WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

An Enhanced Proxy-Based Encryption Scheme for Confidential Data Exchange in Cloud Environments

Megha Dabas[1], Akuthota Manikanta[2], Padam Sujith Kumar[3], Karne Anjan Reddy[4], Kinnerla Aravind[5]

[1]Assistant Professor, Computer Science and Engineering, Guru Nanak Institutions Technical Campus, Telangana, India meghaharshudabas@gmail.com
[2,3,4,5] Computer Science and Engineering, Guru Nanak Institutions Technical Campus, Telangana, India
[2]Akuthotamanikanta653@gmail.com, [3]padamsujith@gmail.com, [4]karneanjanreddy@gmail.com, [5]kinnerlaaravind@gmail.com

ABSTRACT-

This project introduces a Proxy Re-Encryption (PRE) framework aimed at enhancing secure data sharing and management within a cloud-based infrastructure. The primary objective is to enable a cloud owner to securely upload data, fragment it into multiple components, and permit a designated user to access and modify the data without compromising its confidentiality or integrity. Upon uploading, the file is divided into four segments, each processed using the SHA hashing algorithm to generate unique hash values that serve as integrity checkers for the respective data parts. To ensure security during transmission, the owner encrypts the data before granting access rights to specific users. A proxy server, which remains unaware of the file's contents, performs re-encryption on behalf of the owner. This process allows authorized users to decrypt the file using a provided key. The cloud server facilitates this operation by managing re-encryption and delivering both encrypted data and keys to intended recipients. Only users with explicit authorization from the data owner can retrieve and view file content. By employing proxy re-encryption, this system ensures that servers never directly access plain data, thereby maintaining privacy and security standards. Overall, this project fortifies secure cloud data exchange by ensuring robust confidentiality, maintaining data integrity, providing owner-controlled access while allowing safe and selective usage by authorized individuals.

Keywords- Proxy-Based Encryption (PBE), Proxy Re-encryption (PRE), Cloud Security, Confidential Data Exchange, Data Privacy, Cloud Computing, Data Sharing, Cryptographic Protocol, Attribute-Based Encryption (ABE).

I. INTRODUCTION

In today's digital landscape, the Internet of Things (IoT) is revolutionizing the way data is generated, processed, and utilized. The proliferation of IoT devices across domains such as healthcare, smart cities, vehicular networks, industrial automation, and home automation has led to an unprecedented surge in data traffic and network complexity. These interconnected devices continuously collect and transmit critical data, which is often outsourced to cloud servers for storage, analytics, and decision-making. However, this evolution brings forth significant challenges, particularly related to data confidentiality, privacy, integrity, and secure access control.

(One of the fundamental security practices in cloud-based data handling is data encryption before outsourcing. Encrypting the data ensures that even if attackers gain access to the storage system, they encounter only unreadable ciphertext. However, conventional encryption approaches, particularly symmetric key encryption, are increasingly inefficient for modern cloud and IoT systems. In symmetric encryption, both sender and receiver use the same secret key, which introduces a key distribution and management challenge—especially in scenarios where the data owner does not know the users in advance or needs to share data dynamically. This necessitates a decrypt-and-re-encrypt cycle, meaning the owner must remain online and available for every access request, creating scalability and usability bottlenecks.

To address these limitations, the proposed system introduces a Proxy Re-Encryption (PRE)-based framework tailored for secure and scalable data sharing in a cloud-IoT integrated environment. PRE is a cryptographic paradigm where a semi-trusted proxy can transform a ciphertext encrypted under one key (the data owner's) into a ciphertext that can be decrypted by another key (the user's), without learning the plaintext or accessing the private keys. This allows delegated, on-demand data access without compromising security or requiring the data owner to be constantly online. The proxy (cloud server or dedicated Preservice) plays a key role in this transformation but does not become a point of vulnerability, as it never gains access to the underlying data.

To further enhance the system's flexibility and performance, Identity-Based Encryption (IBE) is integrated. IBE replaces traditional public-key infrastructures with a system where public keys can be derived from unique user identifiers such as email addresses or usernames. This greatly simplifies key distribution and eliminates the need for pre-issued certificates or complex key exchanges. Compared to Attribute-Based Encryption (ABE)—which,

while powerful, imposes significant computational overhead—IBE is more suitable for resource-constrained IoT devices, where lightweight cryptographic operations are essential.

Given the high demand for low-latency and efficient data delivery, the framework also incorporates Information-Centric Networking (ICN) principles. In ICN, data is addressed and retrieved based on its content rather than its location, allowing for in-network caching, replication, and optimized delivery. This approach significantly reduces network congestion and latency, especially in environments with high data consumption and dynamic user access patterns, such as IoT ecosystems. By leveraging unique data naming and caching mechanisms, ICN ensures that frequently accessed data is delivered faster and more efficiently.

