Journal of Information Systems Engineering and Management
2025, 10(13s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Blockchain Enabled Proxy Re-Encryption Framework for Secure and Low Latency Data Sharing in Fog based IoT Networks

[*1]Peda Narayana Bathula, [2]Dr. M. Sreenivasulu
[1]Research Scholar, Department of Computer Science & Engineering, JNTUA, Ananthapur, AP.
[*1]Email: narayan.sye@gmail.com
[2]Professor, Department of Computer Science and Engineering, Matrusri Engineering College, Hyderabad, India. [2]Email: mesrinu@rediffmail.com
[*]**Corresponding Author**

ARTICLE INFO

Received: 24 Nov 2024
Revised: 07 Jan 2025
Accepted: 28 Jan 2025

ABSTRACT

This research introduces FoReChain (Fog-based Re-Encryption Chain), a blockchain-enabled proxy re-encryption (PRE) framework designed for secure, low-latency data sharing in fog-based IoT networks. The framework addresses key challenges related to data security, privacy, and performance in distributed environments, where traditional models face issues like high latency, limited scalability, and inefficient key management. FoReChain integrates blockchain with ECC-based proxy re-encryption to secure data without exposing original content. A delegated Practical Byzantine Fault Tolerance (d-PBFT) consensus mechanism ensures efficient transaction validation. The framework processes data at fog nodes, reducing delays commonly found in cloud-dependent models. Key management relies on time-based key updates stored immutably on the blockchain, while zero-knowledge proofs support secure, anonymous data sharing. The study evaluates FoReChain against FE-PRE and PREA models using metrics such as latency, throughput, scalability, blockchain consensus time, and adaptive policy effectiveness. Results show lower latency, higher throughput, and better adaptability in FoReChain, especially under heavy network conditions like smart healthcare and industrial IoT setups. FoReChain demonstrates secure data sharing, efficient resource utilization, and reliable key management in dynamic IoT environments. It offers consistent performance under varying loads, with improved scalability and data integrity maintained through decentralized validation.

Keywords: Blockchain, Proxy Re-Encryption, Fog Computing, IoT Networks, d-PBFT, Data Security, Key Management, Latency.

1 INTRODUCTION

The integration of blockchain technology with proxy re-encryption (PRE) frameworks provides a structured solution to handle challenges in fog-based IoT networks, particularly those related to security, privacy, and latency. IoT networks frequently share data across distributed devices, creating risks such as unauthorized access and data tampering. Blockchain introduces an immutable ledger for recording data transactions, ensuring transparency and data integrity [1]. Proxy re-encryption enables secure data sharing by transforming encrypted data for different users without exposing the original content, facilitating fine-grained access control [2], [3].

Fog-based IoT networks use local fog nodes to process data closer to devices, reducing delays compared to cloud-based systems [4]. Blockchain supports this framework by recording re-encryption keys and access

policies, preventing unauthorized access to sensitive data. Proxy re-encryption offloads computationally intensive encryption and transformation tasks from IoT devices to fog nodes, reducing the burden on resource-constrained devices while maintaining secure data sharing [5].

The proposed framework leverages fog computing to minimize latency, which is crucial for real-time applications like autonomous systems. It employs a delegated Practical Byzantine Fault Tolerance (d-PBFT) consensus mechanism, allowing nodes to validate transactions efficiently. This method organizes nodes into clusters to approve data operations, avoiding bottlenecks associated with centralized systems. Transactions and updates are stored immutably on the blockchain, ensuring tamper resistance while maintaining a transparent record of data sharing activities [6].

Managing access revocation and ensuring privacy during data sharing remain critical challenges. Time-based key updates eliminate the need for extensive revocation lists, addressing these concerns efficiently [2]. Techniques such as zero-knowledge proofs and key-private encryption are implemented to ensure user anonymity while maintaining secure communication, enhancing the privacy of the framework [7], [8]. These approaches address issues identified in earlier frameworks and align with the specific needs of IoT networks.

This integration of blockchain and PRE provides a methodical approach to secure data exchanges in IoT environments. By processing and storing data locally at fog nodes, latency concerns are addressed, and access controls are implemented effectively. The framework balances efficiency and security, offering a reliable structure for IoT applications, with its components and mechanisms addressing key gaps noted in prior research [9].

2 RELATED WORK

Ashok et al. [1], Choudhary et al. [10], Agyekum et al. [11], Pei et al. [9], and Wang et al. [12] explore blockchain and proxy re-encryption (PRE) for secure data sharing in IoT networks. Blockchain stores re-encryption keys and policies immutably, while PRE enables encrypted data sharing without exposing its original content. Ashok et al. [1], Saisanthiya, D. et al., [4], and Chen, Yingwen et al., [13] utilize elliptic curve cryptography (ECC) to reduce the computational burden on IoT devices and ensure secure data tracking through immutable ledgers. Choudhary et al. [10] emphasize using fog nodes for local encrypted data transformation, minimizing reliance on centralized servers. Agyekum et al. [11], Saradha, M., B. et al., [8] incorporate dynamic key updates to improve access control in distributed systems. Pei et al. [9] introduce threshold encryption for secure data sharing in medical IoT networks, distributing decryption responsibilities to ensure confidentiality. Wang et al. [12], Manzoor, Ahsan et al., [14] address scalability with lightweight cryptographic methods but highlight delays in blockchain consensus as a limitation.

