# BSSPD: A BLOCKCHAIN-BASED SECURITY SHARING SCHEME FOR PERSONALDATA WITH FINE-GRAINED ACCESS CONTROL

**Dileep P [1], Tirupati Rao S [2], Revathy P [3]**

[1] Professor, Department of Computer Science and Engineering

[2] Associate Professor, Department of Computer Science and Engineering

[3] Assistant Professor, Department of Computer Science and Engineering

[1] Malla Reddy College of Engineering and Technology,Kompally,Hyderabad,India.

[2] Geethanjali College of Engineering and Technology,Keesara,Hyderabad,India.

[3] Narsimha Reddy Engineering College,Kompally,Hyderabad,India.

## ABSTRACT:

Privacy protection and open sharing is 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, we combined blockchain, ciphertext-policy attribute-based encryption (CP-ABE), and Interplanetary 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.

***Keywords: CP ABE, CSP, IPFS, block chain, BSSPD.***

## 1. INTRODUCTION:

For copyright protection of multimedia information, a variety of digital watermarking techniques have been developed, which are used to protect the multimedia information from being abused. There are two categories of techniques of embedding the watermark for copyright shield in any multimedia information, be it the image, audio or video. The spatial domain technique follows any particular algorithm for embedding of the watermark by directly adding it to the data, and the frequency domain method is to embed it in any of the transform domain. The spatial domain of watermarking is faster but fails in robustness while the frequency domain watermarking is robust but still consumes more resources in terms of power consumption and slower speed of computing (Acken, 1998; Low et al., 1998; Macq and Pitas, 1998; Swanson et al., 1998).

It is better to go for the higher cost of computing to get the benefits of robustness of the watermark when maliciously attacked by the mechanisms of noise, filtering or compression. For the realization of the watermarking mechanisms, the major areas of focus are imperceptibility, robustness, capacity, security, and trustworthiness. The perceptual transparency of the hidden data or information is the imperceptibility. Survival of the watermark information against intentional or unintentional attacks without significant degradation of the quality of the original image is the robustness. The payload for the new signal is defined as the capacity and the undetectability of the watermark information on the corresponding media, which is defined as the security and all these turned to be very important considerations in case of invisible watermarking (Liu and Tan, 2002; Zhu et al., 2006; Gutab and Ghouti, 2007). A well-known survey of watermarking techniques can be found from (Kutter and Hartung, 1999; Mohanty, 1999; Altaibi et al., 2015). There is a trade-off between these parameters as an increase in robustness may appear at the expense of enhanced watermark signals visibility as well as reduced bandwidth. But, the perceptual distortion of the image, due to watermark embedding is not related directly to the magnitude of the watermark signal. It can be observed that the watermark signal of same strength is causing less visual distortion in busy areas of the image than the flat background. In the papers (Podilchuk and Wenjua, 1998; Hannigan et al., 2001) on watermarking, there is less effort to evaluate images in order to consider the upper limit of the power of the watermark signal without

considerable visual distortion. These spatial domain methods neglect the significance of payload capacity and mostly focused on the imperceptibility factors. In Khan and Gutub (2007) the authors proposed an image based message concealment mechanism by use of punctuation marks to encode a secret message and by using modified scytale cipher provides the better result as far as the security is concerned. In Al-Otaibi (2014) the author proposed a data hiding technique with two layers of the security system by including AES cryptography followed by image-based steganography to ensure high security. Methods of LSB matching is proposed in Sharp (2001), which also called ± embedding mechanism (Li et al., 2011). In this method, the cover image pixel value is increased or decreased randomly by one when the secret bit is not equal to the LSB of the pixel belonging to the cover image (Huang et al., 2014). The LSBM modifies both the histogram of an image and the correlation between the adjacent pixels, which helps the steganalysis methods to attack this method (Xia et al., 2016). In Sabeti et al. (2013) the authors proposed complexity based LSB matching scheme, where the LSB matching is used in order to enhance the security against possible attacks. This mechanism uses a local neighborhood analysis to determine the secure locations of an image and then LSB matching used for the embedding process. In Parvez and Gutub (2011) the authors proposed one image steganography algorithm, which determines the number of secret message bits that each pixel of the cover image can store based on a partition scheme of color intensity range. This scheme provides high data hiding capacity and security for the host image.