A major concern in any distributed system is trust management—especially when delegating access to third parties or proxies. To handle this challenge, the proposed system integrates blockchain technology as a secure, decentralized ledger for access control, auditing, and data integrity verification. Blockchain enables tamper-proof logging of data access requests, revocation events, and user activity, providing a robust foundation for accountability and transparency. Furthermore, smart contracts can automate access permissions and ensure that only users meeting predefined criteria can access specific datasets. This decentralization reduces reliance on single points of trust and enhances the resilience and trustworthiness of the entire system.

Collectively, this PRE-based system enhanced with IBE, ICN, and blockchain addresses the major pain points in secure data sharing: complex key management, inefficient re-encryption cycles, performance bottlenecks, and trust in centralized servers. The system supports a clear role-based model with cloud owner, cloud proxy server, and data users, and offers fine-grained, selective access control, identity authentication, and dynamic revocation capabilities.

In conclusion, as the IoT continues to evolve and expand into new areas, there is a pressing need for scalable, secure, and intelligent data sharing frameworks. The combination of Proxy Re-Encryption, Identity-Based Encryption, Information-Centric Networking, and Blockchain in this project forms a powerful and holistic solution for secure, efficient, and privacy-preserving cloud data sharing, particularly in highly dynamic and sensitive environments.

II. LITERATURE REVIEW

A. "Hybrid attribute-and re-encryption based key management for secure and scalable mobile applications in clouds,

Storing data in the cloud offers advantages such as cost-effectiveness, scalability, and ease of access. However, it also introduces several technical hurdles. One key concern is the protection of sensitive information from cloud service providers that, while trustworthy in operation, may still seek to inspect the data. Moreover, cloud data is increasingly accessed via mobile devices, which often have limited computational and communication capabilities, making efficiency a critical factor.

To address these issues, enhanced forms of **attribute-based encryption (ABE)** have been introduced. These improvements enable access control based on specific user attributes, while shifting the computational burden of encryption and decryption onto the cloud service. This strategy not only ensures data confidentiality but also minimizes the processing and data transfer load on mobile devices

Additionally, to streamline the process of user revocation in environments with mobile users, cloud providers can optionally perform **data re-encryption**. This feature helps maintain data privacy while simplifying the revocation process and reducing its associated costs.

The proposed encryption framework has been implemented using widely used mobile and cloud computing platforms. Real-world testing demonstrates the system's practical viability and efficiency. Further simulations, based on these experimental results, confirm the scalability of the protocol under realistic mobile cloud computing workloads.

Utilizing cloud storage has become increasingly popular due to its notable benefits, such as reduced infrastructure costs, scalable resource allocation, and anytime-anywhere data access. However, despite these advantages, outsourcing sensitive data to third-party cloud servers introduces complex security and privacy concerns. Chief among these is the risk posed by honest-but-curious cloud providers—entities that follow protocol but may attempt to analyze and infer information from the data they store.

To protect data confidentiality, especially in scenarios involving highly sensitive information such as personal records, financial data, or healthcare files, encryption must be employed before uploading to the cloud. Yet, traditional encryption methods, while effective at securing data, are often inefficient for practical use in modern environments—particularly when mobile devices are involved. These devices typically have limited computational power, battery life, and network bandwidth, making them ill-suited for intensive cryptographic operations.

In response to these limitations, researchers have developed advanced Attribute-Based Encryption (ABE) schemes. ABE allows for fine-grained access control by enforcing that only user with certain attributes (e.g., role, department, clearance level) can decrypt specific pieces of data. However, standard ABE can be computationally expensive for users, especially when large policies or datasets are involved.

To reduce the processing load on mobile users, outsourced ABE schemes have been proposed. These schemes allow the cloud to handle the majority of the encryption and decryption workload while still preserving user data privacy. The cloud transforms the ciphertext using a transformation key, and the mobile device only needs to perform a lightweight final decryption step. This delegation of computation significantly reduces the processing burden and energy consumption on mobile clients.

Additionally, user revocation is a major challenge in cloud-based access control systems. When a user's privileges are revoked, the system must ensure that they can no longer access the encrypted content. Traditionally, this requires re-encrypting the data and redistributing new keys to all authorized users, which is highly inefficient. The proposed system addresses this by enabling optional re-encryption by the cloud provider. This capability allows the cloud to update ciphertexts in a way that excludes revoked users, without needing to reissue new keys to everyone else. Importantly, this process is designed to maintain data confidentiality, ensuring the cloud still cannot view the plaintext content.

