ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

A NOVEL PROXY RE-ENCRYPTION TECHNIQUE FOR SECURE DATA SHARING IN CLOUD ENVIRONMENT

E. MOUNIKA REDDY[1], B. RAKESH[2], B. SHRAVAN[3], B. YESHWANTH[4],

JEET PRAMOD KANTROR[5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— In general, Cloud Computing refers to the storage and access of data through the internet rather than on a local computer hard drive. Cloud services assist in reducing the amount of space and money required for data storage. Data that must be accessed from the cloud must be protected. However, cloud owners and users have a big hurdle in terms of security and personal data privacy. Due to the data owners' lack of trust, they save their data in an encrypted format that is inaccessible to outsiders. The phrase "proxy re-encryption" (PRE) refers to a popular way of delivering encrypted data stored in the cloud. When a data owner wants to share encrypted data with both the data user and the cloud server (proxy), the data owner generates re-encryption data and sends it to the proxy, which can use it to convert the data holder's cipher texts into the user's plaintexts without having to look at the plaintexts beneath. The implementation demonstrates that our proposed work protects privacy while also allowing for secure data sharing via cloud computing.

Index Terms – Cloud computing, proxy re-encryption (PRE), secure data sharing, cloud security, data privacy, encrypted data, access control, cryptography, ciphertext transformation, secure cloud storage, privacy preservation, cloud data protection.

I. INTRODUCTION

THE Internet of Things (IoT) has emerged as a technology that has great significance to the

world nowadays and its utilization has given rise to an expanded growth in network traffic volumes over the years. It is expected that a lot of devices will get connected in the years ahead. Data is a central notion to the IoT paradigm as the data collected serves several purposes. in applications such as healthcare, vehicular networks, smart cities, industries, and manufacturing, among others [1]. The sensors measure a host of parameters that are very useful for stakeholders involved. Consequently, as enticing as IoT seems to be, its advancement has introduced new challenges to security and privacy. IoT needs to be secured against attacks that hinder it from providing the required services, in addition to those that pose threats to the confidentiality, integrity, and privacy of data. A viable solution is to encrypt the data before outsourcing to the cloud servers. Attackers can only see the data in its encrypted form when traditional security measures fail. In data sharing, any information must be encrypted from the source and only decrypted by authorized users in order to preserve its protection. Conventional encryption techniques can be used, where the decryption key is shared among all the data users designated by the data owner. The use of symmetric encryption implies that the same key is shared between the data owner and users, or at least the participants agree on a key. This solution is very inefficient. Furthermore, the data owners do not know in advance who the intended data users are, and, therefore, the encrypted data needs to be decrypted and subsequently encrypted with a key known to both the data owner and the users. This decrypt-and-encrypt solution means the data owner has to be online all the time, which is practically not feasible. The problem becomes increasingly complex when there are multiple pieces of data and diverse data owners and users. Although simple, the traditional encryption schemes involve complex key management protocols and, hence, are not apt for data sharing. Proxy re-encryption (PRE), a notion first proposed by Blaze et al. [2], allows a proxy to transform a file computed under a delegator's public key into an encryption intended for a delegate. Let the data owner be the delegator and the data user be the delegate. In such a scheme, the data owner can send encrypted messages to the user temporarily without revealing his secret key. The data owner or a trusted third party generates the re-encryption key. A proxy runs the re-encryption algorithm with the key and revamps the ciphertext before sending the new ciphertext to the user. An intrinsic trait of a PRE scheme is that the proxy is not fully trusted (it has no

