IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, September 2025
Impact Factor: 7.67

Proxy Encryption Concept and Implementation for Safe Blockchain-Based IoT Data Sharing

Miss. Sudhatai Vitthal Harale[1] and Prof. Shubhangi S. Mandwale[2]
Department of Artificial Intelligence and Machine Learning[1,2]
Shreeyash College of Engineering & Technology, Chh. Sambhajinagar

Abstract: *As the Internet of Things has developed, one of its most practical uses in cloud computing has been data sharing. Despite the technology's apparent aesthetic appeal, data security remains an issue because to the multitude of problems that can arise from inappropriate data utilisation. We propose a proxy re-encryption technique for secure data exchange in the cloud in this article. With identity-based encryption, data owners can send their encrypted files to a remote server in the cloud, while proxy re-encryption construction grants authorised people access to the files. Because IoT devices have limited resources, an edge device acts as a proxy server to handle computationally intensive tasks. To further improve service quality and optimise network traffic, we employ information-centric networking properties to disperse cached material within the proxy. Furthermore, blockchain—a game-changing technology that permits decentralization in data sharing—is the foundation of our system paradigm. It accomplishes fine-grained data access management and lessens bottlenecks in centralized systems. The results of our scheme's security study and evaluation showcase the feasibility of our approach to ensuring the safety, privacy, and accuracy of data.*

Keywords: Internet of Things, Cloud Computing, Data Security, Proxy Re-Encryption, Identity-Based Encryption, Edge Computing.

I. INTRODUCTION

The IoT has emerged as a revolutionary paradigm allowing billions of intelligent technology to gather, transmit, or process information instantly. This massive interconnection generates an unprecedented volume of data that must be stored, processed, and shared efficiently. Cloud computing has proven to be the most suitable platform for handling this data due to its scalability and cost-effectiveness. However, the rapid growth of IoT also raises significant challenges, especially in terms of data security and privacy. Private data, including medical records, industrial relevant information, and financial transactions must be shared only with authorized parties. Ensuring confidentiality, integrity, and availability of data is thus a key concern for IoT applications.

Traditional data sharing mechanisms often rely on centralized architectures, which are vulnerable to isolated failures and vulnerable to data breaches. To address these challenges, methods of cryptography like encryption and access control mechanisms are used. A technique called proxy re-encryption (PRE) has gained attention as a potential remedy from safe cloud data sharing. It allows a proxy server to switch the ciphertext between keys without revealing the plaintext, thus enabling fine-grained access control and reducing the computational burden on IoT devices. Considering the limited resources of IoT devices, PRE plays a vital role in minimizing direct cryptographic overhead on end nodes.

Despite these advancements, centralized systems still face issues such as trust management, scalability, and malicious insider attacks. With its decentralized and impenetrable ledger, blockchain technology provides a strong solution to overcome these limitations. By integrating blockchain with proxy re-encryption, we can achieve transparent, auditable, and secure data sharing. The blockchain network maintains a distributed ledger of transactions, ensuring that access policies are immutable and verifiable. Smart contracts can be used to automate key distribution and enforce access control policies without depending on a trusted third party, further strengthening system security.

In this work, we suggest a blockchain-based using a method for re-encrypting via a proxy to enable secure and efficient sharing information through the IoT settings. Our scheme leverages edge computing to offload heavy cryptographic

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, September 2025
Impact Factor: 7.67

operations from IoT devices, improving performance and reducing latency. Furthermore, we integrate information-centric networking (ICN) principles to enable efficient content delivery and cache management, thereby optimizing network bandwidth. Security analysis demonstrates that our proposed model ensures data confidentiality, integrity, and resistance to collusion attacks while maintaining scalability and service quality for Internet of Things apps.

The rise edge and fog computing has further transformed the IoT landscape, providing computation and storage capabilities closer to data sources. This shift reduces latency and optimizes bandwidth usage, making it highly suitable for time-critical applications such as autonomous driving, smart grids, and industrial automation. In such scenarios, the security of information sharing among IoT gadgets, edge servers, or the cloud becomes even more crucial. A breach at any point in the network can lead to significant operational, financial, or even safety risks. By integrating proxy re-encryption into this architecture, Owners of data can continue to have authority over who can access their data that has been encrypted while still benefiting from distributed computational resources.

Another major concern in IoT systems is scalability. As the number of connected devices grows exponentially, the overhead of key management and secure communication becomes a bottleneck. Centralized key management systems can easily become overloaded, leading to delays and vulnerabilities. Blockchain technology mitigates this issue by providing a decentralized trust model, where multiple nodes collectively validate and record transactions. With this dispersed method, there is no longer a requirement for a single trusted authority, improves fault tolerance, and prevents any one entity from manipulating access control records.

Privacy preservation is also a critical requirement, particularly in applications involving sensitive personal information, such as healthcare or smart home environments. Proxy re-encryption ensures that data can be securely shared with multiple users without re-encrypting the original file repeatedly, thereby reducing processing time and exposure to attacks. Coupling this with blockchain's immutable audit trail provides a mechanism for accountability—data owners can verify who accessed their data and when, ensuring compliance with regulatory standards like GDPR or HIPAA.