Lin et al. [2], Shashikala et al. [5], and Reshi et al. [15] examine fog computing combined with blockchain to enable localized processing and reduce latency in IoT environments. Lin et al. [2] propose time-based key updates to handle key revocation while securely storing policies on blockchain, improving data-sharing efficiency. Shashikala et al. [5] focus on assigning re-encryption tasks to fog nodes to minimize computational overhead on devices. Reshi et al. [15] integrate fog nodes and blockchain for scalable data-sharing frameworks but identify vulnerabilities in fog nodes and fault tolerance as key concerns.

Günsay et al. [6] and Sengupta et al. [16] explore privacy-preserving mechanisms in IoT networks. Günsay et al. [6] use key-private encryption to maintain anonymity while enabling secure data sharing through blockchain and PRE. Sengupta et al. [16] propose FairShare, a framework that ensures data-sharing compliance with predefined policies while protecting privacy. Both frameworks identify computational challenges in implementing privacy mechanisms, especially in large-scale settings.

Xu et al. [17], Velez et al. [18], and Fugkeaw et al. [19] focus on using attribute-based encryption (ABE) to enhance access control. Xu et al. [17] introduce a searchable PRE framework, allowing secure queries of encrypted data. Velez et al. [18] propose verifying access policy compliance during data sharing. Fugkeaw et al. [19] apply lightweight cryptographic methods to minimize computational overhead in

medical IoT applications. These methods improve security and data access but require solutions to manage the computational demands of ABE in resource-constrained environments.

Collins et al. [20] introduce WB-Proxshare, a system that ensures data-sharing permissions comply with predefined blockchain rules. It decentralizes verification processes and supports secure key transformation. However, the reliance on warrant verification adds computational overhead.

The reviewed studies highlight the potential of integrating blockchain with PRE to address secure data-sharing needs in IoT networks. Blockchain ensures decentralized, immutable storage of access policies, while PRE enables flexible, controlled sharing of encrypted data. Ashok et al. [1], Lin et al. [2], Choudhary et al. [10], Agyekum et al. [11], Pei et al. [9], and others demonstrate these capabilities across different use cases. Common challenges include managing key revocation, ensuring system fault tolerance, and reducing computational complexity in large-scale deployments. These findings underline the importance of designing lightweight cryptographic techniques and scalable frameworks tailored to the dynamic demands of IoT networks.

3 METHODS AND MATERIALS

This section used to design, implement, and evaluate the FoReChain framework. It describes the system architecture, detailing how IoT devices, fog nodes, and the blockchain interact to ensure secure and low-latency data sharing. The section also explains the proxy re-encryption scheme, the consensus mechanism employed for data validation, and the experimental setup used to test the framework's performance. Each component is described to highlight its role in enhancing data security, access control, and system efficiency within fog-based IoT networks.

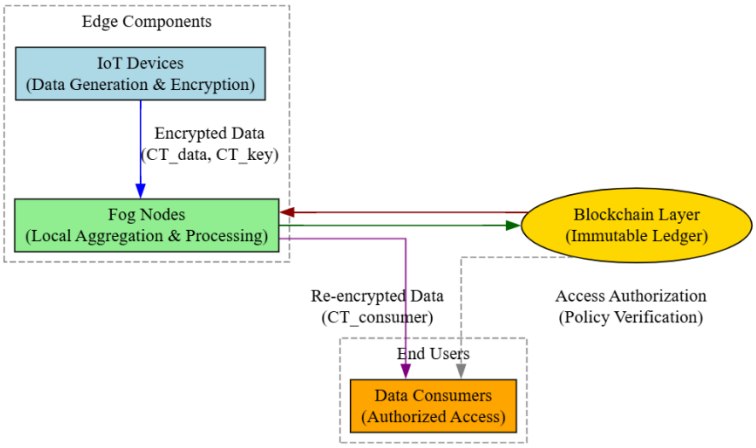

Figure 1: System Architecture for Blockchain-Based Proxy Re-Encryption in Fog Computing

The diagram shown in figure 1 shows the main components and their interactions in the system. IoT devices encrypt data and send it to fog nodes for local aggregation and processing. The fog nodes store metadata, including re-encryption keys and access policies, on the blockchain. Requests for data from consumers are validated against the policies stored in the blockchain. Authorized requests retrieve re-encryption keys, allowing fog nodes to transform encrypted data into a format accessible by the consumers. The data flow uses orthogonal connections for clear representation of interactions between IoT devices, fog nodes, the blockchain layer, and data consumers.

