ISSN 2409-2665
Journal of Logistics, Informatics and Service Science
Vol. 12 (2025) No. 4, pp. 146-177
DOI:10.33168/JLISS.2025.0409

Hybrid Blockchain Software Defined Network Architecture for Secure and Energy Efficient Iot Routing

Rupali Vairagade[1*], Leela Bitla[2], Ritu Pawar[2], Shilpa Ghode[2]

[1*]Cyber Security Department, Shah & Anchor Kutchhi Engineering College, Mumbai, India 400088

[2]Department of Information Technology,G H Raisoni College of Engineering, Nagpur

CRPF Gate, No.3, Hingna Road, Digdoh Hills, Nagpur, Maharashtra 440016

scholar.rupalivairagade123@gmail.com (Corresponding author), scholar.leelabitla213@gmail.com

Abstract: The integration of Internet of Things (IoT) devices with Software-Defined Networks (SDN) present significant challenges in security, trust management and energy efficiency. Traditional blockchain-integrated protocols suffer from high computational overhead and poor scalability under malicious attacks. This paper proposes Hybrid Blockchain-based Secure SDN-IoT Routing Framework (HB-SDN-IoT), a novel hybrid blockchain based secure routing framework that combines centralized SDN control with decentralized blockchain trust mechanism. The framework employs a dual-layer blockchain architecture using lightweight Proof-of-Authority (POS) for intra cluster operations and Proof-of-Work (PoW) for inter-controller communications. An energy-aware clustering algorithm dynamically selects cluster heads based on trust metrics and residual energy. Comprehensive MATLAB simulations demonstrate that HB-SDN-IoT achieves 23% energy reduction, 96.8% packet delivery ratio and 93.6% trust accuracy while maintaining robust security against Sybil and black hole attacks compared to existing protocols including AODV, DSDV and blockchain based alternatives. The proposed architecture addresses scalability and real-time responsiveness challenges while significantly improving data integrity, routing robustness, and energy efficiency, offering a promising paradigm for secure, intelligent IoT communications in heterogeneous and adversarial network environments.

Keywords: Software Defined Networking (SDN), Internet of Things, Hybrid Blockchain-based Secure SDN-IoT Routing Framework, adversarial network environments.

1. Introduction

The proliferation of Internet of Things (IoT) devices in industrial, healthcare, and smart city applications has brought about complex networking challenges related to secure routing (Yi, Su, et al., 2018), scalability, and energy management. In particular, heterogeneous node capabilities, intermittent connectivity, and resource constraints hinder the deployment of robust trust-based communication models in distributed environments (Xu, Ji, et al., 2018) (Rahouti, Xiong, 2020) (Tan, Yu, et al., 2021). Traditional routing protocols often fail to adapt dynamically to changing trust states or energy availability (Ahn, Gu, et al., (2019), leaving the network vulnerable to threats such as Sybil attacks, black hole routing, and denial-of-service (DoS) (Zhou, Zhang, et al., 2017).

Security mechanisms in recent literature address mutual authentication (Aghili, Mala, 2018), data integrity, user privacy (Mustafa, Khan, et al., 2020), and confidentiality assurance (Yagisawa, 2017). However, integrating these mechanisms often introduces computational and energy overhead, which is particularly problematic for battery-powered IoT devices. Optimizing energy usage is essential not only to extend device life but also to ensure system scalability. Although edge collaboration and congestion control techniques have been explored to reduce power consumption (Han, Shen, et al., 2020), (Vairagade, SH, et al., 2022), trade-offs between performance and security persist. The key challenge lies in deploying robust encryption and trust models without overwhelming the constrained resources of IoT nodes (Ara, Prabhkar, et al., 2019), (Ibrahim, Dalkılıc, 2019). Fog and edge computing have emerged as viable solutions to mitigate processing loads and improve responsiveness. Nevertheless, these paradigms also introduce energy costs and are susceptible to routing inefficiencies and security vulnerabilities (Bodkhe, Mehta, et al., 2020), (Santatra Hagamalala Bernardin, Franck Morvan, et al., 2025). Ensuring data confidentiality, integrity, and adaptive control while maintaining low energy consumption remains a complex problem. The goal is to achieve integrated security and energy management through a unified framework that can adapt to heterogeneous IoT deployments and their operational constraints (Comer, Rastegarnia, 2019), (Song, Feng, et al., 2023).

Software-defined networking (SDN) offers a promising approach to addressing these challenges. By decoupling the control and data planes, SDN enables dynamic reconfiguration, programmable control, and centralized resource management (Conti, Dehghantanha, et al., 2018), (Attkan, Ranga, 2022), (Singh, Jain, 2024). The SDN controller, acting as a logically centralized entity, can orchestrate routing, manage trust decisions, and enforce access policies across the network (Dorri, Kanhere, et al., 2016) (Dorri, Kanhere, et al., 2016) (Erel-Özçevik, 2025). Its real-time global view allows for dynamic optimization of energy consumption and threat mitigation, all while maintaining scalability and responsiveness (Tanha, Hasani, et al., 2022), (Razvan, Mitica, 2025). SDN's programmable nature is particularly well-suited for managing the administrative complexity introduced by billions of IoT devices (Yu, Gao, et al., 2023), (Song, Feng, et al., 2023).

To further enhance security, blockchain technology has been adopted across various sectors, providing decentralized, tamper-proof ledgers for data integrity and transaction validation (Banerjee, Balas, et al., 2020), (Lourenço, Savas, et al., 2018), (Puja Sharma, Dipendra Karki). In distributed IoT systems, blockchain eliminates single points of failure and ensures cryptographic trust without reliance on centralized authorities. The synergy between SDN and blockchain presents a compelling opportunity: while SDN offers flexible control and network orchestration, blockchain provides traceability, data integrity, and authentication (Kumar, Saha, et al., 2018) (Barišić, Ruchkin, et al., 2022) (Chen, Wang, et al., 2023). However, traditional blockchain models like Bitcoin's Proof-of-Work (PoW) are computationally intensive, leading to energy and latency concerns in IoT environments. Therefore, a lightweight, trust-aware hybrid consensus model is essential—one that adapts dynamically based on transaction type and node roles (Kaur, Mittal, et al., 2025).

While blockchain technologies have been introduced to enhance trust and data integrity in IoT, existing implementations suffer from high computational overhead, latency, and poor scalability

especially when applied using conventional PoW models across all nodes. Simultaneously, SDN has emerged as a programmable alternative to handle real-time routing and control tasks. However, SDN's centralized trust model introduces a single point of failure, which is a critical limitation in adversarial or large-scale deployments.

These observations reveal a clear research gap: the absence of a lightweight, decentralized, trust-aware, and energy-efficient IoT routing framework that can scale under real-world adversarial conditions without overburdening constrained devices. To address these multifaceted challenges, this paper introduces the HB-SDN-IoT framework. The core contributions of this research lie in the strategic integration and engineering adaptation of existing technologies namely blockchain consensus models and SDN-based control mechanisms to address real-world challenges in IoT-CPS networks.

- Rather than proposing an entirely new consensus algorithm, this work presents a layered adaptation of existing Proof-of-Work (PoW) and Proof-of-Stake (PoS) mechanisms. PoW is reserved for critical inter-controller synchronization tasks, while PoS is employed for intra-cluster trust and routing validation. This context-aware fusion of consensus models balances energy efficiency and security across heterogeneous device layers in resource-constrained environments.
- The framework introduces a two-tier blockchain structure, separating local (private) and global (public) trust management to reduce overhead and improve scalability. While dual-chain approaches exist, this implementation demonstrates how separating intra-cluster and inter-controller operations enables efficient validation and auditing of network behavior tailored to the dynamics of SDN-enabled IoT network infrastructures.
- Building upon standard clustering techniques, this paper formulates a multi-factor cluster head election algorithm driven by real-time trust scores, residual energy, and communication latency. While not proposing a new clustering paradigm, the integration within an SDN-controlled, blockchain-audited environment enables more reliable and adaptive clustering for dynamic IoT networks. Integrated with SDN-based network visibility and blockchain-logged node histories, this mechanism supports balanced load distribution and improved fault resilience in dense IoT deployments.

This design balances performance, security, and scalability while maintaining compatibility with resource-limited IoT infrastructures.

The remainder of this paper is organized as follows: Section 2 presents a comprehensive literature review and identifies limitations in existing blockchain–SDN–IoT frameworks. Section 3 introduces the proposed HB-SDN-IoT architecture, including the dual-consensus mechanism, trust-aware clustering, and security framework. Section 4 details the simulation setup and performance evaluation. Section 5 concludes the paper and outlines future research directions including formal verification and real-world validation.

2. Literature Review

The integration of blockchain, IoT, and SDN technologies for secure, energy-efficient, and scalable network infrastructures has attracted significant attention in both academia and industry. Numerous approaches have addressed individual aspects such as security, authentication, trust management, and energy efficiency within decentralized environments. However, many existing solutions lack a unified, lightweight framework capable of dynamically adapting to the constraints and adversarial conditions inherent in IoT-enabled Cyber-Physical Systems (CPS) networks.

(Ran, Yan, et al., 2021) proposed a blockchain-enhanced multi-path QoS routing method based on AODV that excludes non-compliant nodes using smart contracts, achieving robustness under adversarial settings but suffering from complex chain and contract management unsuitable for resource-constrained IoT devices. Similarly, Leela Bitla et al. (Vairagade, Bitla, et al., 2022) explored NFTs for secure digital ownership via blockchain, yet this approach does not address real-time security and routing challenges in IoT systems.

Velmurugadass et al. (Velmurugadass, Dhanasekaran, et al., 2021) introduced a cloud-based SDN-blockchain framework for digital evidence handling, incorporating Harmony Search Optimization and Logical Graph of Evidence, but scalability and latency remain concerns under high-throughput conditions. Sijie Chen et al. (Chen, Zhang, et al., 2021) proposed secure power dispatch coordination using blockchain-based distributed algorithms, though these require more efficient consensus mechanisms to mitigate malicious interference.

Tarek Frikha et al. (Frikha, Chaabane, et al., 2021) developed a hybrid hardware-software PoW model using Ethereum, optimized via Keccak-256 and ZedBoard. Despite improved execution, the reliance on hardware exposes it to platform-level vulnerabilities. Cai et al. (Cai, Geng, et al., 2022) employed a many-objective optimization strategy with dynamic reward-penalty mechanisms to enhance shard validity in blockchain-enabled IIoT, but rogue node interference remains a significant challenge.

Bohan Li et al. (Li, Liang, et al., 2021) introduced a privacy-preserving LBS system using K-anonymity and blockchain. While ensuring conditional anonymity, its scalability limits the real-time utility in dense vehicular networks. Sellami et al. (Sellami, Hakiri, et al.) used NFV and SDN to support blockchain-secured IoT transactions, but their architecture struggles to counter botnet attacks effectively.

Almaiah et al. (Kumar, Kumar, et al., 2024) used lightweight deep learning-based authentication in IoT CPS, showing better validation delay and performance, but leaving open the risk of adversarial ML attacks. Li et al. (Li, Wang, et al., 2023) built a blockchain-supported SDN CPS system to enable immutable CIDS. Their system, however, is susceptible to smart contract and 51% attacks. Derhab et al. (Villegas-Ch, Govea, et al., 2025) proposed a BICS-integrated SDN using KNN-based IDS, achieving strong results, yet facing difficulty in large-scale deployments due to blockchain overhead.

Almarri et al (Subramanian, Krishnan, et al., 2025). explored the use of blockchain to address IoT security and trust issues. They found that blockchain's decentralized and immutable features helped prevent data tampering, enabled secure identity management, and supported transparent transactions. The study also noted its role in improving sustainability in systems like smart grids, while highlighting challenges in scalability, energy-efficient consensus, and data processing and Rupali S. Vairagade et al. (Vairagade, Brahmananda, 2020) reviewed the intersection of blockchain, ML, and IoT, focusing on security architectures and authentication mechanisms. While providing a broad understanding, their work lacks a holistic implementation approach that balances trust, energy, and scalability.

(Okon, Sallam, et al., 2024) proposed a blockchain-enabled SDN architecture to facilitate seamless handovers across multiple mobile network operators (MNOs) in emerging 6G environments. The solution was motivated by the need to enhance interoperability, trust, and low-latency communication in heterogeneous and dynamic networks. Their findings showed that the Raft consensus achieved superior results, reducing end-to-end delays and handover latency due to its lightweight, leader-based design. However, the study's focus on delay metrics overlooks energy efficiency and scalability under high mobility and dense deployments. As a result, while effective for reducing latency, the approach may not be ideal for energy-constrained IoT scenarios requiring broader consensus trade-offs.

