www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 05, May 2023, pp : 424-429

e-ISSN : 2583-1062

Impact Factor : 5.725

PROXY RE ENCRYPTION SCHEME FOR SECURE DATA STORING IN CLOUD USING BLOCKCHAIN TECHNOLOGY

Vivek Pandiya Raj[1], Snega. M[2], Subithra. R[3], Swarnashri. S[4], Tamil Selvi. N[5]

[1]Assistant Professor, Department Of Computer Science & Engineering, Vivekanandha College Of Technology For Women, Namakkal, Tamil Nadu, India

[2,3,4,5]Ug Scholar, Department Of Computer Science & Engineering, Vivekanandha College Of Technology For Women, Namakkal, Tamil Nadu, India

DOI: https://www.doi.org/10.58257/IJPREMS31201

ABSTRACT

Data sharing has been identified as one of the Internet of Things' most useful uses in cloud computing. Data security continues to be one of the challenges this technology has, even though it has been visually appealing, as improper usage of data results in a number of negative effects. We suggest a proxy re-encryption strategy to protect data sharing in cloud contexts in this study. Data owners can utilize identity-based encryption to outsource their encrypted data to the cloud, while proxy re-encryption construction will enable legitimate users access to the data. Due to the limited resources of Internet of Things devices, an edge device operates as a proxy server to conduct demanding computations. Furthermore, we use information-centric networking features to effectively deliver cached content in the proxy, thereby improving performance making efficient use of the network capacity and raising the quality of the service. Our system concept is also built on the blockchain, a ground-breaking technology that enables decentralized data sharing. It accomplishes fine-grained data access control while reducing bottlenecks in centralized systems. The results of our plan's security analysis and evaluation demonstrate its potential for maintaining the security, confidentiality, and integrity of data.

Keywords: blockchain, safe data sharing, Internet of Things

1. INTRODUCTION

Today's world has come to recognize the Internet of Things (IoT) as a technology of great significance, and as a result, network traffic levels have risen steadily over time as a result of its use. In the upcoming years, many devices are probably going to be connected. Data is a key idea in the IoT paradigm since the information gathered serves numerous purposes in areas like manufacturing, transportation networks, smart cities, healthcare, and other areas. For the involved stakeholders, the sensors measure a wide range of parameters that are very helpful. As tempting as IoT may seem, new security and privacy risks have arisen as a result of its development. IoT needs to be safeguarded from cyberattacks that prohibit it from carrying out its functions. When symmetric encryption is used, it is assumed that both the data owner and the users have access to the same key, or at the very least that they have come to an agreement on a key. This answer is incredibly ineffective. The data must first be decrypted with a key that is known to both the data owner and the users before being encrypted again since the data owners do not know in advance who the intended data users are. Because the data owner must be online constantly to use this decrypt-and-encrypt solution, it is practically impossible. When there are several data types, different data owners, and different data users, the problem becomes more and more complicated. Traditional encryption techniques, while straightforward, involve complicated key management protocols and are therefore not suitable for data sharing. A proxy can convert a file computed using a delegator's public key into an encryption meant for a delegate thanks to a technique called proxy re-encryption (PRE), which was first described by Blaze et al. Both the delegator and the delegate should be the owner of the data. A technique like this allows the owner of the data to send the user encrypted messages while keeping his secret key a secret. The re-encryption key is produced by either the data owner or a reliable outsider. A proxy re-encrypts the ciphertext using the key and runs the re-encryption algorithm before providing the updated ciphertext to the user. A PRE plan's inherent quality is the proxy cannot be fully trusted because it is unaware of the private key belonging to the data owner. This is considered to be a top contender for securely granting access to encrypted data, which is an essential element in any scenario involving data sharing.

2. RELATED WORKS

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

Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash [1] 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, communication technologies, 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 machine-to-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.

