Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 9, September : 2023

SECURE DATA SHARING IN THE CLOUD USING BLOCK CHAIN DATA STORAGE METHODS

Dr. Prasuna Grandhi
Associate Professor
Department of CSE
St. Ann's College of Engineering & Technology, Chirala

Dr. Hari Kishan Chapala
Professor & HOD
Department of CSE – AIML
St. Ann's College of Engineering & Technology, Chirala

Dr. Ratna Raju Mukiri
Associate Professor
Department of CSE
St. Ann's College of Engineering & Technology, Chirala
mukiriratnaraju001@gmail.com

ABSTRACT: Cloud Computing provides large amount of computational resources storage capacity and many kinds of data services. Data sharing in the cloud is the practice of exchanging files between various users via cloud technology.Blockchain data sharing can give businesses a secure way to store and share data. Since this network is decentralized, and data is transmitted across a peer-to-peer network under the protection of an unchangeable cryptographic signatureData should further be shared with users outside trusted domains using encryption. Data owners can outsource their encrypted data to the cloud using identity-based encryption security encryption keys will grant legitimate users access to the data. With the Internet of Things devices stating resource-constrained an edge device to server handle intensive computations. The performance and security evaluation demonstrate that this scheme can realize the dynamic sharing of blockchain data while protecting transaction privacy and has advantages in computing overhead, which is better applicable to the Controlled sharing of blockchain data..We present secured and efficient scheme that incorporates an Inner-Product Encryption (IPE) scheme decryption of data is possible to use product of the private key associated with a set of attributes specified by the data owner and the associated cipher text is equal to zero. It moderates the bottlenecks in centralized systems and fine-grained get into control to data. The data owners store their files in the cloud after encrypting the data using the ERSA which combines the RSA algorithm, XOR operation, and SHA-512.It is suggested to employ a hybrid attribute-based proxy re-encryption method that

enables the proxy server to change attribute-encrypted cypher texts into identity-based encrypted cypher texts so that users with limited resources can access the previously encrypted material..

INDEX TERMS: access control, identity-based encryption, data Security, ; fine-grained access control; Inner-Product Encryption (IPE); Internet of Things (IoT); attribute-based, encryption, Privacy Preserving Algorithms.

1. INTRODUCTION

Realizing data security sharing in a distributed environment has always been a research hotspot. Blockchain technology, which forms the backbone of Bitcoin, has seen widespread use. Blockchain is a distributed ledger technology maintained collaboratively by numerous parties. [1]. A capacity asset is requested on-demand adaptable, and QoS-assured is take in the cloud allowing users to access their data from any device with Internet connectivity whenever they need it [2]. The data should be publicly accessible and other data that are imperative to keep private to protect business-critical data that must be security according to the EU's General Data Protection Regulation (GDPR) [3]. The trusted third party generates the re-encryption key and proxy runs the re-encryption algorithm with the key and revamps the cipher text before sending the new cipher text to the user. An intrinsic trait of a PRE scheme is that the proxy is trusted [4]. This is seen as a prime candidate for delegating access to encrypted data in a secured manner in crucial component in any data-sharing aspects [5]. In the task of the data owners can be changed from the encryption and decryption process of cipher text to the generation process of a re-encryption key which distributes the overload on the data owners [6]. Attribute-based encryption (ABE), an encryption scheme first proposed achieves many access control and data security by granting different access rights to users based on their attributes [7]. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism security password is a secret word or phrase that gives a user access to a particular program or system [8].

