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

**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.

**Existing System**

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.

**Proposed System**

From the above point of view, to better protect data security and personal privacy, it is very urgent to design a whole user-centric data-sharing scheme to solve the above problems. In this scheme, we do not need to rely on any trusted third party to store and disseminate data, nor do we worry that the data will be inaccessible. Fortunately, with the emergence and development of Bitcoin [10], as a decentralized and self-organized cryptocurrency, its underlying technology blockchain can elegantly help us realize such a data security sharing scheme [11–14]. In this project, we proposed a data sharing scheme based on blockchain. The main contributions of this paper are as follows:

1. A user-centric data security sharing scheme named BSSPD is proposed, which combines blockchain, CP-ABE, and IPFS. The data owner encrypts his sharing data and stores it on IPFS to maximize decentralization, and BSSPD allows the data owners to have fine-grained access control over their data. Moreover, it supports revoking permissions of a specific data user at an attribute level without affecting others
2. In BSSPD, the data owner publishes data-related information and distributes decryption keys for data users through the blockchain. To avoid denial of service attacks, data users need to complete a proof of work (PoW) before registering, which is like the mining process of Bitcoin, and the data owner can adjust the target of PoW according to the number of data users in the system
3. BSSPD sets ciphertext keyword indices for each data related data user. Combined with CP-ABE, it further prevents the privacy disclosure that data labels may cause to the data owner and protects the data user’s privacy during retrieval
4. We experimented with our scheme on the EOS blockchain and provided the detailed implementation of algorithms and Smart Contracts. Together with the security analysis, it proved that our scheme is feasible
5. We used five MacBooks to build an EOS private chain in the laboratory environment and simulated our scheme. Analysis of storage and computing overhead proved that BSSPD.

**Literature survey**

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. MedRec thus enabled the emergence of data economics, supplying big data to empower researchers while engaging patients and providers in the choice to release metadata. 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.

Liang et al. [20] proposed an innovative user-centric health data sharing solution by utilizing a decentralized and permissioned blockchain to protect privacy using channel formation scheme and enhance the identity management using the membership service supported by the blockchain. A mobile application is deployed to collect health data from personal wearable devices, manual input, and medical devices, and synchronize data to the cloud for data sharing with healthcare providers and health insurance companies. To preserve the integrity of health data, within each record, a proof of integrity and validation is permanently retrievable from cloud database and is anchored to the blockchain network. Moreover, for scalable and performance considerations, this work adopted a tree-based data processing and batching method to handle large data sets of personal health data collected and uploaded by the mobile platform.

Fan et al. [21] proposed a scheme based on a blockchain to solve the privacy issues in content-centric mobile networks for 5G. This paper implemented the mutual trust between content providers and users. Besides, the openness and tamper-resistant of the blockchain ledger ensure the access control and privacy of the provider. With the help of a miner, selected from users, this work can maintain the public ledger expediently. Also, in return, this work shared the interesting data with low overhead, network delay and congestion, and then achieve green communication.

Zhang et al. [22] established a mutual trust data sharing framework to break these data barriers. The framework is based on the distributed and temper-proof attributes of blockchain. This work implemented a prototype based on Hyperledger Fabric. The proposed system combined supervision and fine-grained data access control based on smart contracts, which provided a secure and trustless environment for data sharing. This work further compared this system with existing data sharing schemes.

Zhou et al. [23] proposed a double-blind paper review system to preserve the authors and reviewers’ anonymity. This system also addressed issues concerning the reviewer’s payment, inconsistent review metrics, and biased reviews. The proposed solution utilized the Hyperledger Fabric blockchain with the InterPlanetary File System (IPFS). The blockchain smart contracts provided a base for financial transactions between paper publishers and the reviewers. Hence, this work introduced AcadCoin, a novel cryptocurrency used for supporting said financial transactions. Also, the Hyperledger blockchain provided user access control to achieve double blindness in reviews. Along with the Hyperledger blockchain, the IPFS is used to store the paper documents, review documents and open metrics documents to reduce the storage requirement of the blockchain. A broad system architecture is constructed to combine the blockchain and the file storage system. This system architecture distributed the nodes of the system to related parties. Finally, the blockchain network is implemented and tested using the Hyperledger Composer Playground environment.

Patel et al. [24] examined the blockchain concept, which enables parties to establish consensus without relying on a central authority. This work developed a framework for cross-domain image sharing that uses a blockchain as a distributed data store to establish a ledger of radiological studies and patient-defined access permissions. The blockchain framework is shown to eliminate third-party access to protected health information, satisfy many criteria of an interoperable health system, and readily generalize to domains beyond medical imaging. Relative drawbacks of the framework include the complexity of the privacy and security models and an unclear regulatory environment. Ultimately, the large-scale feasibility of such an approach remains to be demonstrated and will depend on several factors which this paper discussed in detail.

**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 services,” IEEE Transactions on Network Science and Engineering, 2020.
14. Y. Xu, J. Ren, G. Wang, C. Zhang, J. Yang, and Y. Zhang, “A blockchain-based nonrepudiation network computing service scheme for industrial IoT,” IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3632– 3641, 2019.
15. M. Swan, “Blockchain thinking: the brain as a decentralized autonomous corporation [commentary],” IEEE Technology and Society Magazine, vol. 34, no. 4, pp. 41–52, 2015.
16. G. Zyskind, O. Nathan, and A. Pentland, “Decentralizing privacy: using blockchain to protect personal data,” in 2015 IEEE Security and Privacy Workshops, pp. 180–184, San Jose, CA, 2015.
17. A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “Medrec: using blockchain for medical data access and permission management,” in 2016 2nd International Conference on Open and Big Data (OBD), pp. 25–30, Vienna, 2016.
18. Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, “Medshare: trust-fewer medical data sharing among cloud service providers via blockchain,” IEEE Access, vol. 5, pp. 14757–14767, 2017.
19. A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, “Secure and trustable electronic medical records sharing using blockchain,” AMIA Annual Symposium Proceedings, vol. 2017, pp. 650–659, 2017.
20. X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, “Integrating blockchain for data sharing and collaboration in mobile healthcare applications,” in 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 1–5, Montreal, QC, 2017.
21. K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, “Blockchain based efficient privacy preserving and data sharing scheme of content-centric network in 5g,” IET Communications, vol. 12, no. 5, pp. 527–532, 2017.
22. G. Zhang, T. Li, Y. Li, P. Hui, and D. Jin, “Blockchain-based data sharing system for AI-powered network operations,” Journal of Communications and Information Networks, vol. 3, no. 3, pp. 1–8, 2018.
23. I. Zhou, I. Makhdoom, M. Abolhasan, J. Lipman, and N. Shariati, “A blockchain-based file-sharing system for academic paper review,” in 2019 13th International Conference on Signal Processing and Communication Systems (ICSPCS), pp. 1–10, Gold Coast, Australia, 2019.
24. V. Patel, “A framework for secure and decentralized sharing of medical imaging data via blockchain consensus,” Health informatics journal, vol. 25, no. 4, pp. 1398–1411, 2018.