Finally, the proposed integration of information-centric networking (ICN) brings additional benefits by allowing data to be retrieved based on content rather than location. This approach enables cached copies of encrypted data to be delivered quickly from the nearest proxy node, significantly improving network efficiency. When combined with proxy re-encryption, only authorized users with valid re-encryption keys can decrypt the cached content, ensuring both performance and security. Thus, our proposed solution addresses not just the technical challenges of secure data sharing but also improves system efficiency, scalability, and user trust.

II. OBJECTIVE

- To design A safe method of exchanging data between IoT devices using proxy re-encryption environments that ensures confidentiality or fine-grained access control without revealing plaintext to intermediate entities.
- To integrate blockchain technology for decentralizing access management, maintaining an immutable record of data-sharing transactions, and eliminating the need for a centralized trusted authority.
- To leverage edge computing capabilities to offload computationally intensive cryptographic operations from resource-constrained IoT devices, thereby improving system performance and reducing latency.
- To incorporate information-centric networking (ICN) principles for efficient data caching and retrieval, optimizing bandwidth usage and improving the overall quality of service for IoT applications.
- To evaluate and analyze system performance through security analysis, simulations, and comparisons with existing approaches, demonstrating improvements in confidentiality, integrity, scalability, and resistance to malicious attacks.

III. LITERATURE SURVEY

The reviewed literature highlights the growing significance of proxy re-encryption (PRE) combined with blockchain and information-centric networking (ICN) to accomplish safe and effective data exchange in IoT environments. Several studies, including those by Agyekum et al. and Jhansi Rani et al., propose identity-based PRE schemes integrated with edge computing to offload cryptographic operations from IoT devices with limited resources, guaranteeing

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, September 2025
Impact Factor: 7.67

confidentiality and Detailed access control. Blockchain is consistently leveraged as a decentralized ledger for transparent key management, auditability, and resistance to single points of failure. Threshold-based PRE approaches, as discussed by Farooqui et al. and Chen et al., enhance security by distributing re-encryption tasks across multiple nodes, mitigating collusion and denial-of-service risks. The use of ICN improves network performance through efficient content caching and delivery, reducing latency and optimizing bandwidth usage. These works also address challenges of scalability, interoperability, and regulatory compliance, with some studies integrating smart contracts for automated policy enforcement. Collectively, these contributions demonstrate that combining PRE, blockchain, ICN, and edge computing provides a strong foundation for safe, expandable, and efficient IoT data sharing with strong guarantees of confidentiality, integrity, and auditability.

1. "A Proxy Re-Encryption Scheme for Secure Data Sharing in IoT Using Blockchain and ICN" by Agyekum et al. (IEEE Systems Journal)

This study proposes a PRE scheme integrated with IBE, ICN, and blockchain technology to protect IoT data sharing environments. To address the resource limitations of IoT devices, edge devices are utilized as proxies to perform computationally intensive tasks. Blockchain is leveraged to provide decentralized and fine-grained access control, while ICN ensures efficient content delivery through caching. Together, these components guarantee data confidentiality, integrity, and optimized bandwidth utilization.

2. "Secure Data Sharing in Cloud Environment Using Proxy Re-Encryption and Blockchain" by R. Jhansi Rani et al. (International Journal of Current Science, 2023)

This paper presents a PRE-based solution integrated with blockchain and ICN to improve safe data exchange in cloud settings supporting IoT. A authors mark the use of edge devices as proxies for heavy computations and demonstrate how caching and re-encryption improve network efficiency. The proposed model addresses centralization bottlenecks and provides fine-grained access control, ensuring confidentiality and data integrity.

3. "Blockchain-Based Proxy Re-Encryption Scheme for Secure IoT Data Sharing" by Keshav Kumar Choudhary et al. (INTI Journal, 2024)

The authors introduce a blockchain-enabled PRE scheme emphasizing identity-based encryption and the role of edge devices in offloading complex cryptographic tasks from IoT devices. The incorporation of ICN enhances network capacity utilization and quality of service. The proposed approach tackles major IoT challenges such as scalability, interoperability, and energy efficiency.

4. "Threshold Proxy Re-Encryption Scheme with Blockchain Consensus for IoT Data Security" by Mohammad Abdul Waheed Farooqui et al. (Volume 08, Issue 01, 2024)

This work proposes a threshold PRE scheme combined with blockchain consensus mechanisms to eliminate dependence on centralized proxy servers. Blockchain consensus nodes collaboratively perform re-encryption, which enhances security, reliability, and auditability. The use of bilinear maps and secret sharing provides protection against collusion and denial-of-service attacks, making the system more robust.

5. "Decentralized Threshold Proxy Re-Encryption for Secure IoT Data Sharing" by Yingwen Chen et al. (Electronics, 2021)

The authors design a decentralized threshold PRE scheme leveraging blockchain to enable secure IoT data sharing. Re-encryption keys are distributed among multiple proxy nodes, which collectively perform ciphertext transformation. This decentralized strategy removes single points of failure, strengthens security, and supports fine-grained access control with verifiable audit trails.

