleceng.2022.108342

Ahakonye, L. A. C., Kim, D.-S., & Nwakanma, C. I. (2024). Tides of Blockchain in IoT Cybersecurity. *Sensors*, 24(10), 3111. https://doi.org/10.3390/s24103111

Harvey, P., et al. (2025). Throughput of ASCON Compared with Popular IoT Encryption Algorithms. *Military Cyber Affairs*, 7(1), Article 1126.

Anjum, A., et al. (2025). Opportunistic access control scheme for enhancing IoT-enabled healthcare security using blockchain and machine learning. *Blockchain: Research and Applications*, 100174.

Gopalan, S., et al. (2024). Enhancing IoT Security: A Blockchain-Based Mitigation Framework for Deauthentication Attacks. *IEEE Access*, 12, 10234-10245.

Pathak, A., Al-Anbagi, I., & Hamilton, H. J. (2023). TABI: trust-based ABAC mechanism for edge-IoT using blockchain technology. *IEEE Access*, 11, 36379–36398. https://doi.org/10.1109/access.2023.3265349

Rathee, G., Ahmad, F., Jaglan, N., & Konstantinou, C. (2022). A secure and trusted mechanism for industrial IoT network using blockchain. *IEEE Transactions on Industrial Informatics*, 19(2), 1894–1902. https://doi.org/10.1109/tii.2022.3182121

Senturk, A., & Terazi, S. (2025). Blockchain-Based IoT Security and Performance Analysis. *Sakarya University Journal of Computer and Information Sciences*, 8(1), 12-26. https://doi.org/10.35377/saucis.1607145

Ghadban, R. M., et al. (2025). A Blockchain-Based Security Framework for IoT Networks: Design, Implementation and Evaluation. *Informatica*, 49(2), 159-172.

Dutta, P., et al. (2024). AI-protected Blockchain-based IoT environments: harnessing the future of network security. *Journal of Network and Computer Applications*, 103945.

Majumder, S. (2025). A Scalable Blockchain Framework for Secure IoT Communication. *International Journal of Information Engineering and Electronic Business (IJIEEB)*, 17(4), 26-40. https://doi.org/10.5815/ijieeb.2025.04.03

Natraj, N. A., Kishore, B., & Bhore, S. (2025). A lightweight blockchain framework for secure IoT data management: design, implementation and performance analysis. *SGS Engineering Science*, 1.

Ramezan, G., & Meamari, E. (2024). Zk-IoT: securing the internet of things with zero-knowledge proofs on blockchain platforms. *2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 1–7. https://doi.org/10.1109/ICBC59979.2024.10634342

Zhao, X., et al. (2024). Lightweight Authentication Protocol for Industrial IoT Using Blockchain. *IEEE Internet of Things Journal*, 11(5), 4589-4601.

Yang, Y., et al. (2021). Decentralized mutual authentication for IoT using blockchain. *IEEE Transactions on Dependable and Secure Computing*, 19(4), 2384-2396.

Barazanchi, I., & Hashim, H. (2023). Decentralized security framework for IoT devices using smart contracts. *Journal of Systems Architecture*, 134, 102789.

Maurya, V., et al. (2025). Blockchain-driven security for IoT networks: State-of-the-art, challenges and future directions. *Peer-to-Peer Networking and Applications*, Springer. https://doi.org/10.1007/s12083-024-01812-w

Elgountery, Y., et al. (2023). Blockchain Architecture for IoT: Comparative Survey. *Computer Sciences & Mathematics Forum*, 6(1), 7. https://doi.org/10.3390/cmsf2023006007

Ray, P. P., Kumar, N., & Dash, D. (2020). BLWN: Blockchain-Based Lightweight Simplified Payment Verification in IoT-Assisted e-Healthcare. *IEEE Systems Journal*, 15(1), 134–145.

Zhang, Y., Choo, K.-K. R., Gai, K., Zhu, L., & Xiao, J. (2022). Blockchain-Empowered Efficient Data Sharing in Internet of Things Settings. *IEEE Journal on Selected Areas in Communications*, 40(12), 3422–3436.

Maftei, A. A., Petrariu, A. I., Lavric, A., & Popa, V. (2023). Massive Data Storage Solution for IoT Devices Using Blockchain Technologies. *Sensors*, 23(3), 1570.

