

# A Blockchain-Powered Security Exchange For Individual Information With Detailed Access Management

<sup>1</sup> Ms. Bheemireddy Lakshmi Bhavani, <sup>2</sup> Ms. Gangula Susmitha Reddy, <sup>3</sup> Ms. Thalla Gayathri, <sup>4</sup> Ms.

Gujjeti Navya, <sup>5</sup> Dr. A.Ramesh Babu

<sup>1, 2, 3, 4</sup> Students, CSE, <sup>5</sup> HOD, IT

<sup>1, 2, 3, 4, 5</sup> JBIET, Hyderabad

## ABSTRACT

*In the AI-driven era, safeguarding privacy while enabling open data sharing is paramount. Existing data-sharing solutions rely heavily on cloud servers, raising concerns about data ownership, security, and privacy. While encryption and access control mitigate some risks, dependence on Cloud Service Providers (CSPs) remains a challenge. To address this, we propose BSSPD, a blockchain-based security sharing scheme for personal data. BSSPD integrates blockchain, ciphertext-policy attribute-based encryption (CP-ABE), and InterPlanetary File System (IPFS) to maximize decentralization. Data owners encrypt and store data on IPFS, while CP-ABE encrypts access keys based on specific policies. Blockchain facilitates data owner authentication and key distribution. Fine-grained access control and attribute-level revocation enhance security without compromising usability. Ciphertext keyword search protects data user privacy during retrieval. Security analysis and EOS blockchain simulations demonstrate BSSPD's feasibility and performance. Our approach offers a robust solution to the challenges of data governance in the AI era, empowering users with greater control over their personal data while ensuring security and privacy.*

*Index Terms: Secured Data, Personal Data, Access Control, Ciphertext, Blockchain*

## 1. INTRODUCTION

The advent of 5G and Internet of Things (IoT) technology has ushered in an era of unprecedented data generation, facilitating the rapid implementation of artificial intelligence (AI) systems [1]. However, this surge in data availability has brought about profound challenges in ensuring data security and privacy protection. As AI capabilities for data mining and analysis continue to advance, concerns over personal privacy have become paramount in the realm of data governance and sharing [2].

Traditionally, individuals and organizations have often opted to outsource their data to cloud servers for sharing and dissemination purposes [3]. This practice, while convenient, poses significant risks, particularly regarding the security and privacy of sensitive data. Data generated by IoT devices, in particular, are intricately linked to human life and activities, encompassing a wide range of personal information related to aspects such as work, healthcare, and daily routines [4]. The potential ramifications of unauthorized access or data breaches are immense, potentially leading to severe repercussions for individuals whose personal data is compromised or linked to their real identities.

In this context, the challenge of integrating data to derive value while simultaneously safeguarding data security and privacy has emerged as a critical concern for companies operating in the big data and AI domains [5]. The need to strike a balance between leveraging data for innovation and protecting individual privacy has become increasingly pressing in contemporary data-driven environments.

To address these challenges, researchers have proposed numerous secure sharing schemes within the cloud environment [6–9]. These schemes aim to mitigate security and privacy risks associated with data sharing, offering various encryption and access control mechanisms. However, a common limitation of these schemes is their significant reliance on Cloud Service Providers (CSPs) [10]. These schemes typically assume the CSP to be a trusted third-party entity, incorporating security models that hinge on the CSP's presumed trustworthiness. The prevailing assumption underlying these schemes is that while CSPs may have access to the data they host, they are not inclined to misuse or compromise it [11]. However, this trust model overlooks the potential risks associated with malicious behavior or security breaches on the part of CSPs. Despite their best efforts to ensure data security, CSPs are not immune to vulnerabilities or external threats, making overly dependent on them a precarious proposition.

## 2. LITERATURE SURVEY

In the realm of cloud computing, ensuring secure and efficient data sharing among resource-limited users has garnered significant attention from researchers. Various cryptographic techniques and access control mechanisms have been proposed to address the challenges of data security and privacy protection in cloud environments. The following literature survey provides an overview of key research contributions in this field, highlighting their methodologies and contributions.

Li et al. [1] proposed a secure attribute-based data sharing scheme tailored for resource-limited users in cloud computing environments. Their approach leverages attribute-based encryption (ABE) to enforce fine-grained access control over shared data, ensuring that only users with specific attributes can access sensitive information. By distributing decryption keys based on user attributes, the scheme enables efficient and secure data sharing while minimizing the computational burden on resource-constrained devices.