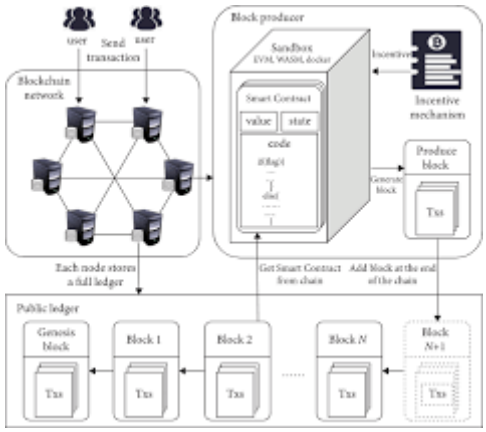
## 2. EXICITING SYSTEM:

As early as 2015, Swan pointed out that there was not yet an acceptable “health data common” model with appropriate privacy and reward systems for public sharing of personal health data and quantified self-tracking data. Simultaneously, the author believes that blockchain can precisely provide such a structure for creating a secure, remunerated, and owner-controlled health data sharing. Zyskind et al. described a distributed personal data management system that ensures users own and control their data. The system encrypts the data collected from the user’s mobile phone and stores it off-chain and only stores the data’s hash value on the blockchain. Meanwhile, two acceptable transaction types named Taccess and Tdata are defined, in which Taccess is used to implement access control management, and Tdata is used for data

storage and retrieval. Azaria et al. proposed MedRec system, a blockchain-based decentralized record management system for electronic medical records (EMRs). MedRec provides patients with a comprehensive and immutable log, and the patients can access their medical information at any time across providers and locations.

**PROPOSED SYSTEM:**

ABE is considered the most appropriate technology to solve data security and privacy protection problems in a distributed environment. Therefore, recently, researchers have used ABE to achieve fine-grained access control over data on the blockchain. Jemel and Serhrouchni proposed a decentralized access control mechanism. For the first time, researchers used blockchain nodes to execute a CP-ABE algorithm to verify user access rights' legitimacy. The scheme designs two types of transactions: SetPolicy and GetAccess. But it does not use Smart Contracts, and it is obvious that the scheme is unable to achieve more complex requirements. Sun et al. constructed a model of secure storage and effective sharing for electronic medical data based on ABE and blockchain, which provides better access control. Doctors use ABE to encrypt patients' medical data and store it on IPFS. However, it also does not use Smart Contracts. It only broadcasts some ABE parameters stored in transactions, which cannot achieve more complex business functions. Wang et al. proposed a sharing scheme in which users distribute secret keys. It realizes that the data owner has a fine-grained access control on his data. At the same time, the Ethereum Smart Contract is used to realize the retrieval of ciphertext keywords. However, it requires multiple off-chain communication between users, and more importantly, it does not implement the permit revocation. Pournaghi et al. proposed a secure and efficient sharing scheme based on blockchain and ABE entitled MedSBA to record and store medical data. It implements the update and revocation of permissions by broadcasting a new strategy to cover the previous transaction, but this will lead to users who do not want to be revoked to update their keys**.**




## 3. METHODOLOGY

To implement this project we have designed following modules

1) New User Signup: using this module user can get signup with the application and all this details saved in Blockchain

2) User Login: using this module user can login to application

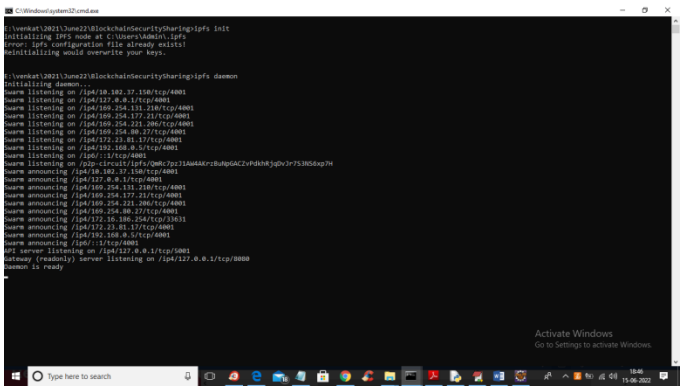
3) Share Secured Data: using this module data owner can upload messages and images and then select sharing usernames and then encrypt data and then encrypt decryption keys by using sharing user details and only those users can decrypt data who has their names in decryption keys