Sefati, S. S., et al. (2024). Cybersecurity in a Scalable Smart City Framework Using Blockchain and Federated Learning for Internet of Things (IoT). *Smart Cities*, 7(5), 2802–2841. [25]
Liu, X., Wang, L., & Yang, Y. (2021). Blockchain in IoT: A survey of applications, challenges, and solutions. *Future Internet*, 13(6), 137.

Blockchain-Based Iot Security and Performance Analysis - Sakarya University Journal of Computer and Information Sciences, accessed March 10, 2026, http://saucis.sakarya.edu.tr/en/download/article-file/4466356

Lightweight Encryption Algorithms for IoT - MDPI, accessed March 10, 2026, https://www.mdpi.com/2073-431X/14/12/505

Blockchain Solutions for Enhancing Security and Privacy in Industrial IoT - MDPI, accessed March 10, 2026, https://www.mdpi.com/2076-3417/15/12/6835

Trajectory Optimization for UAV-Aided IoT Secure Communication Against Multiple Eavesdroppers - MDPI, accessed March 10, 2026, https://www.mdpi.com/1999-5903/17/5/225

Lightweight cryptography for IoT: A comprehensive survey of algorithms, implementations, and standardization, accessed March 10, 2026, https://wjaets.com/sites/default/files/fulltext_pdf/WJAETS-2025-0967.pdf

Comparative Performance Analysis of Lightweight Cryptographic Algorithms on Resource-Constrained IoT Platforms - PMC, accessed March 10, 2026, https://pmc.ncbi.nlm.nih.gov/articles/PMC12473500/

(PDF) Balancing Security and Efficiency: A Power Consumption Analysis of a Lightweight Block Cipher - ResearchGate, accessed March 10, 2026, https://www.researchgate.net/publication/385547984_Balancing_Security_and_Efficiency_A_Power_Consumption_Analysis_of_a_Lightweight_Block_Cipher

Blockchain-Integrated IoT Systems: A Secure Framework for Decentralized Data Management - apecpublisher.com, accessed March 10, 2026, https://apecpublisher.com/wp-content/uploads/2025/07/FET-12-4-8.pdf

Unlocking a Promising Future: Integrating Blockchain Technology and FL-IoT in the Journey to 6G - IEEE Xplore, accessed March 10, 2026, https://ieeexplore.ieee.org/iel8/6287639/10380310/10614448.pdf

A federated edge intelligence framework with trust based access control for secure and privacy preserving IoT systems - PMC, accessed March 10, 2026, https://pmc.ncbi.nlm.nih.gov/articles/PMC12521663/

When Mathematical Methods Meet Artificial Intelligence and Mobile Edge Computing - MDPI, accessed March 10, 2026, https://www.mdpi.com/2227-7390/13/11/1779

An AI-Driven Framework for Integrated Security and Privacy in Internet of Things Using Quantum-Resistant Blockchain - MDPI, accessed March 10, 2026, https://www.mdpi.com/1999-5903/17/6/246

Tides of Blockchain in IoT Cybersecurity - PMC - NIH, accessed March 10, 2026, https://pmc.ncbi.nlm.nih.gov/articles/PMC11124985/

Blockchain Technology for IoT Security and Trust: A Comprehensive SLR - MDPI, accessed March 10, 2026, https://www.mdpi.com/2071-1050/16/23/10177

Lightweight Encryption for IoT Security | PDF | Internet Of Things - Scribd, accessed March 10, 2026, https://www.scribd.com/document/782245207/Lightweight-Encryption-Algorithms-pdf-task-1

A survey on consensus methods in blockchain for resource-constrained IoT networks, accessed March 10, 2026, https://www.semanticscholar.org/paper/A-survey-on-consensus-methods-in-blockchain-for-IoT-Salimitari-Chatterjee/621810704a37a5d03377a8ae931f0c5b3c98dcf8

A hybrid multi-node QKD-ECC architecture for securing IoT networks - PMC, accessed March 10, 2026, https://pmc.ncbi.nlm.nih.gov/articles/PMC12464159/

(PDF) Performance Evaluation of Lightweight Encryption Algorithms for IoT-Based Applications - ResearchGate, accessed March 10, 2026, https://www.researchgate.net/publication/349097545_Performance_Evaluation_of_Lightweight_Encryption_Algorithms_for_IoT-Based_Applications