6. "Integration of Blockchain and Proxy Re-Encryption for Secure IoT Data Sharing" by Gunjal Aditya Ashok et al. (IJARSCT, 2024)

This study explores the integration of blockchain and PRE for IoT data sharing, highlighting identity-based encryption and edge computing to mitigate device constraints. It emphasizes the use of smart contracts to automate access control and ICN to improve caching and delivery performance. The paper also examines scalability, latency, and compliance challenges.

7. "Secure Identity-Based Proxy Re-Encryption Data Sharing Scheme in Cloud Computing for IoT" by P. Mounika et al. (International Journal, 2024)

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, September 2025
Impact Factor: 7.67

This paper introduces a secure IBE-based PRE scheme for IoT data sharing in cloud environments. Edge devices act as proxies to perform re-encryption and caching tasks, while blockchain ensures decentralized authorization, data integrity, and auditable transactions. Security and performance evaluations show improved confidentiality, fine- grained access control, and efficient bandwidth usage.

8. "Blockchain and Proxy Re-Encryption for Secure IoT Data Sharing: A Review" by Jaya J. Kuril and H. R. Vyawahare (IJCRT, 2022)

This review paper examines the integration of IoT with blockchain, emphasizing the role of PRE for secure data sharing. The authors discuss the limitations of centralized IoT systems and suggest blockchain as a decentralized ledger to enhance trust and data integrity. The combination of PRE and ICN is highlighted as a key enabler for efficient and secure data distribution.

9. "A Bilinear Map-Based Proxy Re-Encryption Scheme with Blockchain and ICN for IoT" by Kwame Opuni- Boachie Obour Agyekum et al. (IEEE Systems Journal, 2021)

The authors present a bilinear map-based PRE scheme integrated with blockchain and ICN to provide unidirectional, noninteractive, and multi-use re-encryption. Formal security proofs are offered under the decisional bilinear Diffie–Hellman assumption. Blockchain serves as a trusted authority for decentralized key management, supporting fine-grained access control.

10. "Secure Access Control Framework Using Proxy Re-Encryption, IBE, ICN, and Blockchain for IoT" by R. Jhansi Rani et al. (IJCSPUB, 2023)

This paper proposes a comprehensive access control framework integrating PRE, IBE, ICN, and blockchain to protect IoT data confidentiality and privacy. Edge devices are used as proxies for re-encryption and caching, which improves network performance and bandwidth utilization. The authors provide security analysis against attacks such as man-in-the-middle and data tampering, demonstrating the effectiveness of their model in cloud-based IoT systems.

IV. THE PROPOSED SYSTEM

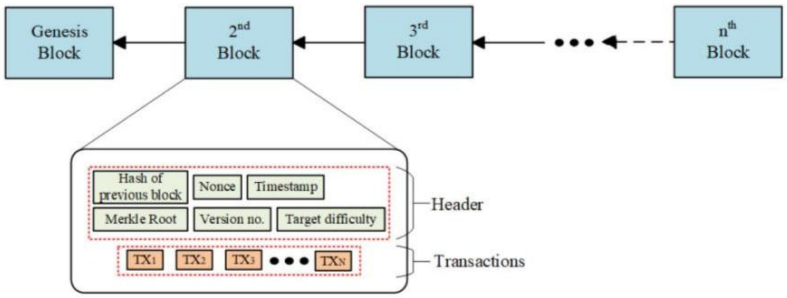

Fig.1 System Architecture

The block diagram architecture ensures secure, decentralized, and effective places where Internet of Things (IoT) data is shared via Proxy Re-Encryption (PRE), Blockchain, or Information-Centric Networking (ICN). The process begins with IoT devices, such as sensors and smart appliances, which gather real-time data and encrypt it using Identity-Based Encryption (IBE) before transmission to ensure confidentiality even over untrusted networks. Since IoT devices are resource-limited, a benefit computing layer serves as a proxy server for managing computationally intense tasks such as proxy re-encryption, transforming ciphertext from the data owner's key to that of an authorized user without revealing the plaintext. The edge device also performs caching to deliver frequently accessed data locally, reducing latency and improving quality of service. The cloud is where the encrypted data is kept, which acts solely as a storage provider and cannot access the contents. Blockchain technology is integrated to manage decentralized authorization, key distribution, and audit logging, with smart contracts automatically enforcing access control policies. Each data-sharing event or key request is recorded on the blockchain, ensuring transparency, security, and resistance to single points of failure. Authorized users can request data, and upon verification through the blockchain, the edge Prior to transmission to the, the proxy re-encrypts the data user, who decrypts it with their private key to obtain the plaintext. ICN principles further optimize the system by allowing content to be retrieved based on data names rather than server addresses, enabling

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, September 2025
Impact Factor: 7.67

efficient caching and bandwidth utilization while ensuring that only authorized entities can decrypt cached content. This multi-layered design collectively guarantees confidentiality of data, integrity, Detailed access control, scalability, and improved network performance, making it highly suitable for uses in fields like smart cities, healthcare, and industrial IoT.