idea of the data owner's secret key). This is seen as a prime candidate for delegating access to encrypted data in a secured manner, which is a crucial component in any data sharing scenario. In addition, PRE allows for encrypted data in the cloud to be shared to authorized users while maintaining its confidentiality from illegitimate parties Data disclosures can be minimized through the use of encryption since only users delegated by the data owner can effectively access the outsourced data. Motivated by this scenario, this article proposes an improvement in IoT data sharing by combining PRE with identity-based encryption (IBE), information-centric networking (ICN), and blockchain technology. Shamir [3] first presented the notion of IBE, in which a sender encrypts a message to a recipient using the identity (email) as the public key. It is a very powerful primitive used to combat numerous key distribution problems and has consented to the development of several cryptographic protocols, including public-key searchable encryption [4], [5], secret handshakes [6], and chosen ciphertext attack (CCA) secure public-key encryption [7]. IBE is preferred over attribute-based encryption (ABE) because ABE involves heavy computations on data encryption, decryption, and key management, and these processes are not convenient for the resource-constrained IoT devices. The strength of this article is increased by borrowing the idea of ICN to cater for the growth in information sharing. The appeal for low-latency applications introduced the notion of ICN [8]–[11], where data owners can distribute and assign unique names to their data which can be replicated and saved in network caches [12], [13]. This ensures that there is an efficient data delivery and utilization of network bandwidth, which is a prerequisite for the IoT ecosystem regardless of the enormous growth in network volumes. On issues of trust, a decentralized, distributed system that can smoothen secure and trusted data sharing was introduced by Nakamoto [14]. This is the blockchain technology, and it has gained much attention due to its ability to preserve data privacy. Although there exist optimization issues when storing vast sizes of data, emerging system applications have used the blockchain for access control in database management. Data confidentiality and user revocation can also be achieved using blockchain.

II. RELATED WORK

A. *Decentralizing privacy: Using blockchain to protect personal data*

The recent increase in reported incidents of surveillance and security breaches compromising users' privacy call into question the current model, in which third-parties collect and control massive amounts of personal data. Bit coin has demonstrated in the financial space that trusted, auditable computing is possible using a decentralized network of peers accompanied by a public ledger. In this paper, we describe a decentralized personal data management system that ensures users own and control their data. We implement a protocol that turns a block chain into an automated access control manager that does not require trust in a third party. Unlike Bit coin, transactions in our system are not strictly financial -- they are used to carry instructions, such as storing, querying and sharing data. Finally, we discuss possible future extensions to block chains that could harness them into a well-rounded solution for trusted computing problems in society.

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

For future Internet, information-centric networking (ICN) is considered a potential solution to many of its current problems. However, concern regarding the protection of user data persists. This paper presents an access control mechanism that will allow users to set fine-grained access policies for applications in named data networking (NDN), a popular ICN architecture. Using an attribute-based encryption scheme with an immediate revocation of privileges, data security is guaranteed. The mechanism inserts a Cloud Proxy Server to mediate the access to the protected data and to inspect for revocation. As an optional feature, the NDN router can add Cloud Proxy Server functions. According to the experiments, the proposed security mechanism proved functional in terms of processing time, memory usage, and file size, which influence both storage and transmission and demonstrate efficiency in manipulating dozens of attributes in an access policy.

C. *A Medical Data Sharing Scheme Based on Blockchain Attribute-Based Searchable Encryption*

Aiming at the problems of low sharing efficiency and easy privacy leakage of electronic medical records, a blockchain-based attribute-based searchable encrypted electronic medical record sharing scheme is

proposed to achieve fine-grained access control of users' search privileges in one-to-many data sharing scenarios, and at the same time, solve the inefficiency of ciphertext retrieval. In this paper, the shared medical data is divided into structured and unstructured data, and the data is stored in a combined on-chain and off-chain mode, which ensures that both participate in the sharing at the same time, and also relieves the storage pressure of the blockchain. Attribute encryption based on ciphertext policy provides fine-grained access control services, and a data dictionary index structure is designed to complete ciphertext search in the index using searchable encryption. Blockchain nodes retrieve ciphertext keywords and search the index to improve the search efficiency of blockchain nodes. Experimental analysis shows that the scheme can quickly perform the search and sharing of electronic medical records.

