ENGINEERING IN ADVANCED RESEARCH SCIENCE AND TECHNOLOGY

ISSN 2350-0174
Vol.03, Issue.03
October-2023
Pages: 959-967

A NOVEL BSSPD: A BLOCK-CHAIN-BASED SECURITY SHARING SCHEME FOR PERSONAL DATA WITH FINE-GRAINED ACCESS CONTROL

***Ms. SRI ARUNA BETHAPUDI**
*Asst. Professor, Department of CSE, **MALLA REDDY ENGINEERING COLLEGE FOR WOMEN,** TELANGANA, India.
KRITIKA.B[1], M. HARINI[2], N. SREE SAI HARSHITHA[3], NUSRAT BEGUM[4]
B. Tech Pursuing, Dept.of CSE, **MALLA REDDY ENGINEERING COLLEGE FOR WOMEN,** TELANGANA, India.

ABSTRACT

Privacy protection and open sharing are the core of data governance in the AI-driven era. A common data-sharing management platform is indispensable in the existing data-sharing solutions, and users upload their data to the cloud server for storage and dissemination. However, from the moment users upload the data to the server, they will lose absolute ownership of their data, and security and privacy will become a critical issue. Although data encryption and access control are considered up-and coming technologies in protecting personal data security on the cloud server, they alleviate this problem to a certain extent. However, it still depends too much on a third-party organization's credibility, the Cloud Service Provider (CSP). In this paper,

1.INTRODUCTION

The development of 5G and Internet of Things technology provides a large amount of training data for the rapid implementation of artificial intelligence (AI). At the same time, data security and privacy protection have become the most interesting topics in data governance and sharing. Powerful data mining and analysis have brought potential threats to personal privacy protection. Traditionally, most people choose to outsource their data to cloud servers for sharing and dissemination. However, most of the data stored in the cloud is very sensitive, especially those data generated by IoT devices that are closely related to human life. These data have their particularities and may contain personal-related information such as life, work, and healthcare; once personal data is stolen or leaked illegally and linked to the data owner's real identity, it may bring great trouble to an individual. Therefore, integrating data and generating value while ensuring data security and privacy have become a significant challenge for all contemporary companies that use big data and AI. At present, researchers have proposed many secure sharing schemes in the cloud environment [1–9]. These schemes seem to solve the security and privacy issues during data sharing. Nevertheless, these schemes all have a standard feature: they are overly dependent on the Cloud Service Provider (CSP). They believe that the CSP is a trusted third-party organization, and the CSP is semi trustable, which means that the CSP will be curious about the data but will not destroy it. It means that the following situations are always inevitable:

1. The CSP itself may make profits from the user's private data, or its insiders may do evil and cause the user's privacy disclosure. Although some methods, such as attribute-based encryption algorithms, can achieve user-defined access policies that seem user centric, these methods still require a trusted third party to generate and manage user keys. It is impossible to exclude the possibility of collusion between these trusted centers. All these will lead to the fact that once the data owners upload their data to the cloud server, they will no longer have their data's absolute possession.
2. The data is centrally stored on cloud servers and managed by the CSP. An inevitable single point of failure may lead that users cannot obtain their data generally by using the cloud service. The CSP can improve data security and service stability by utilizing disaster recovery backup. However, some irresistible factors will prevent users from using cloud services to obtain their data, such as political factors
3. To provide better service, the CSP needs to spend more money to buy servers, hire better employees, rent the data center venues, and so on. These costs are increasing gradually, and the CSP cost is also increasing and the construction of the management platform. Users ultimately pay the operating costs of the CSP.

2.LITERATURE REVIEW

Swan et al. [15] studied on the concept of blockchains, a new form of information technology that could have several important future applications. One is blockchain thinking, formulating thinking as a blockchain process. This could have benefits for both artificial intelligence and human enhancement, and their potential integration.

Blockchain thinking is outlined here as an input-processing-output computational system.

Zyskind et al. [16] described a decentralized personal data management system that ensures users own and control their data. This paper implemented 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 this system are not strictly financial they are used to carry instructions, such as storing, querying, and sharing data. Finally, this paper discussed possible future extensions to block chains that could harness them into a well-rounded solution for trusted computing problems in society.