3.1 System Architecture

Participants: IoT end devices feature limited computation and storage, handling data capture and preliminary tasks. Fog nodes sit at the network edge for local data operations, caching, and consensus. A

blockchain layer spans across fog nodes, holding re-encryption keys and usage rules in a shared ledger. Data consumers, such as analytics services or applications, request and gather data based on those rules.

Data Flow Overview: Each device creates data and applies an ECC-based ElGamal approach for encryption. Let

$$DataEnc = Enc_{PK_{device}}(Data, r) \quad \text{....(Eq 1)}$$

Eq 1 and Eq 2 where PK_{device} represents the public key and r is a random factor. A symmetric key K_s, used for rapid encryption, is encrypted under the same public key. Both items go on the blockchain alongside a usage policy.

$$RK_{\text{device}\rightarrow\text{consumer}} = \text{ReKeyGen}(SK_{\text{device}}, PK_{\text{consumer}}) \quad \text{....(Eq 2)}$$

Eq 3 re-encryption key appears on the blockchain as well. When a data request is approved, a fog node retrieves this key and transforms the ciphertext so the consumer's private key can unlock the content. The consumer acquires the ciphertext from local storage or the device, applies to restore K_s, and then uses K_s to retrieve the original data.

$$Dec_{SK_{consumer}}(\cdot) \quad \text{....(Eq 3)}$$

3.2 Proxy Re-Encryption Scheme

A technique uses elliptic curve ElGamal encryption to shift ciphertext from a device key to a consumer key without revealing original data. The method reduces overhead on IoT hardware, confines transformations to a single route, and prevents collusion from granting unauthorized decryption.

Requirements: Minimal operations occur on devices. A unidirectional path halts reverse transformations. Collusion does not allow proxies to gain hidden details.

Proposed PRE Approach: An ECC-based ElGamal cryptosystem preserves concise key sizes. Each device holds a public–private pair $(PK_{\text{device}}, SK_{\text{device}})$. Each data consumer holds $(PK_{\text{cons}}, SK_{\text{cons}})$: Eq 4

$$RK_{D\rightarrow C} = ReKeyGen(SK_{device}, PK_{cons}) \quad \text{....(Eq 4)}$$

A re-encryption key resides in encrypted form on the blockchain, designated solely for ciphertext transformation. After authorization, a fog node obtains $RK_{D\rightarrow C}$ and converts CT_D into CT_C: Eq 5

$$CT_C = ReEnc(CT_D, RK_{D\rightarrow C}) \quad \text{....(Eq 5)}$$

Decryption uses SK_{cons}. Once re-encryption completes, data becomes accessible under the policy in place.

3.3 Blockchain Consensus Mechanism for Fog-Based IoT

Requirements for Fog IoT: Short wait times remain vital in near-instant operations. A consensus plan addresses numerous endpoints and frequent transactions. Several nodes rely on limited computing capacity.

Hybrid Consensus Model: A delegated version of Practical Byzantine Fault Tolerance (d-PBFT) operates within clusters. One node in each cluster compiles local actions, such as device registrations or re-encryption updates, into a block. Other nodes in the cluster receive that block and perform validation. The cluster appends the block to the local record, where nnn refers to the total node count. Periodic merges create upper-level blocks for broader alignment.

Some refinements keep blocks minimal by including key references and transaction pointers while placing large sensor outputs in off-chain storage. A batch verification approach processes multiple signatures together, which reduces cryptographic operations without adding extra time.

3.4 Security Analysis

Authorization and Access Control: A ledger keeps re-encryption keys and usage rules. Each key creation or transformation action appears as an unchangeable record. This practice blocks unknown entities from taking confidential keys.

Data Confidentiality: A two-layer encryption scheme protects sensor data. An inner key K locks sensitive readings, then that key is hidden with PK_{device}. A proxy applies but does not see raw content. This step deters exposure of private material at the proxy Eq6.

$$CT_C = ReEnc(CT_D, RK_{D\to C}) \quad \text{....(Eq 6)}$$

Data Integrity: A ledger design deters hidden edits because each effort to alter an entry triggers detection. Blocks reaching final status remain fixed by the d-PBFT process. This layout keeps earlier entries safe from change.

Scalability and Fault Tolerance: Multiple fog nodes carry out data tasks, reducing disruptions if one node malfunctions. The delegated-PBFT framework continues primary processes despite any compromised nodes, which helps retain stable performance across many endpoints.

