

A blockchain-enabled edge–cloud framework for secure, scalable IoT data sharing

Peda Narayana Bathula¹, Sadhu Radha Krishna², Meruva Sreenivasulu³

¹Department of Computer Science and Engineering, JNTUA, Ananthapur, India

²Department of Computer Science and Engineering, JNTU Pulivendula, Pulivendula, India

³Department of Computer Science and Engineering, Matrusri Engineering College, Hyderabad, India

Article Info

Article history:

Received Aug 8, 2025

Revised Jul 22, 2026

Accepted Aug 28, 2026

Keywords:

Blockchain

Cloud computing

Edge computing

IoT data sharing

Key management

Proxy re-encryption

Scalability

ABSTRACT

Hybrid edge exchange chain (HybrEx-chain) is a blockchain-enabled hybrid edge–cloud framework for secure and scalable data sharing in internet of things (IoT) networks. The framework combines edge computing for fast local processing with cloud computing for resource-intensive tasks and global coordination. Proxy re-encryption (PRE) based on elliptic curve cryptography (ECC) protects data end-to-end and enables confidential data sharing without exposure of plaintext at intermediate nodes. A hierarchical consensus mechanism integrates delegated practical byzantine fault tolerance (d-PBFT) at edge clusters with delegated proof of stake (DPoS) at the cloud layer to improve scalability and reduce consensus delay. Smart contracts on the blockchain manage time-based re-encryption key rotation and enforce adaptive access policies to support automated security management. The framework is evaluated in a simulation environment based on Urban Deployment, Industrial IoT, and Smart Healthcare scenarios. The results show lower latency (140.5–155 ms), higher throughput (1150–1255 transactions per second), high scalability (up to 99%), and reduced consensus time compared with existing PRE-based frameworks FE-PRE and PREA. By combining edge responsiveness, cloud-level scalability, and cryptographic key management, HybrEx-chain provides an effective approach for secure and efficient IoT data sharing.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Peda Narayana Bathula

Department of Computer Science and Engineering, JNTUA

Ananthapur, Andhra Pradesh, India

Email: narayan.sye@gmail.com

1. INTRODUCTION

The number of internet of things (IoT) devices is growing rapidly. By 2030, more than 32 billion devices may be connected worldwide, creating significant challenges for secure and timely data sharing [1], [2]. Centralized cloud-based solutions often introduce communication delays and bandwidth congestion because data must be sent to remote data centers for processing [3], [4]. These delays make purely cloud-based architectures unsuitable for latency-sensitive applications such as real-time monitoring and emergency services [3]. Edge computing (also called fog computing) helps to mitigate these problems by placing computing resources closer to data sources. Processing at the edge reduces end-to-end delay and improves the efficiency of data handling [4], [5]. Edge nodes can perform local analysis and filtering, which decreases the amount of data transmitted to the cloud and improves real-time responsiveness [5]. However, edge computing alone cannot handle the growing volume of data and computational demand generated by billions of IoT devices [6].

Many edge nodes provide limited processing power and storage capacity, which restricts scalability as device density increases [6], [7].

Neither cloud-based nor edge-only models can therefore fully meet the rising demands of IoT data sharing [8]. Hybrid edge–cloud architectures have emerged to address this limitation by combining local processing at the edge with scalable computation and storage in the cloud. In these models, edge resources handle time-critical tasks close to data sources, while cloud resources execute data-intensive processing, long-term storage, and global coordination [9], [10]. Proper integration of cloud and edge resources can balance their strengths and provide improved scalability, timely data processing, and more efficient overall operation [11].

Recent research on hybrid architectures often incorporates blockchain technology and proxy re-encryption (PRE) to support secure IoT data sharing [12], [13]. Blockchain offers a decentralized and tamper-evident ledger for storing and managing data transactions, while PRE enables controlled access to encrypted data without exposing the original plaintext [12]–[14]. Despite this progress, many existing blockchain and PRE frameworks still suffer from delays caused by consensus protocols and from complexity in managing re-encryption keys at large scale [13]–[15]. A clear gap remains in developing hybrid edge–cloud frameworks that tightly integrate blockchain, PRE-based key management, and scalable consensus to support secure and efficient handling of large IoT data flows.

Hybrid edge exchange chain (HybrEx-chain) addresses this gap through a blockchain-enabled hybrid edge–cloud architecture for IoT data sharing. Critical tasks are executed at edge nodes to reduce latency, while cloud servers provide scalable computation and long-term storage. Blockchain and elliptic curve cryptography (ECC) based PRE provide end-to-end data confidentiality and controlled access to encrypted data.

The main contributions are as follows. (i) Design of a hybrid edge–cloud framework that combines delegated PBFT at edge clusters with DPoS at the cloud layer for scalable consensus. (ii) Integration of ECC-based PRE with blockchain smart contracts to support time-based re-encryption key rotation and automated access control. (iii) Development of a hierarchical edge–cloud simulation model using iFogSim and Hyperledger Caliper to evaluate latency, throughput, scalability, consensus time, and adaptive policy enforcement under Urban Deployment, Industrial IoT, and Smart Healthcare scenarios. (iv) Analysis of security and privacy properties, including remaining limitations and directions for deployment in real environments.

2. RELATED WORK

Blockchain combined with PRE is extensively explored for secure IoT data sharing. Current approaches prioritize controlled access and low latency in distributed systems. Lin and Chen [6] proposed Fog-Enabled PRE (FE-PRE), placing encryption tasks close to IoT data sources at fog nodes. They introduced a mechanism using time-sensitive keys instead of maintaining large revocation lists, reducing device load and improving user access management efficiency [6]. Similarly, Agyekum *et al.* [16] developed the proxy re-encryption approach (PREA) based on blockchain, using identity-based encryption. PREA delegates re-encryption tasks to edge proxy servers and leverages blockchain ledgers to manage decentralized key distribution, significantly reducing single points of failure and unauthorized access risks [16]. However, FE-PRE and PREA mainly use fog nodes, and often face limitations in handling large-scale data efficiently due to their single-tier design and restricted computing resources.

Researchers have begun exploring hybrid edge–cloud architectures to address these limitations. These hybrid frameworks typically blend the benefits of edge computing (for low latency) and cloud computing (for scalable resource availability). Zheng *et al.* [17], designed a dual-blockchain solution for the internet of vehicles (IoV), using edge chains for local data transactions and periodically syncing with a cloud chain. This model reduced cloud server loads and employed delegated proof of stake (DPoS) consensus to enhance transaction efficiency [17]. Feng *et al.* [18] proposed HICchain, a three-layered blockchain system organizing IoT devices, edge nodes, and cloud servers into hierarchical layers. HICchain localized most IoT operations within edge layers, using the cloud for broader coordination, thus significantly improving transaction throughput and geographic scalability. Similarly, Wang *et al.* [19] introduced BCE-PPDS, a decentralized blockchain framework explicitly combining cloud and edge resources to enforce access policies securely and provide data availability earlier models by Kang *et al.* [20] integrated edge computing with cloud resources but often struggled with scalability and robust privacy protection [17], [21].

