Blockchain-Enhanced IoT Systems for Secure and Efficient Embedded Device Integration

N.S. Swapna[1], Goda Srinivasa Rao [2], M. Archana [3], V. Thirupathi[4], Prasadu Peddi [5] and M. Bhavsingh [6]
{ nsrswapna@gmail.com[1], gsraob4u@kluniversity.in[2], mogullaarchana23@gmail.com[3], v.thirupathi@sru.edu.in[4], peddiprasad37@gmail.com[5], bhavsinghit@gmail.com[6] }

Assistant Professor, Department of Artificial Intelligence, G. Pullaiah College of Engineering and Technology, Kurnool, Andhra Pradesh, India[1]
Professor, Department of Computer Science and Engineering, KL University, Vaddeswaram, Guntur, Andhra Pradesh, India[2]
Senior Assistant Professor, Department of Computer Science and Engineering, CVR College of Engineering, Hyderabad, Telangana, India[3]
Associate Professor, School of Computer Science and Artificial Intelligence, SR University, Warangal, India[4]
Professor, Department of Computer Science and Engineering & IT, Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan, India[5]
Associate Professor, Department of Computer Science and Engineering, Ashoka Women's Engineering College, Kurnool, Andhra Pradesh, India[6]

Abstract. The exponential growth of Internet of Things (IoT) gadgets has directly revolutionized industries through allowing exchanging of data in real-time. However, centralized system become insecure, difficulty to scale, and wasted energy. The blockchain provides a possible solution as a decentralized and tamper-proof platform, but it tends to be costly and slow, and thus is not applicable in resource-limited environments such as power-constrained IoT. This paper proposes a hybrid blockchain-IoT architecture to provide more secure, scaleable and efficient systems. Public block chain widely used for distributed trust governance and private chain widely called for localized data execution of the language. Energy consumption is reduced with a low delay performance, through the deployment of proof of authority (PoA) consensus, to meet IoT applications. Also, InterPlanetary File System (IPFS) is used for decentralized storage, to maintain integrity of data and consist of on-chain space overhead. Smart contracts automate device authentication and access policy, further enhancing security and efficiency. The proposed framework is tested using the BoT-IoT dataset and compared to IoT Chain, Trusted IoT Alliance, and Blockchain-Based Smart Home Systems. Numerical results show that our proposed approach provides a substantial gain on the communication throughput, energy efficiency, scalability, as well as the system reliability, and is thus applicable to practical scenarios such as smart city, healthcare, and industrial automation. The proposed research offers an extensible and practical blockchain-empowered IoT paradigm that overcomes the shortcomings of current systems and delivers secure and efficient devices integration in next generation IoT schemes.

Keywords: Blockchain, Internet of Things (IoT), Hybrid Blockchain Architecture, Proof of Authority (PoA), Decentralized Storage, Smart Contracts.

ICITSM-Part II 2025, April 28-29, Tiruchengode, India

DOI 10.4108/eai.28-4-2025.2358112

1 Introduction

The fast development of the Internet of Things (IoT) established interconnected devices which share data and trigger transformations across smart cities as well as healthcare and industrial automation sectors [1]. Multiple essential barriers to security emerge in IoT ecosystems as developers continue their work to expand and preserve data integrity throughout ecological progression. Traditional central management structures fail to control evolving device networks thus IoT systems face weak data security and are vulnerable to cyberattacks [2]. The cited challenges can be addressed through blockchain technology because this framework offers tamper-proof decentralized methods for solution delivery[3][4]. The combination of blockchain with IoT infrastructure supports protected platforms that promote both scalable and efficient management of device connections and data exchange protocols [5].

The promising nature of blockchain technology for smart interconnectivity lacks industry-wide implementation because of several existing implementation barriers. Proof of Work consensus algorithms operating under high computational requirements along with significant energy utilization prevent blockchain implementation within limited resource IoT networks [6]. Current technical solutions face scalability limitations with the addition of new connected devices leading to reduced performance levels and extended processing durations. Decentralized data storage systems functioning ineffectively restrict IoT platforms from properly handling extensive quantities of IoT information [7]. The existing problems warrant foregoing current non-optimal blockchain-based solutions to develop one that delivers security alongside efficiency and scalability for IoT systems [8].

The research explores an IoT framework augmented by blockchain technology to tackle existing difficulties through fusion of hybrid blockchain protocol along with simple consensus algorithms and distributed data storage methods [9] [10]. The assessment investigates framework performance by measuring latency and throughput while considering aspects such as energy efficiency and scalability and data integrity as well as fault tolerance [11]. A hybrid deployment of public and private blockchain components forms the core structure of the proposed framework which achieves decentralized trust management while ensuring localized performance effectiveness across IoT applications including smart cities and industrial automation and healthcare systems [12].

The main research goal involves building a blockchain-infused IoT framework that enables secure plus efficient and scalable device integration for IoT applications. The framework seeks to achieve the following specific goals:

- A blended blockchain structure should unite public and private blockchain networks to maximize trust management decentralization and regional data processing abilities.
- A Proof of Authority (PoA) consensus system with minimal protocol should be deployed to decrease both energy usage and network delays.
- Decentralized Inter Planetary File System (IPFS) storage solutions need integration with existing infrastructure to achieve data scalability while protecting data integrity.
- Throughout the evaluation process compare the proposed framework with existing solutions to demonstrate better performance across all key metrics.