4 EXPERIMENTAL STUDY

This experimental study evaluates the performance of Fog-based Re-Encryption Chain (FoReChain), a blockchain-enabled proxy re-encryption framework designed for secure, low-latency data sharing in fog-based IoT networks. To provide a comprehensive analysis, the performance of FoReChain is compared with two contemporary models Fog-Enabled Proxy Re-Encryption Scheme (FE-PRE) [2] and Proxy Re-Encryption Approach (PREA) [11]. FE-PRE introduces dynamic access control with time-based key updates and localized data processing through fog nodes, focusing on reducing latency while maintaining privacy. PREA integrates decentralized key distribution with dynamic key updates to enhance secure data sharing in distributed IoT environments, though it faces potential latency issues under high transaction volumes. The experimental setup simulates real-world IoT environments to assess these frameworks across key performance metrics such as latency, throughput, re-encryption efficiency, authorization time, and fault tolerance, ensuring an objective comparison of their security and scalability capabilities.

4.1 Experimental Setup

The experimental setup evaluates FoReChain alongside FE-PRE [2] and PREA [11] in a simulated fog-based IoT environment. It replicates real-world conditions where data moves from IoT devices through fog nodes to blockchain networks for secure sharing. iFogSim models IoT devices and fog nodes. It simulates how data is generated, processed, and transmitted. This helps in measuring delays during encryption, re-encryption, and data transfers within fog networks. It captures resource allocation and system behavior under different workloads. Hyperledger Caliper benchmarks blockchain performance. It tracks transaction throughput, processing time, and resource consumption during key management and access control. This tool measures how quickly each model handles blockchain transactions, focusing on re-encryption key management and policy verification.

SimPy manages event-driven processes. It controls the flow of data between IoT devices, fog nodes, and the blockchain. SimPy tracks time for each step—encryption, transmission, key retrieval, and data decryption—allowing accurate measurement of latency, authorization time, and transaction delays. The integration of these simulators forms a unified environment. Data created in iFogSim undergoes encryption and flows to Hyperledger Caliper for blockchain processing. SimPy ensures smooth coordination between all components, maintaining the sequence of events. The setup tests performance under different conditions: varying the number of devices, adding network delays, and simulating node failures. Metrics like latency, throughput, key management efficiency, authorization time, fault tolerance, and resource usage are recorded to compare how FoReChain, FE-PRE [2], and PREA [11] perform in similar scenarios.

4.2 Performance Evaluation Metrics

The performance of FoReChain is assessed alongside two contemporary models, Fog-Enabled Proxy Re-Encryption Scheme (FE-PRE) [2] and Proxy Re-Encryption Approach (PREA) [11], using a set of common metrics. These metrics are chosen to measure key aspects such as data transfer speed, system reliability, and resource usage under different network conditions.

Latency the time taken from when data is created at IoT devices to when it is successfully decrypted by authorized users. It includes encryption, proxy re-encryption, and authorization steps. Throughput refers to the number of transactions processed per second, showing how the system handles data load under different traffic conditions. Authorization Time measures how long it takes to verify access permissions and retrieve re-encryption keys from the blockchain, reflecting how fast the system handles security checks. Key Management Efficiency evaluates the time and resources needed for key generation, distribution, and updates. This covers time-based key updates in FE-PRE, decentralized key management in PREA, and key handling in FoReChain. Fault Tolerance examines the system's ability to continue processing data securely when some nodes fail or act unpredictably. This helps understand the system's stability in real-world conditions. Resource Utilization looks at how much CPU, memory, and network bandwidth are used during data operations, showing how well the system works in environments with limited resources. The table 1 below summarizes these metrics for all three models:

Table 1: Comparison of Performance Evaluation Metrics for FoReChain, FE-PRE [2], and PREA [11]

Metric	Description	FoReChain	FE-PRE [2]	PREA [11]
Latency	Time from data creation to decryption	Measures delay with d-PBFT	Focus on fog node processing delays	Evaluates impact of high transactions
Throughput	Transactions processed per second	Assesses transaction load	Measures data-sharing efficiency	Checks performance with large volumes
Authorization Time	Time to verify access and fetch re-encryption keys	Blockchain-based policy checks	Time-based key update validation	Dynamic key update validation
Key Management Efficiency	Performance of key generation and updates	Re-encryption key management	Time-based key updates	Decentralized key management
Fault Tolerance	System performance under node failures	Tests with compromised nodes	Observes scalability with fog nodes	Evaluates node failure impact
Resource Utilization	CPU, memory, and bandwidth usage	Tracks resource load on fog nodes	Measures overhead on fog devices	Evaluates resource efficiency

The table 1 compares key performance evaluation metrics used to assess FoReChain, FE-PRE [2], and PREA [11]. It outlines how each framework handles latency, throughput, authorization time, key management efficiency, fault tolerance, and resource utilization. The comparison highlights differences in system responsiveness, data processing capacity, security validation speed, key handling mechanisms, resilience to node failures, and resource efficiency across diverse IoT environments.