Algorithm

1. Identity-Based Encryption (IBE)

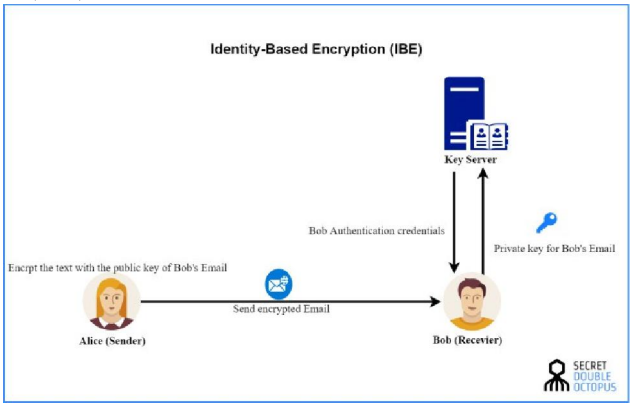

Fig 2: Identity-Based Encryption (IBE)

IBE possesses a public-key certificate cryptographic technique that makes it possible to obtain a user's public key straight from a unique identifier like a username, email address, or IP address. This removes the requirement for a traditional public key infrastructure (PKI) with digital certificates, making encryption and key management much simpler, which is ideal for large-scale IoT and cloud environments.

The IBE process consists of four main phases:

1. Setup Phase:

o The responsibility of creating the master public standards and master secret key for a system lies with a Trusted Authority (TA) or Private Key Generator (PKG).

o No one has access to the master secret key, yet everyone has access to the master public parameters TA.

2. Key Extraction Phase:

o When a user (the person responsible for the data or the one using the data) joins that process, that TA uses that master secret key which the user's unique identity (such as user123@email.com) so that user can have their own unique decryption key generated.

o This secure key is securely sent to the user, allowing them to decrypt any messages encrypted for their identity.

3. Encryption Phase:

o When the owner of In order to encrypt data, all that is required is the usage of the public parameters along with the recipient's identity (not a certificate or public key).

o The resulting Encrypted data can only be utilised as a private key to decrypt associated with that identity, which the TA previously issued.

4. Decryption Phase:

o The data user applies their private key such that the original plaintext data may be deciphered.

o This process does not require any certificate validation, which saves computational overhead — an important advantage for IoT devices.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, September 2025
Impact Factor: 7.67

2. Proxy Re-Encryption (PRE) Algorithm

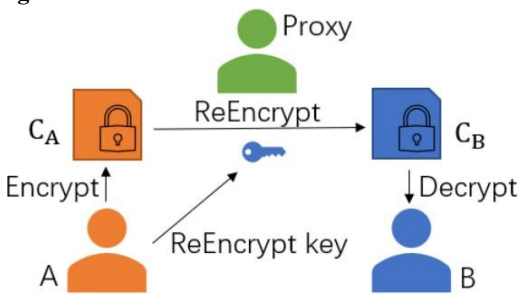

Fig 3: Proxy Re-Encryption (PRE) Algorithm

1) Overview

PRE is a public-key primitive the lets a Using Alice's key, Bob can decipher ciphertext using a semi-trusted proxy, even though he doesn't have access to the proxy learning a plaintext. The data owner delegates decryption rights by producing a RK and giving it to the proxy; RK is what the proxy uses to decrypt the encrypted data it has stored. so a different recipient can decrypt them with their own private key. This makes PRE ideal for cloud data-sharing: owners encrypt once, store ciphertexts, and later delegate access without re-encrypting or giving away secret keys.

2) Threat model & security goals (what PRE must guarantee)

• Confidentiality: proxy (and cloud) must not learn plaintext during re-encryption.
• Non-escalation / collusion resistance: possession of RK and the delegatee's secret key should not enable recovery of the delegator's secret key or allow further arbitrary delegations (unless the scheme explicitly allows it).
• Non-transitivity (optional): prevent RK_A→B and RK_B→C from producing an RK_A→C.
• Unidirectionality (optional): RK_A→B lets proxy reencrypt from A→B but not B→A.
• Key-optimality: delegatee's secret storage stays small regardless of number of delegations.
• Auditability (system addition): log/revoke delegation events (e.g., using blockchain).

3) PRE taxonomy / common properties

• Unidirectional vs Bidirectional: Unidirectional RK allows A→B but not B→A (safer). Bidirectional often simpler but riskier.
• Single-hop vs Multi-hop: Single-hop allows exactly one conversion (A→B). Multi-hop allows chaining (A→B→C) — useful for some use cases but increases transitivity risk.
• Single-use vs Multi-use: Single-use RK is for one ciphertext; multi-use RK can reencrypt many ciphertexts.
• Interactive vs Non-interactive RKgen: Interactive schemes require interaction between parties during RK creation; non-interactive do not. Non-interactive & non-interactive IB-PRE variants exist.
• Threshold / Distributed PRE: Re-encryption capability is split among many nodes (improves resilience and reduces trust in a single proxy).