Sundareswaran et al. [2] focused on ensuring distributed accountability for data sharing in cloud environments. Their work addresses the challenge of maintaining accountability and traceability in distributed data sharing scenarios, where multiple entities may be involved in accessing and processing shared data. Through the use of cryptographic techniques and distributed consensus mechanisms, the proposed scheme enhances transparency and accountability, thereby mitigating the risk of unauthorized data access or manipulation.

Chu et al. [3] introduced a key-aggregate cryptosystem designed to facilitate scalable data sharing in cloud storage systems. The key-aggregate approach allows data owners to efficiently manage access control policies by aggregating multiple decryption keys into a single compact key. This enables flexible and efficient data sharing while reducing the computational overhead associated with managing large numbers of encryption keys.

Yu et al. [4] proposed a framework for achieving secure, scalable, and fine-grained data access control in cloud computing environments. Their approach integrates cryptographic techniques, such as attribute-based encryption and proxy re-encryption, to enforce access control policies based on user attributes and roles. By decoupling data encryption and access control enforcement, the scheme achieves scalability and flexibility in managing access control policies for large-scale cloud deployments.

Li et al. [5] focused on addressing the challenges of sharing personal health records (PHRs) in cloud computing environments. Their approach employs attribute-based encryption to enable secure and scalable sharing of PHRs while preserving patient privacy. By encrypting PHRs with fine-grained access control policies based on patient

attributes, the scheme ensures that only authorized healthcare providers can access sensitive medical information.

Cai et al. [6] proposed a collective data sanitization mechanism to prevent sensitive information inference attacks in social networks. Their approach leverages collective data anonymization techniques to protect user privacy while preserving the utility of shared data for analysis and collaboration. By sanitizing sensitive information at the collective level, the scheme mitigates the risk of privacy breaches and unauthorized data disclosures in social network environments.

Cai and Zheng [7] introduced a private and efficient mechanism for data uploading in smart cyber-physical systems (CPSs). Their approach addresses the challenges of data privacy and efficiency in CPS environments by employing cryptographic techniques and distributed consensus mechanisms. By encrypting data at the source and leveraging efficient data aggregation techniques, the scheme ensures privacy-preserving data uploads while minimizing communication overhead and computational costs.

Zhou et al. [8] proposed an academic influence-aware and multidimensional network analysis framework for research collaboration navigation based on scholarly big data. Their approach leverages advanced network analysis techniques to identify influential researchers, detect collaboration patterns, and navigate research collaboration networks effectively. By integrating scholarly big data analytics with network visualization techniques, the framework provides researchers with valuable insights into research collaboration dynamics and opportunities for collaboration.

In summary, the literature survey highlights various approaches and techniques for ensuring secure and efficient data sharing in cloud computing environments. From attribute-based encryption and access control mechanisms to collective data sanitization and network analysis techniques, researchers have developed a diverse array of solutions to address the complex challenges of data security and privacy protection in cloud environments. These contributions provide valuable insights and methodologies for designing secure and privacy-preserving data sharing systems in the era of big data and cloud computing.

### 3. METHODOLOGY

#### a) Proposed Work:

The proposed system, named BSSPD (Blockchain-based Security Sharing Scheme for Personal Data), aims to address the limitations of existing data-sharing systems by leveraging a combination of blockchain technology, ciphertext-policy attribute-based encryption (CP-ABE), and the Interplanetary File System (IPFS).

BSSPD utilizes the InterPlanetary File System (IPFS)[27,28] for decentralized storage of encrypted data. By storing data across a distributed network of nodes, BSSPD reduces reliance on centralized servers and enhances data resilience and availability.

BSSPD employs ciphertext-policy attribute-based encryption (CP-ABE) to enforce access control policies. Data owners encrypt shared data and define access policies based on specific attributes.

Blockchain technology is utilized in BSSPD for managing data-related information and distributing decryption keys securely. Data owners publish data-related transactions on the Blockchain[21], enabling transparent and auditable access control.

To protect data user privacy, BSSPD incorporates ciphertext[30] keyword search mechanisms. This enables users to retrieve encrypted data based on keyword queries without revealing plaintext content, preserving confidentiality and preventing unauthorized data disclosure.