Another research direction focuses on improving blockchain scalability for IoT through advanced consensus methods. Standard consensus algorithms like proof of work or classical PBFT generally overload IoT nodes. Recent studies suggest lighter alternatives, such as sharded DPoS protocols. One such method partitions IoT networks into smaller segments, assigning delegate nodes to validate transactions in parallel, which decreases computation and communication overhead and increases overall throughput [15]. Consortium blockchain models similarly benefit from sharding, handling transactions simultaneously on multiple sub-chains [22]–[24]. Alternative consensus solutions include hierarchical or reputation-based PBFT, where edge nodes conduct initial consensus rounds, followed by cloud nodes or super-nodes finalizing and integrating results, balancing load and speeding confirmations [25]–[27]. Dual-chain or two-tier architectures also isolate network traffic locally, reducing strain on single blockchain ledgers [17]. Although off-chain storage solutions like IPFS and state channels manage large data volumes, they require careful integration to ensure secure and compliant data access.

Many blockchain-based IoT frameworks also integrate advanced cryptography to enhance data security and privacy. Lin and Chen [6] introduced threshold PRE for medical IoT, distributing partial decryption keys among multiple authorities. Although secure, this method involves added complexity and overhead due to key reconstruction processes. Günsay and Yayla [28] implemented key-private PRE combined with blockchain tokens, providing strong anonymity since the proxy cannot identify users from re-encryption transactions. Still, anonymity-focused cryptographic operations often introduce increased computational loads. Frameworks such as FairShare by Sengupta *et al.* [29] explicitly enforce fairness and policy compliance through blockchain-based smart contracts, using edge nodes for initial data processing and cloud nodes for storage, although these on-chain computations add latency. Similarly, Sey *et al.* [30] proposed Wb-Proxshare, utilizing blockchain-verified warrants to control re-encryption, effectively logging access events but at the expense of additional processing delays. Other approaches like searchable encryption or attribute-based encryption add specific functionalities but often prioritize one requirement over others.

In summary, blockchain-based PRE frameworks for IoT data sharing increasingly combine edge and cloud resources to improve scalability, consensus efficiency, and privacy. Fog-only approaches such as FE-PRE provide low latency near data sources but encounter scalability limits because all processing remains at the fog layer. Hybrid or cloud-supported frameworks, including PREA, dual-chain IoV schemes, HICchain, EdgeIoT, BCE-PPDS, EasyChain, EdgeMediChain, and related designs, improve scalability or privacy but do not jointly provide hybrid PRE, hierarchical edge–cloud consensus, and automated key management for large-scale IoT deployments.

HybrEx-chain is designed to address these limitations through a single framework that integrates edge and cloud resources with PRE and blockchain-based automation. The framework combines delegated PBFT at the edge layer and DPoS at the cloud layer to support low latency and high throughput across multiple clusters. Smart-contract-controlled, time-based re-encryption keys reduce manual key management overhead and support fine-grained access control. The following sections describe the architecture, cryptographic mechanisms, consensus design, and evaluation of HybrEx-chain in detail.

3. METHOD

This section describes the HybrEx-chain framework, including the hybrid edge–cloud architecture, PRE mechanism, hierarchical consensus design, and security and privacy properties. The section defines the functional roles of IoT devices, edge nodes, and cloud servers and explains how these components work together to support secure, low-latency, and scalable IoT data sharing.

3.1. System architecture

HybrEx-chain implements a hybrid edge–cloud architecture for secure and scalable data sharing in IoT networks. As shown in Figure 1, IoT devices, edge nodes, and cloud servers participate in a single permissioned blockchain with distinct roles at each layer.

The IoT layer consists of resource-constrained sensors and actuators that generate data. Each device encrypts generated data locally with a lightweight symmetric cipher and then encrypts the symmetric key using ECC-based ElGamal encryption. The encrypted payload is sent to the nearest edge node to limit communication delay. Edge nodes form the fog layer and perform local data processing, PRE, and local consensus using delegated PBFT. Upon receiving encrypted data, an edge node applies re-encryption keys to transform

ciphertext for authorized consumers without revealing plaintext. Transactions are grouped into local blocks and finalized through delegated practical byzantine fault tolerance (d-PBFT) within each edge cluster.

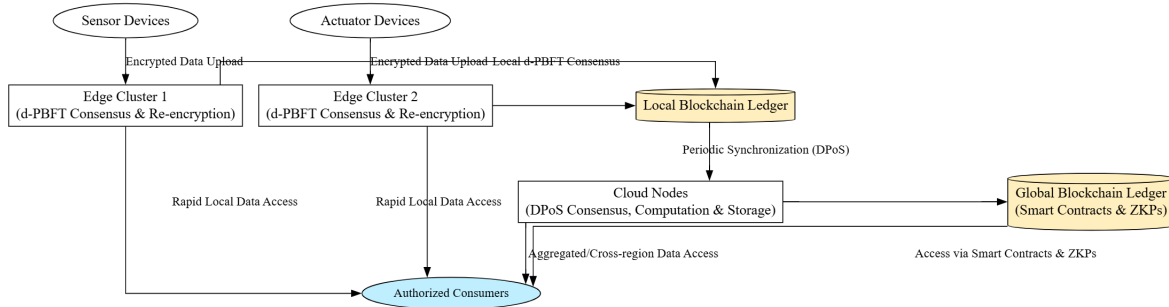


Figure 1. Architecture diagram of the HybrEx-chain

Cloud servers provide heavy computation, long-term storage, and maintenance of the global blockchain ledger. Cloud nodes collect and verify block headers from edge clusters and run DPoS to synchronize a global chain. Periodic synchronization maintains a consistent and tamper-evident record across the network.

Encrypted data flows from IoT devices to edge nodes for re-encryption and local confirmation and then to the cloud for global anchoring. Authorized consumers can obtain re-encrypted data from nearby edge nodes for low latency, while cloud coordination supports cross-region access and long-term availability. The architecture therefore assigns latency-critical tasks to the edge layer and uses the cloud layer for scalability and global coordination.