4) View Shared Messages: using this modules data users can view all messages shared by data owner and this message will display and get decrypted if user has access permission in decryption keys

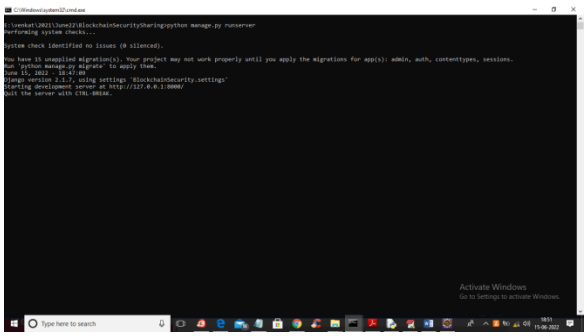
5) Storage Overhead Graph: using this module we will display encryption and decryption time overhead graph

**SCREEN SHOTS**

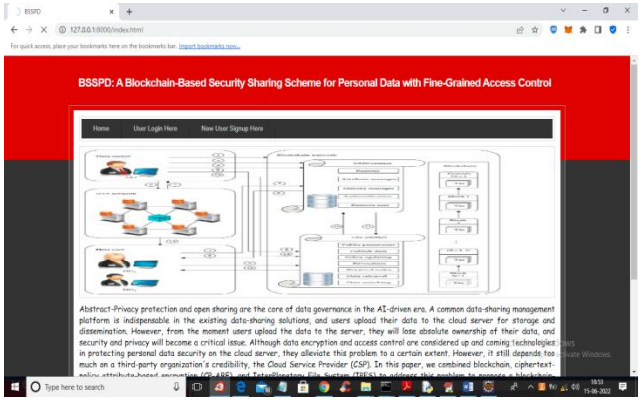
To run project first double click on ‘Start_IPFS.bat’ file to start IPFS server and get below screen



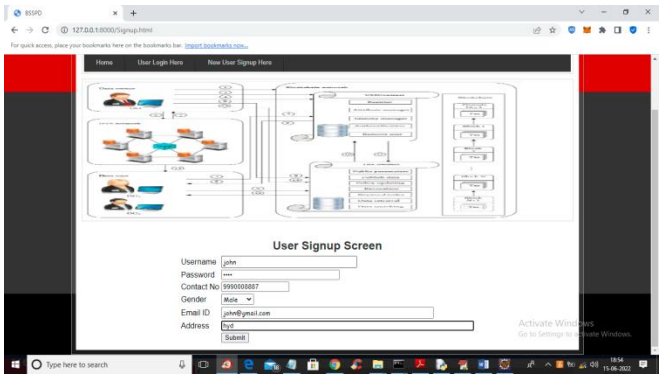

In above screen IPFS server started and now double click on 'runServer.bat' file to start python DJANGO server and get below screen



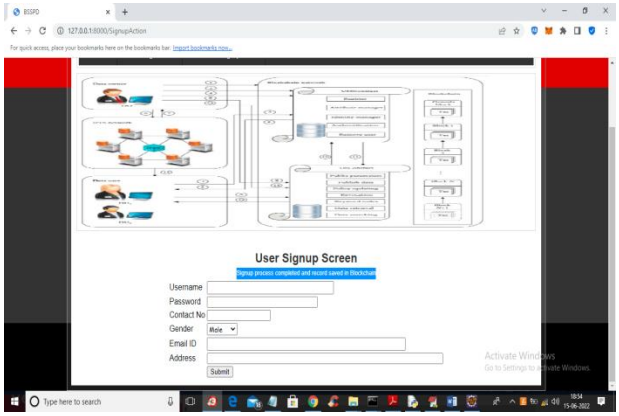

In above screen python DJANGO server started and now open browser and enter URL as 'http://127.0.0.1:8000/index.html' and press enter key to get below screen