### b) System Architecture:

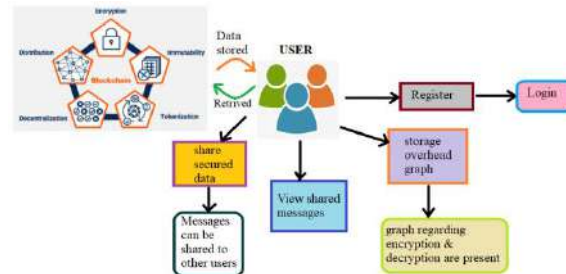


Fig1 Proposed Architecture

The system architecture comprises two main components: the User Module and the Blockchain Module.

The User Module facilitates user interactions, including registration, login, viewing shared messages, and sharing secured data. Users register and authenticate their identity through the registration and login functionalities. Upon logging in, users can view shared messages and securely share data with other users. Additionally, the Storage Overhead Graph feature provides insights into encryption and decryption time overheads, aiding users in understanding system performance.

The Blockchain Module handles data encryption, immutability, tokenization, decentralization, and distribution aspects. Encryption ensures data security during storage and retrieval processes. Immutability guarantees that once data is stored on the Blockchain[21], it cannot be altered or tampered with. Tokenization enables secure token-based authentication for users. Decentralization and distribution mechanisms ensure that data is stored and retrieved from multiple nodes in a decentralized network, enhancing fault tolerance and resilience against single points of failure.

Together, these modules form a robust system architecture that ensures secure, efficient, and decentralized data sharing while maintaining confidentiality, integrity, and availability of shared information.

### c) Modules:

To implement this project we used the following modules are New User and Existing User.

These modules description are given below:

#### A) New User Signup:

The New User Signup module enables individuals to register and establish an account within the BSSPD system. Users furnish essential details during signup, securely stored on the Blockchain[21]. This module serves as a foundational step for users to gain access to the secure data sharing platform, establishing their presence and eligibility to participate in data exchange activities.

#### B) User Login:

The User Login module grants access to registered users of the BSSPD platform. Users verify their identity by entering credentials such as username and password, accessing system features securely. By enforcing stringent

authentication measures, this module ensures that only authorized individuals can log in and utilize the platform's functionalities, safeguarding against unauthorized access and preserving data security.

**i) Share Secured Data:** The Share Secured Data module empowers data owners to share information securely with designated users. Owners upload data, setting access policies based on user attributes. Utilizing CP-ABE, the module encrypts data and decryption keys according to these policies, then stores them securely on IPFS. This approach guarantees that only authorized users possessing requisite attributes can decrypt and access the shared data, maintaining confidentiality and integrity.

**ii) View Shared Messages:** The View Shared Messages module permits users to access and decrypt data shared with them. Authorized users can view and interact with the shared content, ensuring that only individuals with appropriate permissions can access the data. By enforcing strict access controls, this module upholds data privacy and security, safeguarding against unauthorized viewing or manipulation of sensitive information.

**iii) Storage Overhead Graph:** The Storage Overhead Graph module offers visual representations of encryption and decryption time overheads. Through graphical depictions, users can comprehend the duration required for these processes, aiding in assessing system performance. This data empowers users to make informed decisions concerning data sharing and access, ensuring optimal utilization of resources while maintaining efficient encryption and decryption operations within the system.

#### d) Blockchain Integration:

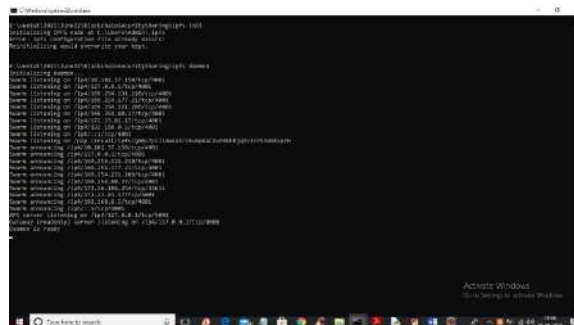
Blockchain integration in BSSPD ensures decentralized data storage by distributing data across multiple nodes, enhancing fault tolerance and high availability. This approach reduces the risk of a single point of failure, providing a resilient storage mechanism for shared personal data.

Each data block in BSSPD is associated with a unique hash code verified by the blockchain before storage. This verification process ensures data integrity and authenticity. Any attempt to tamper with the data would alter the hash code, causing verification failure and effectively making the data tamper-proof.