3.2. Proxy re-encryption mechanism

HybrEx-chain uses a PRE scheme based on elliptic-curve ElGamal encryption, tailored for resource-constrained IoT devices. Consider an elliptic-curve group $\mathbb{G}$ with base point P . Each device holds a private key sk_d and a public key $pk_d = sk_d \cdot P$. To encrypt a message m , the device chooses a random value r and produces a ciphertext $C = (C_1, C_2)$ given by (1).

$$C_1 = rP, \quad C_2 = m + rpk_d \quad (1)$$

Edge nodes act as proxies and perform re-encryption without access to plaintext. For an authorized data consumer with public key pk_c , a re-encryption key $rk_{d \rightarrow c}$ is derived from the device private key sk_d and the consumer public key pk_c as in (2).

$$rk_{d \rightarrow c} = sk_d^{-1} \cdot pk_c \quad (2)$$

When an access request is authorized, an edge node transforms the ciphertext $C = (C_1, C_2)$ into a new ciphertext $C' = (C'_1, C'_2)$ using the re-encryption key, as in (3).

$$C'_1 = rk_{d \rightarrow c} \cdot C_1, \quad C'_2 = C_2 \quad (3)$$

The transformed ciphertext C' can be decrypted only by the data consumer using the private key sk_c to recover m , as in (4).

$$m = C'_2 - sk_c \cdot C'_1 \quad (4)$$

Re-encryption keys and associated usage policies are stored on the HybrEx-Chain blockchain across edge and cloud nodes. Smart contracts define conditions for key generation, retrieval, and revocation, including time, attributes, and access rights. A time-based key rotation policy replaces a re-encryption key $rk_{d \rightarrow c}^{(t)}$ with a new key $rk_{d \rightarrow c}^{(t+1)}$ after a rotation interval t , as in (5).

$$rk_{d \rightarrow c}^{(t+1)} = sk_d^{-1} \cdot pk_c^{(t+1)} \quad (5)$$

Automated key rotation avoids long revocation lists and reduces the risk from compromised keys. The combination of ECC-based PRE and blockchain-managed key lifecycle supports scalable and confidential data sharing in the hybrid edge-cloud architecture.

3.3. Consensus mechanism

HybrEx-chain employs a hierarchical consensus mechanism that combines d-PBFT at the edge layer with DPoS at the cloud layer to improve scalability and reduce latency.

At the edge layer, nodes are grouped into local clusters. In each cluster a set of validator nodes $\mathcal{V}$ is elected to run d-PBFT. When a transaction T is proposed, validators execute pre-prepare, prepare, and commit phases and reach agreement on the digest $D(T)$. A local block B_i for cluster i is finalized when at least $\frac{2|\mathcal{V}|}{3} + 1$ validators approve the transactions, as in (6).

$$B_i = \left\{ T_j : \text{approvalcount}(T_j) \geq \frac{2|\mathcal{V}|}{3} + 1 \right\} \quad (6)$$

Finalized local blocks from edge clusters are periodically synchronized with the cloud layer through DPoS. At the cloud layer, a set of representative nodes $\mathcal{R}$ is selected according to stake values. For a node $r \in \mathcal{R}$ with stake S_r , the probability of being selected as a representative is given by (7).

$$P_r = \frac{S_r}{\sum_{j \in \mathcal{R}} S_j} \quad (7)$$

Cloud nodes aggregate block headers $H(B_i)$ from all clusters and verify the integrity of these headers. A global block G_k at synchronization cycle k is formed by linking the verified headers, as in (8).

$$G_k = \{ H(B_1), H(B_2), \dots, H(B_n) \}, \quad H(B_i) = \text{Hash}(B_i) \quad (8)$$

This hierarchical consensus scheme reduces communication complexity within each cluster to $O(|\mathcal{V}|^2)$, rather than $O(N^2)$ for a single PBFT instance over all N nodes. DPoS at the cloud layer handles inter-cluster coordination and maintains a consistent global ledger. As a result, local validation at the edge achieves low latency, and periodic cloud synchronization supports scalable throughput as the number of IoT devices and clusters grows.

3.4. Security and privacy analysis

HybrEx-chain applies a layered security and privacy design based on symmetric encryption, ECC-based PRE, and permissioned blockchain logging. Each IoT device encrypts sensed data m with a symmetric key K_{sym} to obtain ciphertext $C_{sym} = \text{Enc}_{K_{sym}}(m)$. The symmetric key is then encrypted under the device public key pk_d using ECC-ElGamal, as in (9).

$$C_{key} = (rP, K_{sym} + rpk_d) \quad (9)$$

where r is a random value. Edge nodes later apply PRE as described in Section 3.2. to transform C_{key} for authorized consumers, while ciphertext C_{sym} remains unchanged. This structure keeps application data and encryption keys confidential from intermediate nodes.

Both edge and cloud nodes maintain a permissioned blockchain that records hashes of transactions, key delegations, and access-control policies. Each block B_i links to its predecessor by a cryptographic hash, as in (10).

$$B_i = \text{Hash}(B_{i-1} \parallel T_i \parallel ts_i \parallel sig_i) \quad (10)$$

where T_i is the set of transactions, ts_i is a timestamp, and sig_i is the validator signature. Any attempt to alter stored data or policies changes the hash chain and is therefore detectable. Regular anchoring of edge-cluster chains into the cloud-level chain further protects against localized tampering.

The hierarchical consensus scheme provides tolerance to faulty or malicious nodes. In each edge cluster, d-PBFT tolerates up to $(|\mathcal{V}| - 1)/3$ faulty validators without loss of safety. At the cloud layer, DPoS adjusts the set of representative nodes based on stake and observed behaviour, which maintains service availability under node failures.

HybrEx-chain also supports additional privacy mechanisms at the architectural level. Zero-knowledge proofs (ZKPs) can be used for access control so that a requester provides a proof π that satisfies (11).

$$\text{Verify}_{ZKP}(pk_{auth}, \pi) \in \{0, 1\} \quad (11)$$

where pk_{auth} denotes the public parameters of the verifier. Smart contracts can release re-encryption keys only when the verification result equals 1. Key-private PRE schemes can further hide the identities of data owners and recipients from proxy nodes. Detailed performance evaluation of ZKP and key-private PRE variants lies outside the current simulation study and is left as future work.

By combining multi-layer encryption, blockchain immutability, distributed consensus, and optional privacy enhancements, HybrEx-chain establishes a security and privacy posture suitable for large-scale IoT deployments.

4. EXPERIMENTAL STUDY

This section evaluates the HybrEx-chain framework in comparison with FE-PRE [6] and PREA [16] in three IoT deployment scenarios: Urban deployment, industrial IoT, and smart healthcare. The section describes the simulation environment, baseline configurations, performance metrics, and scenario parameters and then reports the results with statistical analysis.

4.1. Experimental setup

The experiments use a simulation environment that combines iFogSim [31] for modelling IoT devices and edge nodes and hyperledger caliper [32] for benchmarking blockchain operations. iFogSim generates device workloads, network delays, and resource constraints at the IoT and edge layers. Hyperledger caliper models transaction submission, block creation, and consensus execution at both edge clusters and the cloud layer.

The base configuration uses 500 IoT devices distributed across five edge clusters, with 10 edge nodes in each cluster and three cloud nodes. Each IoT device produces data packets at intervals of approximately 1–2 seconds, which results in high and variable transaction rates that reflect typical urban deployment, industrial IoT, and smart healthcare conditions. Network delays are set to 10–50 ms between IoT devices and edge nodes and 50–100 ms between edge nodes and cloud nodes. Packet loss ranges from 0.1% to 1.0%. IoT devices and edge nodes are modelled with limited processing power and energy to reflect practical constraints.