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 9, September : 2023

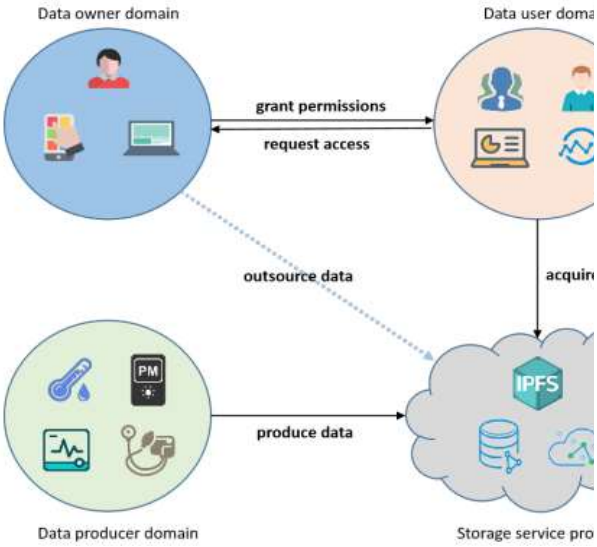


Figure1: Traditional data-sharing architecture

2. RELATED WORK

Most of the past work partly addresses the problem of securely sharing IoT data. It is nearly impossible to device-embedded security and solves the security problems to IoT devices in computing and power resources of the Internet of things make the execution of different security algorithms tougher on the device [9]. Attribute-based proxy encryption techniques are adopted to enforce the cipher text and the private key of the user with in an attribute set in the ABE scheme and decryption is possible to match between the set of attributes and private key and the cipher text [10]. The traditional proxy re-encryption mechanism relies on semi-trusted third-party service providers to complete data sharing [11]. The latest revolution in Internet mobile and machineto-machine (M2M) technologies is first phase of the IoT expected to bridge diverse technologies to enable new applications and connecting physical objects together in support of intelligent decision making [12]. Attribute-based access control (ABAC) is an access control model the policies over subjects performing operations on objects are defined based on assigned attributes [13]. The fact is cloud administration providers are continually acquiring a large volume of client data to similar server because of their reduced operating costs and attention to efficiency [14]. Multiple customers are able to examine the personal information of a single individual consumer to perhaps considerably contenders [15].

3. SYSTEM DESIGN

Blockchain is a special data format generated by merging data blocks in chains in sequential sequence based on a verifiable and trustworthy consensus method in a peer-to-peer network setting [16].The physician might share the patient's data depending on the kind of ailment is treating with other healthcare professionals in the same hospital and therefore have a different access policy on the data [17]. In medium access control (MAC), in the system administrator labels data with confidentiality levels and labels

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 9, September : 2023

users with clearance levels. The model of the system is depicted including the entities and their functions described below. Distribution and control of data access rights using the blockchain consensus process, finish the node's registration, and safeguard the key. Check the user's access[18].

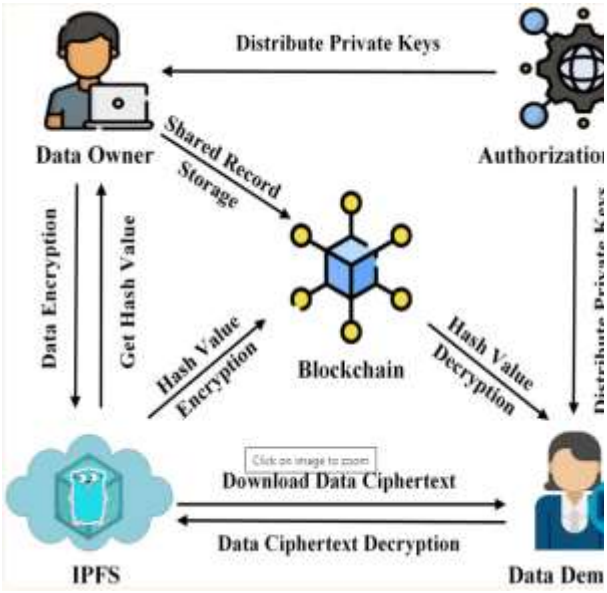


Figure 2: System model

4. PROPOSED SYSTEM

Propose a dynamic adjustment mechanism for user permissions for transaction data sharing. Blockchain miner nodes divide the work into agents and manage the proxy re-encryption key parameters separatelyA pre-verification system is proposed in which only customers with particular attributes is verification process and many advantages to a reconfirmation system to intermediate contingent multi-imparting component such as verifying characteristics and information before re-encryption [19]. In a blockchain network, events are usually recorded in logs. As operational logs of the blockchain network are continually generated, displaying the logs visually can provide a more intuitive understanding of the entire process of events and enable identity tracking of both sides of data-sharing[20].While protecting transaction privacy but also better adapt to the data access in the open environment of the blockchain network in terms of functionality and computational overhead control sharing.