2.2 Divertible protocols and atomic proxy cryptography

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

[1] First, we introduce the notion of divertibility as a protocol 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 2-party protocols and is compatible with Okamoto and Otha'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-log-based 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

2.2 Identity-based cryptosystems and signature schemes

A. Shamir [3] In this paper we introduce a novel type of cryptographic scheme, which enables any pair of users to communicate securely and to verify each other's signatures without exchanging private or public keys, without keeping key directories, and without using the services of a third party. The scheme assumes the existence of trusted key generation centers, whose sole purpose is to give each user a personalized smart card when he first joins the network. The information embedded in this card enables the user to sign and encrypt the messages he sends and to decrypt and verify the messages he receives in a totally independent way, regardless of the identity of the other party. Previously issued cards do not have to be updated when new users join the network, and the various centers do not have to coordinate their activities or even to keep a user list. The centers can be closed after all the cards are issued, and the network can continue to function in a completely decentralized way for an indefinite period

2.4 Public key encryption with keyword search

D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano [4]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.

2.5 Building an encrypted and searchable audit log

B. R. Waters, D. Balkans, G. Durfee, and D. K. Smatters [5] Audit logs are an important part of any secure system, and they need to be carefully designed in order to give a faithful representation of past system activity. This is

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 05, May 2023, pp : 424-429

e-ISSN : 2583-1062

Impact Factor : 5.725

especially true in the presence of adversaries who might want to tamper with the audit logs. While it is important that auditors can inspect audit logs to assess past system activity, the content of an audit log may contain sensitive information, and should therefore be protected from unauthorized parties.Protecting the contents of audit logs from unauthorized parties (i.e., encrypting it), while making it efficiently searchable by authorized auditors poses a problem. We describe an approach for constructing searchable encrypted audit logs which can be combined with any number of existing approaches for creating tamper-resistant logs. In particular, we implemented an audit log for database queries that uses hash chains for integrity protection and identity based encryption with extracted keywords to enable searching on the encrypted log. Our technique for keyword search on encrypted data has wide application beyond searchable audit logs.

3. PROPOSED SYSTEM

This system proposes an improvement in IoT data sharing by combining PRE with ID-based encryption (IDBE), information-centric networking (ICN), and blockchain technology.In the proposed system, the data owner propagates an access control list which is stored on the blockchain. Only the authorized users are able to access the data. We propose a secure access control framework to realize data confidentiality, and fine-grained access to data is achieved. This will also guarantee data owners' complete control over their data

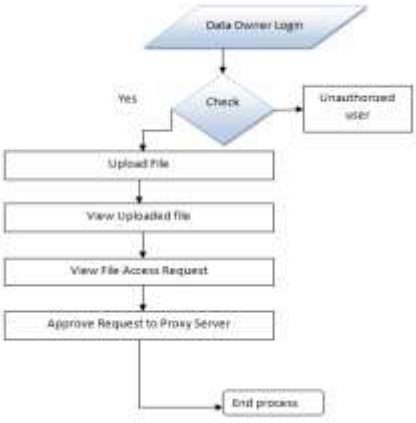
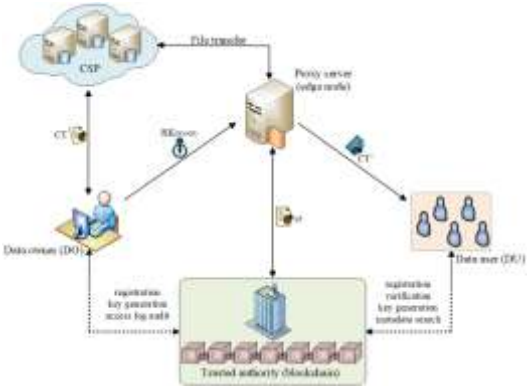


Fig .1

We give a detailed description of our PRE scheme and the actualization of a complete protocol that guarantees security and privacy of data.In the proposed system, the data is divided into 3 different blocks and stored in the cloud for the enhanced security model and then the proxy re-encryption approach is made for securing the data in the cloud.