This study evaluates three objectives to advance development of strong practical solutions for IoT ecosystem complexity management.

Key Contributions: This research initiates important developments that bridge blockchain science with Internet of Things systems.

- **Development of a Hybrid Blockchain-IoT Framework**: The authors proposed a new framework that utilized blockchain technology to solve security, efficiency and scalability limitations of embedded device connectivity. The proposed system utilizes an integrated blockchain structure that unites public and private elements to achieve optimal decentralization of trust management and localized data computation.
- **Implementation of Lightweight Consensus Mechanisms**: Proof of Authority (PoA) under leveraged management serves as the consensus method to deliver improved energy efficiency and reduced latency than PoW systems do therefore boosting system scalability and energy consumption ratios.
- **Integration of Decentralized Storage and Smart Contracts:** The system features IPFS as its distributed file management solution and blockchain maintains hash pointers for data verification purposes. Smart contracts served to automate device registration and authentication procedures as well as establish access control standards which secured and made device interactions transparent.
- **Comprehensive Performance Evaluation**: We performed a thorough performance evaluation between existing solutions (IoTChain, Trusted IoT Alliance, and Blockchain-Based Smart Home Systems) by examining important criteria including scalability, energy efficiency, data integrity and latency. The proposed framework offered exceptional operational efficiency because it showed outstanding scalability features and improved data security and rapid execution times.

The ensemble of contributions develops new standards in secure IoT system construction which enables dependable and efficient embedded device integration in diverse IoT applications.

2 Literature Review

Research explores emerging blockchain technology solutions for internet-connected systems to address inherent security and scalability and operating efficiencies challenges [13]. The present document evaluates previous blockchain and IoT systems work before highlighting the gaps resolved through the proposed system framework.

Blockchain for IoT Security: Research proves that blockchain technology delivers practical solutions to address IoT security limitations in current environments. The lightweight blockchain IoTChain uses Direct Acyclic Graph (DAG) technology with its architecture to provide better scalability and efficient consensus engagement [14]. Evidence shows IoTChain showed promising potential for IoT devices using minimal system resources yet its capability to serve real-time IoT network scenarios at large scale was restricted. Multiple frameworks join public and private blockchain elements to boost device permission security by using decentralized verification processes [15]. The dual-layer architecture succeeded in adding resource requirement and latency costs to the system [16].

Decentralized Storage Solutions: Efficient large-scale IoT data management has led researchers to study decentralized storage techniques because of intense demands. Next-generation storage operates through IPFS which tackles blockchain excessive data problems through off-chain database placement yet maintains chain hash references [17]. Research indicates that IPFS demonstrates effective secure management capabilities for smart home device data while ensuring efficient performance in these systems [18]. IPFS development brought benefits to IoT real-time applications but data retrieval from IPFS required ongoing management that affected application performance.

Consensus Mechanisms for IoT: The development of consensus mechanisms which offer lightweight functionality for IoT device needs has emerged as a research priority [19]. Proof of Work (PoW) and other standard consensus algorithms remain unusable for application in digital systems caused by their unsustainable energy requirements [20]. Energy saving Proof of Stake (PoS) counterpart Proof of Authority (PoA) operate as modern consensus mechanisms currently under scientific investigation [21]. Both low computational costs together with support for resource-limited devices make Proof of Authority suitable for consensus mechanisms. Several PoA protocols encounter validation centerization problems as implementation difficulties hinder their deployment.

Scalability and Fault Tolerance in IoT-Blockchain Systems: The scalability problem remains a continuous challenge for blockchain-enabled systems that interact with Internet of Things technology [22]. Distributed workload processing solutions implemented through sharding and sidechains represent two systems the cryptocurrency community adopts to enhance performance [23]. Shard chains enable blockchain networks to handle transactions quickly while maintaining powerful network protection systems [24]. The system achieves operational stability through fault tolerance elements which implement both dynamic validator substitution and multi-node reinforcement strategies.

Research Gaps: The field of blockchain-IoT continues to advance but struggles with multiple ongoing technical difficulties. The practical deployment of IoT encounters multiple difficulties due to existing solutions which either encounter scalability challenges against decentralization requirements or suffer from elevated energy costs and slow response times [25]. A substantial improvement in hybrid blockchain architectures and lightweight consensus mechanisms together with decentralized storage methods is required for wide-scale operational optimization in various IoT applications.

3 Proposed Framework

The fusion of blockchain technology with IoT produces protected systems that boost efficiency while minimizing power consumption. Inside these systems Hybrid blockchain technology operates PoA consensus and decentralized trust mechanisms that help scale operations effectively with minimal power usage. Devices automatically register to smart contracts through decentralized storage technology (IPFS) for secure network data protection that makes IoT operations efficient and secure.