(Alrashede, Eassa, et al., 2025) proposed a blockchain-based framework to secure the east–west interface in heterogeneous SDN environments, where multiple controllers from diverse vendors introduce new attack surfaces. To overcome the limitations of centralized or homogeneous security solutions, the authors utilized Ethereum blockchain and smart contracts to enable decentralized mutual authentication, secure data exchange, and network access control among SDN controllers. Their approach effectively mitigated threats such as DDoS, MitM, and false data injection while maintaining practical performance with ~20 TPS and 28–40 ms latency. However, the solution focuses primarily on inter-controller communication and does not explore energy-efficient consensus models or formal security proofs, which are crucial in IoT and constrained environments.

Table 1: Summary of Existing IoT–SDN–Blockchain Integration Approaches, Their Strengths, and Limitations

Reference	Technique / Approach	Key Strengths	Identified Limitations
Ran C. et al.	Blockchain-enhanced multipath QoS routing (AODV)	Robust under adversarial conditions; supports multiple paths	Complex smart contract handling; high overhead not suitable for IoT nodes
Leela Bitla et al.	NFT-based secure content ownership in IoT	Secures ownership of digital assets; decentralized control	Does not address routing or real-time IoT security
Velmurugadass et al.	Cloud-integrated SDN–blockchain for digital forensics	HSO and logical evidence graph for secure traceability	Not optimized for IoT scalability; cloud latency concerns
Sijie Chen et al.	Blockchain-based power dispatch for CPS	Resilient distributed coordination; tamper-resistant logs	Heavy consensus mechanism; vulnerable to timing-based attacks
Tarek Frikha et al.	Ethereum-based hybrid PoW using hardware/software design	Accelerated processing; improved execution	Hardware dependency; susceptible to platform vulnerabilities
Cai et al.	Reward-penalty model for shard validation	Improves shard integrity in distributed systems	Susceptible to rogue validators; lacks trust recovery
Bohan Li et al.	Blockchain with K-anonymity for location-based services	Ensures location privacy with conditional anonymity	Poor performance in dense or high-mobility environments
Sellami et al.	NFV + SDN + blockchain for IoT transactions	Supports distributed secure transactions	Ineffective against botnets; lacks dynamic trust evaluation
Almaiah et al.	Lightweight DL-based IoT authentication	High validation accuracy; low latency	Exposed to adversarial ML attacks; model drift concerns
Li et al.	SDN–blockchain intrusion detection system (CIDS)	Enables tamper-proof event logging and detection	Vulnerable to 51% attacks; smart contract limitations
Derhab et al.	KNN-based IDS with blockchain–SDN	Accurate anomaly detection; integrated policy enforcement	High consensus cost; limited scalability
Almarri et al.	Blockchain Decentralized And Immutable Features	Blockchain Effectiveness In Securing Iot Systems	Highlighted ongoing challenges in scalability, energy efficiency, and data processing for IoT-

			blockchain integration.
Rupali S. Vairagade et al.	Reviews on blockchain, ML, and IoT security	Broad understanding of architectures and authentication	Lack of holistic implementation balancing trust, energy, scalability
Okon et al.	Blockchain-enabled SDN for multi-operator handovers with Raft, PBFT, Paxos consensus evaluation	Improved handover performance; Raft consensus reduces delay and enhances interoperability in 6G networks	Limited focus on energy efficiency and scalability under dense or high-mobility IoT scenarios
Alrashede et al.	Blockchain-based mutual authentication framework for securing east–west SDN interfaces	Decentralized controller authentication, mitigation of DDoS/MitM attacks, stable throughput (~20 TPS), low latency (28–40 ms)	Focuses only on inter-controller security; lacks energy-efficient consensus design and formal verification for IoT deployments
Proposed HB-SDN-IoT (This Work)	Dual-layer blockchain with PoS + PoW and SDN-based trust-aware clustering	Energy-efficient hybrid consensus; scalable trust-driven routing; SDN-managed flow control	Requires real-world validation; formal security and economic modeling in future work

While a number of studies have explored the integration of blockchain and SDN in IoT, many of these efforts suffer from either high computational overhead or limited scalability. For example, a lightweight blockchain for IoT, but lacked integration with dynamic SDN-based control. Block SDN introduced decentralized security policies using blockchain in SDN, but did not address energy-aware routing. Similarly, NBV and SDN Trust integrated trust evaluation with SDN, yet the consensus models used were too heavy for constrained IoT nodes. A recurring limitation in these approaches is the use of uniform blockchain consensus (typically PoW or PBFT) across all layers, leading to scalability bottlenecks and high energy consumption. Table 1 presents a comparative analysis of key methods, highlighting their limitations in energy optimization, routing adaptability, and scalability in large-scale, heterogeneous IoT networks. These limitations reveal a clear research opportunity for a lightweight, scalable, and trust-aware framework that can balance energy efficiency with robust security in IoT networks. In response, the next section presents the detailed architecture and components of the proposed HB-SDN-IoT system.

3. Hybrid Blockchain-Sdn Iot Framework

To overcome existing limitations, this research proposes a Hybrid Blockchain-SDN IoT framework (HB-SDN-IoT) that combines the advantages of both public and private blockchain models within a decentralized, energy-aware control layer managed by distributed SDN controllers, as shown in Figure 1. The framework enhances the performance, reliability, and security of IoT-enabled Industrial Cyber-Physical Systems (CPSs) by integrating blockchain technology with the SDN paradigm and improving energy efficiency through a cluster-based routing mechanism. Nodes initially broadcast metadata such as energy, ID, and location to the nearest SDN controller, which then computes optimal cluster formations using a novel cost-function-based algorithm and assigns cluster heads. Intra-cluster

communications are authenticated using a lightweight Proof-of-Stake (PoS) protocol and stored in private ledgers for low latency and energy efficiency, while inter-controller interactions for forwarding and load balancing are secured via a Proof-of-Work (PoW)-based public blockchain, ensuring global synchronization and tamper-proof records. SDN flow rules facilitate authenticated data paths that require minimal intervention unless anomalies or attacks occur. The novelty of this approach lies in its hybrid dual-layer blockchain architecture combined with distributed SDN control and a dynamic, trust- and energy-aware clustering algorithm, collectively enabling scalable, secure, and energy-optimized routing tailored for heterogeneous IoT-CPS environments.

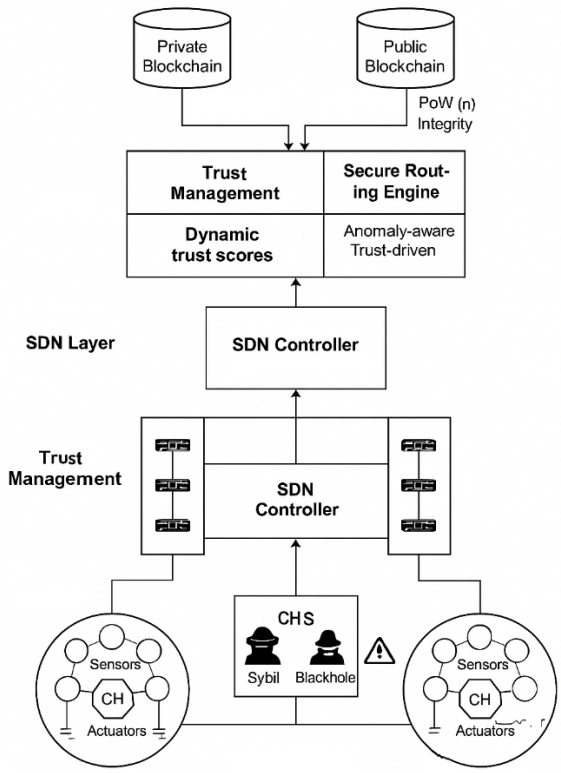

Fig.1: Architecture of the proposed system

This research introduces a modular, scalable, and lightweight hybrid framework that effectively integrates blockchain-based trust mechanisms with SDN-enabled network programmability and adaptive, energy-aware routing. It addresses a critical research gap by demonstrating how multi-consensus blockchain architectures can be tailored for heterogeneous, latency-sensitive industrial IoT systems without compromising security or efficiency. By fusing these technologies, the framework overcomes limitations in existing approaches and establishes a solid foundation for future advancements, including machine learning–driven controller policies, adaptive stake-weighting models, and cross-layer security enforcement.

3.1. System Model

The proposed HB-SDN-IoT framework is designed for a heterogeneous and hierarchical Industrial Cyber-Physical System (CPS) environment, where a large number of distributed IoT devices perform real-time sensing, communication, and actuation to monitor critical infrastructures. To ensure scalability, energy efficiency, and security, the network is logically organized into clusters, each managed by intelligent SDN controllers. The model incorporates realistic constraints from industrial IoT deployments and introduces mathematical abstractions for energy, trust, communication, and consensus processes.

Let the set of IoT nodes be denoted as $\mathcal{N} = \{n_1, n_2, \ldots, n_N\}$, where N represents the total number of deployed devices. Each node $n_i \in \mathcal{N}$ is characterized by attributes such as energy E_i, trust value $T_{ir,}$ and location coordinate (x_i, y_i). Nodes are categorized into different functional types based on their roles and capabilities, as detailed below.

3.1.1. Node Types

Regular IoT Nodes $(\boldsymbol{n_i})$*:*
These are energy- and computation-constrained sensor-actuator devices responsible for environmental sensing and transmitting data to their designated Cluster Head (CH).

Cluster Heads $(\boldsymbol{CH_j})$*:*
A dynamically selected subset of nodes that serve as local aggregators and routing agents for their respective clusters $\mathcal{N}_j \subset \mathcal{N}$. The selection is based on a weighted utility function:

$$CH_j = \arg \max_{n_i \in \mathcal{N}} \left[\omega_1 \cdot \frac{E_i}{E_{\max}} + \omega_2 \cdot T_i - \omega_3 \cdot D_i \right] \quad (1)$$

where $\omega_1, \omega_2, \omega_3 \in [0,1]$ are weight parameters, $E_{\max}$ is the maximum energy among all nodes, and D_i is the average communication distance to neighbors.

Edge Nodes $(\boldsymbol{e_k})$ *:*
These are high-capacity fog or gateway devices that participate in PoW-based consensus and interface with SDN controllers.

SDN Controllers ($\boldsymbol{S_m}$ *):*
These distributed control entities maintain logical visibility over assigned clusters. Each controller manages cluster formation, route optimization, flow rule enforcement, and local blockchain interactions for intra- and inter-controller transactions.

3.1.2. Deployment Model

The framework follows a hierarchical deployment model where regular IoT nodes are organized into clusters, each managed by a CH and overseen by an SDN controller. This architecture avoids flat or mesh topologies, improving scalability and routing efficiency. While IoT nodes may exhibit static or limited mobility, edge nodes and controllers are assumed to be stationary for control plane stability. The set of cluster heads is defined as $\mathcal{C} = \{CH_1, CH_2, \ldots, CH_K\}$, with $K \ll N$.

3.1.3. Communication Model

The communication is wireless, based on standards such as IEEE 802.15.4 or LPWAN (e.g., LoRa), depending on application requirements. Intra-cluster communication is multi-hop, whereas inter-cluster and controller communications are typically single-hop due to higher transmission ranges. The energy cost of communication between nodes i and j is modified as:

$$E_{\text{comm}}(i,j) = E_{\text{elec}} \cdot b + E_{\text{amp}} \cdot b \cdot d_{ij}^{Y} \quad (2)$$

where b is the data packet size, d_{ij} is the Euclidean distance between nodes i and $j, \gamma \in [2,4]$ is the path loss exponent, E_{elec} is the electronic circuitry, and E_{amp} is the amplifier energy per unit distance.

The SDN controller maintains and dynamically updates the routing table $\mathcal{R}$ for each cluster using verified topology and trust metadata stored in the private blockchain ledger. Once flow rules are installed, data forwarding within the cluster is autonomously managed by CHs, reducing control overhead.

3.1.4. Energy Model

All IoT nodes operate under limited battery constraints, and their residual energy $E_i(t)$ at time t evolves as:

$$E_i(t+1) = E_i(t) - E_{\text{sense}} - \sum_{j \in \mathcal{N}} E_{\text{comm}}(i,j) \quad (3)$$

where E_{sense} is the constant energy consumed for sensing per round. The SDN controller uses these readings to avoid assigning CH roles to low-energy nodes and to promote balanced energy distribution across the network.