.Figure: System Architecture

4. ALGORITHM

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 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.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 05, May 2023, pp : 424-429

e-ISSN : 2583-1062

Impact Factor : 5.725

5. MODULE DESCRIPTION

5.1 LIST OF MODULES

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

5.2 MODULE DESCRIPTIONS

5.2.1 Data Owner

In Data Owner module, Initially Data Owner must have to register their detail. Then Trusted authority should approve every new data owner. Only if the trusted authority approves the data owner, the data owner can able to login or else it's not possible to login to the system. In every login the data owner should provide the private key apart from username and password. After successful registration data owner can login and upload files into cloud server with the block splitted into 3 various parts and encrypted for more security purpose. He/she can view the files that are uploaded in cloud. Data Owner can approve or reject the file request sent by data users. After request approval data owner will send the secret key and verification object through mail.

5.2.2 Data User

In this module, we develop Data user part. Where the new data user should register the details and then the trusted authority should approve the new data user. Only if the data user is approved by the trusted authority, the data user can able to get the key or login to the system, or else the data user cannot able to login into the system. In every login the data user should provide the private key apart from username and password. Once the authenticated data user logs in, the data user can able to search the available files, by entering the keyword of the file. To get the access of the file, the data user must provide the request. Only if the request is accepted, they data user can able to download the file which the data user requested. These data users must access the shared data from the CSP which is a semi trusted party that offers storage services to the data. It houses the encrypted data from the owner and the data is received through a secure communication channel. They provide data-sharing services without being able to learn anything about the plaintext.

5.2.3 Trusted Authority

The trusted authority is the entity which approves the new data Owner or data user in the system. 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 blockchain network. A data user is verified before access is granted.

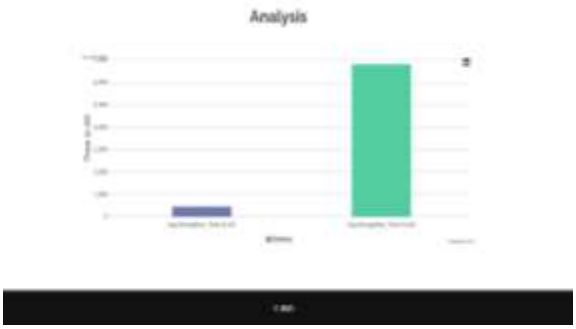
5.2.4 Proxy Server

In this module, we implement the Proxy server. In Proxy re-encryption a User may encrypt his file with his own public key and then store the ciphertext in an honest-but-curious server. When the receiver is decided, the sender can delegate a re-encryption key associated with the receiver to the server as a proxy. Then the proxy re-encrypts the initial ciphertext to the intended receiver. Finally, the receiver can decrypt the resulting ciphertext with her private key. The security of PRE usually assures that (1) neither the server/proxy nor non-intended receivers can learn any useful information about the (re-)encrypted file, and (2) before receiving the re-encryption key, the proxy cannot re-encrypt the initial ciphertext in a meaningful way

5.2.5 CSP

In this module, we develop Cloud Service Provider (CSP). For the implementation of cloud storage, we use Drive HQ cloud service provider where the files uploaded by the data owner are stored in the cloud service as blocks and fragments. Moreover, if an attacker is uncertain about the locations of the fragments, the probability of finding fragments on all of the nodes is very low. Therefore, we fragment the given Data file and upload in the Cloud so that no attacker will obtain the data file. In cloud systems, the probability for an attacker to obtain a considerable amount of data, reduces significantly. However, placing each fragment once in the system will increase the data retrieval time.

6. RESULT



7. CONCLUSION

1`zqA permanent and unchangeable record of every transaction is created by blockchain technology. Fraud, hacking, data loss, and other information-related crimes are impossible with this unbreakable digital ledger. While decentralized financial institutions have been reshaped by blockchain technology, its application possibilities are more wide-ranging. Then, we introduce a block chain-based system model that supports flexible authorization on encrypted data. It is possible to implement fine-grained access control, which can effectively assist data owners in preserving privacy. Comparing our plan to other plans, the analysis and outcomes of the suggested model demonstrate how effective it is..