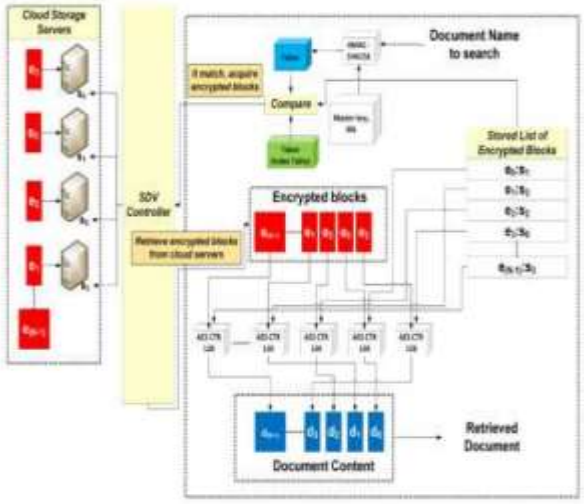


Figure3: Proposed system

A. Data security storage method

Close-to-home data is leaked if this PKE device is unable to secure a client's disc and get the content [21]. The possibility is gadget will only share information in the interested in specific qualities to order to

guarantee the confidential data and the identity of the receiver is not leaked data is providers and recipients must verify the authenticity of each other [22].

Algorithm: Data security storage method for on-chain and off-chain collaboration.

1: Obtain the ciphertext hash value HCH of the data returned by IPFS;

2: Generating elliptic curves Ep(a,b);

3: Obtain the elliptic curve group *(x,y)*;

4: **if** data owner encrypts ciphertext hash value HCH **then**

5: The elliptic curve is obtained by Eq. (3), and *y* is obtained;

6: Get all the points that satisfy Ep(a,b), and get the base point G(x0,y0);

7: Generate the private key r for the data demander and compute the public key R=rG using the base point G(x0,y0);

8: The data demander transmits its own public key R to the data owner;

9: The data owner encrypts the data hash HCH using the public key R of the data demander;

10: Outputting the encrypted hash value ciphertext *C* and uploading it to the blockchain for storage;

11: The data demander decrypts the hash ciphertext *C* with his own private key *r* and obtains the decrypted hash value;

12: **end if**

B. ATTRIBUTE-BASED ENCRYPTION ALGORITHM

ABE is a public key encryption mechanism designed with group decryption goals rather than single users [23]. This mechanism evolved from the older identity-based encryption (IBE) method where the public key is usually a string that uniquely identifies one user such as its social security number [24]. The information about the shared secret for attribute-based encryption the access structure contains the set of authorized attributes. One consequence of using monotone access structures is that negative attributes is efficiently used when constructing the access tree in other words monotone access structures is support logical NOT gates [25].

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 9, September : 2023

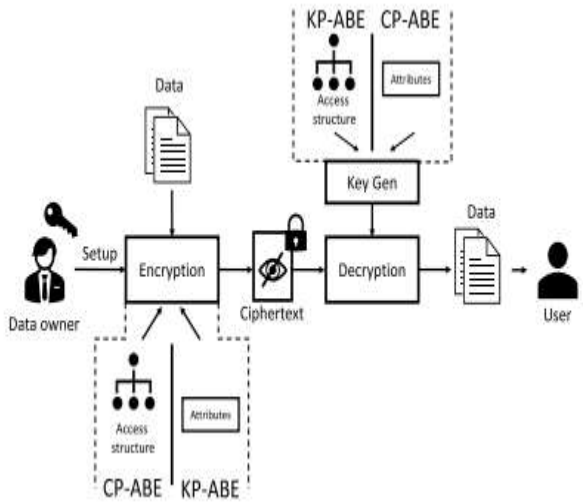


Figure 4: ABE General Model.

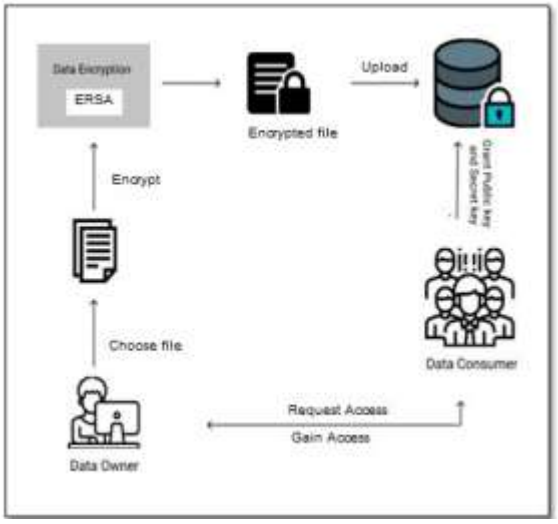


Figure5: A framework of Data Sharing Model on Cloud

5. BASIC CONSTRUCTION ALGORITHM

Attribute-based encryption model is construction structure based on the following 4 primary algorithms: setup, encryption, key generation, and decryption.

