Research Journal of Computer Systems and Engineering

ISSN: 2230-8571, 2230-8563

Volume 01 Issue 02 - 2020 (July to December)

Page 07:12

Cloud Blockchain Based Data Sharing by Secure Key Cryptographic Techniques with Internet of Things

Mr. Yadu Prasad Gyawali
Assistant professor, Mid-West University,
Birendranagar, Surkhet, Nepal
yadu@mwu.edu.np/yadu.gyawali@gmail.com
Orcid ID: https://orcid.org/0000-0001-6320-1916

Dr. Mohit Angurala
Assistant Professor & Head of the department, Department of computer science and Engineering, Khalsa College of Engineering and Technology, Amritsar, Punjab, India
https://orcid.org/0000-0002-9506-5864

Dr. Manju Bala
Director, khalsa college of Engineering and Technology, Amritsar
Email id: drmanju571@gmail.com
Orcid id: 0000-0002-2313-0284

Article History

Received: 15 July 2020
Revised: 20 September 2020
Accepted: 22 November 2020

Abstract

The largest difficulties in cloud computing applications nowadays are related to trust computing, which has become increasingly important in recent years. In cloud computing, the user is given secure and effective storage so they can share some of their data as well as provide others access to it via searches. Therefore, by offering the security approach that has been presented in this study, the secured blockchain is offered.In this research, we addressed an main issue of secure data sharing usingcloud Blockchain Based key cryptographic data sharing (CBKCrypDS) in cloud service for IoT environment. The data sharing, i.e., transaction that can be secured through peer-to-peer blockchain is using cryptographic techniques.The experimental result shows the encryption and decryption time, latency and throughput is compared with other blockchain based techniques.

Keywords: Data Sharing, Blockchain, IoT, Cryptography, Key Aggregate Cryptosystem

1. Introduction

In many IT sectors using cloud computing for their efficiency and reliability of data which are applied to it. The important element of security is discussed in privacy and security of cloud computing has been discussed in the terms of authentication, control of accessibility, confidentiality, integrity and so on[1,2]. It seems a big challenge in cloud environment to provide privacy and security, especially in big data with cross cloud environment. The blockchain technology is the key to solve those issues in information technology of new generation [3,4].The data encryption with 16 rounds occurs in data encryption method.This paper clearly explains security and privacy issue in IoT to resolve by block

chain technology with cloud Blockchain Based key cryptographic data sharing (CBKCrypDS). The proposed work provides more privacy and efficient of data sharing by using CBKCrypDSwith wallet generator. Lastly, security analysis and performance analysis is proposed to share data in cloud environment as suitable of proposed scheme.The rest of the paper presents section 2 discuss literature survey, section 3 presents research methodology, section 4 describes experimental results and section 5 is conclusion.

2. Literature Survey

In this section, the previous works are discussed is listed. Work in [5] discussed blockchain technologies to improve privacy situation. A paradigm of blockchain is distributed computing of decentralized system. Nitesh Singh et al., 2018 [6] proposes a structure that envelops various environments as for information imparting to blockchain innovation as the foundation of this framework. Works[7,8] Propose a privacy-based blockchain to maintain exchange of Electronic Medical Record (EMR) information, called BPDS. Works [9,10] Examine the potential of blockchain to have assured cloud provenance of knowledge and existing vulnerabilities in the cloud of blockchain.

3. RESEARCH METHODOLOGY

The proposed framework addresses the secure exchange of data with the aid of blockchain as seen in Figure 1. cloud Blockchain Based key cryptographic data sharing (CBKCrypDS)in the cloud for data storage sharing powerful encryption method that supports scalable delegation in sense that a constant-size decryption key may decrypt any subset of cypher texts. A constant size aggregate key may be issued by the hidden key holder for customizable cypher text option in cloud storage. A cryptographic approach is more suitable, with validated encryption based on number-theoretical assumptions.

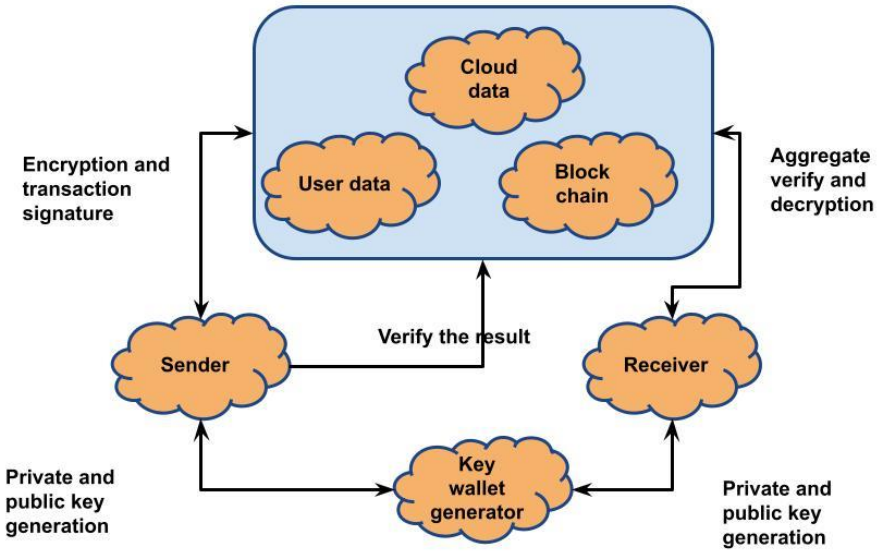

Figure 1: Proposed methodology

In the proposed system, we'll concentrate on how to make private key cryptography secure for users to share encrypted data. It is crucial to avoid disclosing a user's private key to other users.