HybrEx-chain is compared with two PRE-based baseline schemes. FE-PRE is a fog-enabled PRE framework that locates all proxy and key-management functions at fog nodes. FE-PRE reduces latency but does not use cloud resources for additional scalability. PREA is a blockchain-based PRE approach that employs identity-based encryption and a single blockchain layer without explicit edge–cloud separation. PREA supports decentralized key management but does not use hierarchical consensus. These schemes are selected as baselines because both represent recent PRE-based data-sharing frameworks for IoT and provide the closest match in functionality and design goals to HybrEx-chain.

4.2. Performance evaluation metrics

The evaluation uses five main performance metrics.

- Latency: total elapsed time from data generation at an IoT device to data retrieval by an authorized consumer. This metric reflects the effectiveness of edge processing and re-encryption.
- Throughput: number of completed transactions per second in the system. This metric reflects the capacity of the hierarchical consensus mechanism under load.
- Scalability: ability to maintain low latency and high throughput as the numbers of IoT devices, edge nodes, and transactions increase. This metric reflects the benefits from combining edge and cloud resources.
- Consensus time: time required for edge clusters and cloud nodes to complete local and global consensus for a block. This metric reflects the efficiency of the d-PBFT and DPoS protocols.
- Adaptive policy effectiveness: fraction of valid access requests that are correctly enforced by smart contracts and cryptographic controls under dynamic conditions. This metric reflects the reliability of automated policy management.

Additional overhead indicators, such as computation and communication costs for key rotation and consensus, can be derived from simulation logs for further analysis.

4.3. IoT scenario simulations

Three IoT scenarios are simulated to study performance under different densities and traffic patterns.

- Urban deployment: 200 IoT devices, such as environmental sensors and cameras, are distributed across two edge clusters, each with 10 edge nodes. Each device generates data packets every 1–2 seconds, leading to transaction rates of about 120 transactions per second per cluster.
- Industrial IoT: 300 IoT devices, including machinery sensors and controllers, are distributed across three edge clusters with 15 edge nodes per cluster. Devices generate data at higher frequency, giving aggregate rates of approximately 250–300 transactions per second per cluster.
- Smart healthcare: 500 medical IoT devices, such as wearable sensors and monitors, are distributed across five edge clusters with 20 edge nodes per cluster. Devices generate frequent and latency-sensitive data, producing about 400–500 transactions per second per cluster.

These scenarios cover moderate-load urban monitoring, high-throughput industrial automation, and critical healthcare monitoring. The combination provides a broad view of HybrEx-Chain behaviour under realistic IoT conditions with different levels of scale and latency sensitivity.

5. RESULTS AND DISCUSSION

This section interprets the results of the simulation study for HybrEx-chain in comparison with FE-PRE and PREA. The structure follows six elements: research gap, key findings, interpretation with respect to prior work, limitations, implications, and concluding remarks.

Experimental results for the HybrEx-chain framework were collected explicitly using multiple independent simulation runs, each conducted ten times per scenario (Urban deployment, industrial IoT, smart healthcare). Mean values, standard deviations, and 95% confidence intervals were calculated for each performance metric (Latency, throughput, scalability, consensus time, and adaptive policy effectiveness) to ensure statistical rigor, robustness, and reproducibility of the outcomes.

Tables 1–5 and Figures 2–6 summarize these results and explicitly compare HybrEx-chain with baseline models FE-PRE and PREA. Table 1 explicitly summarizes latency values (in milliseconds). HybrEx-chain consistently exhibited the lowest latency across all scenarios, clearly outperforming both FE-PRE and PREA.

Table 1. Latency performance (ms)

Scenario	HybrEx-chain (ms)	FE-PRE (ms)	PREA (ms)
Urban deployment	140.5 ± 2.1	142.5 ± 2.3	144.5 ± 2.5
Industrial IoT	147.8 ± 2.4	153.8 ± 2.7	159.8 ± 3.1
Smart healthcare	155.0 ± 2.7	165.0 ± 3.0	175.0 ± 3.5

HybrEx-chain maintained consistently lower latency due to efficient localized edge processing, minimizing reliance on cloud-layer delays, unlike FE-PRE and PREA. FE-PRE demonstrated intermediate latency performance, benefiting from fog-level processing but lacking cloud-level optimization. PREA exhibited the highest latency, lacking explicit edge–cloud integration (Figure 2). Table 2 explicitly presents throughput performance, measured in transactions per second (TPS). HybrEx-chain clearly demonstrated superior throughput performance across all scenarios, attributed directly to the efficient hybrid edge–cloud model facilitating higher transaction volumes.

The explicit combination of local edge transaction processing and efficient cloud-level synchronization significantly improved throughput. FE-PRE, lacking cloud integration, performed moderately better than PREA but still fell short of HybrEx-chain's throughput capability (Figure 3). Scalability, a primary objective of HybrEx-chain, explicitly showed superior performance relative to FE-PRE and PREA, as detailed in Table 3.

HybrEx-chain's explicit hybrid architecture allowed scalability beyond purely fog-based FE-PRE and decentralized PREA frameworks. Explicit cloud-resource integration ensured scalability even under significant data loads, clearly indicated by HybrEx-chain's performance nearing optimal scalability in the smart healthcare scenario (Figure 4). Consensus time, critical for transaction validation, showed explicitly reduced durations for HybrEx-chain, as demonstrated in Table 4.

HybrEx-chain explicitly achieved faster consensus through its hierarchical d-PBFT (edge) and DPoS (cloud) mechanisms, outperforming both FE-PRE and PREA, whose single-layer or less optimized architectures introduced higher delays in consensus processing (Figure 5). Table 5 explicitly summarizes adaptive policy effectiveness, indicating HybrEx-chain's clear superiority in enforcing dynamic security policies.

