

SAFEGUARDING THE DIGITAL WORLD DATA SHARING WITH PROXY RE-ENCRYPTION USING BLOCKCHAIN

¹Dr. S. Vijayarangam,² U. Mani Kanta,³ T. Swetha,⁴ S. Nishitha,⁵ Shaik Sohail

¹Professor,²³⁴⁵B.Tech Students

Department Of Computer Science & Engineering

Sri Indu College Of Engineering & Technology, Sheriguda, Ibrahimpatnam

ABSTRACT

The evolution of the Internet of Things has seen data sharing as one of its most useful applications in cloud computing. As eye-catching as this technology has been, data security remains one of the obstacles it faces since the wrongful use of data leads to several damages. In this article, we propose a proxy re-encryption approach to secure data sharing in cloud environments. Data owners can outsource their encrypted data to the cloud using identity-based encryption, while proxy reencryption construction will grant legitimate users access to the data. With the Internet of Things devices being resource-constrained, an edge device acts as a proxy server to handle intensive computations. Also, we make use of the features of information centric networking to deliver cached content in the proxy effectively, thus improving the quality of service and making good use of the network bandwidth. Further, our system model is based on block chain, a disruptive technology that enables decentralization in data sharing. It mitigates the bottlenecks in centralized systems and achieves fine-grained access control to data. The security analysis and evaluation of our scheme show the promise of our approach in ensuring data confidentiality, integrity, and security.

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 for stakeholders involved. very useful

Page | 1887

Index in Cosmos JUNE 2025, Volume 15, ISSUE 2 UGC Approved Journal 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 decryptand-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 datasharing 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 cipher-text 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 resourceconstrained 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

Page | 1888

Index in Cosmos JUNE 2025, Volume 15, ISSUE 2 UGC Approved Journal 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.

PRE, together with IBE and the features of ICN and blockchain, will enhance security and privacy in data-sharing systems. PRE and IBE will ensure fine-grained data access control, while the concept of ICN promises a sufficient quality of service in data delivery because the in-network caching provides efficient distribution of data. The blockchain is optimized to prevent storage and data-sharing overheads and also to ensure a trusted system among entities on the network. In our article, the data owner propagates an access control list which is stored on the blockchain. Only the authorized users are able to access the data. The contributions of this article are summarized as follows

• We propose a secure access control framework to realize data confidentiality, and finegrained access to data are achieved. This will also guarantee data owners' complete control over their data.

To improve data delivery and effectively utilize the network bandwidth, edge devices serve as proxy nodes and perform re-encryption on the cached data. The edge devices are assumed to have enough computation capabilities than the IoT devices and as such provide high performance



networking.

II. LITERATURE SURVEY

TITLE: Internet of Things: A survey on enabling technologies, protocols, and applications.

AUTHOR: A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash,

ABSTRACT: This paper provides an overview of the Internet of Things (IoT) with emphasis on enabling technologies, protocols, and application issues. The IoT is enabled by the latest developments in RFID, smart sensors. technologies, communication and Internet protocols. The basic premise is to have smart sensors collaborate directly without human involvement to deliver a new class of applications. The current revolution in Internet, mobile, and machineto-machine (M2M) technologies can be seen as the first phase of the IoT. In the coming years, the IoT is expected to bridge diverse technologies to enable new applications by connecting physical objects together in support of intelligent decision making. This paper starts by providing a horizontal overview of the IoT. Then, we give an overview of some technical details that pertain to the IoT enabling technologies, protocols, and applications. Compared to other survey papers in the field, our objective is to provide a more thorough summary of the most relevant protocols and application issues to enable researchers and application developers to get up to speed quickly on how the different protocols fit together to deliver desired functionalities without having to go through RFCs and the standards specifications. We also provide an overview of some of the key IoT challenges presented in the recent literature and provide a summary of related research work. Moreover, we explore the relation between the IoT and other emerging technologies including big data analytics and cloud and fog computing. We also present the need for better horizontal integration among IoT services. Finally, we present detailed service use-cases to illustrate how the different protocols presented in the paper fit together to deliver desired IoT services.

Page | 1889

TITLE: Divertible protocols and atomic proxy cryptography.

AUTHOR: M. Blaze, G. Bleumer, and M. Strauss,

ABSTRACT: First, we introduce the notion of divertibility as a proto- col property as opposed to the existing notion as a language property (see Okamoto, Ohta (OO90)). We give a definition of protocol divertibility that applies to arbitrary 2party protocols and is compatible with Okamoto and Ohta's definition in the case of interactive zero-knowledge proofs. Other important examples falling under the new definition are blind signature protocols. We propose a sufficiency criterion for divertibility that is satisfied by many existing protocols and which, surprisingly, generalizes to cover several protocols not normally associated with divertibility (e.g., Diffie Hellman key exchange). Next, we introduce atomic proxy cryptography, in which an atomic proxy function, in conjunction with a public proxy key, converts ciphertexts (messages or signatures) for one key into ciphertexts for another. Proxy keys, once generated, may be made public and proxy functions applied in untrusted environments. We present atomic proxy functions for discrete-logbased encryption, identification, and signature schemes. It is not clear whether atomic proxy functions exist in general for all public-key cryptosystems. Finally, we discuss the relationship between divertibility and proxy cryptography.

