Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, No.4, May : 2024

A BLOCKCHAIN-BASED SECURITY SHARING SCHEME FOR PERSONAL DATA WITH FINE-GRAINED ACCESS CONTROL

Karuna Manjusha Yarraguntla1, Sowmya Irlapati2, Prathyusha Gayam3, Shanthi Vemulapalli4 Department of Computer Science and Engineering, Andhra Loyola Institute of Engineering and Technology, Vijayawada, India
1karunamanjusha1221@gmail.com, 2smya3787@gmail.com, 3gayamprathyusha2002@gmail.com, 4shanthichowdhary70@gmail.com

Abstract—
In the era of AI-driven advancements, safeguarding privacy and facilitating open data sharing are pivotal aspects of data governance. Existing solutions rely on a general data- sharing organization platform where users upload their data to cloud servers for storage and distribution. Although technologies like data encryption and access control address these issues to some extent, they heavily depend on the credibility of 3rd party entities, specifically Cloud Service Providers (CSPs). This paper introduces a solution named Blockchain-Based Security Sharing Scheme for Personal Data (BSSPD), combining blockchain, ciphertext-policy attribute-based encryption (CP-ABE), and the Inter Planetary File System (IPFS) to tackle these challenges. In this user approach, data owner encrypt their communal data, maximizing decentralization by storing it on IPFS. To enhance data user privacy, ciphertext keyword search is employed during data retrieval. The security of BSSPD is thoroughly analyzed, and the scheme is simulated on the EOS blockchain, demon- strating its feasibility. The paper also provides a comprehensive examination of storage and computing overhead, affirming the good performance of BSSPD.
Index Terms—BSSPD, Blockchain, Security

I. INTRODUCTION

Conventionally, individuals opt to subcontract their data to cloud servers for sharing and broadcasting. Yet, the data stored in cloud, particularly susceptible data generated by IoT devices intertwined with human life, poses unique challenges. Such data may encompass personal information related to life, work, and health care.

While these schemes appear to address security and privacy issues during data sharing, they share a common characteristic: an excessive reliance on the Cloud Service Provider (CSP). They assume the CSP to be a trusted third-party organiza- tion, operating under the assumption that the CSP is semi-trustable—curious about the data but not destructive. However, certain inevitable situations arise from this dependency.

Firstly, the CSP may exploit users' private data for profit, or insiders within the CSP may engage in malicious activities leading to privacy disclosure. Consequently, once data owners upload their data to the cloud server, they forfeit absolute possession of their data.

Lastly, to provide superior service, the CSP incurs escalating costs, encompassing server acquisition, hiring skilled person- nel, renting data center venues, and platform construction. Ultimately, users bear the increasing operating costs of the CSP.

II. LITERATURE REVIEW

In recent years, the paradigm of secure data sharing in cloud computing has garnered significant attention due to its crucial role in preserving the confidentiality and integrity of sensitive information. This literature review examines key contributions in the field, addressing challenges such as fine-grained access control, accountability, scalability, and privacy across various cloud computing applications.

1. Li et al. [5] addressed the challenge of secure data sharing for resource-limited users in cloud environments by devis- ing a secure attribute-based data sharing mechanism. Their scheme, leveraging

attribute-based encryption (ABE), enables fine-grained access control while mitigating computational overhead.