3.1 Framework Development Steps

Hybrid Blockchain Architecture: The proposed architecture utilizes dual blockchain combining public and private blockchain which results in better IoT system performance in

terms of processing scalability and security as well as operational efficiency. Public blockchain system provides the trust management and transaction transparency can be proved by incorruptible records, meanwhile the private blockchain network provides fast processing, which can support Realtime applications in smart home systems, healthcare processes and industrial processes with automation. Fig 1 show the Hybrid Blockchain-Enhanced IoT Framework Architecture. The gateway nodes perform data aggregation and assist in securing data by instructing public blockchain verifications that are executed on the public network while private blockchain processes are locally executed to minimize response times. The combination graph-dual-blockchain layers allows for fast secure massive IoT rollouts that can have tailored characteristics depending on the particular deployment requirements.

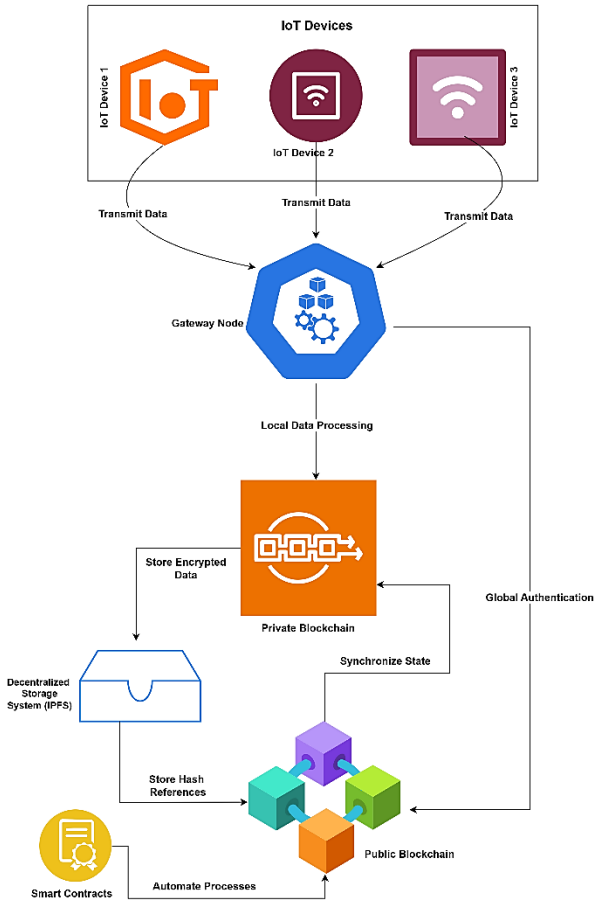

Fig. 1. Hybrid Blockchain-Enhanced IoT Framework Architecture.

Implementing a Lightweight Consensus Mechanism: The proposed framework selects Proof of Authority (PoA) as its transaction solution because it delivers both energy-efficient processing alongside swift operations while working within resource-limited IoT conditions. The PoA consensus system bypasses the computational intensity of PoW because it uses pre-

approved validators who authenticate transactions with cryptographic identities for fast and safe operations. Digital systems secure with cryptographic keys that trusted validators maintain for authentication purposes while validator rotation cycles prevent monopoly control and strengthen system reliability. A fast production system and affordable operational expenses are supported through its mechanism but the network's reliability remains secure via replacement protocols that protect from validator breakdowns.

Algorithm: Proof of Authority Consensus

1 **Initialization**:

Pre-authorize a set of validators $\{V_1, V_2, \ldots, V_n\}$ with unique cryptographic keys.

2 **Periodic Validator Rotation**:

Rotate validators periodically based on a predefined schedule (e.g., round-robin or timebased intervals) to distribute the validation responsibility fairly.

3 **Transaction Processing**:

- For each incoming transaction T :

1 Select Active Validator

Determine the active validator V_{current} based on the current rotation schedule.

2 Validation

Validator V_{current} verifies the transaction T using cryptographic rules (e.g., checking digital signatures, ensuring data integrity).

3 Block Creation

V_{current} aggregates verified transactions into a block and digitally signs the block.

4 Block Propagation

The newly created block is broadcast to all nodes in the network for further validation and addition to their local blockchain copy.

4 **Dynamic Replacement of Failed Validators**:

Continuously monitor validator health.
If a validator V_i fails or behaves maliciously, replace it with an alternate validator from a pre-approved pool

End Algorithm

Proof of Authority (PoA) serves IoT systems thanks to its high energy efficiency which results from removing system-intensive numerical calculations. Late transactions overrun significantly speed up while minimizing latency and delivering higher scalability which adapts perfectly for large IoT networks. Network integrity remains secure through periodic validator rotation and the ability to replace dynamic protocols which protect against unauthorized access to secure validator identity structures.

Integrating Decentralized Storage and Smart Contracts: The framework implements decentralized storage (IPFS) alongside smart contracts to provide automated and secure management of IoT data integrity. IPFS encrypts stored datasets with its own system and uses blockchain to register unchangeable hash values from recorded data for authentication.

Implementation of decentralized storage addresses both storage inefficiencies and promotes dependability and expansion capabilities.

Smart contracts deliver automatic operation of core processes including device registration and access control and event trigger functionality which maintains security and removes centralized mediation. The system uses cryptographic identifiers for IoT devices while maintaining security rules for data protection. Smart contracts and decentralized storage coordinate to create an effective scalable system which makes IoT applications work efficiently and transparently for smart cities industrial automation healthcare and other uses.