3.1 Data Sharing

The key aggregation is mainly useful for efficiency and flexible of delegation which we expected property. The sharing of data from content provider as confidential manner in selective scheme with expansion of ciphertext by authorized user of distributing single aggregate key.

3.2 Cloud Architecture:

It is made up of a few building pieces, namely cloud servers (C1, C2) and (many) Customers. Cloud servers that store encrypted data do content-based image retrieval using a sizable cloud database with minimal processing resources. Following acceptance of Ia, C1 uses Improved Image Encryption System (IIES) protocols with C2 to transform Ib into principal image using key sk.

3.3 Transaction of blockchain

Blockchain are used to transact with the main components of procedure which are based on the address. Each and every blocks are carried data in blockchain and next block is addressed in output. The series of signature is used to protect the carried transaction out is known as e-stamps. This signature is useful to verify the recipient of the data which are sent by the owner and it will identify the verified signature and previous node of public key. The transaction blocks are linked only after confirmation from the genius block with previous block address to the most current block using the hash function of cryptographic of the previous block.

3. EXPERIMENTAL RESULTS

The experimental result is carried out by using parameters are:
1. Latency:A packet's latency is amount of time it takes to travel from source to destination. Round-trip time is occasionally referred to as the network's latency.
2. Throughput: It refers to a network's ability to quickly encrypt and decrypt data from one location to another through an Internet connection.
3**. Encryption time:T**otal amount of time needed to convert plain text into cypher text is known as the encryption time. Throughput of encrypted method is then determined utilizing calculated encryption time. It provides encryption rate.
4. **Decryption time:**Total amount of time required to transform encrypted text into plain text is known as decryption time. Calculated decryption time is then utilized to calculate throughput of decrypted algorithm. It offers rate of decryption.

Table 1 Comparison of Performance in memory size of proposed system and Existing Algorithm

S.No	Data size(KB)	Memory size(KB)			
		ELIB	RPCA	BWH	CBKCrypDS
1	100	48	58	66	32
2	200	50	52	54	36
3	400	52	56	58	38
4	600	64	60	66	54
5	800	70	68	70	66
6	1000	74	69	76	67

Table 1 compares the performance of the proposed architecture and the present algorithm in terms of memory size. It provides the image size in KB and compares it to the memory size in KB.

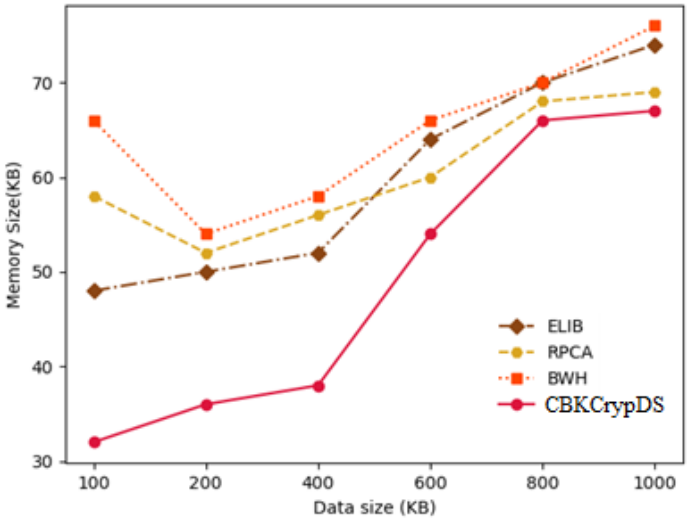

Figure 2- Comparison of Performance in memory size of proposed system and Existing Algorithm

The above figure 2 shows Comparison of Performance in memory size of proposed system and Existing Algorithm.