B. Decentralizing privacy: Using blockchain to protect personal data,"

The growing number of reported surveillance cases and data breaches has raised serious concerns about the traditional data management model, where centralized third-party services collect and control vast amounts of personal user information. This centralized control model is increasingly seen as a vulnerability, undermining user privacy and trust.

Bitcoin, through its decentralized architecture and public ledger, has proven that secure, verifiable computing can be achieved without relying on a central authority. Inspired by this principle, the paper introduces a decentralized system for managing personal data that places full control and ownership in the hands of users.

This system is powered by a blockchain-based protocol that functions as a self-executing access-control manager, eliminating the need to trust any intermediary or third-party service provider. In contrast to Bitcoin, where transactions are financial in nature, the transactions in this system serve functional purposes. They include operations such as storing, retrieving, and sharing data, all of which are recorded immutably on the blockchain.

The design emphasizes transparency, auditability, and user autonomy, ensuring that only the data owner can grant access rights and modify data-sharing permissions. The use of a decentralized ledger makes every interaction traceable and secure, addressing key privacy concerns inherent in centralized systems.

The paper also explores future directions for blockchain technology, suggesting enhancements that could expand its capabilities beyond cryptocurrency. These improvements could transform blockchains into a more comprehensive solution for a range of trusted computing applications across sectors like healthcare, identity management, and secure communications, ultimately contributing to a more privacy-preserving digital society.

C. An access control mechanism to ensure privacy in named data networking using attribute-based encryption with immediate revocation of privileges

In the development of the future Internet, Information-Centric Networking (ICN) has emerged as a promising architectural approach to address many of the limitations faced by today's networks. Despite its advantages, a significant concern remains regarding the protection of user data within such architectures.

This paper introduces an access control framework designed specifically for Named Data Networking (NDN), one of the most widely studied ICN models. The proposed system empowers users to define fine-grained access policies, ensuring that only authorized parties can retrieve the requested data.

To enforce these policies securely, the system utilizes attribute-based encryption (ABE), which supports the immediate revocation of access rights when needed. This ensures robust protection and dynamic control over who can access sensitive information.

A key component of the design is the introduction of a Cloud Proxy Server, which acts as an intermediary between users and data sources. This proxy is responsible for managing access requests and enforcing revocation rules. Moreover, in certain implementations, NDN routers themselves can optionally be extended to perform the functions of the Cloud Proxy Server, further integrating security into the network infrastructure.

Experimental evaluations show that the proposed mechanism is practical and efficient. It performs well across various metrics, including processing time, memory consumption, and file size, all of which are critical to both data storage and transmission. The system demonstrates the capability to handle complex access policies involving multiple attributes, making it a scalable and effective solution for secure data management in ICN-based networks.

At the core of the system is an Attribute-Based Encryption (ABE) scheme. ABE is a powerful cryptographic tool that enables encryption based on a set of attributes (e.g., roles, organization, clearance level). The encryption ensures that only users whose attributes match the defined policy can decrypt the data. Importantly, the scheme includes immediate revocation capabilities, allowing the data owner or system to revoke access rights without needing to re-encrypt and redistribute data to other authorized users.

III. DATASET DESCRIPTION:

The dataset utilized in this project is dynamically generated within the system and is organized through multiple relational database tables designed to support the secure sharing of encrypted data in a cloud environment. Rather than relying on external or publicly available datasets, the system simulates real-time data generation through user interactions across various modules such as Admin, Cloud Owner, Cloud Proxy Server, and Data User. When a cloud owner uploads a file, it is divided into four separate segments, and each segment is individually processed using the Secure Hash Algorithm (SHA) to produce unique hash values for integrity verification. These segments, along with their respective hash values and encryption keys, are stored as structured records in the database. The database maintains comprehensive tables including attributes such as user IDs, names, email addresses, login credentials, file names, encryption keys, timestamps, and system-generated activity logs. The Cloud Owner table captures file details, hash values, and upload metadata, while the Data User table records user registration, access requests, and download history. The Proxy Server table logs the generation and usage of re-encryption keys used to securely delegate file access without revealing plaintext data. Admin activities, system attacks, and user login

sessions are also documented to ensure accountability and traceability. Each table contains multiple rows depending on the number of registered users, uploaded files, and access operations performed. Thus, the dataset, although internally generated, represents a complex and realistic simulation of a cloud-based data-sharing system, capturing detailed transactional and cryptographic information across various components of the application.

PROXY RE -ENCRYPTION (PRE):

Proxy Re-Encryption is a cryptographic technique that allows a semi-trusted intermediary, known as a proxy, to convert a ciphertext originally encrypted for one user into a ciphertext that can be decrypted by another user. Importantly, this transformation happens without the proxy gaining access to the plaintext or any secret keys. In the context of this project, the data owner encrypts a file using their public key and generates a re-encryption key, which is shared with the cloud proxy server. When a data user is authorized to access the file, the proxy server uses this re-encryption key to transform the ciphertext into a form that the recipient can decrypt with their private key.