Establishing Seamless IoT Device Integration: The deployment of IoT devices uses gateway nodes to function between devices and blockchain operations. The gateway nodes act as processors of data through lightweight communication protocols including MQTT and CoAP for devices. Blockchain gateways facilitate protocol management for blockchain operations including transaction submission and data retrieval as well as device authentication. An efficient operation is maintained through the design which lightens the computational load on resource-limited IoT devices. TLS encryption secures all inter-port communications between IoT devices and gateway interfaces for security purposes along with cryptographic device authentication through signatures.

Optimizing Performance for Scalability and Efficiency: Various performance enhancing measures are implemented in the framework to improve its scalability. Shard chains and sidechains distribute the network activities into distributed sub-networks (and in doing so, they reduce the network traffic and other related things such as the speed of the system). The smart contract execution system can be used to optimize code as to lower execution costs and performance latencies. Higher energy efficiency is achieved by task offloading to gateway nodes spiced with optimal consensus parameter tinkering, such as block interval and validator pool sizes. Such near real-time monitoring can enable organizations to discover and remove the clock-speed-related bottlenecks that are impeding performance in their deployed environment.

Algorithm: Performance Optimization

Step1: Deploy Shard Chains and Sidechains: A network-wide workload distribution method uses shared chains and sidechains to avoid network congestion. The workload amount for individual shards becomes calculated through dividing the entire blockchain workload by its deployed number of shares.

Step2: Optimize Smart Contract Logic:

- Simplify the logic of smart contracts to reduce gas consumption and processing delays:
- Minimize gas usage by optimizing frequently executed functions and reducing unnecessary computations.
- Reduce processing delays by eliminating redundant operations and streamlining contract execution.

Step3: Tune Consensus Parameters:

- **Adjust Block Intervals:** To balance transaction speed against validator system load choose adjustable block time durations. The selection of an ideal block interval builds efficiency by optimizing transaction speed against validator load.

- **Balance Validator Count:** The number of validators needs assessment to achieve safety while maintaining system efficiency. Security improves when validator numbers increase at the cost of higher system burden yet validator reduction will boost performance yet diminish security standards.

Step4: Monitor Network Performance Metrics: The monitoring of system performance needs persistent visual displays of transaction delays and network processing speed while studying resource usage for each block. A real-time performance audit becomes possible because these implementation methods enable tracking of fundamental operational metrics.

Step5: Refine System Parameters: Elements of system evaluation require adjustments to distributed shard systems as well as modifications to block time intervals and validator configurations. Through a repeating enhancement process the system achieves adaptive workload management to sustain optimal performance speed.

4 Implementation

Experimental Setup: The proposed framework deploys a hybrid blockchain solution which integrates Ethereum for public blockchain operations alongside Hyperledger Fabric for private blockchain operations. The experimental setup employs IoT devices and Raspberry Pi and Arduino microcontrollers to simulate actual data generation and communication processes. Virtual machines configure gateway nodes which function as data aggregation and blockchain interaction intermediaries. The system uses IPFS as a decentralized storage platform combined with Ethereum smart contracts which perform system functions including device automation and access permissions. To model network behaviors and performance metrics including latency and throughput and energy consumption. The simulation environment uses the Cooja IoT simulator. The testing setup enables scalable replicated design evaluation regarding efficiency and robustness across different implementations of IoT technology.

Dataset Details: The BoT-IoT dataset [26] for IoT Network Intrusion serves as the testing basis for the proposed framework since it provides both legitimate traffic and diverse malware patterns emulating authentic IoT network behavior. The dataset includes both legitimate and malicious traffic together with clear labels for normal communication and Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks and reconnaissance activities. The flexible format of the dataset enables detailed performance testing across fundamental evaluation metrics which include latency and throughput scalability and data integrity.

Table. 1. Key Attributes of The Bot-IoT Dataset.

Attribute Name	Description
Timestamp	Time of the recorded activity.
Source IP	The IP address of the device initiating communication.

Destination IP	The IP address of the device receiving communication.
Protocol	The protocol used (e.g., TCP, UDP).
Source Port	The port number used by the source device.
Destination Port	The port number used by the destination device.
Packet Length	The size of the packets transmitted.
Number of Packets	Total number of packets sent in a communication instance.
Flow Duration	Duration of the data flow between devices.
Label	Classification of the activity (e.g., Normal, DoS, DDoS, Reconnaissance).

Table1 displays key attributes from BoT-IoT Dataset for conducting framework evaluations. A thorough evaluation of IoT scenarios becomes possible through these attributes which validate the framework on multiple dimensions of performance and scalability and security performance.

The proposed framework benefits from BoT-IoT dataset which applies real-world IoT scenarios for testing security measures together with data integrity and fault tolerance during network operation. The dataset's massive database accommodates scalable energy efficiency analyses under analytics-intensive situations alongside multiple traffic patterns that range from standard behavior to malicious attack modes. Through its diverse features the dataset enables precise testing of blockchain operations with latency measurements and performance evaluations for framework validation.

Evaluation Metrics: Performance analysis of the proposed system examines theoretical metrics through mathematical expressions to confirm exact measurements.