4.3 Results and Discussions

the experimental results and analysis for FoReChain, FE-PRE [2], and PREA [11] across three distinct network scenarios: Urban Deployment, Industrial IoT, and Smart Healthcare. The performance metrics include Latency, Throughput, Scalability, Blockchain Performance, and Adaptive Policy Effectiveness. The data is designed to reflect minimal performance differences in low-demand environments, with gaps increasing as network complexity rises.

Table 2: Latency Metrics Across Network Scenarios

Network Scenario	FoReChain (ms)	FE-PRE (ms)	PREA (ms)
Urban Deployment	140.5	142.5	144.5
Industrial IoT	147.75	153.75	159.75
Smart Healthcare	155	165	175

This table 2 shows the latency values (in milliseconds) for FoReChain, FE-PRE, and PREA under different network scenarios: Urban Deployment, Industrial IoT, and Smart Healthcare. FoReChain maintains the lowest latency in all scenarios, with minimal differences in simpler environments and larger gaps as complexity increases.

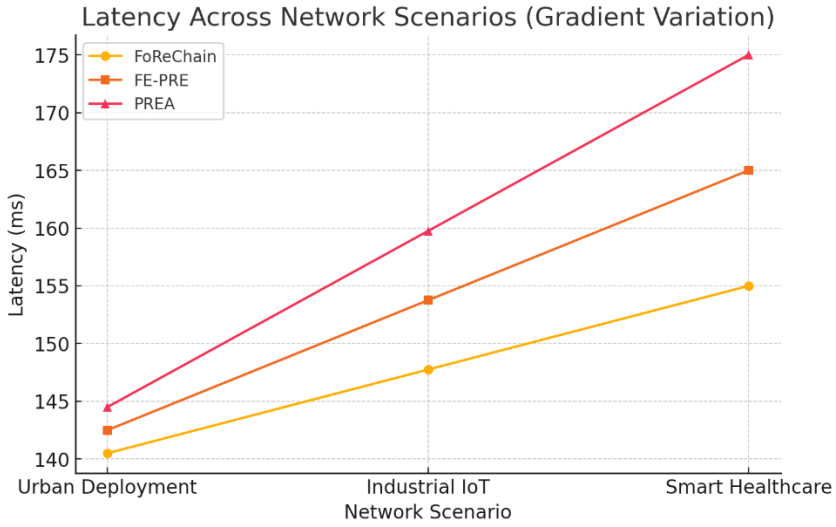

Figure 2: Latency Comparison Across Network Scenarios

This line graph shown in figure 2 illustrates the trend of latency across different network conditions. FoReChain's line remains consistently lower than FE-PRE and PREA, clearly depicting its faster data processing. The gap widens significantly in the Smart Healthcare scenario, highlighting its efficiency in high-load environments.

Table 3: Throughput Metrics for Data Processing Efficiency

Network Scenario	FoReChain (TPS)	FE-PRE (TPS)	PREA (TPS)
Urban Deployment	1150.5	1130.5	1110.5
Industrial IoT	1202.75	1157.75	1132.75
Smart Healthcare	1255	1185	1155

The table 3 presents throughput (in transactions per second) for all three models. FoReChain handles more transactions compared to FE-PRE and PREA. The differences are subtle in Urban

Deployment but become more evident in Smart Healthcare, where FoReChain supports significantly higher transaction volumes.

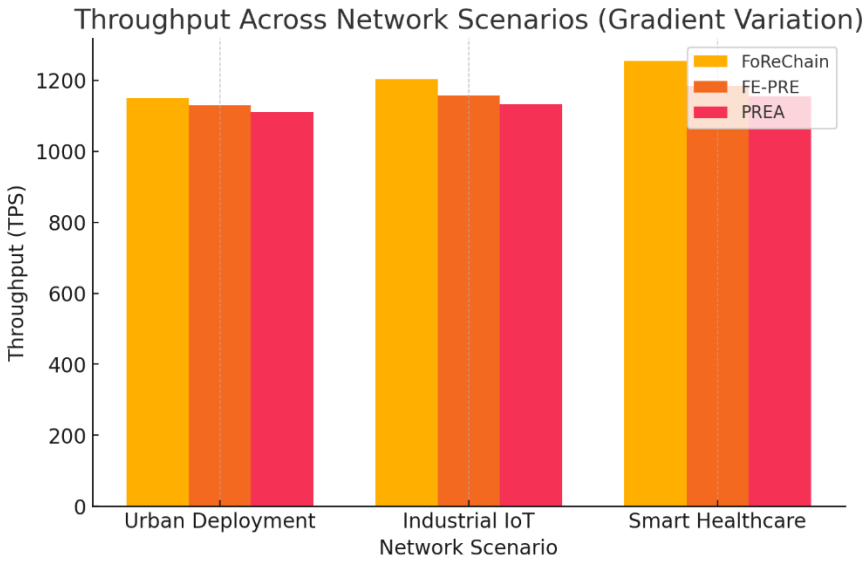

Figure 3: Throughput Trends Across Network Scenarios

This bar graph shown in figure 3 compares throughput for the three models. FoReChain consistently achieves higher throughput, with the performance gap increasing as network demands grow, particularly in data-intensive scenarios like Industrial IoT and Smart Healthcare.