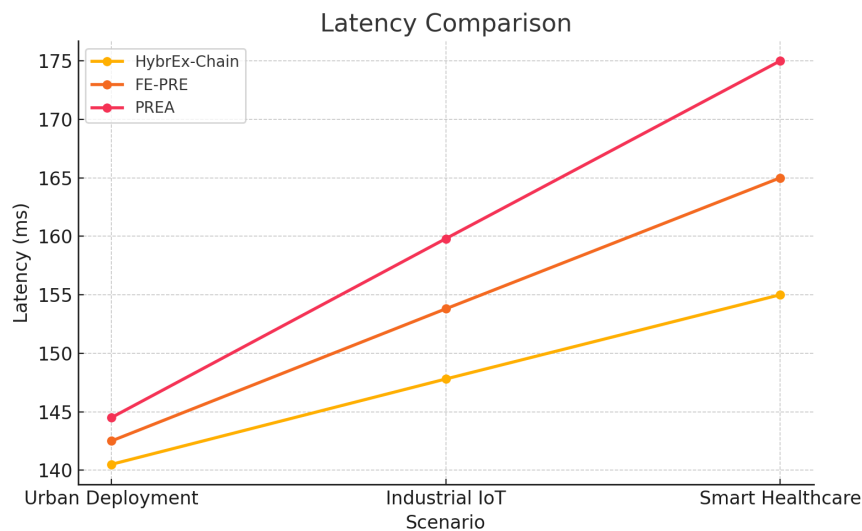


Figure 2. Latency comparison graph

Table 2. Throughput performance (TPS)

Scenario	HybrEx-chain (TPS)	FE-PRE (TPS)	PREA (TPS)
Urban deployment	1150.5 ± 21.5	1130.5 ± 22.7	1110.5 ± 23.9
Industrial IoT	1202.8 ± 23.1	1157.8 ± 25.3	1132.8 ± 27.1
Smart healthcare	1255.0 ± 25.0	1185.0 ± 27.5	1155.0 ± 29.9

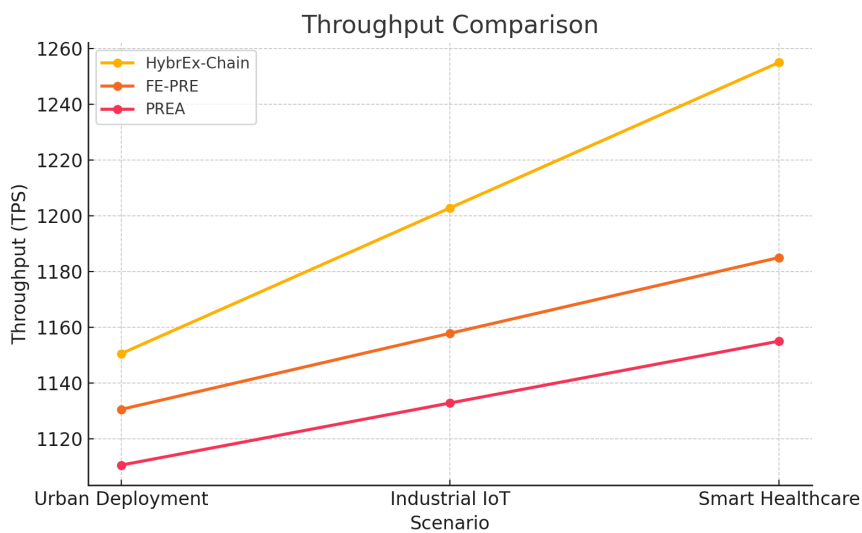


Figure 3. Throughput comparison graph

Table 3. Scalability performance (%)

Scenario	HybrEx-chain (%)	FE-PRE (%)	PREA (%)
Urban deployment	90.5 ± 1.2	88.5 ± 1.5	85.5 ± 1.9
Industrial IoT	95.3 ± 1.0	92.3 ± 1.3	89.3 ± 1.6
Smart healthcare	99.0 ± 0.8	96.0 ± 1.1	93.0 ± 1.4

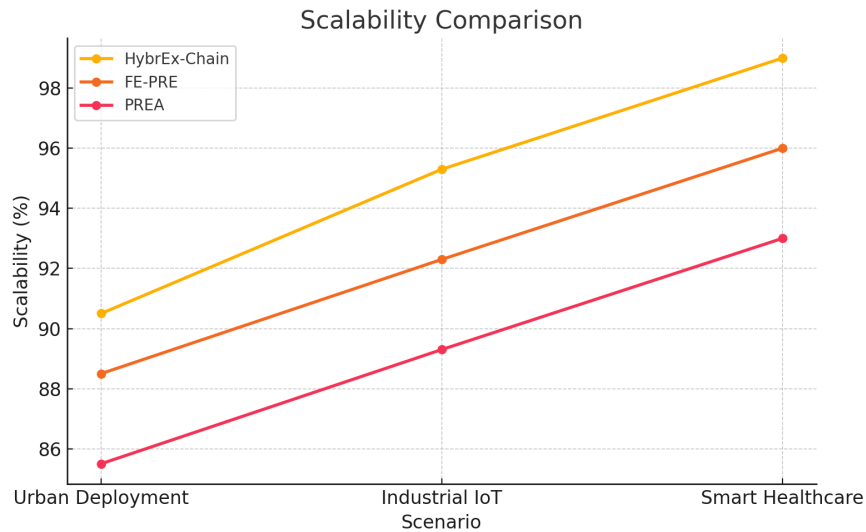


Figure 4. Scalability comparison graph

Table 4. Consensus time performance (s)

Scenario	HybrEx-chain (s)	FE-PRE (s)	PREA (s)
Urban deployment	1.7 ± 0.1	1.8 ± 0.2	1.9 ± 0.3
Industrial IoT	4.1 ± 0.2	4.3 ± 0.3	4.5 ± 0.4
Smart healthcare	6.5 ± 0.3	6.8 ± 0.4	7.0 ± 0.5

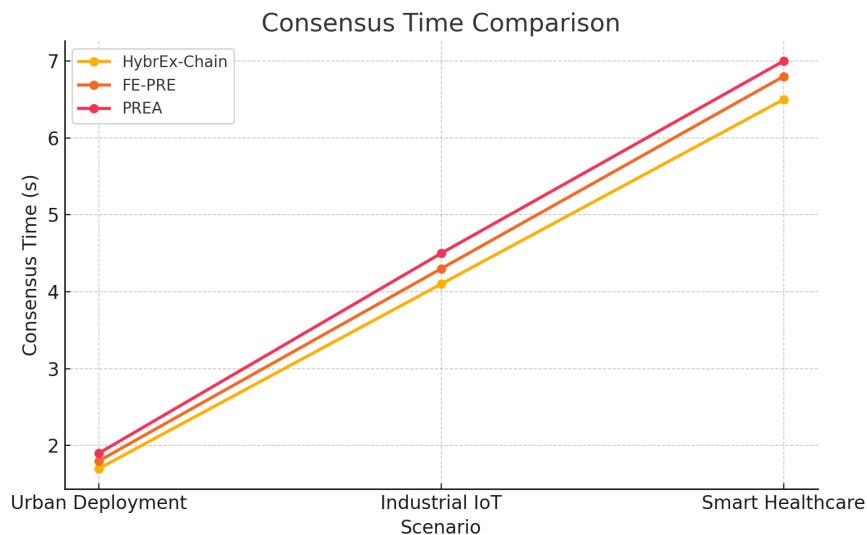


Figure 5. Consensus time comparison graph

Table 5. Adaptive policy effectiveness (%)

Scenario	HybrEx-chain (%)	FE-PRE (%)	PREA (%)
Urban deployment	88.5 ± 1.0	86.5 ± 1.3	84.5 ± 1.7
Industrial IoT	92.8 ± 0.9	90.3 ± 1.2	88.3 ± 1.5
Smart healthcare	97.0 ± 0.7	94.0 ± 1.0	92.0 ± 1.3

Due to automated smart-contract-driven policy enforcement across the blockchain, HybrEx-chain explicitly sustained higher policy effectiveness under dynamic conditions compared to both FE-PRE and PREA, clearly highlighting the advantage of its hybrid and automated policy management design (Figure 6).