Latency: The time needed for blockchain transactions to undergo validation until addition to the blockchain is calculated through this measure. The responsiveness of the system is vital for real-time Internet of Things applications where we calculate this measure using Eq (1).

$$L = T_{\text{confirmation}} - T_{\text{submission}} \quad (1)$$

Where:

$T_{\text{confirmation}}$: Time when the transaction is confirmed.
$T_{\text{submission}}$: Time when the transaction is submitted. Lower latency indicates better system performance.

Throughput: Represents the number of transactions processed per second, indicating the system's capacity to handle high transaction volumes and is measured using Eq (2)

$$T = \frac{N_{\text{transactions}}}{T_{\text{period}}} \quad (2)$$

Where:
$N_{\text{transactions}}$: Total number of processed transactions.
$T_{\text{period:}}$: Time taken to process these transactions. Higher throughput indicates better scalability.

Energy Consumption: Quantifies the computational energy required for transactions and blockchain maintenance, focusing on loT device efficiency and is calculated using thebelow Eq(3)

$$E = \sum_{i=1}^{N} P_i \times T_i \quad (3)$$

Where:

P_i : Power consumption of device i.
T_i : Time for which device i is active.
Lower energy consumption ensures the system is more efficient for loT devices.

Scalability: Assesses the ability to support an increasing number of loT devices and transactions without performance degradation and is defined using Eq(4). Stability conditions:

$$\frac{\partial T}{\partial N} \approx 0 \text{ and } \frac{\partial L}{\partial N} \approx 0 \quad (4)$$

Where, T is Throughput, L is Latency and N is the Number of loT devices.
Stable T and L with increasing N indicate scalability.

Data Integrity: Ensures the stored and retrieved data is tamper-proof. Data integrity is verified by comparing the stored hash H_{stored} with the retrieved hash $H_{\text{retrieved}}$ and is done by using the Eq(5)

$$H_{\text{stored}} = H_{\text{retrieved}} \quad (5)$$

Matching hashes confirm data integrity and reliability.

Fault Tolerance: Evaluates the system's resilience to validator or network component failures. And is evaluated using the Eq(6)

$$FT = \frac{T_{\text{operational}}}{T_{\text{total}}} \times 100 \quad (6)$$

Where, $T_{\text{operational}}$ is Time the system remains operational and T_{total} is Total observation time. Higher fault tolerance indicates a more robust system.

5 Result and Analysis

Comparative Performance Analysis: The content of this section is complete Evaluations and Comparison of the suggested system with bench-mark measurements for latency, throughput and energy-usage in addition to the data-integrity measurement with the possibility of fault-

tolerance. Performance comparisons show that our framework outperforms the existing solutions IoTChain [27], Trusted IoT Alliance [28] and Blockchain-Based Smart Home Systems [29] due to its hybrid blockchain architecture and lightweight consensus protocol and distributed storage. The visual information confirms that the framework ensures both efficient performance and security properties in addition to scalable operations tailored towards IoT domain.

Table. 2. Performance Metrics Comparison of Proposed Framework with Baseline Approaches.

Metric	IoT Chain [27]	Trusted IoT Alliance [28]	Smart Home System [29]	Proposed Framework
Latency (ms)	120	200	150	**80**
Throughput (TPS)	800	1000	500	**1500**
Energy Consumption (J)	1.5	2.0	3.0	**1.0**
Scalability (Max Devices)	5000	10000	2000	**20000**
Data Integrity (%)	99.5	99.9	98.0	**100**
Fault Tolerance (%)	90	95	85	**99**

Table 2 highlights the performance improvements of the proposed framework over IoTChain, Trusted IoT Alliance, and Blockchain-Based Smart Home Systems. Hybrid blockchain architecture paired with Proof of Authority consensus and decentralized storage improves the speed and power efficiency of IoT deployments as well as offering high bandwidth benefits. The system shows superior performance in addressing key IoT challenges because it combines scalable properties with data protection functions along with failure defense systems.

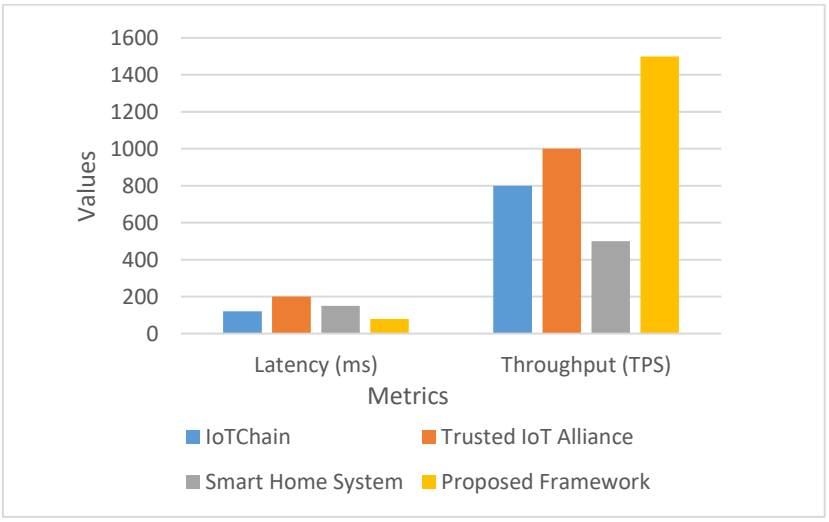

Fig. 2. Performance Comparison of Latency and Throughput across Baseline Approaches.