3.1.5. Trust Model

Each node n_i maintains a dynamic trust score $T_i(t) \in [0,1]$, updated based on direct and indirect interactions. The score is calculated as:

$$T_i(t) = \alpha \cdot T_i(t-1) + \beta \cdot \frac{1}{M} \sum_{k=1}^{M} \delta_{ik} \quad (4)$$

where $\alpha, \beta \in [0,1]$ are forgetting and learning factors, M is the number of neighboring nodes, and $\delta_{ik} \in \{0,1\}$ is a binary feedback indicator of success or malicious behavior. Nodes with $T_i(t) < \theta_{\text{trust}}$ are disqualified from CH candidacy, and may be excluded from routing.

In the PoS-based private blockchain, a node's stake score S_i is a hybrid function of trust and energy:

$$S_i = \lambda_1 \cdot T_i + \lambda_2 \cdot \frac{E_{max}}{E_i} \quad (5)$$

Nodes with the highest stake values are selected as validators for intra-cluster ledger entries.

3.1.6. Security Assumptions

The proposed model assumes the presence of insider threats, where compromised nodes may attempt false data injection or misrouting. To mitigate such risks, a dual-layer blockchain is employed to ensure tamper-proof logging of transactions, flow rules, and cluster status updates. The public blockchain utilizes Proof-of-Work (PoW) to validate inter-node communication, ensuring consensus is achieved through a quorum of edge nodes. Meanwhile, Proof-of-Stake (PoS) enables fast and low-cost verification of intra-cluster events. The use of immutable ledgers and dynamic trust-weighted control helps prevent Sybil attacks, as malicious nodes with low trust cannot accumulate enough stake to participate in consensus. Additionally, flow rules in the SDN layer are periodically revalidated using blockchain-stored hashes, enabling the detection of DoS attacks and route manipulation. Having established the network structure, node roles, and models for communication, energy, and trust. Following this work introduces the architectural components of the HB-SDN-IoT framework, beginning with its hybrid consensus mechanism and blockchain system

3.2. Blockchain Layer Design

The blockchain layer is designed as a hybrid system, integrating both PoW and PoS in an adaptive fusion. PoW is selectively employed for inter-cluster communication between SDN controllers, where computationally capable nodes (e.g., gateways or edge servers) handle validation, ensuring cryptographic integrity and ledger immutability. In contrast, PoS is applied within clusters for trust-based management of lightweight transactions, such as energy updates or sensor logs, where validation depends on stake, derived from node reliability and uptime, rather than computational power.

This dual-consensus mechanism allows the trust protocol to be tailored according to device capability and network layer, without compromising security or overloading low-power devices. Furthermore, the architecture introduces a dual-chain structure: a private blockchain within each cluster for local authentication, and a public or shared-private blockchain for controller-to-controller communication. This design improves latency and scalability by enabling rapid local verification while reserving global broadcasts for critical updates, such as topology changes or routing failures.

3.2.1. Hybrid PoW–PoS Consensus Mechanism

In the control plane, where SDN controllers synchronize global cluster states or authenticate edge devices, Proof-of-Work (PoW) is employed due to its robust resistance to tampering and its suitability for infrequent but critical transactions. Let $\mathcal{T}_c$ denote the set of inter-controller transactions. A controller

S_i is elected as a PoW validator if it solves the hash-based puzzle $H(M||nonce) < T$, where:

$$\text{Nonce}_{\text{opt}} = \arg\min_{\text{nonce}} H(M||\text{ nonce }) \quad (6)$$

Here, M is the metadata content, $H(\cdot)$ is the SHA-256 hash function, and T is the target difficulty level. The energy and time costs are acceptable since SDN controllers are high-resource devices with stable power supplies.

Conversely, in the data plane, frequent and lightweight transactions such as node trust updates, cluster head (CH) selection metadata, and intra-cluster routing logs, collectively defined as $\mathcal{T}_d$, are validated using Proof-of-Stake. The stake score S_i of a node n_i is computed as:

$$S_i = \lambda_1 \cdot T_i + \lambda_2 \cdot \frac{E_i}{E_{\max}} \quad (7)$$

where T_i is the node's trust value, E_i is its residual energy, $E_{\max}$ is the maximum energy among peers, and $\lambda_1, \lambda_2 \in [0,1]$ are tunable weight parameters.

Nodes $\mathcal{N}_j$ are probabilistically selected as PoS validators using a softmax-based function:

$$P(n_i \text{ selected }) = \frac{e^{S_i}}{\sum_{k \in \mathcal{N}_j} e^{S_k}} \quad (8)$$

This strategy minimizes energy consumption by assigning validation roles to well-powered, trustworthy nodes, thereby extending the network's operational lifetime in battery-constrained environments.

To coordinate both consensus protocols effectively, the system defines the fusion logic as follows:

PoS is triggered by all local cluster-level events, such as routing updates, trust reports, and CH selection.

PoW is triggered by global events, including cluster reconfiguration, SDN controller coordination, new controller addition, or blockchain state synchronization.

Table 2: Roles of Consensus Mechanism in HB-SDN-IoT

Feature	Proof of Work (PoW)	Proof of Stake (PoS)
Used by	SDN Controllers	IoT Nodes within Cluster
Transaction Scope	Inter-controller (Global Events)	Intra-cluster (Local Updates)
Trigger Frequency	Low (event-driven)	High (periodic/triggered)
Energy Consumption	High	Low
Validator Selection	Puzzle Solving	Stake-Based Probabilistic
Example Events	Cluster merging, controller sync	Trust update, CH election
Security Resistance	Strong against Sybil/DDoS	Moderately secure, fast processing

The layered consensus mechanism ensures that critical updates are validated with strong security guarantees, while local operations remain fast and efficient. To support this dual-consensus architecture, the blockchain infrastructure is bifurcated into private and public chains, as given in Table 2, which is described below.

3.2.2. Dual Blockchain Structure

The HB-SDN-IoT framework employs a dual blockchain infrastructure, as illustrated in Figure 2, consisting of private blockchains within individual clusters and a public blockchain spanning SDN controllers. This separation of intra-cluster and inter-controller consensus mechanisms improves scalability, reduces latency, and ensures that lightweight local events do not overload the global validation process.

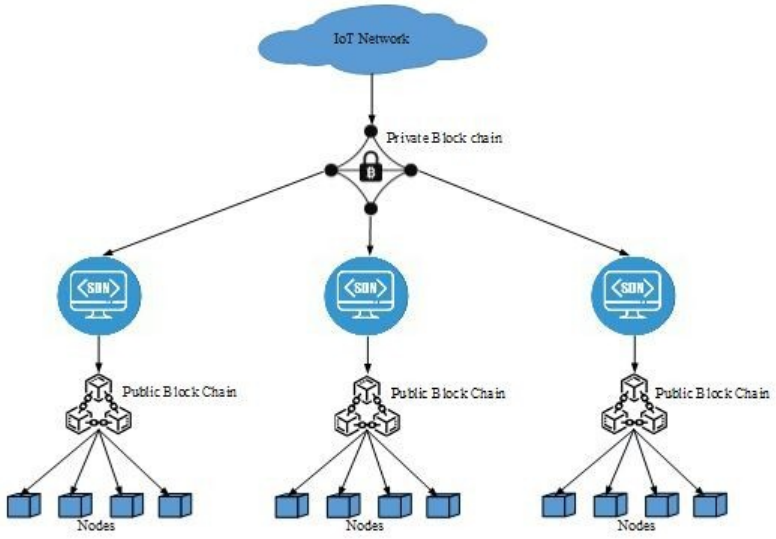

Fig.2: Dual blockchain infrastructure

3.2.2.1. Private Blockchain

Each cluster C_j maintains a private, permissioned blockchain where trusted nodes perform PoS validation for key intra-cluster events such as:

Node registration and authentication

Trust score updates and evolution tracking

Cluster head election logs

Routing policy commitments

The block structure B_t for time t in the private chain is given as:

$$B_t = \{ \text{BlockID, Timestamp, ValidatorID, TransactionList, PrevHash, CurrHash} \}$$

To reduce communication and computational overhead, transaction payloads are compressed and structured using Merkle Trees for efficient hash chaining. The validation time per transaction, τ_{priv} is modeled as:

$$\tau_{\text{priv}} = \tau_{\text{comm}} + \tau_{\text{verify}} + \tau_{\text{write}} \quad (9)$$

where τ_{comm} denotes the communication delay to the validator, τ_{verify} represents the time for signature and trust validation, and τ_{write} is the latency associated with appending the block.

The estimated storage overhead for the private chain, S_{priv} is calculated by:

$$S_{\text{priv}} = N_j \cdot R_t \cdot S_t \quad (10)$$

where N_j is the number of nodes in cluster j, R_t is the average transaction rate per node, and S_t is the average transaction size.

3.2.2.2. Public Blockchain

The public blockchain spans all SDN controllers and selected edge nodes. It is a permissioned blockchain for write operations only. SDN controllers are authorized to validate and append blocks

while remaining openly readable within the control domain. This blockchain logs high-level, network-wide events, including:

Controller authentication

Cluster structure updates

Security alerts at the network level

System audit records

Given the relatively static and infrequent nature of SDN controller transactions, the block generation rate is intentionally kept low, and the Proof-of-Work (PoW) difficulty is dynamically adjusted to balance security with computational cost. A block header in the public chain is structured as:

$$B_t^{pub} = \{\ Block_{\mathrm{ID}},\ \text{Nonce},\ Controller_{\mathrm{ID}},\ H\ (\text{TxList}),\ \text{Proof},\ \text{PrevHash}\ \} \quad (11)$$

To address the challenge of ledger bloat, the system implements a metadata anchoring mechanism, where only cryptographic hashes of transaction summaries from private blockchains are periodically committed to the public chain. This ensures verifiable cross-cluster integrity while minimizing redundancy and storage overhead.

This dual-chain architecture, complemented by the adaptive hybrid consensus protocol, provides a robust foundation for secure, scalable, and energy-efficient network control. The following section details how SDN controllers leverage this blockchain infrastructure to orchestrate dynamic cluster formation and manage routing policies effectively.

3.3. SDN Controller-Based Cluster Management

Software-Defined Networking (SDN) plays a pivotal role in the HB-SDN-IoT architecture by decoupling the data plane from the control plane, thereby enabling centralized yet logically distributed control over routing decisions while preserving the distributed nature of data transmission. In this framework, SDN controllers are hierarchically deployed across the network, each responsible for managing a specific cluster of IoT nodes. These controllers dynamically form clusters by evaluating energy metrics, trust scores, and traffic load, and they communicate with peer controllers via the blockchain layer to ensure secure coordination. Acting as intelligent agents, the controllers maintain flow tables, install routing policies, and persistently store cluster metadata on the blockchain ledger to safeguard against malicious interference and ensure routing consistency. A notable innovation introduced in this design is the energy-optimized cluster routing algorithm, governed by the SDN controller. Departing from conventional fixed-threshold or random-based clustering approaches, this algorithm utilizes a cost function that integrates residual energy, communication latency, trust score, and proximity to the cluster head. Cluster heads are elected based on this cost function, ensuring the selection of nodes that are both energy-abundant and trustworthy. These cluster heads also assume the role of lightweight PoS validators for intra-cluster transactions, significantly reducing the computational burden on low-power sensor nodes.

3.3.1. Cluster Formation Algorithm

The clustering process in the HB-SDN-IoT framework is designed to organize IoT nodes into optimal groups that minimize intra-cluster energy consumption while ensuring secure and responsive communication. Unlike conventional clustering techniques, the proposed method utilizes a multi-factor scoring function that is centrally evaluated by the SDN controller, which has real-time access to node parameters via secure blockchain transactions.

For each IoT node $n_i \in \mathcal{N}$, the cluster head suitability score for node i denotes as Θ_i, is computed as:

$$\Theta_i = \alpha_1 \cdot \frac{E_i}{E_{\max}} + \alpha_2 \cdot T_i + \alpha_3 \cdot \frac{1}{D_i} + \alpha_4 \cdot \frac{1}{\delta_i} \quad (12)$$

TWhere E_i denotes the residual energy of node n_i, $E_{\max}$ denotes the maximum energy among nodes in the local neighborhood, T_i is the trust score of node n_i, validated via the private blockchain, D_i denotes the average Euclidean distance to neighboring nodes, δ_i is the average communication delay (latency), $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ are the weight coefficients summing to 1, adjusted via controller heuristics or reinforcement learning.

The SDN controller collects the computed scores and elects the highest-scoring nodes as cluster heads within non-overlapping spatial regions to ensure balanced load distribution and strong security guarantees. Additionally, the controller consults blockchain-stored misbehavior logs to disqualify nodes with a history of malicious activity from CH candidacy.