• **Setup**: The algorithm that takes any implicit security parameter and creates public parameters and a master key. In this step the universe of attributes is defined.

• **Encryption**: The algorithm that applies encryption to a message.

• **Key Generation**: The algorithm that generates decryption keys based on a set of attributes.

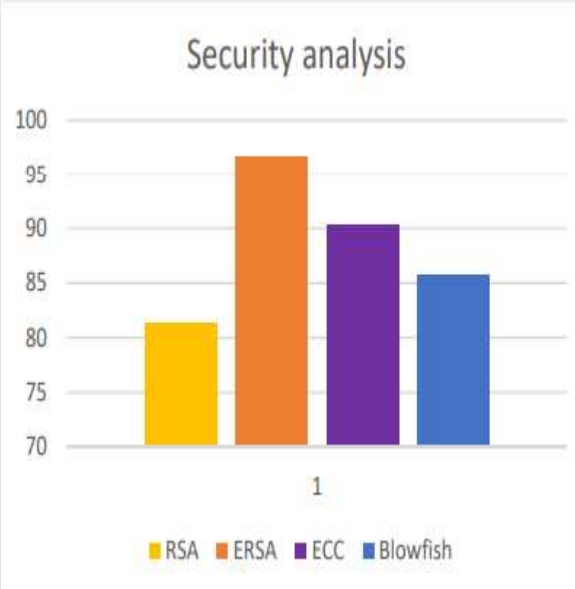
• **Decryption:** The algorithm that decrypts a cipher text to obtain the underlying message.

The ABE scheme use determines the user attributes and the access structure are associated and main difference between the following two main ABE schemes: key-policy ABE (KP-ABE) and cipher text-policy ABE (CP-ABE). In KP-ABE, the cipher texts are labelled with a set of attributes while the user's private key is the one associated with the access policy. The RSA algorithm is an asymmetric cryptography algorithm to uses a public key and a private key. The public key is shared openly while the private key is secret and cannot be shared with others [26].

6. RESULT AND DISCUSSION

The proposed technique's outcome is discussed with an experimental evaluation which includes performance metrics is

comparative analysis with graphical plots. The performance of the ERSA algorithm is compared to the existing encryption algorithms. The RSA, and Elliptic Curve Cryptography (ECC) based on encryption time, decryption time, and security analysis. Recently industry has been adopting ABAC as their standard for access control, is very least it is expected for them to have an organizational role hierarchy into which access control is modelled. This comparison is proved the proposed algorithm works in cryptography algorithms (RAS and ECC). The Blowfish algorithm scores less time in encryption and decryption than ERAS, but it's a symmetric key block cipher while ERSA is an asymmetric cipher. The performances of ERSA, and RSA in terms of security level



7. CONCLUSION AND FUTURE WORK

We propose a traceable and secure data-sharing scheme based on blockchain technology. Our solution features a data protection method based on attribute encryption to enable fine-grained access control for shared data. To enhance data security, we employ a collaborative on-chain and off-chain data storage scheme, which also alleviates storage pressure on the chain. To strengthen data confidentiality the owner encrypts his data using the ERSA method and then uploads it to the cloud and only based on the secret key file SHA-512 and the private key data consumer authorized to access the data. Furthermore we designed a conceptual architecture that proposes to relevant mechanisms should work together to address the identified research gaps. The ERSA is great defence against attacks is small primary key and by using the NF algorithmFurthermore it enables real-time identity tracking for both parties involved in data sharing, while ensuring data encryption protection both on and off the chain.To enhance data security we employ a collaborative on-chain and off-chain data storage scheme, which also alleviates storage pressure on the chain

8. 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] B. Li, D. Huang, Z. Wang, and Y. Zhu, "Attribute-based access control for ICN naming scheme," IEEE Trans. Dependable Secure Comput., vol. 15, no. 2, pp. 194–206, Apr. 2016.