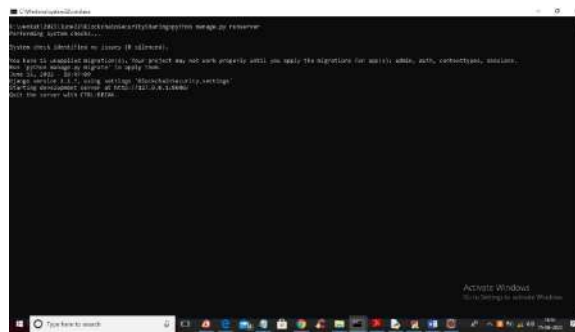
BSSPD leverages Blockchain to control and manage data access effectively. Blockchain[21] distributes keys and access policies to authorized users based on predefined criteria. Only those users meeting the specified criteria can decrypt and access the shared data, providing fine-grained access control and ensuring precise management of data access.

## 4. EXPERIMENTAL RESULTS

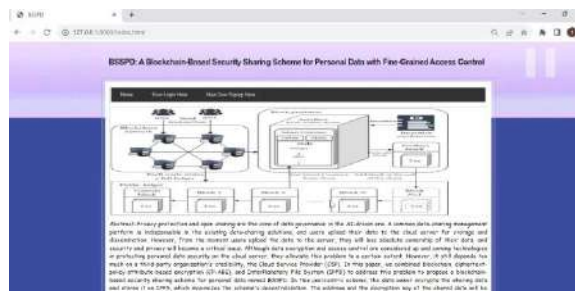
To run project first double click on 'Start\_IPFS.bat' file to start IPFS server and get below screen



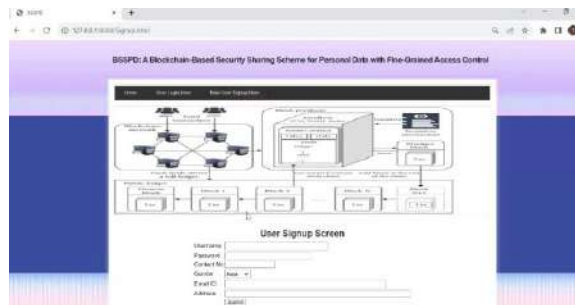
In above screen IPFS server started and now double click on 'runServer.bat' file to start python DJANGO server and get below screen



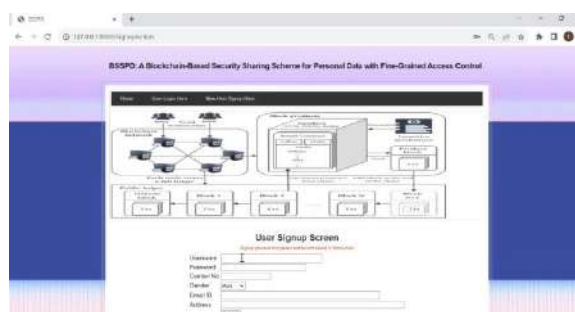
In above screen python DJANGO server started and now open browser and enter URL as ‘http://127.0.0.1:8000/index.html’ and press enter key to get below screen



In above screen click on ‘New User Sign Up Here’ link to add new user to Blockchain

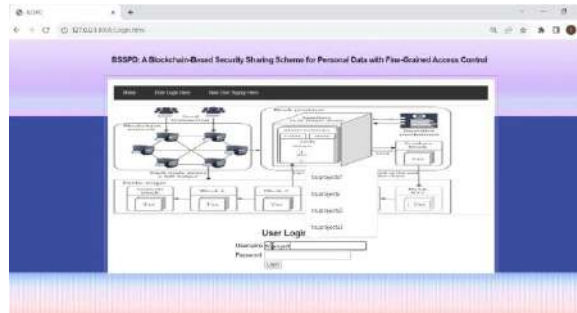


In above screen user is sign up and press button to get below output

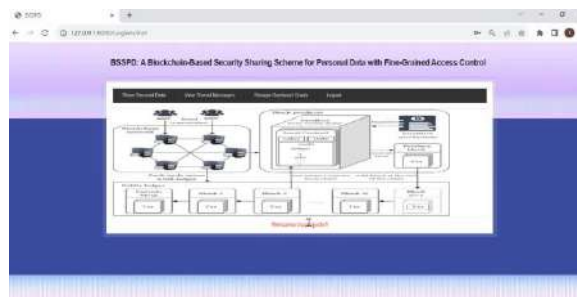


In above screen user sign up process completed and similarly you can add any number of users and now click on ‘User Login Here’ link to get below login screen