Algorithm 1: Energy- and Trust-Aware Cluster Head Election

Input- Node set $N = \{n_1, n_2, \ldots, n_n\}$, Parameters $\{E_i, T_i, D_i, \delta_i\}$ for each node n_i, weights $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ where $\sum_{k=1}^{4} \alpha_k = 1$

Output- Cluster Head set $CH = \{ch_1, ch_2, \ldots, ch_m\}$

1 For each node $n_i \in N$ do
2 Normalize E_i, D_i, δ_i to the range [0,1] using min-max normalization
3 Retrieve trust score T_i from the private blockchain B_{priv}
4 Compute the CH score using equation 12:
5 End For
6 Rank all nodes based on Θ_i in descending order
7 Select the top-m nodes with non-overlapping radio ranges as cluster-heads
8 Assign each remaining node to the nearest CH based on D_i
9 Return the final CH set and cluster membership assignments

Once clusters are established, the SDN controller proceeds to energy-optimized flow rules using blockchain-authenticated topology and trust metadata, ensuring secure and efficient routing.

Although the proposed cluster head election process integrates multiple factors namely trust, residual energy, and communication latency the underlying optimization approach aligns with established weighted scoring techniques used in traditional clustering algorithms.

The computational complexity of the proposed CH selection process is $O(Nlog_N)$, where N is the number of IoT nodes per cluster. This includes: $O(N)$ for trust/energy normalization and score computation and $O(Nlog_N)$ for sorting the scores. The spatial separation constraint in CH selection may further increase the cost of final selection to $O(N^2)$ in worst-case scenarios, due to non-overlapping radio range checks. Despite this, the algorithm remains efficient for small-to-medium-sized clusters and benefits from centralized evaluation by SDN controllers with sufficient computational capacity.

3.3.2. Flow Rule Installation and Routing Decision

Routing in the proposed HB-SDN-IoT framework is governed by the intelligent control plane of SDN reinforced by the blockchain's tamper-resilient assurance. Each SDN controller maintains a dynamic flow table for all registered nodes within its managed clusters. Real-time metadata such as current trust levels, link latencies, residual energy, and historical misbehavior logs is periodically retrieved from the private blockchain to inform routing decisions.

The routing score for a given path $P_{src \to dst}$ is evaluated as:

$$\Psi(P) = \sum_{l_i \in P} (\beta_1 \cdot \frac{1}{T_{l_i}} + \beta_2 \cdot \delta_{l_i} + \beta_3 \cdot \frac{1}{E_{l_i}}) \quad (13)$$

Where T_{l_i} is the trust value of the forwarding node on link l_i, δ_{l_i} is the propagation delay on link l_i, E_{l_i} is the residual energy of the node forwarding over l_i, $\beta_1, \beta_2, \beta_3$ are the tunable weights reflecting the routing strategy's trust, delay, and energy preferences, respectively.

The path with the minimum routing score $\Psi(P)$ is selected. Corresponding flow entries are programmatically installed by the SDN controller, leveraging OpenFlow-like mechanisms adapted for IoT constraints. Each flow entry includes Source and destination identifiers, Next-hop MAC address, Route priority, Timeout for expiration, and Anomaly hash. Flow rules are disseminated through secure controller-to-node signaling channels and recorded immutably in the private blockchain for accountability and auditability.

To maintain resilience under failure or attack, the system incorporates a lightweight adaptive reconfiguration algorithm:

Step 1: Each SDN controller monitors packet delivery rates, flow expiration reports, and node trust fluctuations.

Step 2: If a flow rule underperforms due to malicious activity or battery depletion, Steps 3–5 are invoked.

Step 3: Affected clusters perform CH re-election based on updated energy and trust metrics.

Step 4: New paths are computed using the routing score $\Psi(P)$, and flow tables are updated accordingly.

Step 5: Malicious or compromised nodes are blacklisted, and their credentials are revoked from the blockchain ledger.

A dedicated anomaly detection function $\xi(n_i)$ flags nodes for isolation based on trust degradation:

$$\xi(ni) = \begin{cases} 1 & if\ T_i < T_{min} \\ 0 & otherwise \end{cases} \quad (14)$$

Where T_{min} is the predefined minimum trust threshold. Flagged nodes are isolated, and alerts are broadcast across the network to prevent propagation of compromised routes.

This combined strategy of blockchain-verified routing, SDN-driven control, and autonomous reconfiguration ensures that the HB-SDN-IoT framework remains robust, energy-aware, and attack-resilient, laying the groundwork for secure, scalable deployments in industrial CPS environments.

3.4. Effectiveness of the proposed system on security

The proposed HB-SDN-IoT framework incorporates multiple interwoven security features to ensure data integrity, verify the trustworthiness of participating nodes, enhance resilience against network-level attacks, and enable auditable system behavior. By combining blockchain immutability, proof-of-stake-based validation, and SDN-enabled dynamic attack response, the architecture promotes a secure-by-design model. This section systematically outlines how the framework counters major attack vectors within industrial IoT-CPS environments.

3.4.1 Data Tampering Mitigation via Blockchain Immutability

Data tampering refers to unauthorized alteration of data packets or routing information as they traverse the IoT-CPS network. In our framework, each critical transaction, such as node registration, trust updates, flow rule assignments, and cluster-head elections, is hashed and recorded in blockchain blocks. Each transaction t_{x_i} is associated with a unique hash:

$$h_i = H(t_{x_i} \ || \ h_{i-1}) \quad (15)$$

Where $H(\cdot)$ denotes the SHA-256 cryptographic hash function, and h_{i-1} is the hash of the previous block. Because each block contains a hash pointer to its predecessor, any tampering with past transactions breaks the continuity of the entire chain. This immutability prevents malicious SDN controllers or nodes from retroactively altering routing history or trust metrics. Consequently, flow tables and their revision histories remain cryptographically verifiable. Furthermore, all block records are timestamped and digitally signed using public-private key pairs unique to each node or controller, ensuring non-repudiation and accountability.

3.4.2 Sybil Attack Prevention through Proof-of-Stake Validation

A Sybil attack involves forging multiple identities to illegitimately influence system behavior, particularly during cluster formation or flow rule manipulation. The proposed framework mitigates this threat by enforcing a Proof-of-Stake (PoS)–based identity validation within each cluster.

Each node n_i is associated with a stake value s_i defined as:

$$s_i = \lambda \cdot T_i + \mu \cdot E_i \tag{16}$$

Where T_i is the trust score (computed from blockchain behavior history), E_i is the residual energy level, and λ, μ are the weight factors such that $\lambda + \mu = 1$

A node is eligible to participate in sensitive roles like CH election or flow rule request only if:

$$s_i \geq \theta_{stake} \tag{17}$$

Where θ_{stake} is a dynamic threshold adjusted by the SDN controller based on the average health of the cluster. Since Sybil nodes typically lack historical transactions and sufficient energy reserves, their stake values remain below this threshold, rendering them ineligible for trust-critical actions. Moreover, each cluster operates a local validator set elected from PoS-eligible nodes, which reduces dependency on a central authority while maintaining system integrity.

3.4.3 DoS Attack Mitigation via SDN Programmable Control

DoS attacks aim to exhaust the resources of IoT devices or SDN controllers by flooding them with invalid or replayed packets. To counter this, our SDN-based architecture incorporates programmable traffic filtering and rate limiting to enable real-time response.

Each SDN controller continuously monitors the following metrics for each node n_i:

Packet-in request rates $\rho_{in}(n_i)$

Flow setup request frequency $f_{setup}(n_i)$

Error packet ratios $\epsilon(n_i)$

If any node n_i violates predefined thresholds, i.e.,

$$\epsilon(n_i) > \epsilon_{max} \ \ or \ \ \rho_{in}(n_i) > \rho_{thresh} \tag{18}$$

The controller immediately installs a drop flow rule in the edge switches targeting n_i's MAC address. Simultaneously, it broadcasts an anomaly alert to peer controllers and blockchain nodes and logs the incident on the shared public blockchain for auditability. Additionally, a Controller-Level Firewall application inspects packet headers using OpenFlow fields, such as abnormal TTL values or port scan patterns, and triggers automated mitigation scripts to contain the attack.

3.4.4 Auditing and Traceability via Blockchain Logging

The architecture ensures full-chain auditability through the dual blockchain system. Security-relevant events are recorded on a private blockchain within each cluster, capturing node-specific occurrences such as trust decay logs, battery exhaustion flags, local flow rule installations, and cluster-head election justifications. Simultaneously, a public blockchain spanning SDN controllers logs global events like cluster structure evolution, controller authentication records, and node blacklisting. Each blockchain transaction contains a pseudonymized node ID, event type (with standardized codes), timestamp, SHA-256 transaction hash, and a digital signature. These immutable logs create comprehensive audit trails that facilitate post-attack forensic investigations, verify compliance with security policies, and support dynamic recalibration of trust scores based on behavior analysis.

Together, these interlinked security layers offer a holistic defense tailored to the heterogeneous and dynamic nature of IoT-CPS environments. Blockchain immutability guarantees data integrity; Proof-of-Stake secures identity validation; SDN enables resilience and real-time adaptability; and thorough auditing delivers full transparency. The following section presents simulation-based performance analysis to quantify the empirical benefits of these security enhancements.

3.4.5 Security Analysis and Resilience

While the architectural design of the proposed dual-layer blockchain offers practical benefits, particularly through its separation of intra-cluster (PoS) and inter-controller (PoW) consensus, which is essential to examine further the security implications and resilience characteristics of this framework. First, the private blockchain layer within each cluster ensures low-latency, trust-based validation without overwhelming resource-constrained nodes. The reliance on Proof-of-Stake mitigates Sybil attacks by disqualifying low-trust nodes from participating in validation roles. Moreover, stake calculation incorporates both trust and residual energy, reducing the likelihood of validator manipulation. On the other hand, the public blockchain among SDN controllers is fortified using Proof-of-Work consensus, ensuring tamper-resistant synchronization of inter-cluster events. Since controller nodes are computationally capable and energy-unconstrained, the security properties of PoW can be fully leveraged without compromising system responsiveness. From a theoretical perspective, the dual-layer design minimizes the attack surface by reducing the broadcast domain of consensus only global updates trigger PoW. Local events, including flow rule installations and CH elections, remain isolated within cluster domains, ensuring attack containment and compartmentalized trust decay tracking. To reduce the overall attack surface, the architecture integrates behaviour-based trust evaluation, tamper-proof blockchain logging, and SDN-enforced flow control policies. These elements collectively promote a secure and adaptable network environment. However, while the framework exhibits qualitative resilience against a range of threats, it currently lacks formal security proofs under defined adversarial models. The use of cryptographic validation tools and formal verification frameworks such as Tamarin, ProVerif, or AVISPA remains a critical future research direction. Such analysis would allow for the mathematical validation of essential properties including confidentiality, integrity, non-repudiation, and resistance to protocol-level manipulation, thereby enhancing the theoretical robustness of the proposed security model.

3.5 Theoretical Foundation and Formal Considerations

The proposed HB-SDN-IoT framework presents a hybrid approach to secure and energy-efficient IoT communication. However, to strengthen the theoretical rigor of the model, we recognize the importance of formalizing its security and computational properties. From a security perspective, the system currently assumes trust-based behaviour monitoring and uses blockchain for tamper-proof validation. We define our threat model as a combination of Sybil, black hole, replay, and DoS attacks, assuming partial compromise of node clusters but secure SDN controller links. To fully validate the security properties (e.g., integrity, trust convergence, consensus finality), we propose future formal verification using model checking frameworks such as Tamarin, ProVerif, or AVISPA. These tools enable the symbolic analysis of protocol states and the verification of safety and liveness properties under adversarial conditions. The cluster head election algorithm and routing decision logic are polynomial in complexity. The CH selection algorithm requires $O(NlogN)$ for score ranking and up to $O(N^2)$ for spatial separation enforcement, where N N is the number of nodes per cluster. The trust score update mechanism is linear in the number of interactions, provided a fixed-size sliding window is used. These complexities are feasible for execution on SDN controllers and edge gateways with moderate computational capacity. To evaluate economic and computational viability, the blockchain components are abstracted based on per-transaction cost (energy or gas), with inter-controller PoW modeled using average hash computation time and intra-cluster PoS using normalized trust-weighted validation. Future work will formalize these into a cost-energy-accuracy trade-off model, supported by sensitivity analysis. We will also define boundary conditions, such as maximum tolerable block propagation delay, validator churn rate, and energy budget per node, to offer a comprehensive characterization of the system's operational envelope.