2. Accountability, another essential aspect of cloud data sharing, has been tackled by Sundareswaran et al. [8], who introduced a framework ensuring distributed accountability across cloud environments. Their approach enhances trans- parency and trust by tracking and auditing data access ac- tivities comprehensively.
3. Scalability has emerged as a critical requirement in cloud storage systems, leading to the development of innovative solutions such as the key-aggregate cryptosystem proposed by Chu et al. [4]. This cryptosystem facilitates efficient and scalable data sharing by aggregating encryption keys, thereby streamlining access control mechanisms in cloud storage.
4. Yu et al. [11] proposed a method for achieving secure, scalable, and fine-grained data access control in cloud comput- ing, further contributing to the enhancement of cloud security.
5. Privacy concerns in healthcare applications were ad- dressed by Li et al. [6], who introduced a scalable and secure approach to sharing personal health records in cloud computing using attribute-based encryption.
6. In the context of social networks, Cai et al. [1] presented a collective data-sanitization approach to prevent sensitive information inference attacks, highlighting the importance of preserving privacy in online interactions.
7. Addressing privacy and efficiency concerns in emerging IoT applications, Cai and Zheng [2] proposed a private and efficient mechanism for data uploading in smart cyber-physical systems.
8. Zhou et al. [12] introduced an academic influence-aware multidimensional network analysis for research collaboration navigation based on scholarly big data, shedding light on collaborative research dynamics.
9. Differential privacy, a crucial privacy-preserving concept, was applied by Cai et al. [3] to develop a framework for esti- mating urban traffic flows via taxi companies while preserving individual privacy.
10. The seminal work of Nakamoto [7] on Bitcoin in- troduced a remedy for double-spending via a peer-to-peer network. Transactions are timestamped and hashed into an un- broken chain of proof-of-work, creating an immutable ledger. The longest chain serves as evidence of transaction sequence and originates from the most substantial CPU power pool.
11. The paper introduces a deduplicatable data auditing mechanism built on blockchain technology. Initially, we de- velop a client-side data deduplication scheme using bilinear- pair techniques to ease the workload for users and service providers. [10]
12. Xu et al. [9] also proposed a blockchain-enabled dedu- plicatable data auditing mechanism for network storage ser- vices, contributing to the advancement of secure and auditable cloud storage solutions.

These studies collectively underscore the multifaceted na- ture of secure data sharing in cloud computing and highlight the diverse approaches and technologies employed to address associated challenges.

III. SYSTEM OVERVIEW

The existing system relies on centralized servers or cloud solutions with limited access control and security, contrasting with BSSPD's blockchain-based approach emphasizing de- centralization and user control. BSSPD utilizes blockchain's immutability and advanced encryption for improved privacy and transparency in data sharing. Offering fine-grained access control and decentralized storage, BSSPD aims to overcome traditional system limitations and enhance data security and user empowerment.

A. Existing System:

The existing system prior to the implementation of the BSSPD (Blockchain-Based Security Sharing Scheme for Per- sonal Data with Fine-Grained Access Control) likely involves conventional approaches to personal data sharing and access control. In a traditional setting, data sharing may occur through centralized servers or cloud-based solutions with standard access control mechanisms. However, these existing systems might have limitations when it comes to fine-grained access control, privacy, and the security of personal data.

In the absence of BSSPD, data sharing practices may rely on more conventional security measures, potentially utilizing username-password combinations or basic access controls. The centralized nature of these systems might pose risks in terms of a single point of failure and susceptibility to unauthorized access or data breaches. Additionally, the existing systems may not provide users with the level of control over their shared data that BSSPD aims to achieve.

As BSSPD introduces a blockchain-based solution with advanced encryption techniques and decentralized storage, the existing systems may lack the enhanced security features and fine-grained access control that this innovative scheme promises to deliver. The transition from the existing system to BSSPD represents an evolution towards a more secure, transparent, and user-centric approach to personal data sharing.

B. Proposed System:

The proposed system, the Blockchain-Based Security Shar- ing Scheme for Personal Data with Fine-Grained Access Control (BSSPD), revolutionizes personal data security by introducing a sophisticated framework built on blockchain technology. This innovative system is designed to address the limitations of traditional data-sharing approaches and elevate the standards of privacy, security, and user control. Key com- ponents and features of the proposed BSSPD system include:

- Blockchain Technology: BSSPD leverages the decentral- ized and tamper-resistant nature of blockchain to establish a secure foundation. Blockchain ensures transparency, immutability, and trust in the data-sharing process.
- Fine-Grained Access Control: Unlike conventional sys- tems, BSSPD prioritizes fine-grained access control, en- abling data owners to specify detailed access policies based on attributes. This ensures that only users with specific attributes can access and decrypt shared data.
- Ciphertext-Policy Attribute-Based Encryption (CP-ABE): The integration of CP-ABE adds an additional layer of security. It allows data owners to encrypt data with access policies based on user attributes, reinforcing privacy and enabling more nuanced access control.
- Inter Planetary File System (IPFS): BSSPD incorporates IPFS for decentralized and secure storage of encrypted data. IPFS provides a reliable and distributed file system, contributing to the overall decentralization of the data- sharing process.
- User-Centric Model: The proposed system places users at the center, empowering them with complete control over their shared data. Data owners have the authority to set access policies, grant or revoke access rights, and maintain fine-grained control over their personal information.
- Security Mechanisms: BSSPD employs advanced encryp- tion techniques, ensuring that data remains confidential and secure throughout the sharing process. This includes the encryption of data on IPFS and the use of blockchain to store open information and operational records se- curely.
- Smart contracts: Utilizing Smart contracts on the blockchain, BSSPD automates and enforces the execu- tion of access control policies. Smart contracts, such as UMContract for managing data users and DSContract for sharing data, streamline the entire process in a trust-less environment.
- Economic Incentives: BSSPD can potentially introduce a cryptocurrency-based economic system for data sharing, adding a layer of incentives for participants and further enriching the functionality of the system.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, No.4, May : 2024

IV. METHODOLOGY

Our planned scheme, BSPPD, comprises 4 integral mech- anism: IPFS, blockchain, data owner (DO), and data user (DU). The workflow involves the DO encrypting their data and uploading it to IPFS. Subsequently, the DO invoke the Smart contract on the blockchain to save the return address aside with the decryption key. used by BSSPD for security. AES : This is the size (in bits) of a key used for a common encryption method (AES).

PK , SK : These represent the size (in bits) of open and private keys used for another security method (Elliptic Curve Cryptography or ECC).

S : This is the number of different categories used to control who can access data in BSSPD.

PRF : This is the size (in bits) of a key used for a special function that generates random-looking data. All security data pieces and keys (G , F , E , AES , PK , SK , PRF): 256 bits. Number of data access categories (S): 64 bits.

V. RESULTS & DISCUSSIONS

A. Blockchain Efficiency and BSSPD Performance

Just like any computer resource, processing power on blockchains is valuable. Many existing blockchains are criti- cized for being slow. For instance, it takes Bitcoin 10 minutes to create a new block, while Ethereum, despite being faster, still needs about 15 seconds. In this section, we'll evaluate the performance and scalability of our proposed scheme, BSSPD, through experiments.