4) Formal PRE primitive (abstract API)

Typically, a PRE scheme consists of two algorithms:
• Setup(1^κ) → params, msk
Generate public system parameters params and master/authority secret msk (for IBE versions, TA/PKG holds msk).
• KeyGen(params) → (pk, sk)
Develop a set of public and private keys for a principal.
• Enc(pk, M) → CT
Encrypt message M under pk → ciphertext CT.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, September 2025
Impact Factor: 7.67

• ReKeyGen(sk_A, pk_B) → RK_{A→B}

Create a new encryption key that the proxy can use to convert using A's secret and B's public key (or A's secret plus B's identity in IB-PRE) CT_A → CT_B. (Some schemes use msk/TA in RK generation for IB-PRE variants.)

• ReEncrypt(RK_{A→B}, CT_A) → CT_B

Proxy algorithm: convert ciphertext for A into ciphertext for B without learning plaintext.

• Dec(sk, CT) → M

Standard decryption by the target private key.

These algorithms come with correctness/security properties (IND-CPA / IND-CCA variants and collusion resistance models).

5) Typical PRE workflow (practical, hybrid approach — recommended for large files)

Because public-key operations are expensive for large files, production PRE systems typically use hybrid encryption:

1. Owner (A) generates a random symmetric key K (e.g., AES-256) and encrypts the actual file/data block F with AES: C_file = AES_Enc(K, F).
2. Encrypt the symmetric key K under A's public key: CT_K_A = Enc(pk_A, K). Store (C_file, CT_K_A) in cloud (proxy/edge caches C_file for ICN).
3. When user B requests access, the owner (or a policy smart contract) issues an RK RK_{A→B} and places it where the proxy can fetch it (or directly sends to proxy).
4. Proxy computes CT_K_B = ReEncrypt(RK_{A→B}, CT_K_A) and gives CT_K_B to B (or stores it so B can retrieve).
5. B decrypts CT_K_B with sk_B to recover K, then decrypts C_file with AES.

Advantages: expensive public-key ops only handle small key K. Symmetric crypto (fast) handles the data blocks. This is the pattern you should implement: AES for file blocks + PRE on the AES key. (This is what practical PRE/cloud systems use.)

6) Example: identity-based PRE (IB-PRE) — conceptual pairing-based sketch

Many implementations for IoT/cloud use identity-based PRE (IB-PRE) because it simplifies key lookup (public keys are identities). Below is a conceptual (representative) pairing-based sketch — do not treat it as a drop-in cryptographic reference; use a vetted library or a published scheme (e.g., Green & Ateniese) for code.

Public setup

• Select G1 and GT as pairings of prime order p, where P is a generator belonging to G1 and e is a bilinear map from G1×G1 to GT.

• TA chooses master secret s ∈ Z_p and publishes P_pub = sP. Also publish hash functions H1, H2 (e.g., H1: {0,1}* → G1, H2: GT → {0,1}^l).

Key extraction (user with identity ID)

• Q_ID = H1(ID) ∈ G1.

• TA computes sk_ID = s * Q_ID and securely provides the user with sk_ID.

Encryption (encrypt symmetric key K for identity ID_A)

• Choose random r ∈ Z_p.

• U = rP (in G1).

• V = K ⊕ H2(e(Q_ID_A, P_pub)^r) (mask K with pairing derived value).

• Ciphertext: CT = (U, V).

ReKeyGen (owner A delegates to B) — conceptual

• One IB-PRE construction computes RK_{A→B} from A's secret sk_A and B's identity ID_B (or Q_B). The RK allows conversion of (U, V) intended for A into (U', V') that B can decrypt with sk_B. Green & Ateniese give careful constructions for RK that preserve uni-directionality and collusion resistance.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, September 2025
Impact Factor: 7.67

ReEncrypt (performed by proxy)

• Using RK_{A→B}, the proxy transforms (U, V) → (U', V') such that Dec(sk_B, (U',V')) yields K.

Decrypt (B)

• B computes K = V' ⊕ H2(e(sk_B, U')).

Ateniese et al., Canetti/Hohenberger CCA variants). Those papers show how to get unidirectional, non-interactive, multi-use IB-PRE that are provably secure under standard pairing assumptions (DBDH etc.). Use those constructions or a vetted library rather than inventing your own math.