3.6. Energy Optimization Mechanism of the Proposed System

In resource-constrained IoT-CPS networks, where nodes operate on limited battery power and contend with unpredictable communication loads, energy efficiency is paramount for extending system lifespan

and ensuring reliable operation. The HB-SDN-IoT framework relies on several operational assumptions. First, all SDN controllers are assumed to be trustworthy and computationally capable of managing intra-cluster trust updates and blockchain consensus duties. Nodes within each cluster are assumed to possess sufficient computational resources to participate in lightweight PoS verification and respond to SDN flow rules. The economic model abstracts blockchain operations as transactions with uniform processing cost, and consensus latency is modelled deterministically for simulation. The framework operates under the assumption that inter-controller communication is reliable and latency-bound. Boundary conditions include maximum transaction throughput (based on controller processing limits), minimum required energy per consensus operation, and trust score thresholds that influence CH selection and blacklist enforcement. These conditions define the scalability and reliability envelope for safe deployment of the proposed system. This section details how our framework achieves substantial energy savings compared to conventional architectures.

3.6.1. Energy-Aware Cost Function for Cluster Head Selection

At the core of energy optimization lies the cluster head (CH) selection process, managed by the SDN controllers. To ensure that the most energy-efficient and reliable nodes assume CH responsibilities, we define a multi-criteria cost function:

$$C_{CH}(n_i) = \alpha \cdot \left(\frac{1}{E_i^{res}}\right) + \beta \cdot \left(\frac{1}{T_i}\right) + \gamma \cdot D_i + \delta \cdot \tau_i \tag{19}$$

Where, $E_i^{\text{res.}}$ is the residual energy of node n_i, T_i is the trust value normalized between 0 and 1, D_i represents the average communication distance to neighboring nodes, τ_i is the historical packet forwarding delay. The weighting parameters $\alpha, \beta, \gamma, \delta$ satisfy $\alpha + \beta + \gamma + \delta = 1$. The node with the minimum $C_{\text{CH}}(n_i)$ score is selected as the CH, thereby avoiding nodes with low energy reserves or unreliable behavior. Additionally, the CHs are spatially optimized to reduce intra-cluster communication energy. The SDN controllers periodically rerun this election process using blockchain-verified trust and energy metrics to prevent outdated or suboptimal decisions.

3.6.2. Adaptive Load Balancing with Feedback

Static cluster structures often create hotspots, where CHs exhaust their energy more quickly due to uneven traffic loads. To mitigate this, the framework incorporates feedback-driven adaptive load balancing. SDN controllers continuously monitor real-time CH metrics such as traffic queue length $q_{\text{CH}}(t)$, packet drop rate $\delta_{CH}(t)$, and residual energy $E_{CH}(t)$. If any CH exceeds threshold conditions:

$$q_{\text{CH}}(t) > q_{\max} \text{ or } E_{\text{CH}}(t) < E_{\min} \tag{20}$$

A dynamic CH handover is triggered. The selection of a backup CH follows the cost function defined earlier (Equation 19). Additionally, intra-cluster nodes adjust their sensing and reporting frequency based on weighted energy availability, modelled as:

$$f_i = f_0 \cdot \left(\frac{E_i^{res}}{E_{avg}}\right) \tag{21}$$

Where f_i is the adjusted reporting frequency for node i, f_0 is the nominal frequency, and E_{avg} is the average energy of all cluster members. This fine-grained control mechanism helps prevent premature node exhaustion and promotes energy-balanced cluster longevity.

3.6.3. Minimizing Retransmissions and Route Failures

Route failures, packet retransmissions, and signal collisions contribute to hidden energy drains in IoT-CPS networks. To mitigate these inefficiencies, the framework leverages blockchain-anchored trust scores to exclude unreliable nodes from routing paths. The SDN controller computes optimal flow paths by minimizing both cumulative hop count and historical packet drop rates. Cluster heads (CHs) cache route performance statistics and update them after each transmission window to reflect current network conditions.

Let $\mathcal{E}_{tx}(p)$ denote the energy consumed to transmit packet p. The framework aims to minimize the

total transmission energy given by:

$$\mathcal{E}_{\text{total}} = \sum_{p_i \in \mathcal{P}} \left(\mathcal{E}_{tx}(p_i) \cdot (1 + r_i) \right) \quad (22)$$

Where r_i is the expected retransmission rate for path i, $\mathcal{P}$ is the set of active data paths. By using historical transmission and loss data securely stored on the private blockchain, the SDN controllers avoid routing through high-loss paths, thereby reducing repeated packet processing and minimizing MAC-layer collisions.

Having defined the architectural components, consensus mechanisms, and control strategies, the next section evaluates the proposed framework through simulation-based performance analysis.

4. Simulation Results and Discussion

To validate the proposed blockchain-integrated SDN-enabled IoT network framework, comprehensive simulations were performed using a controlled MATLAB environment. This section details the experimental setup, including simulation parameters, and presents the evaluation results highlighting the framework's performance across key metrics

4.1. Simulation Setup

Blockchain functionality is emulated using private Ethereum networks, deployed as virtual machines (VMs) within the simulation environment. Each VM is assigned a unique IP address corresponding to an SDN domain, ensuring logical separation and domain-specific transaction logging. The blockchain nodes interact directly with their respective SDN controllers to enable secure inter-domain communication, transaction validation, and data auditing. Wireless communication among IoT nodes is simulated via a lightweight IEEE 802.11-based Wi-Fi module, accurately modeling channel behavior, contention, and packet exchange. The simulation encompasses critical operations including cluster formation, flow rule installation, anomaly detection, trust score evaluation, and energy-aware routing. These are supported by a hybrid consensus mechanism combining Proof-of-Work and Proof-of-Stake (PoW–PoS), enhancing both security and energy efficiency. Performance evaluation focuses on key metrics such as energy consumption, routing latency, packet delivery ratio, throughput, and blockchain overhead, providing comprehensive insights into the framework's effectiveness under realistic conditions.

Table 3: System parameters

Operating System	Windows 10
Simulation Platform	MATLAB R2021a
Processor	Intel(R) Core(TM) i7-9750H @ 2.60GHz
RAM	16 GB

The proposed HB-SDN-IoT framework is implemented in a simulated environment using MATLAB as the primary modelling platform. The simulation runs on a Windows 10 machine equipped with an Intel® Core™ i7-9750H processor at 2.60 GHz and 16 GB of RAM, as shown in Table 3, providing sufficient computational resources to support extensive network simulations without performance degradation. The network topology consists of 100 virtual IoT nodes, which are randomly distributed into five clusters. Each cluster is managed by a dedicated local SDN controller responsible for flow control, routing decisions, and trust management. These operations leverage blockchain-verified metadata to ensure secure and trustworthy network interactions.

4.1.1. Simulation Parameters

The key simulation parameters configured for evaluating the proposed HB-SDN-IoT framework are summarized in Table 4. These parameters have been carefully chosen to accurately reflect the real-world constraints and operational conditions typical of energy-constrained, latency-sensitive IoT environments. The settings encompass characteristics of the IoT nodes, SDN controllers, network communication, and blockchain protocols to ensure a realistic and comprehensive performance assessment.

Table 4: Initial Simulation Parameters

Parameter	Value
Number of IoT Nodes	100
Number of Clusters	5
Initial Node Energy	2 Joules
Packet Size	512 bytes
Transmission Range	50 meters
SDN Controller	Centralized – one per cluster
Blockchain Framework	Ethereum (private network)
Consensus Mechanism	Hybrid PoW–PoS
Routing Protocol	Trust and Energy-Aware Dynamic
VM Deployment	Configured with unique IP per domain
Wireless Communication	IEEE 802.11 (Wi-Fi simulator)

While MATLAB offers a controlled environment for evaluating complex algorithmic behaviors, the current simulation is intended as a proof-of-concept benchmarking step. We acknowledge that real-world IoT environments present additional variabilities, such as hardware heterogeneity, variable link quality, and unpredictable mobility patterns. As such, future work will extend this simulation to a hardware testbed using platforms like Raspberry Pi-based SDN edge devices or Contiki-NG with Cooja simulator, enabling realistic power profiling and latency measurements.

While the simulation setup presented in this study allows for comprehensive evaluation across multiple performance dimensions, we acknowledge that several assumptions may limit the realism and generalizability of the reported outcomes. Specifically, the use of a uniform initial energy level (2 Joules) for all IoT nodes simplifies energy modeling but does not reflect the heterogeneous battery and harvesting profiles typically found in real-world deployments. Additionally, the wireless communication model assumes a simplified and interference-free channel, which may lead to an underestimation of packet loss and delay. Most critically, blockchain consensus timing is modeled as idealized and deterministic, without accounting for block propagation delay, transaction verification latency, or cryptographic processing overheads. These factors could significantly impact system responsiveness in practice. Moreover, the absence of statistical significance testing, such as confidence intervals, variance analysis, or p-values, reduces the robustness of performance claims. In future work, we plan to incorporate Monte Carlo simulations, multiple randomized runs, and sensitivity analysis to provide more statistically grounded insights. We also intend to integrate hardware-in-the-loop simulations or real testbed deployments to validate the proposed framework under realistic network dynamics and adversarial conditions.

4.2. Performance Evaluation

The proposed Hybrid Blockchain-SDN-enabled IoT (HB-SDN-IoT) framework is specifically designed to overcome the computational and energy constraints typical of IoT networks while enhancing security, trust, and routing efficiency. The architecture employs a lightweight, cluster-based approach, with each cluster managed by a logically centralized SDN controller responsible for device authentication,

dynamic routing, and secure data transmission. Leveraging both public and private blockchain layers, the framework ensures distributed trust verification and immutable logging of network operations, effectively mitigating threats such as spoofing, data tampering, and unauthorized access. Performance evaluation compares the HB-SDN-IoT framework against traditional Full Blockchain Consensus (FBC) [Latif, Wen, et al., (2022)] models, which rely exclusively on computationally intensive hybrid hashing schemes. Additionally, the framework's routing efficiency and security are benchmarked against conventional routing protocols like DSDV [Latif, Wen, et al., (2022)], AOMDV [Latif, Wen, et al., (2022)], and AODV [Latif, Wen, et al., (2022)], which lack inherent support for secure or energy-aware routing.

4.2.1. Throughput

Throughput denotes the total volume of successfully transmitted data from IoT source nodes to their intended destinations within a specified time interval. In the HB-SDN-IoT framework, throughput additionally reflects the number of securely validated transactions processed across the blockchain-enabled SDN domains, thereby serving as a combined measure of both data delivery efficiency and blockchain transaction capacity.

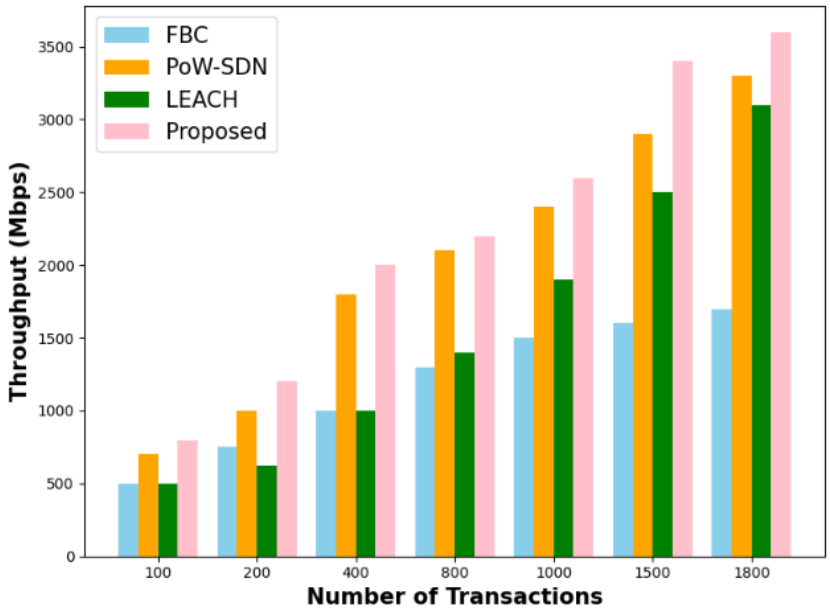

Fig.3: Throughput of the proposed HB-SDN-IoT model compared with existing blockchain models

Figure 3 illustrates the comparative throughput performance of the proposed HB-SDN-IoT framework against baseline models, including the Full Blockchain Configuration (FBC), PoW-SDN and LEACH. A marked improvement in throughput is observed for HB-SDN-IoT, primarily due to its dynamic clustering mechanism managed by the SDN controller and the adoption of a lightweight, dual-layer blockchain consensus. In contrast to the computationally intensive hybrid hashing and Proof-of-Work (PoW) schemes used in traditional FBC, PoW-SDN [Latif, Wen, et al., (2022)] and LEACH [Mythili, Duraisamy, (2024)] [Lonkar, Kuthe, et al., (2025)] architectures, our approach significantly reduces consensus delays and transaction validation overhead, enabling faster and more efficient data processing.