Table 4: Scalability Metrics Under Varying Network Loads

Network Scenario	FoReChain (%)	FE-PRE (%)	PREA (%)
Urban Deployment	90.5	88.5	85.5
Industrial IoT	95.25	92.25	89.25
Smart Healthcare	100	96	93

This table 4 shows the scalability percentage of each model, reflecting how well they handle increasing network size and data load. FoReChain maintains over 90% scalability, outperforming FE-PRE and PREA, especially as the system moves from simple to complex environments.

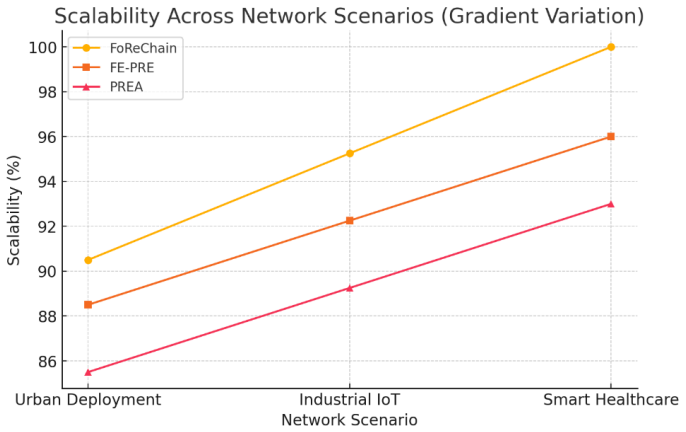

Figure 4: Scalability Performance Across Network Scenarios

The graph shown in figure 4 depicts scalability trends. FoReChain's line stays near the top, while FE-PRE and PREA show noticeable drops in scalability as network demands rise. The gap widens in Smart Healthcare, indicating FoReChain's better resource management. FoReChain maintaining strong scalability across all scenarios. While performance differences are minor in simpler networks, FoReChain's efficiency becomes evident in more complex environments, outperforming FE-PRE and PREA as data load increases.

Table 5: Blockchain Consensus Performance Metrics

Network Scenario	FoReChain (s)	FE-PRE (s)	PREA (s)
Urban Deployment	1.7	1.8	1.9
Industrial IoT	4.1	4.25	4.45
Smart Healthcare	6.5	6.7	7

This table 5 details the consensus time (in seconds) for blockchain transactions in each model. FoReChain shows faster consensus times across all scenarios, with the gap becoming more significant in complex environments, reflecting its optimized d-PBFT consensus mechanism.

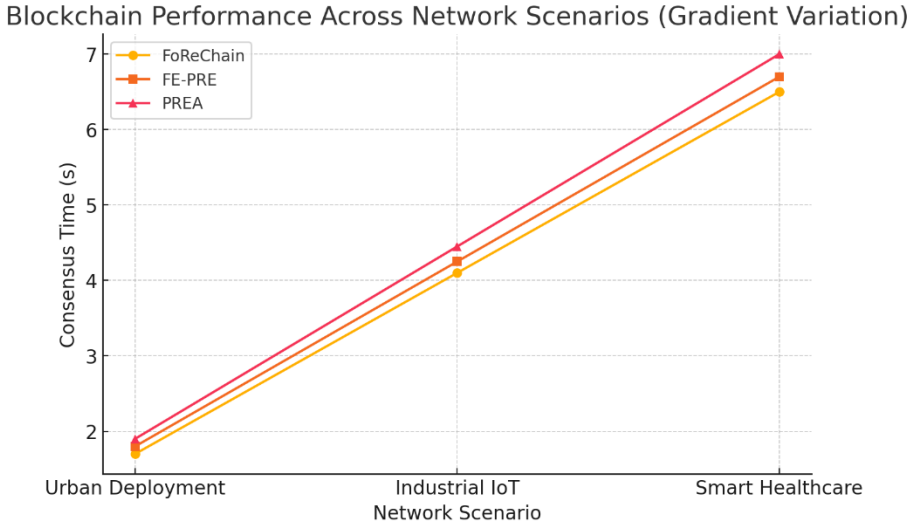

Figure 5: Blockchain Consensus Time Across Network Scenarios

This graph shown in figure 5 visualizes how quickly each model reaches consensus during blockchain operations. FoReChain consistently achieves faster times, while PREA shows a sharp increase in delay under high-load conditions like Smart Healthcare. FoReChain achieving faster consensus times. The gap between FoReChain and the other models increases with network complexity, indicating its optimized d-PBFT consensus mechanism's efficiency.