8. FUTURE ENHANCEMENTS

Sensitive data kept on cloud servers can be managed more safely by providing detailed user access control in cloud environments. The suggested protocol offers a framework via which a sizable volume of different data, including users' private information that requires high confidentiality, can be retrieved effectively and reliably. In the context of cloud computing, we anticipate that the suggested protocol will be effectively and widely deployed. Due to the fact that this method offers more functionalities than previous attribute-based encryption methods, it has the drawback of requiring more calculation in the polynomial equation. Based on the suggested strategy, future research will examine more effective and secure methods.

9. REFERENCES

[1] A. Al-Fuqaha, M. Guiana, M. Mohammedi, M. Aldhabi, and M. Ayyash, “Internet of Things: A survey on enabling technologies, protocols, and applications,” IEEE Common. Surveys Tut., vol. 17, no. 4, pp. 2347–2376, Oct./Dec. 2015.

[2] M. Blaze, G. Blumer, and M. Strauss, “Divertible protocols and atomic proxy cryptography,” in Proc. Int. Conf. Theory Appl. Cryptographic Techno., Springer, May 1998, pp. 127–144.

[3] A. Shamir, “Identity-based cryptosystems and signature schemes,” in Proc. Workshop Theory Appl. Cryptographic Techno., Springer, Aug. 1984, pp. 47–53.

[4] D. Bone, G. Di Crescenzi, R. Ostrovsky, and G. Persian, “Public key encryption with keyword search,” in Proc. Int. Conf. Theory Appl. Cryptographic Techno., Springer, May 2004, pp. 506–522.

[5] B. R. Waters, D. Balkans, G. Durfee, and D. K. Smatters, “Building an encrypted and searchable audit log,” in NDSS, vol. 4. Cite seer, Feb. 2004, pp. 5–6.

[6] D. Balkans et al., “Secret handshakes from pairing-based key agreements,” in Proc. IEEE, Sump. Secure. 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. Kapanen et al., “A data-oriented (and beyond) network architecture,” in Proc. Conf. Appl., Techno., Architectures, Protoc. Compute. Common., Aug. 2007, pp. 181–192.

[9] N. Fodio, P. Sikander, D. Trussed, and G. C. Polyzoa, “Developing information networking further: From PSIRP to pursuit,” in Proc. Int. Conf. Broadband Commun., Newt. Syst., Springer, Oct. 2010, pp. 1–13.

[10] C. Dinowitz, J. Golic, B. Ohlman, and B. Algren, “Secure naming for a network of information,” in Proc. INFOCOM IEEE Conf. Comput. 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 Netw., Aug. 2012, pp. 55–60.

[13] Y. Sun et al., "Trace-driven analysis of ICN caching algorithms on videoon-demandworkloads," in Proc. 10th ACMInt. 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. 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," 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.

[21] J. Han, W. Susilo, and Y. Mu, "Identity-based data storage in cloud computing," Future Gener. Comput. Syst., vol. 29, no. 3, pp. 673–681, Mar. 2013.

[22] H.-Y. Lin, J.Kubiatowicz, andW.-G. Tzeng, "A secure fine-grained access control mechanism for networked storage systems," in Proc. IEEE 6th Int. Conf. Softw. Secur. Rel., Jun. 2012, pp. 225–234.

[23] Y. Zhou et al., "Identity-based proxy re-encryption version 2: Making mobile access easy in cloud," Future Gener. Comput. Syst., vol. 62, pp. 128–139, Sep. 2016.

[24] X. A.Wang, J. Ma, F. Xhafa, M. Zhang, and X. Luo, "Cost-effective secure e-health cloud system using identity based cryptographic techniques," Future Gener. Comput. Syst., vol. 67, pp. 242–254, Feb. 2017.

[25] J. Shao, G. Wei, Y. Ling, and M. Xie, "Identity-based conditional proxy re-encryption," in Proc. IEEE Int. Conf. Commun., Jun. 2011, pp. 1–5.

[26] K. O. B. Obour Agyekum et al., "A secured proxy-based data sharing module in IoT environments using blockchain," Sensors, vol. 19, no. 5, Jan. 2019, Art. no. 1235.