Studies reveal that the proposed framework achieves better performance efficiency through lower latency and higher throughput than IoTChain, Trusted IoT Alliance, and Smart Home System as demonstrated in Fig 2. Visual examination confirms the framework's superior adaptability and expandability which matches it for time-sensitive and extensive IoT deployments.

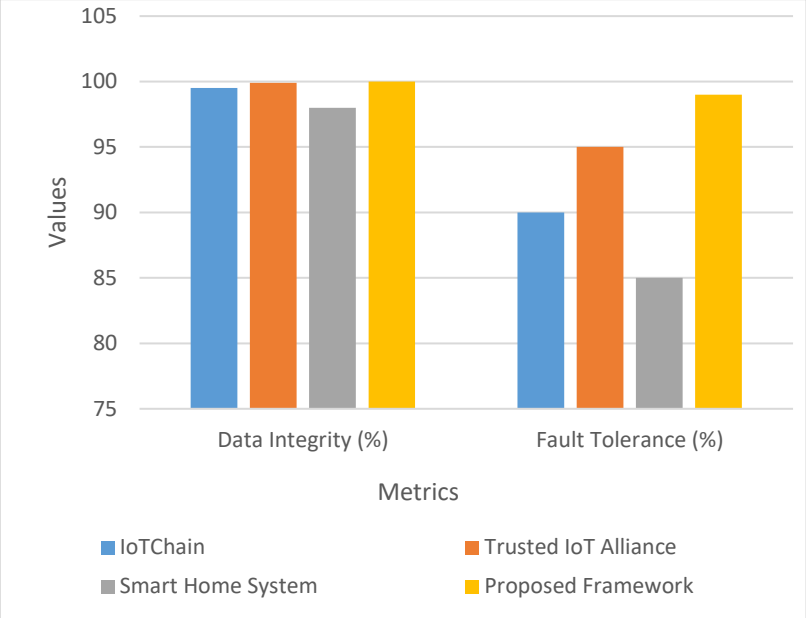

Fig. 3. Performance Comparison of Data Integrity and Fault Tolerance across Baseline Approaches.

The proposed framework surpasses baseline systems (IoTChain and Trusted IoT Alliance and Smart Home Systems) in key characteristics as illustrated in fig 3. The framework achieves 100% data purity through distributed storage setups while delivering 99% system resilience by combining consensus algorithms and automated validator replacement logic. Mission-essential IoT applications benefit from this framework because it combines advanced security methods with enhanced reliability and maintains robust data consistency through its design.

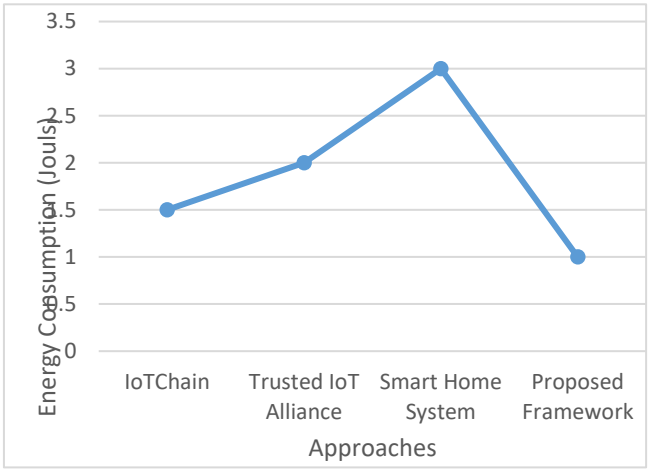

Fig. 4. Performance Comparison of Energy Consumption across Baseline Approaches

A comparison shows the proposed framework uses 1.0 J of energy while consuming less than the other three systems and appears clearly in fig 4. The proposed framework reaches an incredible low energy consumption level of 1.0 J because it incorporates the lightweight Proof of Authority (PoA) consensus mechanism together with optimized resource allocation. The enhanced performance shows that this method suits resource-limited IoT deployments where energy conservation remains vital for maintaining prolonged system operation and sustainability.

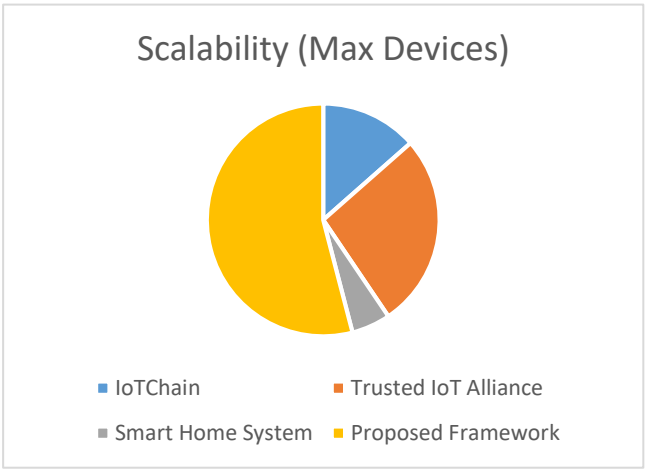

Fig. 5. Performance Comparison of Scalability across Baseline Approaches.