Balancing Security and Efficiency: A Power Consumption Analysis of a Lightweight Block Cipher - MDPI, accessed March 10, 2026, https://www.mdpi.com/2079-9292/13/21/4325

An Adaptive Framework for Intrusion Detection in IoT Security Using MAML (Model-Agnostic Meta-Learning) - MDPI, accessed March 10, 2026, https://www.mdpi.com/1424-8220/25/8/2487

Evaluating machine learning approaches for multiple attack classification with improved computational efficiency in IoT networks - PMC, accessed March 10, 2026, https://pmc.ncbi.nlm.nih.gov/articles/PMC12618690/

Lightweight Blockchain for Authentication and Authorization in Resource-Constrained IoT Networks - IEEE Xplore, accessed March 10, 2026, https://ieeexplore.ieee.org/iel8/6287639/10820123/10925350.pdf

A Lightweight Blockchain Framework for Secure IoT Data Management: Design, Implementation and Performance Analysis - spast.org, accessed March 10, 2026, https://spast.org/techrep/article/download/5196/584/10550

A Comprehensive Survey on Lightweight Cryptographic Algorithms for IoT Devices - IJIRT, accessed March 10, 2026, https://ijirt.org/publishedpaper/IJIRT185322_PAPER.pdf

NIST Selects 'Lightweight Cryptography' Algorithms to Protect Small Devices, accessed March 10, 2026, https://www.nist.gov/news-events/news/2023/02/nist-selects-lightweight-cryptography-algorithms-protect-small-devices

Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices - ResearchGate, accessed March 10, 2026, https://www.researchgate.net/publication/381630837_Efficiency_and_Security_Evaluation_of_Lightweight_Cryptographic_Algorithms_for_Resource-Constrained_IoT_Devices

SP 800-232, Ascon-Based Lightweight Cryptography Standards for Constrained Devices: Authenticated Encryption, Hash, and Extendable Output Functions | CSRC - NIST, accessed March 10, 2026, https://csrc.nist.gov/pubs/sp/800/232/ipd

Throughput of ASCON Compared with Popular IoT Encryption Algorithms - Digital Commons @ USF - University of South Florida, accessed March 10, 2026, https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1126&context=mca

Hyperledger Fabric Blockchain for Securing the Edge Internet of Things: A Review, accessed March 10, 2026, https://journals.mmupress.com/index.php/jiwe/article/view/1198

A Blockchain-Based Security Framework for IoT Networks: Design, Implementation, and Evaluation - Informatica, accessed March 10, 2026, http://informatica.si/index.php/informatica/article/download/8122/4445

Security Audit of IoT Device Networks: A Reproducible Machine Learning Framework for Threat Detection and Performance Benchmarking - PMC, accessed March 10, 2026, https://pmc.ncbi.nlm.nih.gov/articles/PMC12736874/

Performance Evaluation of Deep Learning Models for Classifying Cybersecurity Attacks in IoT Networks - MDPI, accessed March 10, 2026, https://www.mdpi.com/2227-9709/11/2/32

Enhancing IoT security through blockchain integration - Frontiers, accessed March 10, 2026, https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2025.1670473/full

Implementation and Performance Evaluation of Elliptic Curve Cryptography over SECP256R1 on STM32 Microprocessor - Cryptology ePrint Archive, accessed March 10, 2026, https://eprint.iacr.org/2024/1121.pdf

Ascon on FPGA: Post-Quantum Safe Authenticated Encryption with Replay Protection for IoT, accessed March 10, 2026, https://www.mdpi.com/2079-9292/14/13/2668

Simulation Model for Blockchain Systems Using Queuing Theory - MDPI, accessed March 10, 2026, https://www.mdpi.com/2079-9292/8/2/234

A secure and trustworthy blockchain-assisted edge computing architecture for industrial internet of things - PMC, accessed March 10, 2026, https://pmc.ncbi.nlm.nih.gov/articles/PMC12048497/

CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment - Semantic Scholar, accessed March 10, 2026, https://pdfs.semanticscholar.org/0c46/667b9b8ec25b26084f0bb31e42d239c6b57f.pdf

Deep learning approaches for protecting IoT devices in smart homes from MitM attacks, accessed March 10, 2026, https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2024.1477501/full