Azaria et al. [17] proposed a novel, decentralized record management system to handle EMRs, using blockchain technology. This system gives patients a comprehensive, immutable log and easy access to their medical information across providers and treatment sites. Leveraging unique blockchain properties, MedRec manages authentication, confidentiality, accountability, and data sharing crucial considerations when handling sensitive information. A modular design integrates with providers' existing, local data storage solutions, facilitating interoperability and making our system convenient and adaptable. This paper incentivized medical stakeholders (researchers, public health authorities, etc.) to participate in the network as blockchain "miners". This provided them with access to aggregate, anonymized data as mining rewards, in return for sustaining and securing the network via Proof of Work. The purpose of this short paper is to expose, prior to field tests, a working prototype through which we analyze and discuss our approach.

Xia et al. [18] proposed MeDShare, a system that addresses the issue of medical data sharing among medical big data custodians in a trust-less environment. The system is blockchain-based and provided data provenance, auditing, and controlled the shared medical data in cloud repositories among big data entities. MeDShare monitored entities that access data for malicious use from a data custodian system. In MeDShare, data transitions and sharing from one entity to the other, along with all actions performed on the MeDShare system, are recorded in a tamper-proof manner. The design employed smart contracts and an access control mechanism to effectively track the behavior of the data and revoke access to offending entities on detection of violation of permissions on data. The performance of MeDShare is comparable to current cutting-edge solutions to data sharing among cloud service providers. By implementing MeDShare, cloud service providers and other data guardians will be able to achieve data provenance and auditing while sharing medical data with entities such as research and medical institutions with minimal risk to data privacy.

Dubovitskaya et al. [19] proposed a framework on managing and sharing EMR data for cancer patient care. In collaboration with Stony Brook University Hospital, this work implemented framework in a prototype that ensures privacy, security, availability, and fine-grained access control over EMR data. The proposed work can significantly reduce the turnaround time for EMR sharing, improved the decision making for medical care, and reduced the overall cost.

3.EXISTING SYSTEM

3.1 Hyperledger Fabric

Hyperledger Fabric is designed for use in enterprise-level applications, and it is characterized by its modular architecture, permissioned network, and smart contract functionality, known as “chaincode”.

- The platform provides a high degree of security, privacy, and scalability, and it supports the development of custom blockchain solutions for various use cases across industries such as finance, supply chain, and healthcare.

4.PROPOSED SYSTEM

we combined blockchain, ciphertext-policy attribute-based encryption (CP-ABE) and Inter Planetary File System (IPFS) to address this problem to propose a blockchain-based security sharing scheme for personal data named BSSPD. In this user centric scheme, the data owner encrypts the sharing data and stores it on IPFS, which maximizes the scheme’s decentralization. The address and the decryption key of the shared data will be encrypted with CP-ABE according to the specific access policy, and the data owner uses blockchain to publish his data-related information and distribute keys for data users. Only the data user whose attributes meet the access policy can download and decrypt the data. The data owner has fine-grained access control over his data, and BSSPD supports an attribute-level revocation of a specific data user without affecting others. To further protect the data user’s privacy, the ciphertext keyword search is used when retrieving data. We analyzed the security of the BBSPD and simulated our scheme on the EOS blockchain, which proved that our scheme is feasible. Meanwhile, we provided a thorough analysis of the storage and computing overhead, which proved that BSSPD has a good performance.

5.SYSTEM ARCHITECTURE

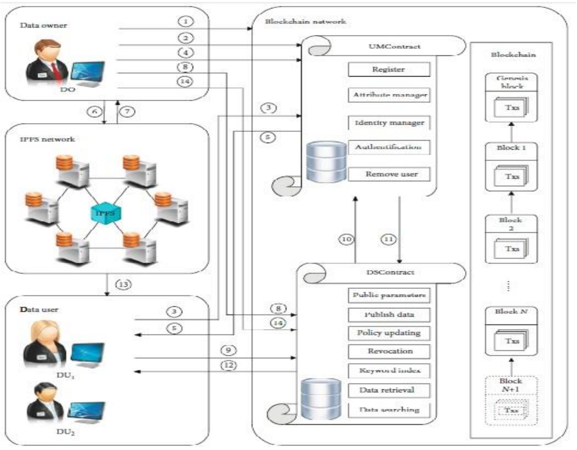
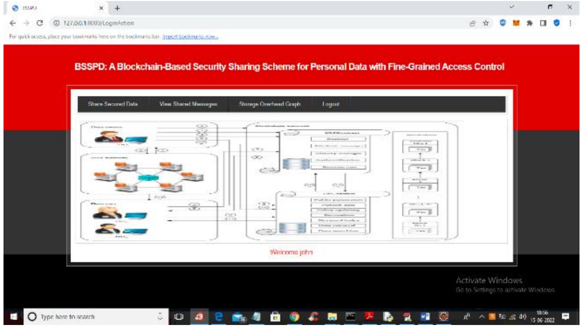