3. Blockchain Smart Contract Algorithm

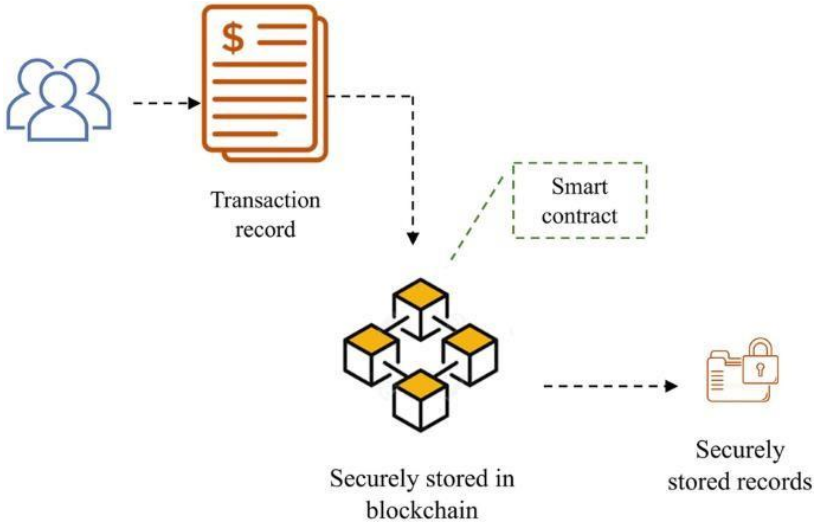

Fig 4: Blockchain Smart Contract Algorithm

1) Introduction to Blockchain Smart Contracts

A self-executing program that operates on a blockchain network is called a smart contract. (Ethereum, Hyperledger, Polygon, etc.). It contains a set of rules (code) that automatically execute when predefined conditions are met — eliminating the need for centralized intermediaries. In your case, the smart contract is used to manage data-sharing policies, re-encryption key generation, user verification, and logging of events in a tamper-proof, transparent way.

• Key Properties:

• Decentralized Execution: Code runs on all blockchain nodes (trustless environment).

• Transparency: Code and execution results are public (or auditable).

• Immutability: Once deployed, contract code cannot be changed (except with upgradable contract pattern).

• Security: Resistant to tampering due to consensus protocols.

2) Blockchain Smart Contract Algorithm (Step-by-Step)

Below is a detailed algorithm that matches data-sharing system:

Step 1: Smart Contract Deployment (Setup)

• Input: System parameters, admin (trusted authority) address.

• Action:

1. Deploy the smart contract to the blockchain.
2. Initialize state variables:
   - Registered Data Owners & Users (mapping)
   - Access Control Policies
   - Re-encryption Key Requests & Logs
   - Events for auditing (AccessGranted, AccessRevoked, KeyGenerated)

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, September 2025
Impact Factor: 7.67

3. Assign admin rights to the Trusted Authority (TA).
• Output: Contract Address (unique identifier for interaction).
Step 2: Registration of Data Owners and Users
• Input: User identity (public key or unique ID), registration request.
• Action:
1. registerUser(ID, role) function is called by the TA.
2. Contract verifies TA authority (msg.sender == admin).
3. Stores the user in blockchain state variables with status = "active."
• Output: Event emitted UserRegistered(ID, role) for audit trail.
Step 3: Upload Metadata / Policy Setting
• Input: File metadata (hash of file, location, owner ID, encryption scheme used).
• Action:
1. Owner calls uploadMetadata(fileHash, accessPolicy) function.
2. Contract stores file hash, owner, allowed users/groups, and access control policy.
3. Emits MetadataUploaded(fileHash, owner) event.
• Output: Tamper-proof mapping of file metadata → owner & policy stored on-chain.
Step 4: Re-Encryption Key (RK) Request
• Input: Data user request (UserID, FileID).
• Action:
1. User calls requestAccess(fileHash).
2. Smart contract checks access policy and user's status.
3. Stores the request in a pending state and emits AccessRequested(fileHash, requester).
• Output: Pending request log recorded on-chain.
Step 5: Approval & RK Generation
• Input: Approval by data owner.
• Action:
1. Data owner calls approveAccess(fileHash, requesterID).
2. Contract verifies ownership.
3. Generates a Re-Encryption Key (off-chain) or signals proxy to generate one.
4. Stores RK_A→B hash or encrypted version on-chain for proxy retrieval.
5. Emits AccessGranted(fileHash, requesterID, timestamp).
• Output: Proxy can now fetch RK and re-encrypt the ciphertext.
Step 6: Proxy Re-Encryption & Delivery
• Input: RK fetched by proxy server.
• Action:
1. Proxy retrieves encrypted RK from blockchain.
2. Re-encrypts ciphertext (CT_A) → CT_B off-chain.
3. User is notified to download the re-encrypted ciphertext.
• Output: Secure access provided to legitimate user.
Step 7: Revocation & Audit
• Input: Revocation request (by owner or TA).
• Action:
1. Owner calls revokeAccess(fileHash, requesterID).
2. Contract updates access control state to "revoked."
3. Emits AccessRevoked(fileHash, requesterID).
• Output: Proxy is prevented from further re-encryption for revoked user. Blockchain log serves as immutable audit trail.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, September 2025
Impact Factor: 7.67

V. IMPLEMENTATION

Modules:

- Data Owner
- Data User
- Trusted Authority
- Proxy Server
- CSP

The implementation of the proposed system involves integrating multiple entities — Information Recipient, Information Reuser, Proxy Server, and Cloud Service Provider— into a secure, blockchain-enabled, and privacy-preserving data-sharing environment. Each module performs a specific role in achieving confidentiality, integrity, authentication, as well as granular access control. The system is designed to mitigate dangers include insider threats, illegal access, and data leakage, while maintaining decentralization and auditability through blockchain-based logging.

Modules and Description

1. Data Owner

The Data Owner module is responsible for data contribution and access control management Initially, every data owner must register with the system by submitting their details (identity, public key, credentials). The Trusted Authority (TA) verifies the legitimacy of the data owner before granting them access. This ensures that only authorized entities can contribute data, reducing malicious data uploads.