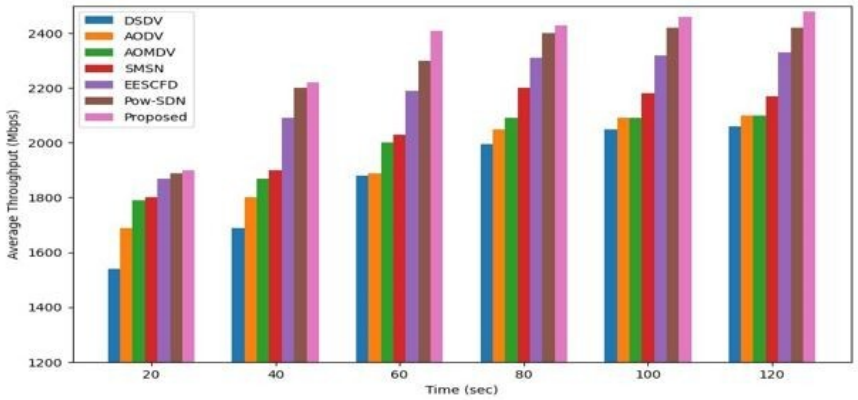

Fig.4: Average Throughput Comparison with Conventional Routing Protocols

Figure 4, further presents the average throughput comparison between the proposed HB-SDN-IoT framework and standard routing protocols such as AODV, AOMDV, and DSDV. The HB-SDN-IoT model demonstrates superior throughput performance, attributed to its intelligent route selection managed by SDN controllers, which dynamically reconfigure paths based on real-time network conditions and blockchain-verified trust metrics. The integrated trust mechanism effectively isolates malicious or selfish nodes, reducing packet drops and improving data delivery reliability. Furthermore, as the number of active connections increases, the SDN controller efficiently balances network traffic and mitigates link failures, maintaining high throughput even in dense and dynamic IoT environments.

4.2.2. End-to-End Delay

End-to-end delay represents the total time taken for a data packet to travel from the originating IoT source node to its final destination within the network. In the HB-SDN-IoT framework, this delay encompasses blockchain validation latency, routing decisions by the SDN controller, and inter-cluster communication delays. Formally, the overall delay is expressed in Equation (23) as the sum of processing time T_{proc}, transmission time T_{trans} , and queuing time T_{queue}:

$$Delay = T_{proc} + T_{trans} + T_{queue} \quad (23)$$

To model realistic IoT traffic, a cluster-based routing approach is utilized with packet sizes varying between 1000 and 3500 bytes and packet counts ranging from 500 to 4000. The delay characteristics are analyzed under these traffic conditions.

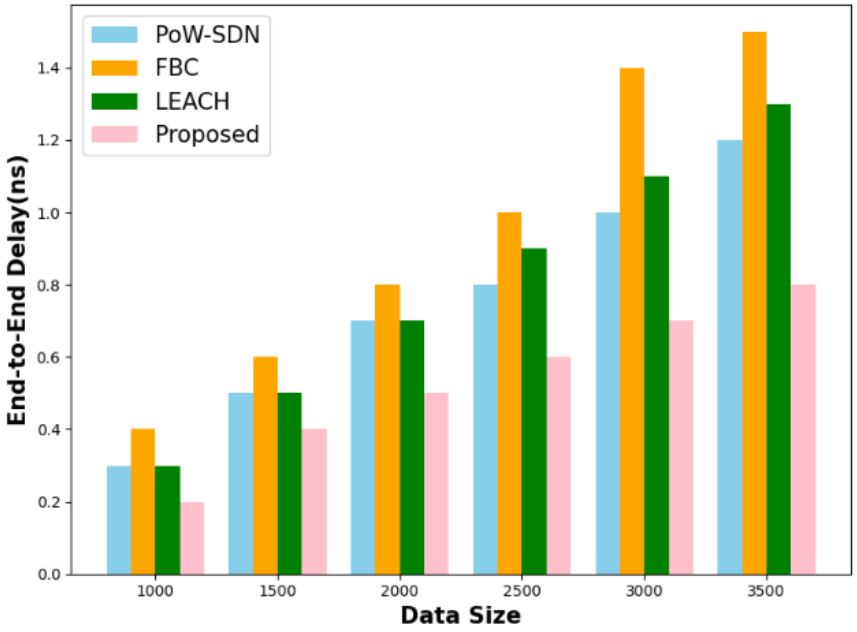

Fig.5: Delay Comparison of HB-SDN-IoT Model

As shown in Figure 5, the HB-SDN-IoT model achieves significantly lower end-to-end delay compared to the Full Blockchain Configuration (FBC), PoW-SDN and LEACH models. This improvement is primarily due to the efficient localized verification enabled by the dual-layer blockchain architecture (public and private), which minimizes redundant broadcasts and consensus delays. Additionally, the SDN controller's adaptive traffic engineering effectively reduces congestion at output buffers, thereby accelerating packet processing and overall transmission times.

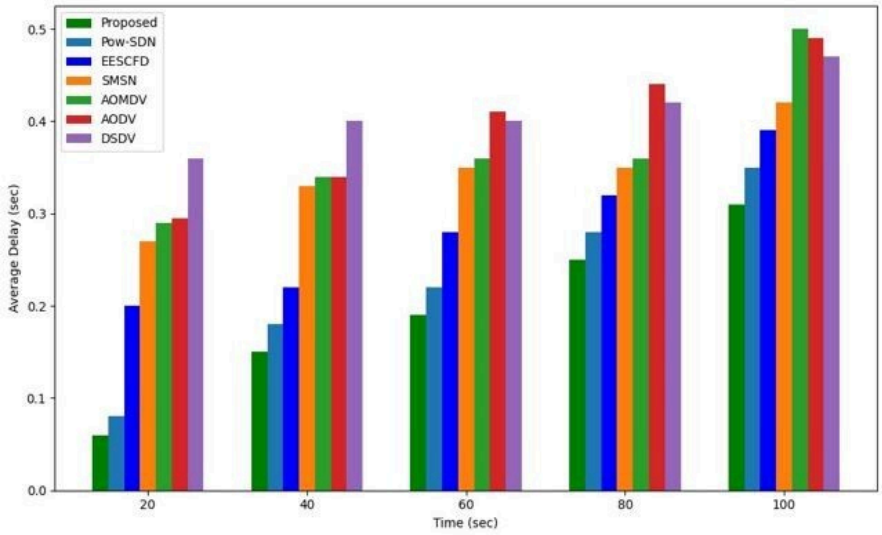

Fig.6: Average Delay Comparison with Conventional and Clustering-Based Protocols

Figure 6 presents the average delay of the proposed HB-SDN-IoT model compared to traditional routing protocols such as AODV, AOMDV, and DSDV, as well as energy-aware clustering protocols like SMSN and EESCFD. The HB-SDN-IoT consistently achieves the lowest delay across varying node densities and packet loads. This superior performance results from its trust-driven, anomaly-aware routing, which proactively avoids network bottlenecks and malicious nodes. Even as traffic intensity

and cluster size grow, the model maintains minimal latency due to controller-coordinated resource scheduling and route prioritization. While delay increases moderately, from approximately 0.5 to 1.6 milliseconds, with larger packet sizes, this rise is primarily attributed to output buffer saturation. Notably, the rate of increase is substantially slower than that observed in baseline protocols.

4.2.3. Energy Consumption

In the HB-SDN-IoT framework, total energy consumption accounts for the combined energy used by distributed IoT edge devices, along with the overhead from SDN controller operations and blockchain validation tasks. The overall energy expenditure is quantified by Equation (24), which incorporates transaction processing, node activity, and controller workload. The symbols and parameters involved are detailed in Table 5.

$$E_{tot} = N_{trans} * T_{trans} + [(N_{cont} * E_{cont}) + (N_{iot} * E_{iot})] \quad (24)$$

Table 5: Notation and Description of the equation

Notation	Description
E_{tot}	Total energy consumption
N_{trans}	Number of transactions
T_{trans}	Time taken per transaction
N_{cont}	Number of SDN controllers
E_{cont}	Energy consumed per SDN controller
N_{iot}	Number of IoT devices
E_{iot}	Energy consumed per IoT device

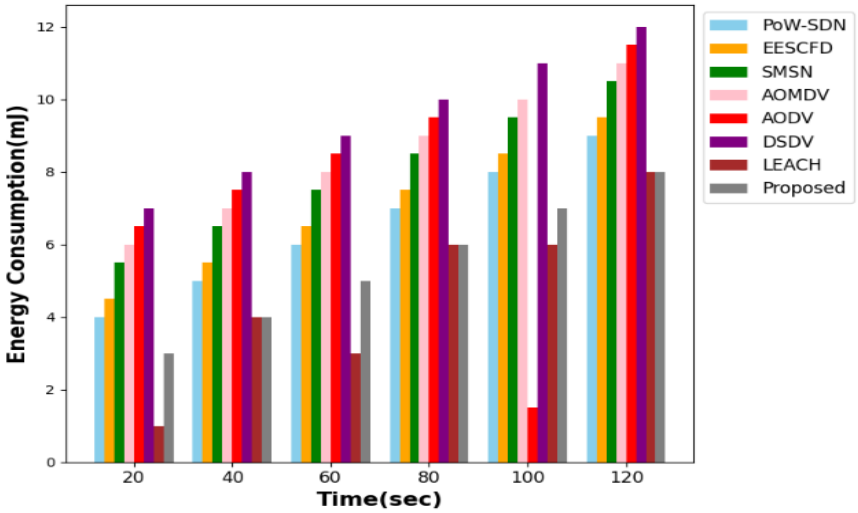

Fig.7: Energy Consumption Comparison of HB-SDN-IoT with Baseline Protocols

As illustrated in Figure 7, the HB-SDN-IoT model achieves a significant reduction in total energy consumption compared to conventional protocols such as AODV, AOMDV, DSDV, LEACH and energy-aware cluster-based protocols like SMSN and EESCFD. This lower energy footprint arises from several architectural advantages: the SDN controller dynamically updates routing paths based on real-time node energy profiles across domains; hybrid blockchain validation reduces the need for costly network-wide consensus operations; and anomaly-aware trust routing effectively avoids black holes and routing loops that cause excessive retransmissions. The proposed model adapts routing decisions according to the residual energy of IoT nodes, dynamically balancing traffic loads to prevent premature

node failures. Furthermore, transaction overhead is minimized through lightweight smart contracts deployed on private blockchains, streamlining control message verification within clusters. Consequently, the network sustains prolonged operational life and balanced energy consumption across IoT devices, which is vital for real-time and mission-critical deployments. Therefore, the HB-SDN-IoT framework not only enhances security and quality of service but also delivers substantial improvements in energy efficiency over state-of-the-art protocols.

4.2.4. Packet Delivery Ratio

Packet Delivery Ratio (PDR) measures the reliability of the network by quantifying the percentage of data packets successfully received at their intended destinations out of the total packets sent.

Table 6: Packet Delivery Ratio (PDR) Comparison

Protocol	PDR (%) at 100 Nodes	PDR (%) at 200 Nodes	PDR (%) at 300 Nodes
AODV	87.3	83.5	78.6
DSDV	88.9	85.1	80.3
SMSN	90.2	86.8	82.5
FBC	91.6	87.4	84.0
LEACH	86.0	86.9	87.1
HEED	88.0	89.0	86.2
HB-SDN-IoT	96.8	94.1	91.2

As given in Table 6, the proposed HB-SDN-IoT framework outperforms all benchmark protocols, particularly as the network scales. The elevated Packet Delivery Ratio (PDR) results from intelligent cluster-based routing, real-time SDN flow optimization, dynamic trust evaluation, and effective avoidance of malicious nodes. This underscores the robustness and reliability of the model in dense network scenarios.

4.2.5. Control Overhead

Control overhead refers to the volume of protocol-specific control messages required to maintain network operations. The proposed HB-SDN-IoT architecture significantly reduces this overhead by decentralizing route updates through SDN controllers and delegating authentication tasks to local private blockchains. This decentralized approach enables efficient routing maintenance with minimal signaling traffic.