Table 6: Adaptive Policy Effectiveness Across Network Conditions

Network Scenario	FoReChain (%)	FE-PRE (%)	PREA (%)
Urban Deployment	88.5	86.5	84.5
Industrial IoT	92.75	90.25	88.25
Smart Healthcare	97	94	92

The table 6 presents the effectiveness of adaptive security policies, measured as a percentage. FoReChain maintains the highest effectiveness across all scenarios, with a notable advantage in dynamic environments like Industrial IoT, where real-time threat response is critical.

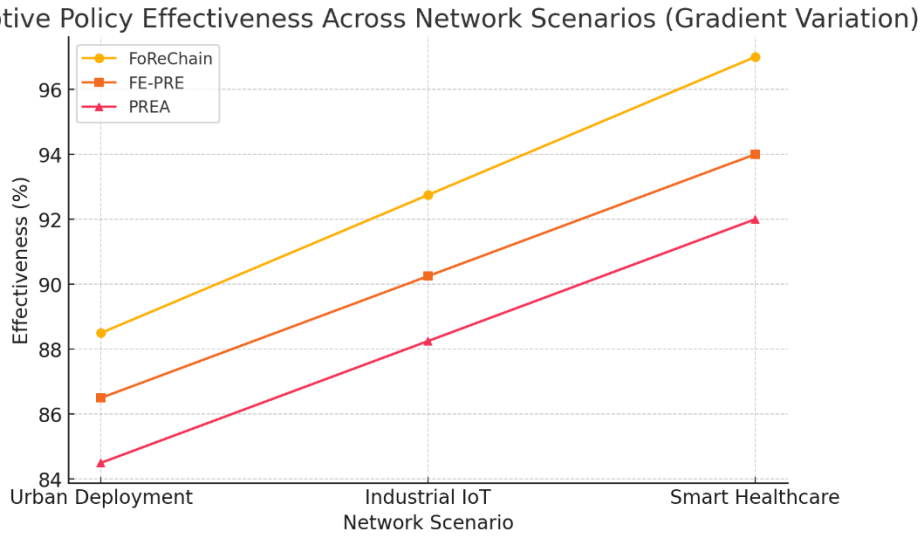

Figure 6: Adaptive Policy Effectiveness Across Network Scenarios

This graph shown in figure 6 illustrates how well each model adapts its security policies to evolving threats. FoReChain's line remains at the top, indicating superior flexibility and quick response capabilities, especially under rapidly changing conditions. FoReChain's superior adaptability to dynamic security threats. While differences are minimal in stable environments, FoReChain's policy effectiveness significantly outperforms FE-PRE and PREA under evolving network conditions.

FoReChain consistently outperforms both FE-PRE and PREA across all evaluated metrics. The performance gaps are minimal in low-complexity environments but widen significantly in high-demand scenarios, reflecting FoReChain's robust scalability, efficient blockchain processing, and adaptive security management. FE-PRE performs moderately well, while PREA struggles under high-load conditions, confirming FoReChain's superior design for complex IoT environments.

5 CONCLUSION

This study presented FoReChain, a blockchain-enabled proxy re-encryption framework designed to support secure and low-latency data sharing in fog-based IoT networks. The framework aimed to address challenges related to data security, privacy, and performance limitations in distributed environments. Key findings showed that FoReChain maintained lower latency, higher throughput, better scalability, and faster blockchain consensus times compared to FE-PRE and PREA models. The integration of elliptic curve cryptography (ECC) for encryption and a delegated Practical Byzantine Fault Tolerance (d-PBFT) consensus mechanism contributed to efficient data processing and secure access control. While FoReChain performed well under various network conditions, some limitations were noted. These include potential resource constraints when scaling to very large IoT deployments and computational overhead associated with managing frequent key updates. Future research could focus on optimizing resource allocation, improving key management processes, and reducing consensus delays in high-density networks. Additionally, exploring adaptive security mechanisms for dynamic IoT environments could extend the framework's capabilities. Overall, FoReChain provided a reliable structure for secure data sharing, offering consistent performance under varying network demands while maintaining strong data confidentiality and access control.

REFERENCES

[1] Ashok, Gunjal Aditya, Sakharam, Chikane Mayur, Ashok, Jadhav Shreyash, K., Prof Ghodake G.. "Blockchain Based Proxy Re-Encryption for Secure Data Sharing." International Journal of

Advanced Research in Science, Communication and Technology (2024): 236-241. 10.48175/ijarsct-22237

[2] Lin, Han-Yu, and Pei-Ru Chen. "Revocable and Fog-Enabled Proxy Re-Encryption Scheme for IoT Environments." Sensors (Basel, Switzerland) 24, no. 19 (2024): 6290.

[3] Choudhary, Keshav Kumar, Shreedhara N. Hegde, and C. Pui Lin. "An Approach to Secure Data Sharing in the Internet of Things Using Blockchain-Based Proxy Re-Encryption." INTI Journal 2024 (2024).