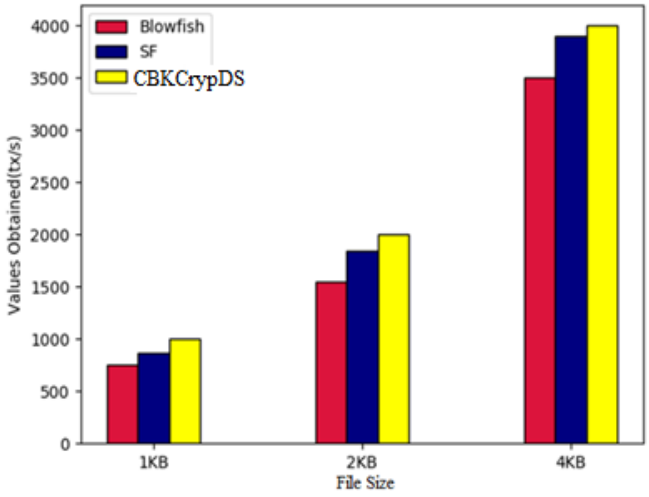

Figure 4: Comparison of Throughput with Existing techniques

The above figure 4 shows the comparison of throughput performance with existing techniques. X axis shows the file size in KB, and the Y axis shows the values obtained in milliseconds. The red, blue, yellow color indicates blowfish, SF, CBK Cryp DS respectively. The below figure 5 shows the comparison of Latency performance with existing techniques. X axis shows the file size in KB, and the Y axis shows the values obtained in milliseconds.

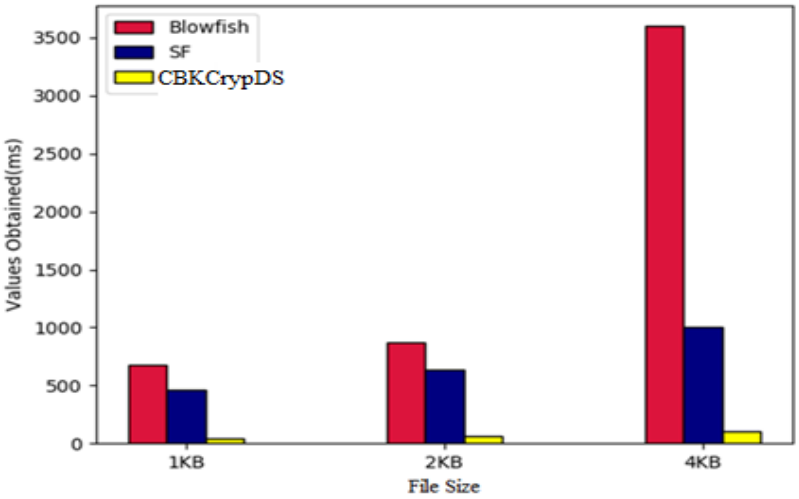

Figure 5: Comparison of Latency with Existing techniques

5. CONCLUSION

In cloud computing, the user is given secure and effective storage so they can share some of their data and provide others access to it via searches. Numerous research have been done to address the problems with transactions, software upkeep, and wallet security on the blockchain.This study introduces a security solution for cloud environments that allows users to share encrypted data called the blockchain-based key aggregation cryptosystem (BKAC).Except for these shared data, which users won't be able to decrypt, the aggregate key will only be generated for the shared data. It is more secure to share data using the cloud Blockchain Based Key Cryptographic Data Sharing (CBKCrypDS) technology.The experimental result shows the throughput is high and latency is low, the encryption and decryption time is low.

REFERENCES

[1] Singh S, Jeong Y.-S, Park J.H, "A survey on cloud computing security: Issues, threats, and solutions", *Journal of Networks and Computer Applications*, vol.75, pp.200-222, 2016.

[2] Y. Yuan, F.Y. Wang, "Blockchain: The state of the art and future trends", *Acta Automat. Sinica*, vol. 22, no. 3, pp. 1882-1894, 2016.

[3] M. Pilkington, "Blockchain technology: Principles and applications", *Soc. Sci. Electron. Publ*. vol.51, no.7, pp.121-122, 2015.

[4] R. Pass, L. Seeman A. Shelat, "Analysis of the blockchain protocol in asynchronous networks", *International Conference on the Theory & Applications of Cryptographic Techniques*, 2017.

[5] Kumarin A, S. Tanwar, S. Tyagi and N. Kumar, "Fog computing for healthcare 4.0 environment: Opportunities and challenges",*Computers and Electrical Engineering*, vol.72, pp. 1-13, 2018

[6] Wang, S., Zhang, Y., & Zhang, Y. (2018). A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. *Ieee Access*, *6*, 38437-38450.

[7] Manzoor, A., Liyanage, M., Braeke, A., Kanhere, S. S., &Ylianttila, M. (2019, May). Blockchain based proxy re-encryption scheme for secure IoT data sharing. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 99-103). IEEE.

[8] Luo, Y., Jin, H., & Li, P. (2019, March). A blockchain future for secure clinical data sharing: A position paper. In *Proceedings of the ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization* (pp. 23-27).

[9] Zhang, G., Li, T., Li, Y., Hui, P., & Jin, D. (2018). Blockchain-based data sharing system for ai-powered network operations. *Journal of Communications and Information Networks*, *3*(3), 1-8.

[10] ObourAgyekum, K. O. B., Xia, Q., Sifah, E. B., Gao, J., Xia, H., Du, X., &Guizani, M. (2019). A secured proxy-based data sharing module in IoT environments using blockchain. *Sensors*, *19*(5), 1235.