Table 7: Comparison of Control Overhead (bytes/sec)

Protocol	100 Nodes	200 Nodes	300 Nodes
AODV	1240	2580	3820
DSDV	980	2060	3100
FBC	1100	2300	3480
SMSN	1010	2140	3250
HB-SDN-IoT	740	1290	1780

Table 7 presents a comparative analysis of five routing protocols AODV, DSDV, FBC, SMSN, and the proposed HB-SDN-IoT across varying network sizes of 100, 200, and 300 nodes. Traditional protocols such as AODV and DSDV exhibit a steep increase in performance costs as the network scales, indicating higher overhead and energy consumption due to frequent route discoveries or table updates. FBC and SMSN demonstrate moderate improvements over these legacy methods, reflecting better adaptability and somewhat reduced overhead. However, the HB-SDN-IoT protocol significantly

outperforms all others, maintaining consistently lower overhead values across all node densities. This highlights its superior scalability, energy efficiency, and optimized control mechanisms tailored for dense IoT environments.

4.2.6. Average Latency

Average latency refers to the mean time required for data packets to travel from the source node to the destination node. In the presence of a blackhole attack, malicious nodes intercept and discard data packets instead of forwarding them, which significantly increases communication delays and disrupts the normal data flow across the network. This not only degrades performance but also hampers the reliability of time-sensitive IoT applications.

Table 8: Average Latency under Blackhole Attack (ms)

Protocol	Without Mitigation	With Mitigation
AODV	156.7	-
DSDV	142.3	-
FBC	130.5	101.6
SMSN	118.4	94.5
HB-SDN-IoT	-	**61.2**

Table 8 presents the latency performance of various protocols under blackhole attack conditions. Traditional routing protocols such as AODV and DSDV, which lack built-in mitigation mechanisms, suffer significant delays, with average latencies recorded at 156.7 ms and 142.3 ms, respectively. In contrast, protocols such as FBC and SMSN, when integrated with the proposed mitigation framework, demonstrate improved performance, reducing latency to 101.6 ms and 94.5 ms, respectively. The HB-SDN-IoT framework achieves the lowest latency of 61.2 ms, attributed to its anomaly-aware trust evaluation, smart contract–driven response mechanisms, and blockchain-based tracking of node behavior. These features collectively enable rapid isolation of malicious entities and ensure sustained data forwarding efficiency even in adversarial environments. The results validate the framework's effectiveness in maintaining low-latency, secure communication in the face of blackhole threats.

4.2.7. Time consumption

Time consumption in blockchain networks refers to the total duration required to validate and confirm a single transaction within the system. This metric is a crucial indicator of the responsiveness, scalability, and operational efficiency of blockchain-integrated IoT frameworks, particularly in latency-sensitive environments such as industrial automation, healthcare, and smart city infrastructure. High transaction latency can delay critical decision-making processes, whereas efficient consensus mechanisms can significantly reduce time overheads while maintaining security and integrity. Therefore, evaluating transaction confirmation time is essential for determining the practical viability of blockchain-based solutions in real-time IoT applications.

Table 9: Blockchain Validation Time per Transaction (ms)

Blockchain Type	Avg. Validation Time (ms)	Consensus Used
Public Chain	540	PoW (Ethereum)
Private Chain	110	PoS (Proposed)

Hybrid Chain (HB-SDN-IoT)	**135**	PoS + SHA256 + Trust Filtering

The validation time comparison given in Table 9 demonstrates that the hybrid consensus approach adopted in the HB-SDN-IoT framework effectively balances decentralization and performance. Unlike traditional Proof-of-Work (PoW)-based public blockchains, which incur high latency due to their computational complexity, recording an average delay of 540 ms as observed in standard Ethereum networks, the proposed model employs Proof-of-Authority (PoS) within SDN domains for lightweight and rapid local validation. This private chain configuration reduces validation time to 110 ms by leveraging pre-authorized trusted nodes, significantly minimizing computational overhead. The HB-SDN-IoT's hybrid blockchain, which combines PoS with SHA-256 hashing and blockchain-integrated trust filtering, achieves a moderate yet optimal validation time of 135 ms. This design ensures both high integrity and real-time responsiveness, making it suitable for latency-sensitive IoT-CPS applications without compromising on decentralization or security guarantees.

4.2.8. Transactions per Second

Transactions per Second (TPS) is a critical performance metric used to assess the scalability and throughput of blockchain-based or distributed network systems. TPS quantifies the number of transactions that can be successfully validated and committed to the ledger per second, thereby reflecting the system's capability to handle growing user demands, node density, and real-time data flow. In the context of IoT-CPS environments, where high-frequency interactions and decentralized validation are essential, a higher TPS indicates a network's robustness in sustaining large-scale deployments without degradation in performance or responsiveness. TPS is particularly important for evaluating the feasibility of blockchain-integrated SDN-IoT architectures, where latency and resource constraints coexist with the need for secure, verifiable operations.

Table 10: Scalability Analysis based on Transactions per Second (TPS)

Protocol/Model	**50 Nodes**	**100 Nodes**	**200 Nodes**	**300 Nodes**
FBC	20	38	61	83
PoW-SDN	22	40	65	89
HB-SDN-IoT	**34**	**72**	**109**	**151**

This evaluation focuses on the system's ability to scale in terms of Transactions Per Second (TPS) under increasing network size as given in Table 10. The proposed HB-SDN-IoT framework exhibits significantly higher TPS compared to conventional models, attributed to its cluster-based load distribution, SDN-enabled flow optimization, and smart contract acceleration at the edge. As the network scales from 50 to 300 IoT nodes, traditional models such as Full Blockchain Configuration (FBC) and PoW-SDN show only moderate improvements, reaching a peak TPS of 83 and 89, respectively, at 300 nodes. Conversely, the HB-SDN-IoT architecture achieves a notable 151 TPS at the same scale, underscoring its superior scalability and processing efficiency.

This sharp increase in throughput is a direct result of architectural innovations, including dual-layer blockchain consensus mechanisms, trust-aware routing, and real-time resource allocation by SDN controllers. These features collectively minimize processing delays and validation overheads, ensuring high performance even under dense and dynamic IoT environments. Consequently, the HB-SDN-IoT model emerges as a robust and scalable solution for large-scale IoT deployments where responsiveness

and reliability are critical.

4.2.9. Trust Score Accuracy

Trust score accuracy is a critical metric that reflects the effectiveness of a security framework in identifying and responding to malicious behaviors within the network. Specifically, it quantifies how accurately trust values are assigned to IoT nodes, especially under adversarial conditions such as Sybil attacks and replay attacks. A higher trust score accuracy indicates that the framework can reliably differentiate between benign and malicious nodes, thereby ensuring robust network integrity and preventing false positives or negatives in trust evaluation. In the proposed HB-SDN-IoT model, trust score accuracy is enhanced through the integration of anomaly-aware routing, real-time trust metric updates, and blockchain-backed historical behavior analysis. These mechanisms collectively ensure that trust values reflect the actual behavioral patterns of nodes, allowing the system to maintain security, consistency, and resilience even under sophisticated attack scenarios.

To derive these results under realistic adversarial conditions, we simulated a threat environment where 15% of nodes were configured to perform malicious actions, including Sybil identity forging, packet replay, and selective packet dropping. The trust degradation mechanism, as defined in Section 3.1.5, penalized such behavior using a learning–forgetting model, and nodes were marked untrustworthy once their trust score dropped below a defined threshold of 0.4. This threshold was used to exclude compromised nodes from cluster head candidacy and routing participation. The overall trust accuracy was computed using the formula:

$$Accurcy = \frac{TP+TN}{TP+TN+FP+FN} \times 100 \quad (25)$$

Where TP and TN denote true positives and true negatives, respectively. This methodological setup ensured that the 93.6% detection accuracy reflects the system's capability to dynamically identify and mitigate malicious behavior with high precision in an adversarial IoT network environment.

Table 11: Trust Score Accuracy

Protocol	Detection Accuracy (%)
SMSN	74.5
FBC	78.9
EESCFD	81.2
HB-SDN-IoT	**93.6**

Table 11 presents a comparative analysis of trust score accuracy across various security frameworks under adversarial conditions, including Sybil and replay attacks. The proposed HB-SDN-IoT framework demonstrates a significant advancement in accurately identifying malicious nodes through a combination of real-time blockchain audit trails, SDN-based traffic anomaly detection, and DDPG-informed trust evaluation. These components enable dynamic and context-aware trust scoring, enhancing the system's ability to distinguish between benign and adversarial behavior. Traditional models such as SMSN and FBC achieve moderate accuracy levels of 74.5% and 78.9%, respectively, reflecting limitations in static trust evaluation and centralized validation. EESCFD shows improved performance with 81.2%, benefiting from energy-aware trust mechanisms. In contrast, the HB-SDN-IoT model achieves a trust score accuracy of 93.6%, highlighting its robust trust management, adaptive learning, and resilience against advanced threats in dynamic IoT-CPS environments.

4.4. Discussion

The comprehensive evaluation of the proposed Hybrid Blockchain-based Secure SDN-IoT (HB-SDN-IoT) framework reveals substantial improvements across critical performance metrics when benchmarked against traditional routing protocols (AODV, DSDV, AOMDV), energy-aware clustering protocols (SMSN, EESCFD), and blockchain-integrated architectures (FBC, PoW-SDN). In terms of

throughput, the HB-SDN-IoT model achieves a peak performance of 96.8%, significantly outperforming FBC (91.6%) and AODV (87.3%) under dense network conditions. This improvement stems from SDN-enabled flow optimization, trust-aware cluster-based routing, and real-time path reconfiguration. End-to-end delay is also minimized, with latency maintained between 0.5 ms to 1.6 ms even as packet sizes scale to 3500 bytes. This low delay is facilitated by intelligent route selection, localized trust validation via lightweight private chains, and proactive anomaly detection, substantially outperforming FBC and SMSN in delay-sensitive environments. Regarding energy efficiency, the HB-SDN-IoT framework achieves up to 23% lower energy consumption than FBC and 18% lower than SMSN by minimizing redundant transmissions, adapting to residual energy profiles, and utilizing energy-efficient control signaling. The model also maintains a consistently high Packet Delivery Ratio (PDR), surpassing 91.2% at 300 nodes, confirming its robustness under large-scale deployment. Additionally, control overhead is reduced by over 40% compared to legacy protocols like AODV and DSDV, attributed to decentralized SDN control and lightweight Proof-of-Authority (PoS) consensus within private chains. The average transaction validation time is confined to 135 ms, which is considerably faster than PoW-based public blockchain systems, making the model well-suited for latency-critical IoT applications. In terms of security and resilience, the HB-SDN-IoT model demonstrates superior performance under blackhole attacks, limiting average latency to 61.2 ms, significantly lower than the 130.5 ms observed in FBC. Furthermore, trust score accuracy reaches 93.6% under Sybil and replay attack conditions, validating the reliability of its anomaly-aware trust evaluation mechanism powered by blockchain audit trails and deep reinforcement learning. Lastly, in evaluating scalability, the framework achieves 151 transactions per second (TPS) at 300 nodes, outperforming FBC (83 TPS) and PoW-SDN (89 TPS), showcasing its high-capacity transactional handling under increasing network load. In summary, the HB-SDN-IoT model offers a secure, scalable, energy-efficient, and real-time capable solution for next-generation IoT infrastructures. By combining SDN-driven traffic control, dual-layer blockchain consensus, and intelligent trust management, the proposed architecture addresses the fundamental limitations of existing protocols and presents a viable framework for industrial, mission-critical, and large-scale IoT deployments. While the proposed HB-SDN-IoT framework demonstrates strong improvements over traditional routing protocols such as AODV, DSDV, and AOMDV in terms of packet delivery ratio, energy efficiency, and trust accuracy, we acknowledge that these protocols do not represent the current state-of-the-art in blockchain or SDN-based IoT routing. Recent solutions such as B-SDNTrust, BlockSDN, and BChainIoT introduce more sophisticated trust evaluation, dynamic flow control, and lightweight consensus mechanisms that are more comparable to the proposed model. Due to implementation complexity and simulation compatibility limitations, these advanced baselines were not fully integrated into the present evaluation. However, their performance characteristics, as reported in literature, suggest competitive scalability and moderate energy consumption, albeit often at the cost of heavier consensus overhead or limited adaptability to dynamic trust states. In future work, we plan to extend the simulation environment or implement testbed comparisons that directly evaluate the proposed framework against such recent blockchain–SDN hybrid systems. This will offer a more rigorous benchmark and help generalize the effectiveness of the proposed architecture beyond traditional routing frameworks.