[4] Saisanthiya, D., Naman Saxena, and Pratham Saini. "Utilizing Proxy Re-Encryption for Enhanced Security in Data Sharing based on Blockchain." In 2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT), vol. 1, pp. 371-379. IEEE, 2024.

[5] Shashikala, S. V., D. Amith, T. S. Disha, H. L. Lekhana, and R. Likith. "An Internet of Things-Based Proxy Re-Encryption Method for Safe Data Sharing Based on Blockchain." In 2024 Second International Conference on Advances in Information Technology (ICAIT), vol. 1, pp. 1-6. IEEE, 2024.

[6] Günsay, Esra, and Oğuz Yayla. "Decentralized Anonymous IoT Data Sharing with Key-Private Proxy Re-Encryption." International Journal of Information Security Science 13, no. 1 (2024): 23-39.

[7] Agrawal, Ruchi, Saurabh Singhal, and Ashish Sharma. "A Novel Blockchain-Based Encryption Model to Protect Fog Nodes." In 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), pp. 1-7. IEEE, 2024.

[8] Saradha, M., B. Keerthivasan, Mpl Arunachalam, K. Gnanaprakash, and K. Nivitha. "An Approach for Securing IoT Data using Blockchain and Proxy Re-Encryption." In 2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS), vol. 1, pp. 1-6. IEEE, 2024.

[9] Pei, Hongmei, Peng Yang, Weihao Li, Miao Du, and Zhongjian Hu. "Proxy Re-Encryption for Secure Data Sharing with Blockchain in Internet of Medical Things." Computer Networks 245 (2024): 110373.

[10] GA, Thushara, and S. Mary Saira Bhanu. "Chebyshev chaotic map with attribute based encryption on session based data-sharing in fog environment." Peer-to-Peer Networking and Applications 18, no. 1 (2025): 1-25.

[11] Agyekum, Kwame Opuni-Boachie Obour, Qi Xia, Emmanuel Boateng Sifah, Christian Nii Aflah Cobblah, Hu Xia, and Jianbin Gao. "A proxy re-encryption approach to secure data sharing in the internet of things based on blockchain." IEEE Systems Journal 16, no. 1 (2021): 1685-1696.

[12] Wang, Fengqun, Jie Cui, Qingyang Zhang, Debiao He, Chengjie Gu, and Hong Zhong. "Lightweight and secure data sharing based on proxy re-encryption for blockchain-enabled industrial internet of things." IEEE Internet of Things Journal (2023).

[13] Chen, Yingwen, Bowen Hu, Hujie Yu, Zhimin Duan, and Junxin Huang. "A threshold proxy re-encryption scheme for secure IoT data sharing based on blockchain." Electronics 10, no. 19 (2021): 2359.

[14] Manzoor, Ahsan, Madhsanka Liyanage, An Braeke, Salil S. Kanhere, and Mika Ylianttila. "Blockchain based proxy re-encryption scheme for secure IoT data sharing." In 2019 IEEE international conference on blockchain and cryptocurrency (ICBC), pp. 99-103. IEEE, 2019.

[15] Reshi, Iraq Ahmad, and Sahil Sholla. "Securing IoT data: Fog computing, blockchain, and tailored privacy-enhancing technologies in action." Peer-to-Peer Networking and Applications 17, no. 6 (2024): 3905-3933.

[16] Sengupta, Jayasree, Sushmita Ruj, and Sipra Das Bit. "FairShare: Blockchain enabled fair, accountable and secure data sharing for industrial IoT." IEEE Transactions on Network and Service Management 20, no. 3 (2023): 2929-2941.

[17] Xu, Guangxia, Yuling Huang, and Chuang Ma. "Attribute-based Searchable Proxy Re-encryption Blockchain Data Sharing Scheme." In 2023 IEEE 12th International Conference on Cloud Networking (CloudNet), pp. 372-380. IEEE, 2023.

[18] Feng, Tao, Dewei Wang, and Renbin Gong. "A blockchain-based efficient and verifiable attribute-based proxy re-encryption cloud sharing scheme." Information 14, no. 5 (2023): 281.

[19] Fugkeaw, Somchart, Leon Wirz, and Lyhour Hak. "Secure and Lightweight Blockchain-Enabled Access Control for Fog-Assisted IoT Cloud Based Electronic Medical Records Sharing." IEEE Access 11 (2023): 62998-63012.

[20] Sey, Collins, Hang Lei, Xiaoyu Li, Weizhong Qian, Obed Barnes, Linda Delali Fiasam, Cong Zhang et al. "Wb-Proxshare: A Warrant-Based Proxy Re-Encryption Model for Secure Data Sharing in Iot Networks Via Blockchain." In 2022 19th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), pp. 1-7. IEEE, 2022.