D. A Revocable Certificateless Sanitizable Signature Scheme With Batch Verification

In medical and healthcare application scenarios, data integrity and user privacy are often concerned the most. A subitizable signature scheme is a common adopted approach since it admits an authorized person to sanitize partial sensitive information of signed messages while keeping the correctness of preserved message and signature pairs. A certificateless subitizable signature scheme further enjoys the merits of certificateless public key systems. That is, it is unnecessary to maintain the public key certificates in traditional cryptosystems or deal with the key escrow problem in identity-based systems. However, the functionality of batch verification for retained message signature pairs and the revocation mechanism are still lack in previous works. To resolve these issues, the authors propose a revocable certificateless subitizable signature scheme with batch verification in this paper. The revocation mechanism is fulfilled by combining user's private key with an updatable time key. Hence, a revoked user is unable to request the renewed time key. We also provide a formal proof that our proposed system satisfies the security requirement of existential unforgeability under adaptive chosen-message attacks (EUF-CMA) in the random oracle model. In comparison to related variants, our system demonstrates superior functionality and computational efficiency.

III. PROPOSED METHODOLOGY

Data that must be accessed from the cloud must be protected. However, cloud owners and users have a big hurdle in terms of security and personal data privacy. Due to the data owners' lack of trust, they save their data in an encrypted format that is inaccessible to outsiders. The phrase “proxy re-encryption” (PRE) refers to a popular way of delivering encrypted data stored in the cloud. When a data owner wants to share encrypted data with both the data user and the cloud server (proxy), the data owner generates re-encryption data and sends it to the proxy, which can use it to convert the data holder's cipher texts into the user's plaintexts without having to look at the plaintexts.

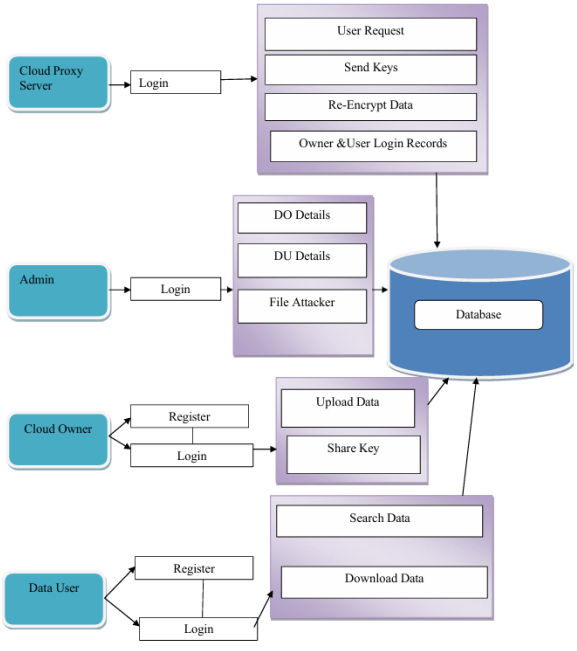
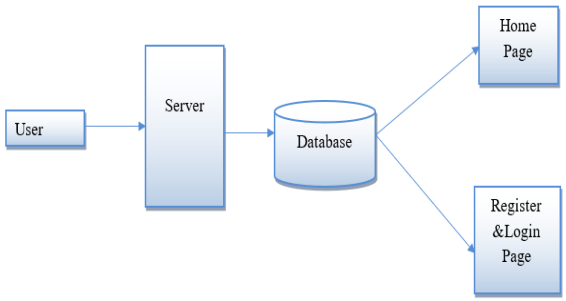


Fig. 1: System Overview

1. User Interface Design

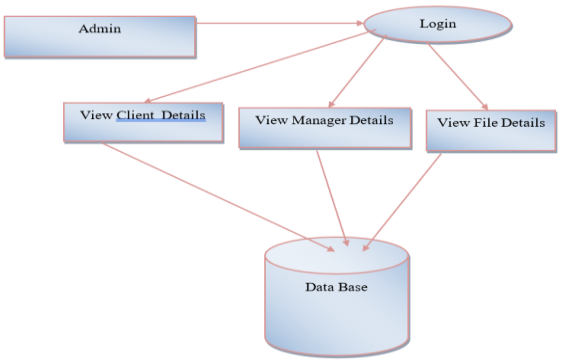
In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server.