[3] S. Misra et al., "Accconf: An access control framework for leveraging in-network cached data in the ICN-enabled wireless edge," IEEE Trans. Dependable Secure Comput., vol. 16, no. 1, pp. 5–17, Feb. 2017.

[4] E. G. AbdAllah, M. Zulkernine, and H. S. Hassanein, "DACPI: A decentralized access control protocol for information centric networking," in Proc. IEEE Int. Conf. Commun., May 2016, pp. 1–6.

[5] Y. Zhang, R. H. Deng, D. Zheng, J. Li, P. Wu, and J. Cao, "Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial IoT," IEEE Trans. Ind. Inform., vol. 15, no. 9, pp. 5099–5108, Jan. 2019.

[6] J.-S. Fu, Y. Liu, H.-C.Chao, B. K. Bhargava, and Z.-J. Zhang, "Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing," IEEE Trans. Ind. Inform., vol. 14, no. 10, pp. 4519–4528, Jan. 2018.

[7 LowleshNandkishorYadav, "Predictive Acknowledgement using TRE System to reduce cost and Bandwidth"IJRECE VOL. 7 ISSUE 1 (JANUARY- MARCH 2019) pg no 275-278

[8] Ashish B. Deharkar and H. R Hajare , "Cloud Computing Based on Predictive Acknowledgement System," International Journal of Advanced Research in Computer and Communication Engineering Vol. 11 Issue 3 March 2022 PP 90-93

[9] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," ACM Trans. Inform. Syst. Secur., vol. 9, no. 1, pp. 1–30, Feb. 2006.

[10] R. Pecori, "S-kademlia: A trust and reputation method to mitigate a sybil attack in Kademlia," Comput. Netw., vol. 94, pp. 205–218, Jan. 2016.

[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] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, and R. Thayer, ''OpenPGP message format,'' Tech. Rep. rfc4880, 2007.

[17] C.-C. Lee, P.-S.Chung, and M.-S. Hwang, ''A survey on attribute-based encryption schemes of access control in cloud environments,'' Int. J. Netw.Secur., vol. 15, no. 4, pp. 231–240, Jul. 2013.

[18] L. Zhou, V. Varadharajan, and M. Hitchens, ''Achieving secure role-based access control on encrypted data in cloud storage,'' IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp

[19] Hongbo Li, Qiong Huang, Sha Ma, JianShen, and Willy Susilo, "Authorized equality test on identity-based ciphertexts for secret data sharing via cloud storage," IEEE Access, vol. 7, pp. 25409–25421, 2019.

[20] Xu An Wang, FatosXhafa, Jianfeng Ma, ZhihengZheng, "Controlled secure social cloud data sharing based on a novel identity based proxy re-encryption plus scheme," Journal of Parallel and Distributed Computing, vol. 130, pp. 153–165, 2019.

[21] M. Kumar and S. Chand, "ESKI-IBE: Efficient and secure key issuing identity-based encryption with cloud privacy centers," Multimedia Tools and Applications, vol. 78, no. 14, pp. 19753–19786, 2019.

[22] Y. Kiran Kumar and R. MahammadShafi, "An efficient and secure data storage in cloud computing using modified RSA public key cryptosystem," International Journal of Electrical and Computer Engineering, 2019.

[23] PriyadharshiniKaliyamoorthy and AroulCanessaneRamalingam, "QMLFD Based RSA Cryptosystem for Enhancing Data Security in Public Cloud Storage

System," Wireless Personal Communications, 2021.

[24] Rohini and ErTejinder Sharma, "Proposed hybrid RSA algorithm for cloud computing," Proceedings of the Second International Conference on Inventive Systems and Control, 2018.

[25] Anuj Kumar, Vinod Jain and AnupamYadav, "A New Approach for Security in Cloud Data Storage for IOT Applications Using Hybrid Cryptography Technique," International Conference on Power Electronics &IoT Applications in Renewable Energy and its Control, 2020.

[26] Khalid El Makkaoui, AbderrahimBeni-Hssane and AbdellahEzzati, " Speedy Cloud-RSA homomorphic scheme for preserving data confidentiality in cloud computing," Journal of Ambient Intelligence and Humanized Computing, 2019