B. Experimental Setup:

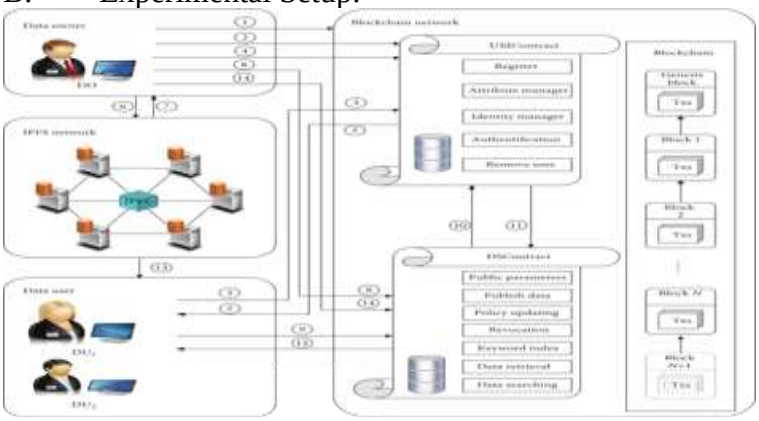

Fig. 1. Structure of BSSPD

- IPFS: Provides a secure and dependable storage service. An inducement mechanism is in place to guarantee that data on IPFS remains consistently available.
- Blockchain: Provisions open information and equipped records throughout the entire scheme. Additionally, it serves as a dependable broadcast channel for transfer messages from the DO to DU. Acting as the cornerstone of trust, the blockchain eliminates the need for a trusted third party. BSSPD incorporates two Smart contracts: UMContract, which manages data users, and DSContract, which facilitates data sharing.
- Data Owner(DO): Accountable for create and deploy the Smart contract within the scheme. The DO has the authority to publish shared data, set access policies, and grant or withdraw a DU's access rights.
- Data User(DU): BSSPD allows users to share data se- curely on the EOS blockchain. It stores important infor- mation like system settings, user data, and details about the data itself in a special area called a Smart contract . Since storing things on the blockchain costs money, it's important to understand how much space BSSPD's Smart contract actually uses.

Breaking Down the Data Size

To analyze this, we'll use some abbreviations: G , F , E : These represent the size (in bits) of different pieces of data

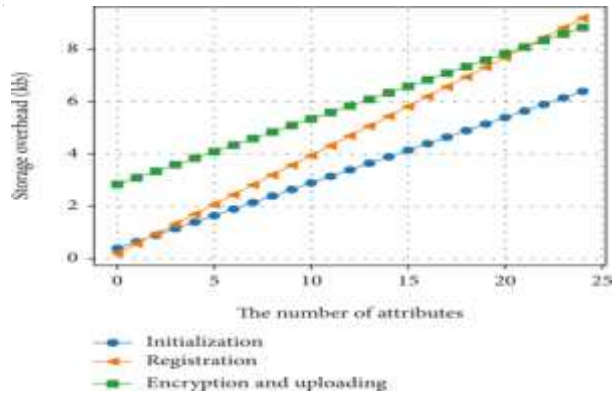

Fig. 2. Storage Overhead Graph

We built a private EOS blockchain with 5 nodes in a controlled lab environment. Each node was a MacBook Pro (2017) equipped with an Intel Core i5 processor at 3.1 GHz and 16 GB of RAM. We used EOS blockchain version v2.0.6 for this experiment.Highlighting the key point of the section (evaluating BSSPD's performance).Providing context for the upcoming technical details(experimental setup).
This rephrased version keeps the core information but improves readability by: Replacing technical jargon with simpler terms ("computing resource" becomes "processing power").Using specific examples ("Bitcoin takes 10 minutes").

C. Adding Data: Attributes vs Data Users

When adding data to the system (AddData operation), two things happen on the blockchain: 1.Uploading data information to the Smart contract . 2.Creating keyword indexes for users who can access the data (Data Users or DUs). According to Figure 2, the number of attributes (data categories) used to control access doesn't significantly affect how long AddData takes. This means adding more categories won't slow down the system. However, the number of DUs with access to the data does impact processing time. Figure 2 shows that adding data for 500 DUs takes considerably longer than for 100 DUs. This is because more time is spent creating search indexes so these users can find the data easily. In short, the number of attributes has minimal impact, but a larger number of DUs will slow down the AddData process.

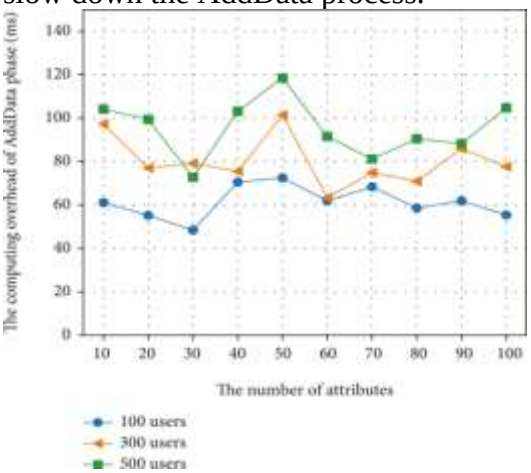

Fig. 3. Overhead varies with data

VI. CONCLUSION

In conclusion, the Blockchain-Based Security Sharing Scheme for Personal Data with Fine-Grained Access Control, abbreviated as BSSPD, marks a significant stride in addressing the crucial aspects of security and privacy in personal data sharing. Grounded in blockchain technology, this innovative

scheme underscores user-centric principles, empowering indi- viduals with complete control over their shared data.