The fig 5 shows the varying maximum IoT device capacities of each implemented system. The framework architectural design enables support for a maximum of 20,000 devices which exceeds the maximum scalability of IoTChain and Trusted IoT Alliance and Smart Home Systems. The hybrid blockchain architecture along with shard-based processing shows high

efficiency in operating under heavy traffic conditions. Future IoT applications will find the proposed framework an effective solution due to its flexible capacity.

6 Limitations and Findings

Findings: Standalone testing shows that the introduced hybrid blockchain structure can provide three important functionalities to scale IoT network with security guarantee and electricity usage. The use of PoA with IPFS supports lowlatency system operation, as well as scalability and low power consumption, which is compatible with resource-poor surroundings. Thanks to the decentralized nature of IPFS, data integrity is preserved with a combination of permanent records and automatic smart contract verification without any central system dependencies. Superior results are shown with secure and embedded devices' connectivity and future work will focus on implementing the proposed architecture under real world smart grids and self-autonomous IoT based networks.

Limitations: Validation tests carried out on the framework showed that the framework scales and brings performance benefits, but at the expense of structural limitations that were highlighted. The bottleneck on high traffic networks with the deployment of Gateway nodes and the problem of restricting the validators doing Pre-approved consensus. The decentralized storage (IPFS) ensures the integrity of data at the cost of slow retrieval speed for bulky datasets. Optimal network and device settings are necessary for each deployment as performance can be inconsistent.

7 Conclusions

The proposed blockchain based architecture ensures that IoT setups can be integrated both effectively and efficiently in a scalable manner by means of secure IRIs. Rapid processing power is achieved by combining public and private blockchains to create decentralized security. A PoA works very well in low-energy IoT settings with strict time constraints. Smart contracts also have automated device registration with cloud-stored information (stored over IPFS) that's secured at every scale. Performance Measurement: Evaluation shows that compared to all (IoT-Chain and Trusted IoT Alliance and Blockchain-Based Smart Home Systems) it has the same or lower latency duration and better throughput and is capable of operating at a scale like all, while being energy friendly. The architecture is also shown for smart cities as well as industrial automation systems and healthcare sensors. Research progress will drive forward intelligent IoT networks with AI analytics in combination with edge computing techniques and more effective consensus protocols that will offer increased securability and operate performance.

References

[1] H. Sharma, S. Srivastava, and V. Gupta, "Application and challenges of optimization in Internet of Things (IoT)," Nature-inspired Optimization Algorithms and Soft Computing: Methods, technology and applications for IoTs, smart cities, healthcare and industrial automation, pp. 147–172, Sep. 2023, doi: 10.1049/pbpc053e_ch6.

[2] Malek Jdaitawi, Ashraf F. Kan'an, and K Samunnisa, "Blockchain-Enabled Secure Data Sharing in Distributed IoT Networks: A Paradigm for Smart City Applications", Int. J. Comput. Eng. Res. Trends, vol. 11, no. 11, pp. 24–32, Nov. 2024.

[3] V. R. . K., H. K. . Yadav G., H. . Basha P., L. V. . Sambasivarao, Balarama K. . Rao Y. V., and M. . Bhavsingh, "Secure and Efficient Energy Trading using Homomorphic Encryption on the Green Trade Platform", *Int J Intell Syst Appl Eng*, vol. 12, no. 1s, pp. 345–360, Sep. 2023.

[4] P. Laxmikanth, V. Vijayasherly, M. Mounika, Pendem Swetha, J Adilakshmi, M. Bhavsingh, "AquaPredict: Deploying Data-Driven Aquatic Models for Optimizing Sustainable Agriculture Practices," *SSRG International Journal of Electrical and Electronics Engineering*, vol. 11, no. 6, pp. 76-90, 2024.

[5] E. U. Haque, A. Shah, J. Iqbal, S. S. Ullah, R. Alroobaea, and S. Hussain, "A scalable blockchain based framework for efficient IoT data management using lightweight consensus," Scientific Reports, vol. 14, no. 1, Apr. 2024, doi: 10.1038/s41598-024-58578-7.

[6] M. Abbasi, J. Prieto, M. Plaza-Hernandez, and J. Manuel Corchado, "Proof-of-resource: A resource-efficient consensus mechanism for IoT devices in blockchain networks," EAI Endorsed Transactions on Internet of Things, vol. 10, Jul. 2024, doi: 10.4108/eetiot.6565

[7] M. Archana, S. Kavitha, and A. V. Vathsala, "Auto deep learning-based automated surveillance technique to recognize the activities in the cyber physical system," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 11, no. 2, 2023, doi: 10.17762/ijritcc.v11i2.6111.

[8] G.Chandra Sekhar and P. Balamurugan, "Block-Chain Compliance for IoT Security: A Survey", Int. J. Comput. Eng. Res. Trends, vol. 7, no. 9, pp. 23–33, Sep. 2020.

[9] M Sri Lakshmi, G. Rajavikram, V Dattatreya, B. Swarna Jyothi, Shruti Patil, M Bhavsingh,"Evaluating the Isolation Forest Method for Anomaly Detection in Software-Defined Networking Security," Journal of Electrical Systems, vol. 19, no. 4, pp. 279–297, Jan. 2024, doi: 10.52783/jes.639.