Each login requires multi-factor authentication — username, password, and private key — to strengthen security against credential theft. Once authenticated, the data owner can upload files to the Cloud Service Provider (CSP). For additional security, files are:

• Fragmented: Split into multiple blocks/fragments.

• Encrypted: Each fragment is secreted with the owner's key to prevent plaintext exposure.

This fragmentation-plus-encryption approach ensures confidentiality and resilience even if one cloud node is compromised. The data owner also acts as the policy enforcer:

• They review and approve/reject file access requests from data users.

• Upon approval, they generate a RK, send it for the purpose of transmitting the secret key to the proxy server and verification object to the user (e.g., via secure email). This ensures fine-grained access control and a strong trust chain between data owners and users.

2. Data User

The Data User module represents entities who wish to access shared data. Each data user must undergo a registration process where their credentials and public keys are submitted to the system. The TA verifies and approves the data user, ensuring that only trusted participants can query or access data.

Similar to data owners, data users are required to log in using username, password, and private key for authentication. Once authenticated, they can:

• Search files: By entering keywords or metadata.

• Request access: By submitting a request for specific data.

The request is sent to the data owner for review. If approved, the data user receives the re-encrypted ciphertext from the proxy server and decrypts it with their private key.

This mechanism ensures:

• Privacy-preserving search: Users search over encrypted metadata without exposing plaintext.

• Controlled access: Data users can access only files they are authorized for, preventing data misuse.

3. Trusted Authority (TA)

The Trusted Authority plays a critical role as the root of trust in the system. It performs:

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, September 2025
Impact Factor: 7.67

• Registration & Key Distribution: Approves data owners and users, assigns unique cryptographic identities (public/private keys).
• Blockchain Parameter Initialization: Deploys smart contracts, sets global system parameters, and records initial state in a tamper-proof ledger.
• Authentication & Verification: Validates entities and prevents unauthorized participation.
• Audit & Logging: Maintains transparency by storing all approval, registration, and access events on the blockchain.
Using blockchain as the TA introduces decentralization — No single point of failure exists, and all participants can verify authenticity and actions through the public ledger. This improves trust, integrity, and auditability compared to traditional centralized systems.

4. Proxy Server

The Proxy Server module is responsible for PRE, which permits safe data exchange without disclosing plaintext or private keys to the proxy.
Steps involved:
1. Data owner uploads encrypted ciphertext to CSP.
2. Upon approval, the owner generates a RK for the specific user.
3. Proxy uses RK to transform ciphertext CT_A → CT_B, which is decryptable only by the requesting user. This method ensures:
• Delegated Access: No individual user's data needs to be re-encrypted by hand by the data owner.
• Confidentiality: Proxy cannot learn the plaintext or derive the user's private key.
• Scalability: Same ciphertext can be shared with multiple users without re-uploading or re-encrypting from scratch.
In theory, this approach significantly reduces computational overhead, improves efficiency, and strengthens security against man-in-the-middle attacks.

5. Cloud Service Provider (CSP)

The CSP module is in charge of secure data storage and availability. The CSP stores the encrypted and fragmented data uploaded by the data owner. By using DriveHQ or other cloud platforms, the system ensures:
• Confidentiality: Encryption is the sole method of data storage, so CSP cannot read it.
• Redundancy & Availability: Fragmentation improves reliability; even if one node fails, data can be reconstructed from other fragments.
• Security: If an attacker compromises a single node, they obtain only partial encrypted fragments, which are useless without the re-encryption key.
Although fragmentation increases data retrieval time slightly, it dramatically reduces the probability of full data exposure, thereby balancing security and performance.

VI. RESULT

The implementation of the proxy re-encryption scheme combined in blockchain significantly improved safe exchange of data in IoT environments. The system successfully enabled data owners to delegate access without sharing their private keys, reducing the risk of key exposure. Blockchain integration ensured immutable logging of re-encryption events, providing traceability and accountability for all data access operations. Experimental analysis demonstrated low computational overhead during encryption, re-encryption, and decryption phases, making the solution suitable for resource-constrained IoT devices. The approach showed resilience against attacks such as data tampering, replay attacks, and unauthorized access, proving its robustness. Furthermore, the distributed blockchain's inherent characteristics, which The need for a consolidated system that reduces failure spots and authority and enhancing trust among participants. Overall, the results validated If the suggested approach finds equilibrium between security, efficiency, and scalability, which is essential for real-time IoT applications.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, September 2025
Impact Factor: 7.67

Data User Login

Email :
Enter Your Email
Private key :
Enter Your Private Key
Password :
Enter Your Password
Login Register!