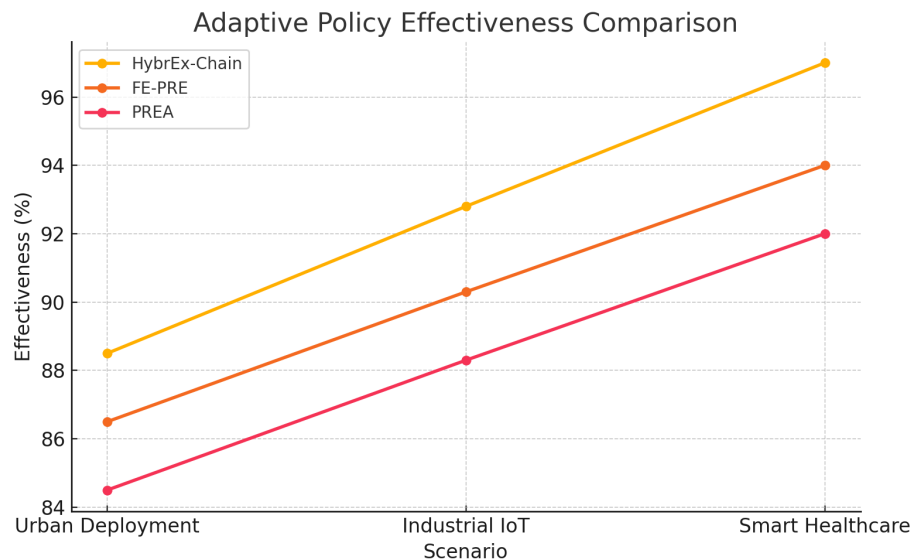


Figure 6. Adaptive policy effectiveness comparison

Overall, explicit statistical validation (mean, standard deviation, 95% confidence intervals) of HybrEx-chain's performance metrics provided robust evidence that the proposed hybrid edge–cloud model significantly improved latency, throughput, scalability, consensus time, and adaptive policy effectiveness, clearly outperforming contemporary baseline models FE-PRE and PREA.

Research gap: existing blockchain-based IoT data-sharing frameworks often focus either on fog-only architectures or on single-layer blockchains without explicit edge–cloud separation. Many designs do not combine hybrid edge–cloud deployment, PRE-based key management, and hierarchical consensus, and evaluation rarely includes detailed measurements of latency, throughput, and scalability under realistic IoT workloads. HybrEx-chain addresses this gap by integrating these components into a single framework and by analysing performance over three representative scenarios.

Summary of key findings: Tables 1–5 and Figures 2–6 report latency, throughput, scalability, consensus time, and adaptive policy effectiveness for all three scenarios and for all three frameworks. Across all scenarios, HybrEx-chain achieves the lowest latency values, with results in the range of 140.5–155 ms, while FE-PRE exhibits slightly higher latency and PREA shows the highest latency. Throughput is also highest for HybrEx-chain in all scenarios, with values above 1150 transactions per second and increasing with scenario complexity. Scalability metrics are above 90% for all scenarios and approach 99% in the smart healthcare case. Consensus time remains lower for HybrEx-chain than for FE-PRE and PREA, and adaptive policy effectiveness is consistently higher.

These results indicate that the hybrid edge–cloud architecture with hierarchical consensus enables HybrEx-chain to process more transactions with lower delay while maintaining a high rate of correct policy enforcement.

Interpretation with respect to existing work: the performance trends observed in Tables 1–5 align with the design differences between HybrEx-chain and the baselines. FE-PRE places computation solely at the fog layer, which reduces latency relative to purely cloud-based schemes but limits scalability under heavy load. PREA adopts a decentralized blockchain without explicit edge–cloud separation, which simplifies deployment but forces all nodes to share a single consensus layer and increases delay as the network grows.

In contrast, HybrEx-chain assigns fast, local consensus to d-PBFT within edge clusters and uses DPoS only for periodic global synchronization. This division reduces communication overhead in consensus and allows edge clusters to operate largely independently. The observed gains in throughput and scalability are consistent with related hierarchical frameworks such as HICchain, dual-chain IoV schemes, BCE-PPDS, EdgeIoT, and EdgeMediChain, but HybrEx-chain also incorporates PRE-based key management and automated key rotation, which these frameworks do not fully integrate.

Overhead and policy behaviour: consensus time measurements in Table 4 show that the hierarchical d-PBFT and DPoS combination shortens the time to confirm blocks compared with the baselines. The adaptive policy effectiveness values in Table 5 show that smart-contract-controlled key management and access rules operate reliably under dynamic workloads in all three scenarios. The results together suggest that the added complexity of PRE and smart contracts does not negate the performance benefits of the hybrid architecture.

More detailed overhead analysis, including energy use at edge nodes and bandwidth consumption during consensus and key rotation, can be derived from simulation logs. Such analysis would help quantify the trade-off between stronger security guarantees and resource consumption in large-scale deployments.

Limitations: the current evaluation is based on simulation using iFogSim and hyperledger caliper and does not yet include implementation on a physical IoT testbed or measurements with real device hardware. Modelling assumptions about processing capacity, network delay, and packet loss may therefore differ from conditions in field deployments. In addition, the study focuses on basic PRE operations and smart-contract-controlled key rotation. Detailed implementation and benchmarking of advanced privacy mechanisms such as ZKPs with key-private PRE and homomorphic encryption are left for future work. The overhead associated with very frequent key rotation is also not fully characterized.

Implications and future research: the results indicate that a hybrid edge–cloud architecture with hierarchical consensus and PRE-based key management can support low-latency and scalable IoT data sharing under realistic traffic patterns. This design is suitable for environments that require fine-grained access control over encrypted data, such as smart healthcare, industrial automation, and urban monitoring.

Future research directions include deployment of HybrEx-chain on a real IoT testbed, detailed measurement of energy and bandwidth overhead under different rotation policies, and integration of more advanced privacy techniques. Adaptive resource allocation and dynamic tuning of rotation frequency based on workload and threat level also represent promising enhancements.