TITLE: Identity-based cryptosystems and signature schemes.

AUTHOR: A. Shamir,

AUTHOR: D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano,

ABSTRACT: We study the problem of searching on data that is encrypted using a public key system. Consider user Bob who sends email to user Alice encrypted under Alice's public key. An



email gateway wants to test whether the email contains the keyword "urgent" so that it could route the email accordingly. Alice, on the other hand does not wish to give the gateway the ability to decrypt all her messages. We define and construct a mechanism that enables. Alice to provide a key to the gateway that enables the gateway to test whether the word "urgent" is a keyword in the email without learning anything else about the email. We refer to this mechanism as Public Key Encryption with keyword Search. As another example, consider a mail server that stores various messages publicly encrypted for Alice by others. Using our mechanism Alice can send the mail server a key that will enable the server to identify all messages containing some specific keyword, but learn nothing else. We define the concept of public key encryption with keyword search and give several constructions

III. SYSTEM ANALYSIS & DESIGN EXISTING SYSTEM

Yu et al. [15] combined key-policy ABE (KP-ABE) and PRE to propose a system for data sharing in the cloud. The data was encrypted using KP-ABE which meant that only an appropriate collection of the attribute secret keys can make decryption possible. Besides the encrypted data, the cloud also managed all attribute secret keys except one special secret key in order to handle revocation of users. When users are revoked, new keys were distributed to the remaining users by the data owner and the encrypted data had to be re-encrypted.

Although the scheme was efficient, the reencryption was performed in a lazy way, and, therefore, the security of the scheme was weakened. Park [16] provided a modification to the scheme in [15], where collusion between the service provider and revoked users is avoided. Their scheme was to basically replace the service provider with a trusted third party, which implies that there should be reliance on stronger trust assumption. Other schemes [17]–[19] have made similar approaches but utilized ciphertext-policy ABE (CP- ABE) rather, in which the access policy is associated with the ciphertext instead of the

Page | 1890

Index in Cosmos JUNE 2025, Volume 15, ISSUE 2 UGC Approved Journal secret keys. Liu et al. [20] also proposed a time constrained access control scheme based on PRE and ABE. ABE was used to design time-based access control policies while PRE was used to update the time attributes. Although these schemes have their advantages, they are not suitable in the context of IoT due to the heavy computations on encryption and decryption.

DISADVANTAGES:

- 1. The re-encryption was performed in a lazy way, and, therefore, the security of the scheme was weakened.
- 2. provided a modification to the scheme in, where collusion between the service provider and revoked users is avoided

PROPOSED SYSTEM

Our system model introduces a blockchain-based PRE approach to data sharing. The additional entities to the data-sharing model as discussed in Fig. 1 are the edge devices and the blockchain. The edge devices serve as proxy nodes and provide reencryption services to the authorized user(s). When the data is cached at the edge of the network, the edge devices provide services to users with high availability and performance. They receive the reencryption key from the data owner, fetch the ciphertext from the CSP, and transform the ciphertext in the identity of the data user. It is an honest-but-curious entity.

The blockchain serves as the trusted authority (TA) that initiates the system parameters. The TA also provides secret keys that are bound to the users' identities. By utilizing this distributed ledger, authenticity, transparency, and verifiability are achieved in the network which enhances the security and privacy of data. Data owners are therefore able to manage their data effectively. The blockchain network registers and issues membership keys to the data owner(s) and user(s). When a user requests data access, the owner generates a re-encryption key by using the identity of the user and sends it to the proxy server. Access rights and policies on the use of the data are instantiated and sent to the block chain network. A data user is verified before access is granted.

ADVANTAGES:



- 1. A secure access control framework to realize data confidentiality and fine-grained access to data are achieved. This will also guarantee data owners' complete control over their data.
- 2. Improve data delivery and effectively utilize the network bandwidth, edge devices serve as proxy nodes and perform reencryption on the cached data.

SYSTEM ARCHITECTURE



Fig. SYSTEM ARCHITECTURE

IV. IMPLEMENTATION MODULES

- 1. DATA OWNER
- 2. DATA USER
- 3. PROXY SERVER
- 4. TRUSTED AUTHORITY
- 5. CSP

MODULE DESCRIPTION

1. DATA OWNER

Data owner should register with the application then login into application after successful login he can perform some operations such as encrypt and upload files into cloud, view all uploads and view request and send re-encrypt request to proxy server with user identity and logout.