By incorporating Ciphertext-Policy Attribute-Based Encryp- tion (CP-ABE) and the InterPlanetary File System (IPFS), BSSPD achieves fine-grained access control and permission revocation, offering a robust solution to the challenges of data security in the digital age. The scheme's implementation on the EOS blockchain has been rigorously analyzed, affirming its practicality and performance.

BSSPD emerges as a beacon of responsible and secure personal data sharing, providing a model that balances the need for accessibility with the imperative of safeguarding privacy. As technology continues to advance, BSSPD stands as a testament to the ongoing commitment to elevating data protection standards in an ever-evolving digital landscape.

ACKNOWLEDGMENT

The commendable efforts of both the project supervisor and the dedicated team of three students who worked diligently on this project are recognized. Their invaluable guidance and col- laborative spirit are deeply appreciated. Furthermore, gratitude is extended to the technical staff and research participants for their significant contributions.

REFERENCES

[1] Zhipeng Cai, Zaobo He, Xin Guan, and Yingshu Li. Collective data-sanitization for preventing sensitive information inference attacks in social networks. IEEE Transactions on Dependable and Secure Computing, 15(4):577–590, 2016.

[2] Zhipeng Cai and Xu Zheng. A private and efficient mechanism for data uploading in smart cyber-physical systems. IEEE Transactions on Network Science and Engineering, 7(2):766–775, 2018.

[3] Zhipeng Cai, Xu Zheng, and Jiguo Yu. A differential-private framework for urban traffic flows estimation via taxi companies. IEEE Transactions on Industrial Informatics, 15(12):6492–6499, 2019.

[4] Cheng-Kang CHU, Sherman Chow, Wen-Guey Tzeng, Jiangying Zhou, and Robert H DENG. Key-aggregate cryptosystem for scalable data sharing in cloud storage. IEEE Transactions on Parallel and Distributed Systems, 25(2):468, 2014.

[5] Jin Li, Yinghui Zhang, Xiaofeng Chen, and Yang Xiang. Secure attribute-based data sharing for resource-limited users in cloud com- puting. Computers and Security, 72:1–12, 2018.

[6] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE transactions on parallel and distributed systems, 24(1):131–143, 2012.

[7] Satoshi Nakamoto and A Bitcoin. A peer-to-peer electronic cash system.
Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf, 4(2):15, 2008.

[8] Smitha Sundareswaran, Anna Squicciarini, and Dan Lin. Ensuring dis- tributed accountability for data sharing in the cloud. IEEE transactions on dependable and secure computing, 9(4):556–568, 2012.

[9] Yang Xu, Ju Ren, Yan Zhang, Cheng Zhang, Bo Shen, and Yaoxue Zhang. Blockchain empowered arbitrable data auditing scheme for network storage as a service. IEEE Transactions on Services Computing, 13(2):289–300, 2019.

[10] Yang Xu, Cheng Zhang, Guojun Wang, Zheng Qin, and Quanrun Zeng. A blockchain-enabled deduplicatable data auditing mechanism for network storage services. IEEE Transactions on Emerging Topics in Computing, 9(3):1421–1432, 2020.

[11] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou. Achieving secure, scalable, and fine-grained data access control in cloud computing. In 2010 Proceedings IEEE INFOCOM, pages 1–9. Ieee, 2010.

[12] Xiaokang Zhou, Wei Liang, I Kevin, Kai Wang, Runhe Huang, and Qun Jin. Academic influence aware and multidimensional network analysis for research collaboration navigation based on scholarly big data. IEEE Transactions on Emerging Topics in Computing, 9(1):246–257, 2018.