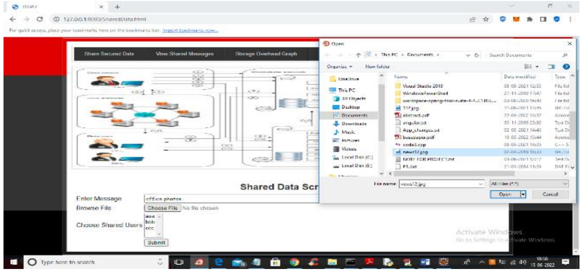
Fig.1 System Architecture



BSSPD: A Blockchain-Based Security Sharing Scheme for Personal Data with Fine-Grained Access Control

Welcome john

In above screen user logged in successfully and now click on 'Share Secured Data' link to share data with other users



Shared Data Scr

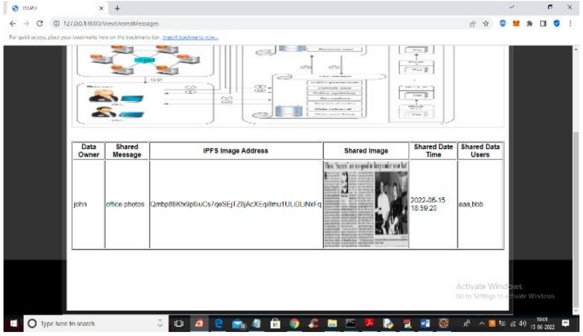
Enter Message: office photes

Browse File: Choose File No file chosen

Choose Shared Users: aaa bbb ccc

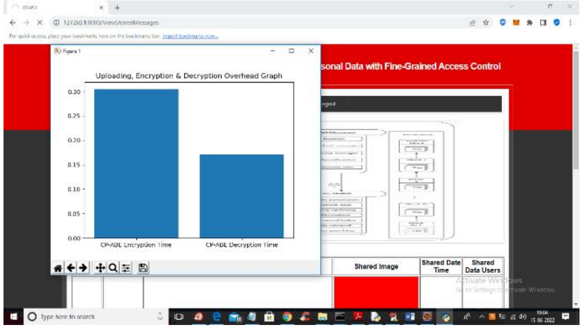
Submit

In above screen user can enter some message and then upload image and by holding CTRL KEY you can select names of users with whom you want to share this data and press button to get below output In above screen 'John' is sharing data with user 'aaa' and 'bbb' and both users can decrypt and view data but user 'ccc' cannot view it.

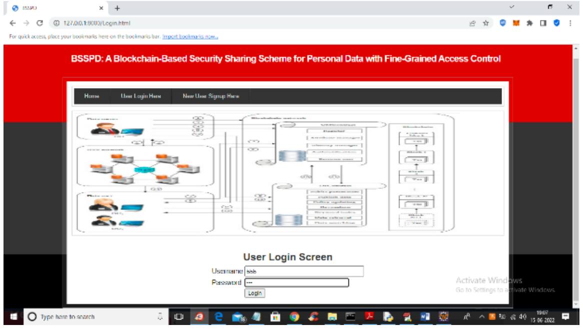

127.0.0.1:8000/ViewSharedMessages
Activate Windows
Go to Settings to activate Windows.
Type here to search

Data Owner	Shared Message	IPFS Image Address	Shared Image	Shared Date Time	Shared Data Users
john	office photos	Qmbp88Kfx9p6uCs7qeSEjTZ8jAcXEqi8mu1ULiDLiNxFq		2022-06-15 18:59:20	aaa,bbb

In above screen we can see data owner name, shared messages with IPFS address and we can see names of shared users list and now we can check weather aaa or bbb can view this data or not and now click on 'Storage Overhead Graph' link to view encryption and decryption time overhead


127.0.0.1:8000/ViewSharedMessages
Figure 1
sonal Data with Fine-Grained Access Control
Uploading, Encryption & Decryption Overhead Graph
0.30
0.25
0.20
0.15
0.10
0.05
0.00
CP-ABE Encryption Time
CP-ABE Decryption Time
Shared Image
Shared Date Time
Shared Data Users
Activate Windows
Go to Settings to activate Windows.
Type here to search

In above screen x-axis represents encryption and decryption and y-axis represents time overhead and now logout and login as 'bbb' user to view shared data.