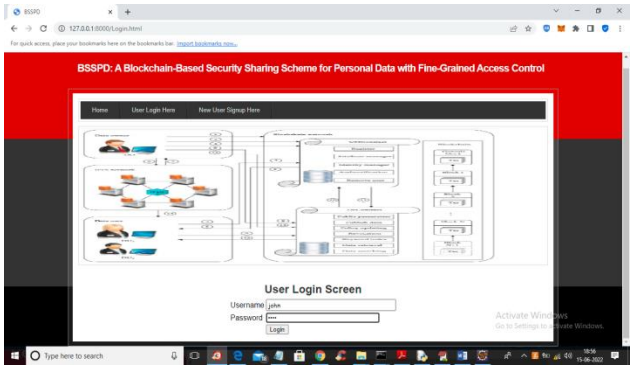

In above screen click on 'New User Signup Here' link to add new user to Blockchain



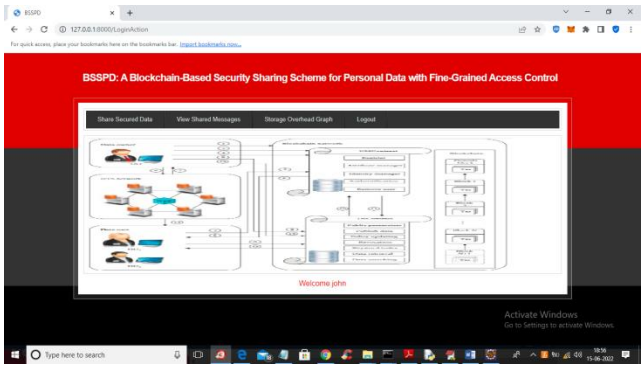

In above screen user is signup and press button to get below output



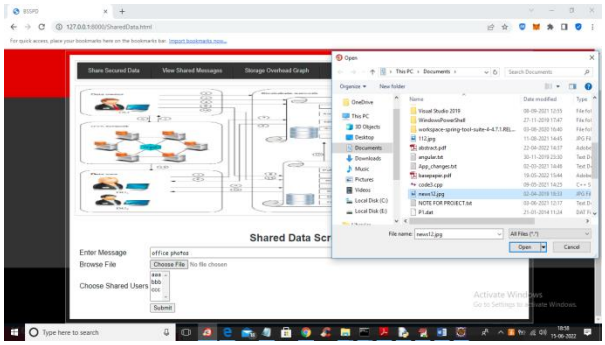

In above screen user signup process completed and similarly you can add any number of users and now click on 'User Login Here' link to get below login screen



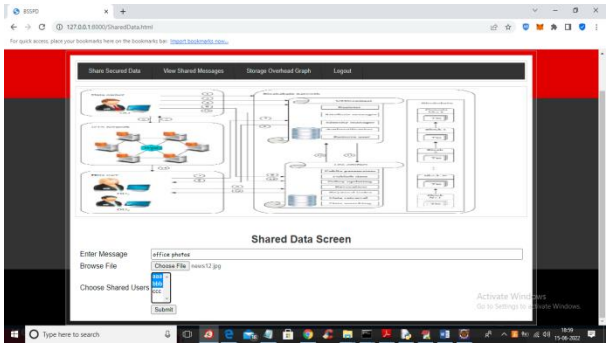

In above screen user is login and press button to get below output



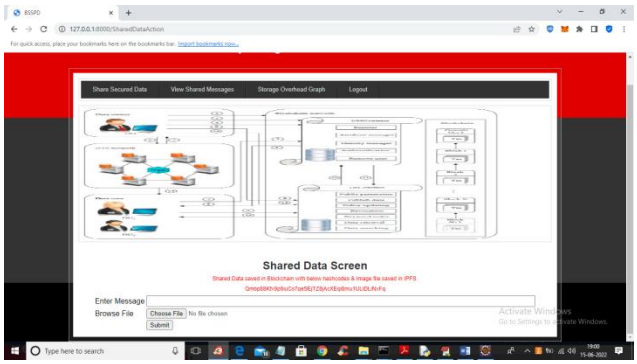

In above screen user logged in successfully and now click on 'Share Secured Data' link to share data with other users