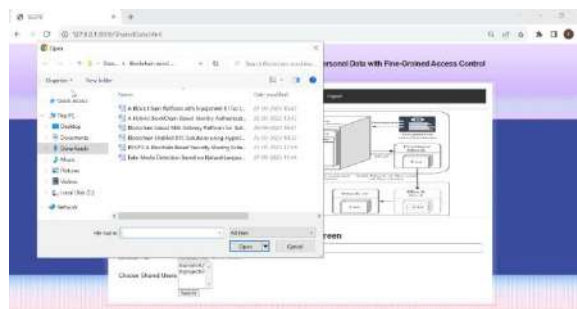




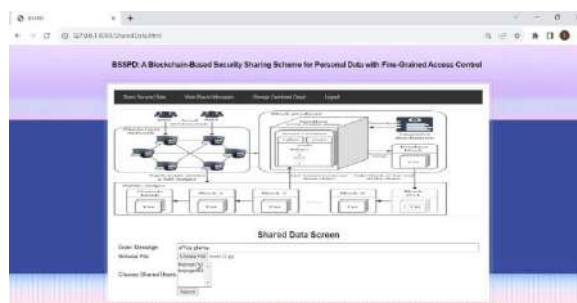
In above screen user is login and press button to get below output



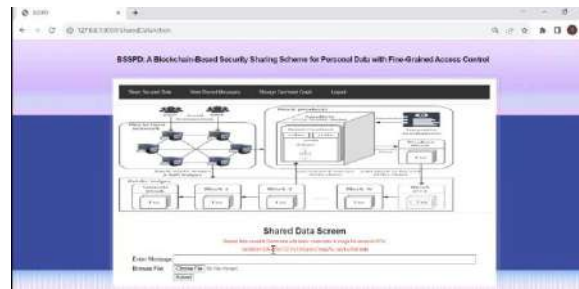
In above screen user logged in successfully and now click on 'Share Secured Data' link to share data with other users



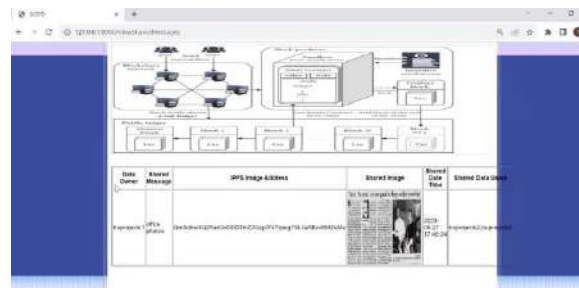
In above screen user can enter some message and then upload image and by holding CTRL KEY you can select names of users with whom you want to share this data and press button to get below output



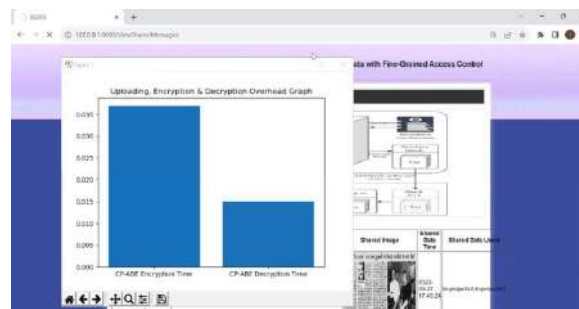
In above screen 'John' is sharing data with user 'aaa' and 'bbb' and both users can decrypt and view data but user 'ccc' cannot view it.



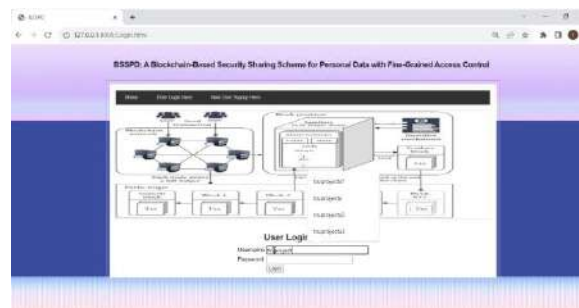
In above screen we can see sharing attributes stored at Blockchain and images and decryption keys stored at IPFS and now click on ‘View Shared Messages’ link to view own messages and other users shared messages so ‘John’ is the data owner so he can view his own upload and others shared data.