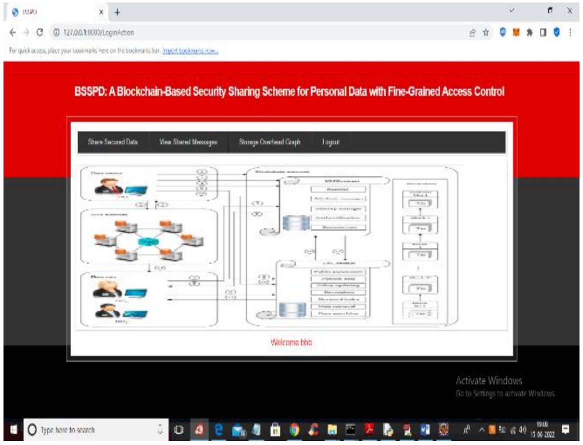
BSSPD: A Blockchain-Based Security Sharing Scheme for Personal Data with Fine-Grained Access Control

User Login Screen

Username: bbb

Password: ***

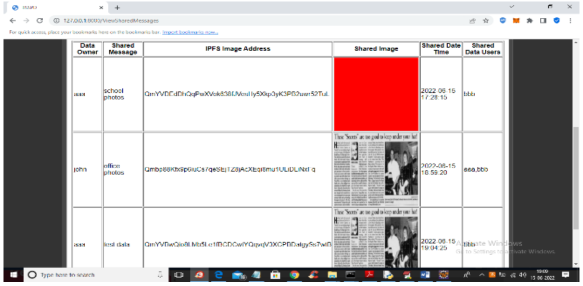
In above screen shared user ‘bbb’ is login and after login will get below output



BSSPD: A Blockchain-Based Security Sharing Scheme for Personal Data with Fine-Grained Access Control

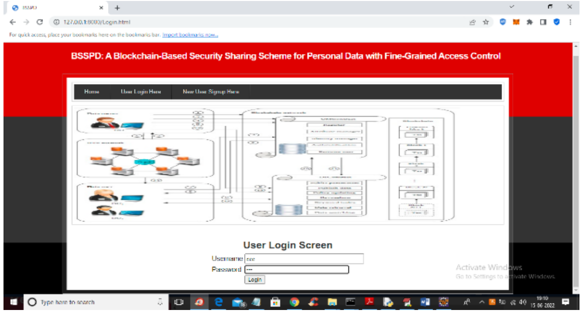
Welcome bbb

Now in above screen ‘bbb’ can click on ‘View Shared Messages’ link to view all users shared data



Data Owner	Shared Message	IPFS Image Address	Shared Image	Shared Date Time	Shared Data Users
aaa	school photos	QmYVDEdDhQqPwXVok838UvesIly5Xkp3yK3PB2uwr52TuL		2022-06-15 17:28:15	bbb
john	office photos	Qmbp88Ktx8p6uCs7qeSEjTZ8jAcXEqi8mu1ULDLiNxFq		2022-06-15 18:59:20	aaa,bbb
aaa	test data	QmYVDwQip8LMb5Lc1fBCDCwfYQqvqV3XCPBDaIgySs7wiB		2022-06-15 19:04:25	bbb

In above screen ‘bbb’ can view shared data from aaa and john and now logout and login as ‘ccc’ and nobody shared data with ‘ccc’ so he cannot access any data



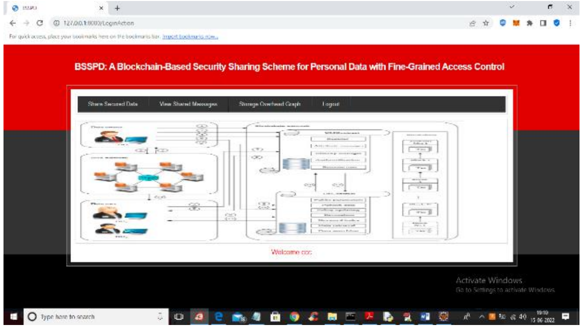
BSSPD: A Blockchain-Based Security Sharing Scheme for Personal Data with Fine-Grained Access Control