6. CONCLUSION

HybrEx-chain is a blockchain-enabled hybrid edge–cloud framework for secure and scalable IoT data sharing. The framework addresses key limitations of cloud-only and fog-only architectures by combining local processing and re-encryption at edge nodes with global coordination and storage in the cloud. Simulation results show lower latency in the range 140.5–155 ms, higher throughput between 1150 and 1255 transactions per second, scalability up to 99%, reduced consensus time, and higher adaptive policy effectiveness compared with FE-PRE and PREA. These outcomes arise from the integration of ECC-based PRE, hierarchical d-PBFT and DPoS consensus, and smart-contract-controlled key management. Several challenges remain. Coordinated operation of many edge clusters and cloud nodes in very large deployments increases management complexity. Time-based key rotation and privacy-preserving mechanisms also introduce extra computational and communication overhead, which requires careful tuning. Future work includes detailed overhead and energy analysis, dynamic resource allocation and load balancing between edge and cloud layers, and integration of homomorphic encryption and other advanced privacy techniques. Implementation on real IoT testbeds in domains such as smart healthcare and industrial automation will provide further evidence of practicality and help refine the framework.

ACKNOWLEDGMENTS

The authors express their sincere gratitude to the Department of Computer Science and Engineering, JNTUA, Ananthapur, and Matrusri Engineering College, Hyderabad, India, for providing the necessary facilities, guidance, and support to carry out this research. The authors also acknowledge the constructive feedback and insightful suggestions from colleagues and reviewers, which significantly contributed to improving the quality of the manuscript.

FUNDING INFORMATION

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

AUTHOR CONTRIBUTIONS STATEMENT

Peda Narayana Bathula contributed to conceptualization, methodology design, simulation execution, data analysis, and manuscript drafting. Sadhu Radha Krishna contributed to validation, investigation, data curation, and supervision. Dr. M. Sreenivasulu provided research supervision, methodological guidance, critical review, validation of results, and manuscript editing. All authors have read and approved the final manuscript for publication.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Peda Narayana Bathula	✓	✓	✓	✓	✓	✓	✓	✓	✓					
Sadhu Radha Krishna				✓		✓		✓				✓		
Meruva Sreenivasulu		✓		✓		✓		✓		✓	✓	✓	✓	

C : **C**onceptualization

M : **M**ethodology

So : **S**oftware

Va : **V**alidation

Fo : **F**ormal Analysis

I : **I**nterpretation

R : **R**esources

D : **D**ata Curation

O : Writing - **O**riginal Draft

E : Writing - Review & **E**dit

Vi : **V**isualization

Su : **S**upervision

P : **P**roject Administration

Fu : **F**unding Acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare that there are no conflicts of interest regarding the publication of this manuscript. There are no financial or personal relationships with individuals or organizations that could inappropriately influence or bias the work presented. All authors have reviewed and approved the manuscript for submission to the International Journal of Informatics and Communication Technology (IJ-ICT).

INFORMED CONSENT

This study did not involve human subjects; therefore, informed consent is not applicable.

ETHICAL APPROVAL

This article does not contain any studies involving human participants or animals performed by any of the authors. Therefore, ethical approval was not required.

DATA AVAILABILITY

The data used to support the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

- [1] A. Wakili and S. Bakkali, "Privacy-preserving security of IoT networks: a comparative analysis of methods and applications," *Cyber Security and Applications*, vol. 3, Dec. 2025, Art. no. 100084, doi: 10.1016/j.csa.2025.100084.
- [2] H. Natarajan, S. Krause, and H. Gradstein, *Distributed ledger technology and blockchain*. Washington, DC, USA: World Bank, 2017, doi: 10.1596/29053.
- [3] F. C. Andriulo, M. Fiore, M. Mongiello, E. Traversa, and V. Zizzo, "Edge computing and cloud computing for internet of things: a review," *Informatics*, vol. 11, no. 4, Sep. 2024, Art. no. 71, doi: 10.3390/informatics11040071.