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 whether aaa or bbb can view this data or not and now click on ‘Storage Overhead Graph’ link to view encryption and decryption time overhead

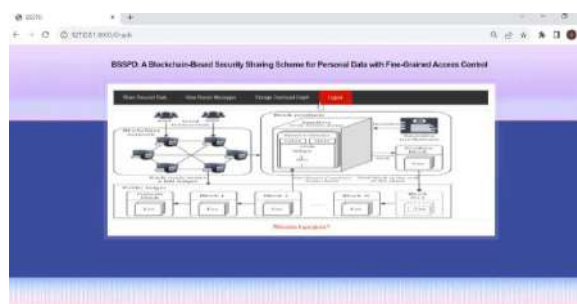


In above screen x-axis represents encryption and decryption and y-axis represents time overhead and now logout and login as ‘bbb’ user to view shared data.

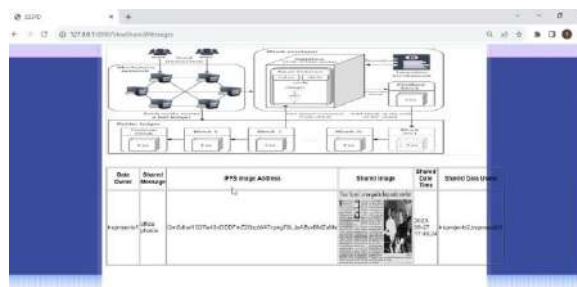


In above screen shared user ‘bbb’ is login and after login will get below output





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



In above screen 'bbb' can view shared data from aaa and john and now logout and output

In above screen 'bbb' can get empty table as nobody shared data with him. Similarly any number of user can sign up and share data.

## 5. CONCLUSION

The integration of Blockchain, CP-ABE (Ciphertext-Policy Attribute-Based Encryption)[30], and IPFS in the BSSPD project showcases a remarkable advancement in data security. This amalgamation achieves decentralized data storage, robust encryption, and precise access control, significantly enhancing data security and privacy. BSSPD's user-centric approach ensures data owners maintain substantial control and ownership over their shared data through well-defined access policies and attribute-based access, fostering trust and confidence in managing personal information.

The incorporation of Blockchain and IPFS improves the efficiency and reliability of data sharing. Decentralized storage via IPFS enhances fault tolerance by reducing reliance on single points of failure, while Blockchain[21] ensures data tamper-proofing and efficient access control, bolstering overall reliability and security. BSSPD emerges as a promising solution for secure and privacy-preserving data sharing, addressing limitations of existing systems and offering a robust framework that empowers users with enhanced control, privacy, and security over their shared data.

## 6. FUTURE SCOPE

The future scope of BSSPD extends beyond personal data sharing to encompass domains like healthcare, finance, and the Internet of Things (IoT). While requiring domain-specific considerations and optimizations, adapting BSSPD principles and mechanisms to these areas holds immense potential for unlocking secure and privacy-preserving data sharing opportunities. In healthcare, for instance, BSSPD could facilitate the secure exchange of sensitive medical information among healthcare providers and patients. Similarly, in finance, BSSPD could enhance data security and privacy in transactions and financial records sharing. Furthermore, in

the IoT realm, BSSPD could enable secure data sharing among interconnected devices, ensuring confidentiality and integrity of shared data streams. By broadening its application scope, BSSPD stands poised to revolutionize data sharing practices across diverse sectors, offering a robust framework for safeguarding sensitive information and fostering trust in data exchange ecosystems.

## 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 deduplicatable 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-less 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, "Blockchainbased 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.
- [25] L. Tan, N. Shi, C. Yang, and K. Yu, "A blockchain-based access control framework for cyber-physical-social system big data," *IEEE Access*, vol. 8, pp. 77215–77226, 2020.
- [26] M. Jemel and A. Serhrouchni, "Decentralized access control mechanism with temporal dimension based on blockchain," in *2017 IEEE 14th International Conference on e-Business Engineering (ICEBE)*, pp. 177–182, Shanghai, 2017.
- [27] X. Sun, S. Yao, S. Wang, and Y. Wu, "Blockchain-based secure storage and access scheme for electronic medical records in ipfs," *IEEE Access*, vol. 8, pp. 59389–59401, 2020.
- [28] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *IEEE Access*, vol. 6, pp. 38437–38450, 2018.
- [29] S. M. Pournaghi, M. Bayat, and Y. Farjami, "MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 11, pp. 4613–4641, 2020.
- [30] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *2007 IEEE Symposium on Security and Privacy (SP '07)*, pp. 321–334, Berkeley, CA, 2007