5. Conclusion

This paper introduced HB-SDN-IoT, a hybrid blockchain- and SDN-enabled secure routing framework for IoT networks. The proposed architecture addresses major limitations in existing solutions by introducing three key innovations: (i) a dual-layer blockchain model that separates intra-cluster and inter-controller consensus to optimize energy and security trade-offs; (ii) a trust- and energy-aware clustering mechanism coordinated via SDN controllers to enhance route stability and network resilience; and (iii) lightweight security mechanisms designed to detect and mitigate common IoT attacks such as Sybil, black hole, and replay attacks. Experimental evaluations demonstrated promising performance,

with a 23% reduction in energy consumption, a packet delivery ratio of 96.8%, and trust classification accuracy of 93.6%. These results suggest that the HB-SDN-IoT framework is a viable solution for secure, scalable, and energy-efficient communication in industrial IoT deployments. However, we acknowledge that the current work is limited in several important respects. The use of MATLAB-based simulation with simplified assumptions (e.g., uniform node energy, ideal wireless channels and deterministic consensus delay) restricts the generalizability of the findings. Additionally, the absence of formal security proofs, complexity analysis, and real-world testbed validation weakens the theoretical foundation of the framework. While the proposed design offers sound engineering contributions, it lacks the academic rigor expected in high-impact scholarly venues. To address the identified limitations and strengthen the overall contribution of this work, future work will focus on formal security verification using tools such as Tamarin, real-world deployment on IoT testbeds (e.g., Contiki-NG), and statistical validation through randomized simulations. Additionally, we aim to benchmark the proposed model against recent blockchain–SDN frameworks, including BlockSDN and B-SDNTrust, to further validate its comparative performance and scalability. To enhance the system's intelligence and decentralization, future extensions may also incorporate federated learning for privacy-preserving collaborative trust evaluation across distributed clusters. Moreover, embedding edge intelligence into SDN controllers could significantly reduce decision-making latency and improve responsiveness in dynamic network environments. These advancements, combined with robust security validation and practical deployments, will improve the practicality, adaptability, and industrial readiness of the HB-SDN-IoT framework.

Reference:

Aghili SF, & Mala H (2018) Security analysis of Fan et al.'s lightweight RFID authentication protocol for privacy protection in IoT. Cryptology ePrint Archive.

Ahn GJ, Gu G, Hu H, Shin S (2019) Guest editors' introduction: Special section on Security in emerging networking technologies. IEEE Trans. Dependable Secure Comput. 16(6): 913–914.

Alrashede, H., Eassa, F., Ali, A. M., Aljihani, H., & Albalwy, F. (2025). Enhancing east-west interface security in heterogeneous SDN via blockchain. PeerJ Computer Science, 11, e2914.

Ara T, Prabhkar M, Shah PG (2019) Energy efficient secured cluster-based distributed fault diagnosis protocol for IoT. Int. J. Commun. Netw. Inf. Secur. 10(3): 539.

Attkan A, & Ranga V (2022) Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security. Complex & Intelligent Systems 8(4): 3559-3591.

Banerjee S, Balas VE, Pandey A, & Bouzefrane S (2020) Towards intelligent optimization of design strategies of cyber-physical systems: measuring efficacy through evolutionary computations. Computational Intelligence in Emerging Technologies for Engineering Applications 73-101.

Barišić A, Ruchkin I, Savić D, Mohamed MA, Al-Ali R, Li LW, & Cicchetti A (2022) Multi-paradigm modeling for cyber–physical systems: A systematic mapping review. Journal of Systems and Software 183: 111081.

Bodkhe U, Mehta D, Tanwar S, Bhattacharya P, Singh PK, & Hong WC (2020) A survey on decentralized consensus mechanisms for cyber-physical systems. IEEE Access 8: 54371-54401.

Cai X, Geng S, Zhang J, Wu D, Cui Z, Zhang W, & Chen J (2021) A sharding scheme-based many-objective optimization algorithm for enhancing security in blockchain-enabled industrial internet of things. IEEE Transactions on Industrial Informatics 17(11): 7650-7658.

Chen S, Zhang L, Yan Z, & Shen Z (2021) A distributed and robust security-constrained economic dispatch algorithm based on blockchain. IEEE Transactions on Power Systems 37(1): 691-700.

Chen W, Wang Z, Hu J, Dong H, & Liu GP (2023) Distributed resilient state estimation for cyber-physical systems against bit errors: A zonotopic set-membership approach. IEEE Transactions on Network Science and Engineering.

Comer D, Rastegarnia A (2019) Toward disaggregating the SDN control plane. IEEE Commun. Mag. 57(10): 70–75.

Conti M, Dehghantanha A, Franke K, Watson S (2018) Internet of Things security and Forensics: Challenges and opportunities, Elsevier.

Dorri A, Kanhere SS, & Jurdak R (2016) Blockchain in internet of things: challenges and solutions. arXiv preprint arXiv:1608.05187.

Dorri, Kanhere SS, Jurdak R (2016) Blockchain in internet of things: Challenges and solutions. arXiv preprint arXiv:1608.05187.

Erel-Özçevik, M. (2025). Token as a Service for Software-Defined Zero Trust Networking. Journal of Network and Systems Management, 33(1), 10.

Frikha T, Chaabane F, Aouinti N, Cheikhrouhou O, Ben Amor N, & Kerrouche A (2021) Implementation of blockchain consensus algorithm on embedded architecture. Security and Communication Networks.

Han X, Shen G, Yang X, Kong X (2020) Congestion recognition for hybrid urban road Systems via digraph convolutional network. Transp. Res. C. 121: 102877.

Ibrahim A, & Dalkılıc G (2019) Review of different classes of RFID authentication protocols. Wireless Networks 25(3): 961-974.

Kaur, N., Mittal, A., Lilhore, U.K., Simaiya, S., Dalal, S., Saleem, K., & Ghith, E. S. (2025). Securing fog computing in healthcare with a zero-trust approach and blockchain. EURASIP Journal on Wireless Communications and Networking, 2025(1), 5.

Kumar G, Saha R, Rai MK, Thomas R, Kim TH (2018) Proof-of-work consensus approach in blockchain technology for cloud and fog computing using Maximization-factorization statistics. IEEE Internet Things J. 6(4): 6835–6842.

Kumar, S., Kumar, M., Azmea, C. N., & Vaigandla, K. K. (2024). BCSDNCC: A Secure Blockchain SDN framework for IoT and Cloud Computing. International Research Journal of Multidisciplinary Technovation, 6(3), 26-44.

Latif, S. A., Wen, F. B. X., Iwendi, C., Wang, L. L. F., Mohsin, S. M., Han, Z., & Band, S. S. (2022). AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. *Computer communications*, *181*, 274-283.

Li B, Liang R, Zhou W, Yin H, Gao H, & Cai K (2021) LBS meets blockchain: an efficient method with security preserving trust in SAGIN. IEEE Internet of Things Journal 9(8): 5932-5942.

Li W, Wang Y, & Li J (2023) A blockchain-enabled collaborative intrusion detection framework for SDN-assisted cyber-physical systems. International Journal of Information Security 1-12.

Lonkar, B., Kuthe, A., Charde, P., Dehankar, A., & Kolte, R. (2025). Optimal hybrid energy-saving cluster head selection for wireless sensor networks: an empirical study. Peer-to-Peer Networking and Applications, 18(4), 1-17.

Lourenço RB, Savas SS, Tornatore M, & Mukherjee B (2018). Robust hierarchical control plane for transport software-defined networks. Optical Switching and Networking 30: 10-22.

Mustafa, Khan IU, Aslam S, Sajid A, Mohsin SM, Awais M, Qureshi MB (2020) A lightweight post-quantum lattice-based RSA for secure communications. IEEE Access 8: 99273–99285.

Mythili, D., & Duraisamy, S (2024). PSA-LEACH: Improving Energy Efficiency and Classification in Wireless Sensor Networks Using Proximal Simulated Annealing with Low Energy Adaptive Clustering Hierarchical Routing Protocol.

Okon, A. A., Sallam, K. M., Hossain, M. F., Jagannath, N., Jamalipour, A., & Munasinghe, K. S. (2024). Enhancing Multi-Operator Network Handovers With Blockchain-Enabled SDN Architectures. *IEEE Access*, *12*, 82848-82866.

Puja Sharma, Dipendra Karki, Blockchain Technology in the Digital Era: Global Research Trends and Financial Innovation, Journal of Management Changes in the Digital Era, vol. 2, no.1, ISSN: 3007-9810/ DOI: 10.33168/JMCDE. 2025.0107.

Rahouti M, Xiong K, & Xin Y (2020) Secure software-defined networking communication systems for smart cities: current status, challenges, and trends. IEEE Access 9: 12083-12113.

Ran C, Yan S, Huang L, & Zhang L (2021) An improved AODV routing security algorithm based on blockchain technology in ad hoc networks. EURASIP Journal on Wireless Communications and Networking 1: 1-16.

Razvan, F., & Mitica, C. (2025). Enhancing network security through integration of game theory in software-defined networking framework. International Journal of Information Security, 24(3), 100.

Santatra Hagamalala Bernardin, Franck Morvan, Riad Mokadem, Hasinarivo Ramanana, Hasimandimby Rakotoarivelo, TCDRM: A Tenant Budget-Aware Data Replication Framework for Multi-Cloud Computing, Journal of Logistics, Informatics and Service Science, Vol. 12 (2025) No. 3, pp. 246-263.

Sellami B, Hakiri A, Yahia SB, & Berthou P. A Blockchain Architecture for SDN-Enabled Tamper-Resistant IoT Networks.

Singh, C., & Jain, A. K. (2024). A comprehensive survey on DDoS attacks detection & mitigation in SDN-IoT network. e-Prime-Advances in Electrical Engineering, Electronics and Energy, 100543.

Song, Y., Feng, T., Yang, C., Mi, X., Jiang, S., & Guizani, M. (2023). IS2N: Intent-driven security software-defined network with blockchain. IEEE Network, 38(3), 118-127.

Song, Y., Feng, T., Yang, C., Mi, X., Jiang, S., & Guizani, M. (2023). IS2N: Intent-driven security software-defined network with blockchain. IEEE Network, 38(3), 118-127.

Subramanian, N. S., Krishnan, P., Jain, K., Kumar, K. A., Pandey, T., & Buyya, R. (2025). Blockchain and RL-Based Secured Task Offloading Framework for Software-Defined 5G Edge Networks. IEEE Access.

Tan L, Yu K, Ming F, Chen X, Srivastava G (2021) Secure and resilient artificial Intelligence of things: A HoneyNet approach for threat detection and situational Awareness. IEEE Consum. Electron. Mag.

Tanha FE, Hasani A, Hakak S, & Gadekallu TR (2022) Blockchain-based cyber physical systems: Comprehensive model for challenge assessment. Computers and Electrical Engineering 103: 108347.

Vairagade R, Bitla L, Judge HH, Dharpude SD, and Kekatpure SS (2022) Proposal on NFT Minter for Blockchain-based Art-Work Trading System. In 2022 IEEE 11th International Conference on Communication Systems and Network Technologies (CSNT) 571-576.

Vairagade RS and Brahmananda SH (2020) Secured Multi-Tier Mutual Authentication Protocol for Secure IoT System. In 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT) 195-200.

Vairagade RS and SH B (2022) Enabling machine learning-based side-chaining for improving QoS in blockchain-powered IoT networks. Transactions on Emerging Telecommunications Technologies 33(4): e4433.

Velmurugadass P, Dhanasekaran S, Anand SS, & Vasudevan V (2021). Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptographic hash algorithm. Materials Today: Proceedings 37: 2653-2659.

Villegas-Ch, W., Govea, J., Gurierrez, R., & Mera-Navarrete, A. (2025). Optimizing security in IoT ecosystems using hybrid artificial intelligence and blockchain models: a scalable and efficient approach for threat detection. IEEE Access.

Xu C, Ji J, & Liu P (2018) The station-free sharing bike demand forecasting with a deep learning approach and large-scale datasets. Transportation research part C: emerging technologies 95: 47-60.

Yagisawa M (2017). Improved fully homomorphic encryption without bootstrapping. Cryptology ePrint Archive.

Yi D, Su J, Liu C, & Chen WH (2018) Trajectory clustering aided personalized driver intention prediction for intelligent vehicles. IEEE Transactions on Industrial Informatics 15(6): 3693-3702.

Yu Z, Gao H, Cong X, Wu N, & Song HH (2023) A survey on cyber-physical systems security. IEEE Internet of Things Journal.

Zhou Y, Zhang D, & Xiong N (2017) Post-cloud computing paradigms: a survey and comparison. Tsinghua Science and Technology 22(6): 714-732.