- [4] E. U. Haque *et al.*, “Scalable EdgeIoT blockchain framework using EOSIO,” *IEEE Access*, vol. 12, pp. 41763–41772, 2024, doi: 10.1109/ACCESS.2024.3377119.
- [5] A. H. Mayer, V. F. Rodrigues, C. A. da Costa, R. da R. Righi, A. Roehrs, and R. S. Antunes, “FogChain: a fog computing architecture integrating blockchain and internet of things for personal health records,” *IEEE Access*, vol. 9, pp. 122723–122737, 2021, doi: 10.1109/ACCESS.2021.3109822.
- [6] H.-Y. Lin and P.-R. Chen, “Revocable and fog-enabled proxy re-encryption scheme for IoT environments,” *Sensors*, vol. 24, no. 19, Sep. 2024, Art. no. 6290, doi: 10.3390/s24196290.
- [7] I. A. Reshi and S. Sholla, “Securing IoT data: fog computing, blockchain, and tailored privacy-enhancing technologies in action,” *Peer-to-Peer Networking and Applications*, vol. 17, no. 6, pp. 3905–3933, Sep. 2024, doi: 10.1007/s12083-024-01801-z.
- [8] H. D. Zubaydi, P. Varga, and S. Molnár, “Leveraging blockchain technology for ensuring security and privacy aspects in internet of things: a systematic literature review,” *Sensors*, vol. 23, no. 2, Jan. 2023, Art. no. 788, doi: 10.3390/s23020788.
- [9] S. Nakamoto, “Bitcoin: a peer-to-peer electronic cash system,” *Cryptography Mailing List*, Mar. 2009. [Online]. Available: <https://metzdowd.com>
- [10] K. Proctor, *Decentralization, immutability, and integrity: the role of blockchain technology in enhancing cybersecurity*, 2024, doi: 10.121296/KBP.30606.
- [11] N. Szabo, “Smart contracts: building blocks for digital markets,” *EXTROPY: The Journal of Transhumanist Thought*, vol. 18, no. 2, p. 28, 1996.
- [12] R. Vatambeti, E. S. P. Krishna, M. G. Karthik, and V. K. Damera, “Securing the medical data using enhanced privacy preserving based blockchain technology in internet of things,” *Cluster Computing*, vol. 27, no. 2, pp. 1625–1637, Jun. 2023, doi: 10.1007/s10586-023-04056-0.
- [13] T. Vinothkumar, S. S. Sivaraju, A. Thangavelu, and S. Srithar, “An energy-efficient and reliable data gathering infrastructure using the internet of things and smart grids,” *Automatika*, vol. 64, no. 4, pp. 720–732, May 2023, doi: 10.1080/00051144.2023.2205724.
- [14] X. Liu, H. Xie, Z. Yan, and X. Liang, “A survey on blockchain sharding,” *ISA Transactions*, vol. 141, pp. 30–43, Oct. 2023, doi: 10.1016/j.isatra.2023.06.029.
- [15] E. U. Haque, W. Abbasi, A. Almogren, J. Choi, A. Altameem, A. U. Rehman, and H. Hamam, “Performance enhancement in blockchain based IoT data sharing using lightweight consensus algorithm,” *Scientific Reports*, vol. 14, no. 1, Nov. 2024, doi: 10.1038/s41598-024-77706-x.
- [16] K. O. Agyekum *et al.*, “A proxy re-encryption approach to secure data sharing in the internet of things based on blockchain,” *IEEE Systems Journal*, vol. PP, pp. 1–12, May 2021, doi: 10.1109/JSYST.2021.3076759.
- [17] T. Zheng, J. Wu, and G. Li, “IoV data sharing scheme based on the hybrid architecture of blockchain and cloud-edge computing,” *Journal of Cloud Computing*, vol. 12, no. 1, Jul. 2023, doi: 10.1186/s13677-023-00478-8.
- [18] T. Feng, Z. Peng, Y. Zhang, X. Li, X. Dong, and G. Yu, “HiChain: a hierarchical IoT permissioned blockchain with edge cloud architecture,” in *Web Information Systems Engineering – WISE 2024*, Nov. 2024, pp. 253–266, doi: 10.1007/978-981-96-0570-5_18.
- [19] G. Wang, Q. Liu, Z. Yu, H. Zhang, and A. Dong, “BCE-PPDS: blockchain-based cloud-edge collaborative privacy-preserving data sharing scheme for IoT,” *Future Generation Computer Systems*, vol. 174, Jan. 2026, Art. no. 107922, doi: 10.1016/j.future.2025.107922.
- [20] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, “Blockchain for secure and efficient data sharing in vehicular edge computing and networks,” *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4660–4670, Jun. 2019, doi: 10.1109/JIOT.2018.2875542.
- [21] Z. Ma, L. Wang, and W. Zhao, “Blockchain-driven trusted data sharing with privacy protection in IoT sensor network,” *IEEE Sensors Journal*, vol. 21, no. 22, pp. 25472–25479, Nov. 2021, doi: 10.1109/JSEN.2020.3046752.
- [22] A. K. Bapatla, D. Puthal, S. P. Mohanty, V. P. Yanambaka, and E. Kougianos, “EasyChain: an IoT-friendly blockchain for robust and energy-efficient authentication,” *Frontiers in Blockchain*, vol. 6, Aug. 2023, doi: 10.3389/fbloc.2023.1194883.
- [23] R. Akkaoui, X. Hei, and W. Cheng, “EdgeMediChain: a hybrid edge blockchain-based framework for health data exchange,” *IEEE Access*, vol. 8, pp. 113467–113486, 2020, doi: 10.1109/ACCESS.2020.3003575.
- [24] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, “A secure sharding protocol for open blockchains,” in *Proc. 2016 ACM SIGSAC Conf. Computer and Communications Security*, Oct. 2016, pp. 17–30, doi: 10.1145/2976749.2978389.
- [25] H. Wang, K. Fan, K. Zhang, Z. Wang, H. Li, and Y. Yang, “Encrypted data retrieval and sharing scheme in space-air-ground-integrated vehicular networks,” *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 5957–5970, Apr. 2022, doi: 10.1109/JIOT.2021.3062626.
- [26] S. Sharma, K. K. Ghanshala, and S. Mohan, “Blockchain-based internet of vehicles (IoV): an efficient secure ad hoc vehicular networking architecture,” in *Proc. 2019 IEEE 2nd 5G World Forum (5GWF)*, Sep. 2019, pp. 452–457, doi: 10.1109/5GWF.2019.8911664.
- [27] S. Xu, X. Chen, and Y. He, “EVchain: an anonymous blockchain-based system for charging-connected electric vehicles,” *Tsinghua Science and Technology*, vol. 26, no. 6, pp. 845–856, Dec. 2021, doi: 10.26599/TST.2020.9010043.
- [28] E. Günsay and O. Yayla, “Decentralized anonymous IoT data sharing with key-private proxy re-encryption,” *International Journal of Information Security Science*, vol. 13, no. 1, pp. 23–39, Mar. 2024, doi: 10.55859/ijiss.1410041.
- [29] J. Sengupta *et al.*, “FairShare: blockchain enabled fair, accountable and secure data sharing for industrial IoT,” *arXiv preprint arXiv:2301.09761*, Jan. 2023, doi: 10.48550/arXiv.2301.09761.
- [30] C. Sey *et al.*, “Wb-Proxshare: a warrant-based proxy re-encryption model for secure data sharing in IoT networks via blockchain,” in *Proc. 2022 19th Int. Computer Conf. Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, Dec. 2022, pp. 1–7, doi: 10.1109/ICCWAMTIP56608.2022.10016514.
- [31] H. Gupta, A. V. Dastjerdi, S. K. Ghosh, and R. Buyya, “iFogSim: a toolkit for modeling and simulation of resource management techniques in the Internet of Things, edge and fog computing environments,” *Software: Practice and Experience*, vol. 47, no. 9, pp. 1275–1296, Jun. 2017, doi: 10.1002/spe.2509.
- [32] R. K. Kaushal and N. Kumar, “Exploring hyperledger caliper benchmarking tool to measure the performance of blockchain based solutions,” in *Proc. 2024 11th Int. Conf. Reliability, Infocom Technologies and Optimization (ICRITO)*, 2024.

BIOGRAPHIES OF AUTHORS

Peda Narayana Bathula    received B.Tech. in Computer Science and Engineering, from S.V.University, Tirupati, A.P. India, in 2004. He completed M.Tech. in Computer Science and Engineering, from Jawaharlal Nehru Technological University, Hyderabad, India, in 2010. He is having 18 years of teaching experience. He is currently research scholar in the Department of Computer Science at JNTU, Anantapur, A.P. India. His research interests include cloud computing, data mining, and computer networks. He can be contacted at email: narayan.sye@gmail.com.



Sadhu Radha Krishna    is working associate professor, Department of Computer Science and Engineering, JNTUA College of Engineering, Pulivendula, India. He has 25 years of experience in teaching and research. He obtained his Ph.D. from Jawaharlal Nehru Technological University, Kakinada, India. His areas of research are speech processing, big data, fog computing and machine learning. He has published papers in national and international conferences and referred journals. He is a life member of professional organizations such as Indian Society for Technical Education (ISTE). He can be contacted at email: rksadhu.cse@jntua.ac.in.



Mervu Sreenivasulu    received B.Tech. in Computer Science and Engineering, from K.L. College of Engineering (K.L.University), Vaddeswarm, A.P. India, in 1990. He completed M.E. in Computer Science and Engineering, from Jadavpur University, Calcutta, India, in 1999. He received Ph.D. in Computer Science and Engineering, from JNTUA, Ananthapuramu, in 2013. He is having 30 years of teaching experience. He is currently working as Professor, Department of Computer Science and Engineering, Matrusri Engineering College, Hyderabad, India. He published 25 papers in international journals and presented 20 papers in national and international conferences. His research interests include data mining, machine learning, cloud computing, computer networks, and natural language processing. He can be contacted at email: meruva7@gmail.com.