User Login Screen

Username: ccc

Password: ***

In above screen user ‘ccc’ is login and after login will get below screen



BSSPD: A Blockchain-Based Security Sharing Scheme for Personal Data with Fine-Grained Access Control

Welcome ccc

Now in above screen ‘ccc’ can click on ‘View Shared Messages’ link to get below output

7.CONCLUSION

In the AI-driven era, a user-centered sharing model is proposed to open data while ensuring data privacy. We combined blockchain, CP-ABE, and IPFS to propose a blockchain-based security data-sharing scheme with fine grained access control and permission revocation. In our proposed scheme, the DO encrypts his data and uploads it to IPFS, then encrypts the returned address and decryption key by CP-ABE. Only DUs whose attributes satisfy the access policy can decrypt and obtain the data. There is no centralized node in the scheme, and the

DO has completed control over his shared data, which promises privacy and security. To achieve the goal, we have implemented our scheme on the EOS blockchain. The security and performance analysis proves that our scheme is feasible and practical and has a good performance. We can also add a cryptocurrency to introduce an economic system for data sharing and further enrich our scheme's functions. At the same time, there are many shortcomings in our scheme. For example, the CPABE we designed with permission revocable does not have the best performance. There are also many types of research on CP-ABE. We can use a CP-ABE with better performance to improve our scheme. Besides, for the searchable encryption algorithm used in our scheme, the DO needs to distribute a secret key for each DU and store it on-chain. It also needs to maintain large amounts of indices for each shared data, which can be further optimized. At present, some researchers have proposed using blockchain to solve the fairness problem in searchable encryption algorithm.

In the future, we will study and discuss the endowment of a better ciphertext searchable algorithm to further optimize our scheme. Simultaneously, to make our scheme more practical, we can combine some studies with ours and put forward a data governance scheme that is more in line with the practical application.

8. REFERENCES

[1] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," Computers & Security, vol. 72, pp. 1–12, 2018.

[2] S. Sundareswaran, A. Squicciarini, and D. Lin, "Ensuring distributed accountability for data sharing in the cloud," IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 4, pp. 556–568, 2012.

[3] Cheng-Kang Chu, S. S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and R. H. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp. 468–477, 2014.

[4] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in 2010 Proceedings IEEE INFOCOM, pp. 1–9, San Diego, CA, 2010.

[5] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE

Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 131–143, 2013.

[6] Z. Cai, Z. He, X. Guan, and Y. Li, “Collective data-sanitization for preventing sensitive information inference attacks in social networks,” IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 4, pp. 1–590, 2018.

[7] Z. Cai and X. Zheng, “A private and efficient mechanism for data uploading in smart cyber-physical systems,” IEEE Transactions on Network Science and Engineering, vol. 7, no. 2, pp. 766–775, 2020.

[8] X. Zhou, W. Liang, K. Wang, R. Huang, and Q. Jin, “Academic influence aware and multidimensional network analysis for research collaboration navigation based on scholarly big data,” IEEE Transactions on Emerging Topics in Computing, no. 1, 2018.

[9] Z. Cai, X. Zheng, and J. Yu, “A differential-private framework for urban traffic flows estimation via taxi companies,” IEEE Transactions on Industrial Informatics, vol. 15, no. 12, pp. 6492–6499, 2019.

[10] S. Nakamoto, “Bitcoin: a peer-to-peer electronic cash system,” 2008, https://bitcoin.org/bitcoin.pdf.

[11] Y. Xu, C. Zhang, G. Wang, Z. Qin, and Q. Zeng, “A blockchain-enabled duplicatable data auditing mechanism for network storage services,” IEEE Transactions on Emerging Topics in Computing, 2020.

[12] Y. Xu, J. Ren, Y. Zhang, C. Zhang, B. Shen, and Y. Zhang, “Blockchain empowered arbitrable data auditing scheme for network storage as a service,” IEEE Transactions on Services Computing, vol. 13, no. 2, pp. 289–300, 2020.

[13] Y. Xu, C. Zhang, Q. Zeng, G. Wang, J. Ren, and Y. Zhang, “Blockchain-enabled accountability mechanism against information leakage in vertical industry.

AUTHOR

Ms.Sri Aruna Bethapudi Assistant ProfessorDepartment of CSE MallaReddy Engineering College for Women, Hyderabad, srikiron@gmail.com