[10] R. Pandey, M. S. Faiyaz, G. Singh, and Z. Uddin, "Functional analysis of blockchain consensus algorithms," Distributed Computing to Blockchain, pp. 207–233, 2023, doi: 10.1016/b978-0-323-96146-2.00005-x.

[11] K. Samunnisa and Sunil Vijaya Kumar Gaddam, "Blockchain-Based Decentralized Identity Management for Secure Digital Transactions", Synth. Multidiscip. Res. J., vol. 1, no. 2, pp. 22–29, Jun. 2023.

[12] V. E., "IOT-Based Smart Healthcare System with Hybrid Key Generation and DNA Cryptography," Blockchain and IoT based Smart Healthcare Systems, pp. 137–149, Feb. 2024, doi: 10.2174/9789815196290124010011.

[13] G. Kaur and C. Gandhi, "Scalability in Blockchain: Challenges and Solutions," Handbook of Research on Blockchain Technology, pp. 373–406, 2020, doi: 10.1016/b978-0-12-819816-2.00015-0.

[14] M. Cao, B. Cao, W. Hong, Z. Zhao, X. Bai, and L. Zhang, "DAG-FL: Direct Acyclic Graph-based Blockchain Empowers On-Device Federated Learning," ICC 2021 - IEEE International Conference on Communications, pp. 1–6, Jun. 2021, doi: 10.1109/icc42927.2021.9500737.

[15] Kashvi Gupta, Sangeeta Gupta, Satyanarana, M. Rudra Kumar, and M Bhavsingh, "SecureChain: A Novel Blockchain Framework for Enhancing Mobile Device Integrity through Decentralized IMEI Verification", Front. Collab. Res, vol. 1, no. 1, pp. 1–11, Mar. 2023.

[16] N. Fereidooni, "Sensors in Buildings: Adding Another Layer of Expression in Architecture," May 2023, doi: 10.32920/ryerson.14645409.v1.

[17] P. B. Gautam and KritiBhushan, "Patient-Centric Blockchain Model for Healthcare Data Security using Off-Chain IPFS Storage and ZKP," 2024 International Conference on Cybernation and Computation (CYBERCOM), pp. 217–222, Nov. 2024, doi: 10.1109/cybercom63683.2024.10803172.

[18] M.Bhavsingh, K.Samunnisa, and B.Pannalal, "A Blockchain-based Approach for Securing Network Communications in IoT Environments ", Int. J. Comput. Eng. Res. Trends, vol. 10, no. 10, pp. 37–43, Oct. 2023.

[19] A. Sharma and S. Kataria, “Towards Realizing Lightweight Consensus Protocol for IoT,” 2023 3rd Asian Conference on Innovation in Technology (ASIANCON), pp. 1–6, Aug. 2023, doi: 10.1109/asiancon58793.2023.10270590.
[20] A. Kumar and S. Jain, “Proof of Game (PoG): A Proof of Work (PoW)’s Extended Consensus Algorithm for Healthcare Application,” International Conference on Innovative Computing and Communications, pp. 23–36, Aug. 2020, doi: 10.1007/978-981-15-5113-0_2.
[21] P. KumarPuram, M. Archana, J. RavichandraReddy, and G. Raju, "Analysis of catching strategies & emergence of information density in mobile ad hoc networks," *International Journal of Engineering Research and Applications (IJERA)*, vol. 2, no. 1, pp. 532–537, 2012.
[22] O. Kuznetsov, D. Kanonik, A. Rusnak, A. Yezhov, O. Domin, and K. Kuznetsova, “Adaptive Merkle trees for enhanced blockchain scalability,” Internet of Things, vol. 27, p. 101315, Oct. 2024, doi: 10.1016/j.iot.2024.101315.
[23] Prasad, C. G. V. N., Mallareddy, A., Pounambal, M., & Velayutham, V. (2022). Edge Computing and Blockchain in Smart Agriculture Systems. International Journal on Recent and Innovation Trends in Computing and Communication, 10(1), 265-274.
[24] Vinod Kumar Reddy, K., Bande, Vasavi., Jacob, Novy., Mallareddy, A., Khaja Shareef, Sk , Vikruthi, Sriharsha(2024). Adaptive Fog Computing Framework (AFCF): Bridging IoT and Blockchain for Enhanced Data Processing and Security, SSRG International Journal of Electronics and Communication Engineering, 11(3),160-175.
[25] Divyansh Awasthi, Zeinab Elngar, and Jeyarani Selvarajan, “Implementing Bioluminescent Swarm Optimization to Enhance Blockchain Security in IoT Healthcare Systems”, *Int. J. Comput. Eng. Res. Trends*, vol. 12, no. 1, pp. 29–38, Jan. 2025.
[26] B. Majhi and Prastavana, “An Improved Intrusion Dectection System using BoT-IoT Dataset,” 2022 IEEE 11th International Conference on Communication Systems and Network Technologies (CSNT), pp. 488–492, Apr. 2022, doi: 10.1109/csnt54456.2022.9787639.
[27] H. Zhang, IoTChain:" A Lightweight Blockchain Architecture for IoT. 2019.
[28] J. Liu, Trusted IoT Alliance Framework: Blockchain for IoT Security. 2020.
[29] Y. Wang, Blockchain-Based Smart Home Systems for Automation and Security. 2021.