ADVANCED ENCRYPTION STANDARD (AES):

AES is a widely used symmetric encryption algorithm that ensures the confidentiality of data through block cipher operations. It encrypts data in fixed-size blocks (128 bits) and supports key lengths of 128, 192, or 256 bits, with longer keys providing stronger security. In this project, AES is used to encrypt each segment of the data file before it is stored in the cloud. As a symmetric algorithm, both the encryption and decryption processes use the same secret key, which is securely shared only with authorized users. AES is known for its speed, efficiency, and robustness, making it ideal for encrypting large volumes of data in cloud storage applications.

SECURE HASH ALGORITHM (SHA):

The Secure Hash Algorithm is used in this project to verify data integrity by generating a unique hash value for each segment of the uploaded file. When the cloud owner uploads a file, it is divided into four parts, and each part is hashed using SHA to produce a fixed-length output that represents the original data. Even a small modification in the file content will result in a significantly different hash, allowing any unauthorized changes to be easily detected. This mechanism is essential for maintaining trust in the integrity of stored and shared data. The SHA algorithm does not involve encryption or decryption; rather, it provides a digital fingerprint for data validation, ensuring that the content remains unchanged throughout its lifecycle in the cloud.

IDENTITY -BASED ENCRYPTION (IBE):

Identity-Based Encryption is a public key encryption mechanism where the public key of a user is derived directly from a known unique identifier, such as an email address or username. This eliminates the need for digital certificates and reduces the complexity associated with key distribution and management. In this project, IBE is used to simplify the encryption process and provide flexibility in granting access to users. When the data owner wants to share a file, they can encrypt it using the recipient's identity, and the user can decrypt it using a corresponding private key issued by a trusted authority. This method not only improves scalability but also enhances usability, especially in cloud environments where the number of users may be large and dynamic. more details and pictures.

IV. CONCLUSION AND FUTURE WORK

As the Internet of Things (IoT) continues to grow, it's become clear that securely and efficiently sharing data is more important than ever. With billions of devices constantly collecting and transmitting sensitive information, protecting that data's privacy, integrity, and confidentiality is a major challenge. To tackle this, we've developed a secure data-sharing approach that combines identity-based proxy re-encryption (IBPRE) with cloud computing.

Our method lets data owners encrypt their files using identity-based encryption before storing them in the cloud. What makes IBPRE especially useful is that it allows owners to grant access to others without needing to share their private keys. This setup offers strong access control and keeps the data secure from end to end, even as it changes hands.

Since many IoT devices don’t have the power to handle complex encryption tasks, we’ve introduced an edge device to act as a middleman. This device takes on the heavy lifting—like re-encrypting data or managing access permissions—so the smaller devices can stay lightweight and responsive.

We’ve also brought in ideas from Information-Centric Networking (ICN) to make the whole system faster and more efficient. ICN helps by caching frequently used data and routing it based on content rather than location. That means users can access information quicker, and the network uses less bandwidth—an important advantage when dealing with IoT data at scale.

To top it all off, we use blockchain technology to manage access control in a secure and decentralized way. Instead of relying on a single authority, access rules and authorizations are recorded in a blockchain ledger, making them transparent and tamper-proof. This gives data owners more control and helps ensure that privacy is maintained at all times.

Our evaluations show that this combined approach doesn’t just improve security—it also makes the system more efficient and scalable than existing methods. By integrating IBPRE, edge computing, ICN, and blockchain, we’ve built a practical solution for secure data sharing in the evolving world of IoT and cloud services.

V. REFERENCES

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

[6] D. 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, Protec. Compute. 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., Newt. Syst., Springer, Oct. 2010, pp. 1–13.

[10] C. Dannewitz, J. Golic, B. Ohlman, and B. Ahlgren, "Secure naming for a network of information," in Proc. INFOCOM IEEE Conf. Compute. Commun. Workshops,2010, pp. 1–6. [11] A. Carzaniga, M. J. Rutherford, and A. L. Wolf, "A routing scheme for content-based networking," in Proc. IEEE INFOCOM 2004, vol. 2, 2004, pp. 918–928.

[12] I. Psaras, W. K. Chai, and G. Pavlou, "Probabilistic in-network caching for information-centric networks," in Proc. 2nd ed. ICN Workshop Inform.-Centric Newt., 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 Newt. Exp. Technol., Dec. 2014, pp. 363–376.

[14] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, vol. 4. Bitcoin.org, 2008. 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 reencryption 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," Compute. 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-encryptionbased key management for secure and scalable mobile applications in clouds," IEEE Trans. Cloud Compute., 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.