If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.



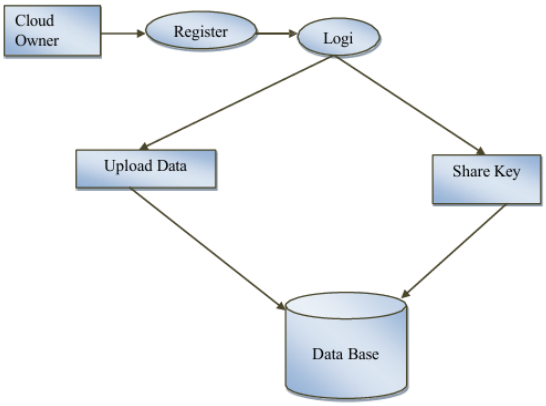
2. Admin

This is the first module. Here admin has a main modules to stores all the information’s of the project. Admin is a login with a user id and password. Admin has a stores all information’s of details. Admin can also have a data owner details. Admin can have a data user details in the database. The admin can have a file attacker to file attack information.



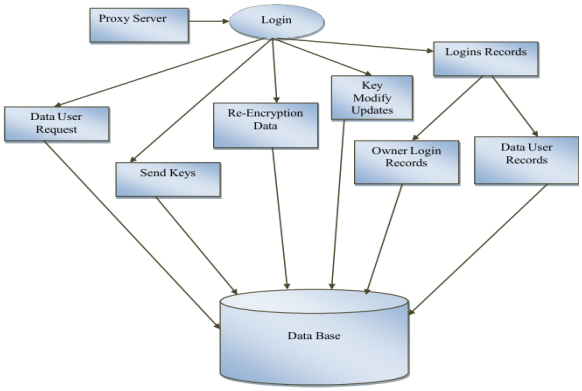
3. Cloud Owner

This is the Second module of this project. In this module cloud owner should register and Login. Cloud owner can store a data in a text format. Cloud owner can also have a key send to the Cloud Proxy Server should approve then the key will send an authentic user. User can access a data.



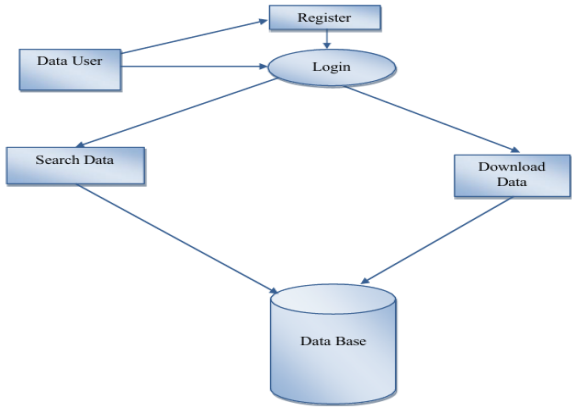
4. Cloud Proxy Server

In this module Cloud Proxy Server has login. After login it will have a data user requests. Data user after register it will takes a permissions from the server. In server it will approve then the data user can login. Cloud Proxy Server has a send keys to the user. Cloud Proxy Server can also are re encrypt a file then forward to the user. Cloud Proxy Server has a key will updates and key will modify. Cloud Proxy Server has a maintains a records of a logins of Cloud Owner and data users.



5. Data User

In this module the data user can also a register with a details. Login it takes permission from the Cloud Proxy Server. Cloud Proxy Server can a approve a user. After approve it was data user can login. Data user can also a search a data. Data user can also a download a file.



IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed proxy re-encryption (PRE) scheme enables secure and privacy-preserving data sharing in cloud environments without exposing plaintext data to the cloud server. The re-encryption mechanism efficiently transforms ciphertexts for authorized users while maintaining data confidentiality and access control. Performance evaluation demonstrates low computational overhead and secure key management during data sharing. Overall, the proposed framework provides an efficient and reliable solution for secure cloud-based data sharing.

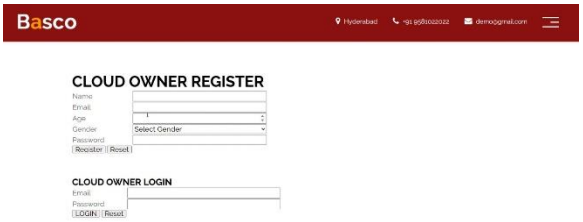


Fig. 2: Cloud Owner Registration

Fig. 3: Upload File

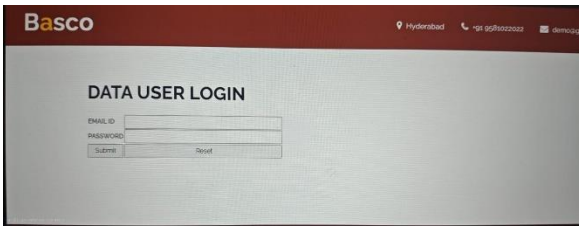


Fig. 4: Data User Login

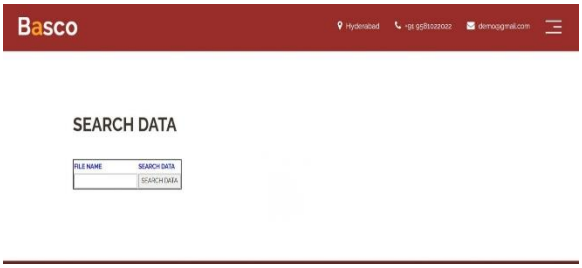


Fig. 5: Search Data

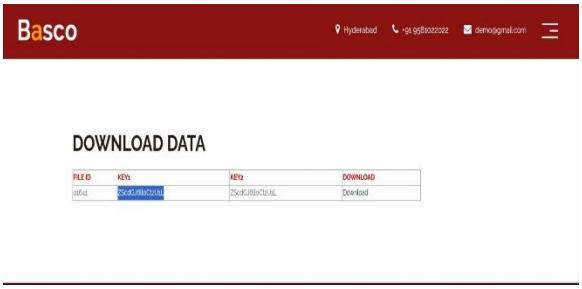


Fig. 5: Download File

V. CONCLUSION

The emergence of the IoT has made data sharing one of its most prominent applications. To guarantee data confidentiality, integrity, and privacy, we propose a secure identity-based PRE data sharing scheme in a cloud computing environment. Secure data sharing is realized with IBPRE technique, which allows the data owners to store their encrypted data in the cloud and share them with legitimate users

efficiently. Due to resource constraints, an edge device serves as the proxy to handle the intensive computations. The scheme also incorporates the features of ICN to proficiently deliver cached content, thereby improving the quality of service and making great use of the network bandwidth.

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.

AUTHORS Profile

Mrs. E. MOUNIKA RE-DDY has received her B.Tech from JNTUH, Hyderabad in 2015, M.Tech degree in Computer science from JNTUH, Hyderabad in 2017. She is dedicated to teaching field from the last 8 years. At present she is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.

Mr. B. RAKESH pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliatedto JNTUH in 2022-2026.

Mr. B. SHRAVAN pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliatedto JNTUH in 2022-2026.

Mr. B. YESHWANTH pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliatedto JNTUH in 2022-2026.

Mr. JEET PRAMOD KANTROR pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliatedto JNTUH in 2022-2026.