2. DATA USER

Data user should register with the application then login into application after successful login he can perform some operations such as can search a file and send request to block chain and view response and decrypt file and download files and logout.

3. TRUSTED AUTHORITY(BLOCK CHAIN)

Here trusted authority can directly login with the username and password then perform some operations such as view users and owners generate Page | 1891

Index in Cosmos JUNE 2025, Volume 15, ISSUE 2 UGC Approved Journal membership key and view all submitted data by proxy server and logout.

4. **PROXY SERVER**

Here proxy server can directly login with the username and password then perform some operations such as view re-encrypt request and get response from cloud like url and upload to block chain ,user and logout.

5. CSP

Here CSP can directly login with the username and password then perform some operations such as view all files and view all request and response and encryption time graph and re-encryption time graph and decryption time graph and all download graph and attacked file graph and logout.

V. SCREENSHOTS

Safeguarding the digital world data sharing with proxy re-encryption
The availability of Thirups have seen data sharing as one of the next and/a applications is that also supporting the spec control on the historicality have have, disk assuring some of an electroders is how income the availability of and disk hand to avail adapting that have disk, any parson or parson or availability and the source adapting the index to the test of the adapting that the disk hand to avail adapting the have availability and the source adapting the index to the source adapting that the disk hand to avail adapting the hand encryption, while parson or exception construction and pars hightness ones assess for 6 adapting. This face, the same and the hand the source adapting the index to adapting the index the source adapting the index to adapting the adapting that and the hand the hand the hand the source is choralized to what are used to assess the datapting the datapting that and the source adapting the add the hand the hand the source is choralized to the data could be assessed to adapting the adapting that and the source adapting the add the source is choralized to adapting the adapting that what are add to assess the source adapting the adapting that and the source adapting the add the source is choralized to advance the adapting the adapting that and the source adapting the adapting that and the source adapting the adapting that and the adapting the adapting that adapting that adapting the adapting that adapting that adapting the adapting that adapting the adapting the adapting the adapting that add the adapting that adapting the adapting that adapting that adapting the adapting the adapting the adapting the adapting the adapting the adapting that adapting the adapting the adapting that adapting the adapting the adapting that adapting the adapting that adapting the adapting the adapting that adapting th
matt blobbai blobs Found Projecu OP Auforij
Safeguarding the digital world data sharing with proxy re-encryption using Blockchain
 Home View-Dennes View-Days Laplat Opticities
Safeguarding the Digital World Data Sharing with Proxy Re-Encryption using Blockchain
VIEW ALL DATA OWNERSK AND GENERATE MEMBERSHIP KEY Kurban Intal Tell (Standarding and Standarding Standard) Standarding Standarding Standarding Standarding Standarding Standarding Standarding Standarding Standarding





Page | 1892





Page | 1893



10000 bis/doar bis/bir Touri hurg/sere CP
Safeguarding the Digital World Data Sharing with Proxy Re-Encryption using Blockchain
IDME Data/over Data User Transfer Angriserer CP
Safeguarding the Digital World Data Sharing with Proxy Re-Encryption using Blockchain
1930. View Miller View Reports Receptors & Langeton McDevelood Attracted States and States and States State
A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain
Welcome: CSP

VI. CONCLUSION 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. Then, we present a blockchain-based system model that allows for flexible authorization on encrypted data. Finegrained access control is achieved, and it can help Page | 1894

data owners achieve privacy preservation in an adequate way. The analysis and results of the proposed model show how efficient our scheme is, compared to existing schemes.

FUTURE SCOPE

In the evolving landscape of data exchange and storage, WEBCLOUD, an internet- linked cloud repository for secure information sharing across systems, presents a promising future. With a growing emphasis on data security, WEBCLOUD offers enhanced protection, ensuring the confidentiality integrity of sensitive and information. Its cross- platform compatibility is poised to become increasingly valuable in a world where seamless data sharing between diverse systems is essential. Integration with emerging technologies such as IoT and AI positions WEBCLOUD as a central hub for managing the vast data generated by these innovations.

REFERENCES

- 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.
- 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, "Identitybased cryptosystems and signature schemes," in Proc. Workshop Theory Appl. Cryptographic Techn., Springer, Aug. 1984, pp. 47–53.
- 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.
- 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.
- 5. D. Balfanz et al., "Secret handshakes from pairing-based key agreements," in Proc.



IEEE, Symp. Secur. Privacy, 2003, pp. 180–196.

- R. Canetti, S. Halevi, and J. Katz, "Chosenciphertext security from identity-based encryption," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., Springer, 2004,pp. 207–222.
- 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.
- 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.

Page | 1895