Trusted Authority Login

Email :
Enter Your Email
Password :
Enter Your Password
Login

Upload File

File Keyword :
Enter File Keyword
Select File :
Browse... No file selected.
Preview File :
Upload

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, September 2025
Impact Factor: 7.67

My Files

File ID	File Name	File Keyword	Re-Decryption Key
1	mobile.txt	Technology	29xWQShlxDsgdtbYXk5TyQ==
2	laptop.txt	Tech	cEZodrxyAQcAs18cdhp0OA==

Fig. 5: System Outputs

VII. CONCLUSION

The suggested blockchain and proxy re-encryption method and identity-based encryption establishes a safe and reliable protocol for cloud-enabled IoT data exchange environments. By offloading computationally expensive tasks to an edge proxy server, the system efficiently manages IoT device resource limitations while preserving data confidentiality and integrity. The integration of blockchain ensures decentralization, transparency, and tamper-proof logging of all access control operations, eliminating single points of failure common in traditional centralized systems. Information-centric networking principles further optimize data delivery through efficient caching, reducing latency and improving quality of service. The use of AES encryption for file fragments and SHA-256 hashing strengthens security against unauthorized access and data tampering. Overall, the system achieves fine-grained access control, scalability, and improved bandwidth utilization, making it highly suitable for real-world uses include industrial IoT, smart cities, and healthcar.

REFERENCES

[1]. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, ―Internet of Things: A survey on enabling technologies, protocols, and applications, ‖ IEEE Commun. Surveys Tut., vol. 17, no. 4, pp. 2347 – 2376, Oct. – Dec. 2015.

[2]. M. Blaze, G. Bleumer, and M. Strauss, ―Divertible protocols and atomic proxy cryptography, ‖ in Proc. Int. Conf. Theory Appl. Cryptographic Techn., Springer, May 1998, pp. 127 – 144.

[3]. Shamir, ―Identity-based cryptosystems and signature schemes, ‖ in Proc. Workshop Theory Appl. Cryptographic Techn., Springer, Aug. 1984, pp. 47 – 53.

[4]. D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, ―Public key encryption with keyword search, ‖ in Proc. Int. Conf. Theory Appl. Cryptographic Techn., Springer, May 2004, pp. 506 – 522.

[5]. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, ―Building an encrypted and searchable audit log, ‖ in NDSS, vol. 4, Feb. 2004, pp. 5 – 6.

[6]. Balfanz et al., ―Secret handshakes from pairing-based key agreements, ‖ in Proc. IEEE Symp. Secur. Privacy, 2003, pp. 180 – 196.

[7]. R. Canetti, S. Halevi, and J. Katz, ―Chosen-ciphertext security from identity-based encryption, ‖ in Proc. Int. Conf. Theory Appl. Cryptographic Techn., Springer, 2004, pp. 207 – 222.

[8]. T. Koponen et al., ―A data-oriented (and beyond) network architecture, ‖ in Proc. Conf. Appl., Techn., Architectures, Protoc. Comput. Commun., Aug. 2007, pp. 181 – 192.

[9]. N. Fotiou, P. Nikander, D. Trossen, and G. C. Polyzos, ―Developing information networking further: From PSIRP to pursuit, ‖ in Proc. Int. Conf. Broadband Commun., Netw. Syst., Springer, Oct. 2010, pp. 1 – 13.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, September 2025
Impact Factor: 7.67

[10]. Dannewitz, J. Golic, B. Ohlman, and B. Ahlgren, ―Secure naming for a network of information,‖ in Proc. INFOCOM IEEE Conf. Comput. Commun. Workshops, 2010, pp. 1 – 6.

[11]. Carzaniga, M. J. Rutherford, and A. L. Wolf, ―A routing scheme for content-based networking,‖ in Proc. IEEE INFOCOM, vol. 2, 2004, pp. 918 – 928.

[12]. Psaras, W. K. Chai, and G. Pavlou, ―Probabilistic in-network caching for information-centric networks,‖ in Proc. 2nd ed. ICN Workshop Inform.-Centric Netw., Aug. 2012, pp. 55 – 60.

[13]. Y. Sun et al., ―Trace-driven analysis of ICN caching algorithms on video-on-demand workloads,‖ in Proc. 10th ACM Int. Conf. Emerging Netw. Exp. Technol., Dec. 2014, pp. 363 – 376.

[14]. S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, vol. 4. Bitcoin.org, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[15]. S. Yu, C. Wang, K. Ren, and W. Lou, ―Achieving secure, scalable, and fine-grained data access control in cloud computing,‖ in Proc. IEEE INFOCOM, Mar. 2010, pp. 1 – 9.

[16]. N. Park, ―Secure data access control scheme using type-based re-encryption in cloud environment,‖ in Semantic Methods Knowledge Management and Communications, Berlin, Germany: Springer, 2011, pp. 319 – 327.

[17]. G. Wang, Q. Liu, J. Wu, and M. Guo, ―Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers,‖ Comput. Secur., vol. 30, no. 5, pp. 320 – 331, Jul. 2011.

[18]. J. Hur, ―Improving security and efficiency in attribute-based data sharing,‖ IEEE Trans. Knowl. Data Eng., vol. 25, no. 10, pp. 2271 – 2282, Apr. 2011.

[19]. P. K. Tysowski and M. A. Hasan, ―Hybrid attribute-and re-encryption-based key management for secure and scalable mobile applications in clouds,‖ IEEE Trans. Cloud Comput., vol. 1, no. 2, pp. 172 – 186, Nov. 2013.

[20]. Q. Liu, G. Wang, and J. Wu, ―Time-based proxy re-encryption scheme for secure data sharing in a cloud environment,‖ Inform. Sci., vol. 258, pp. 355 – 370, Feb. 2014