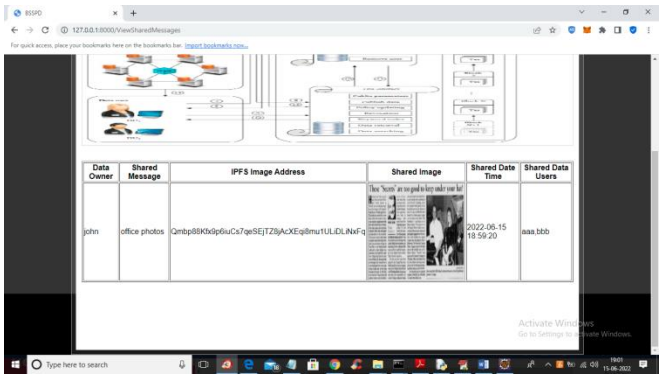

In above screen user can enter some message and then upload image and by holding CTRL KEY you can select names of users with whom you want to share this data and press button to get below output



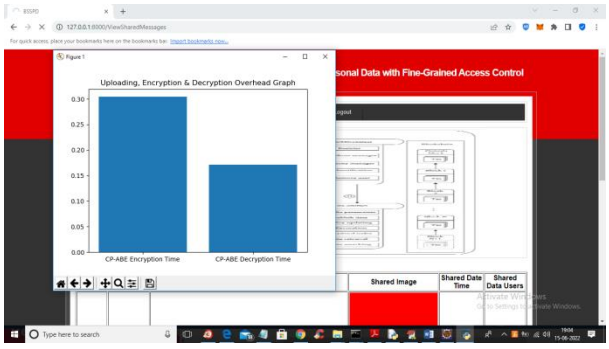

In above screen 'John' is sharing data with user 'aaa' and 'bbb' and both users can decrypt and view data but user 'ccc' cannot view it.



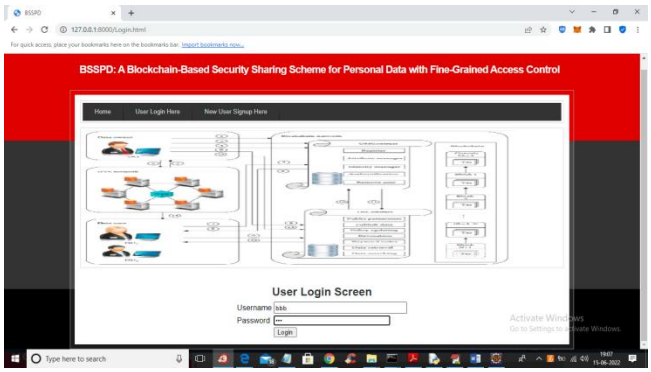

In above screen we can see sharing attributes stored at Blockchain and images and decryption keys stored at IPFS and now click on 'View Shared Messages' link to view own messages and other users shared messages so 'John' is the data owner so he can view his own upload and others shared data.



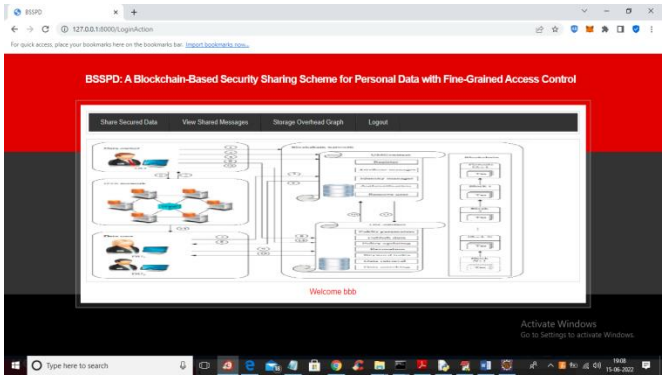

In above screen we can see data owner name, shared messages with IPFS address and we can see names of shared users list and now we can check weather aaa or bbb can view this data or not and now click on 'Storage Overhead Graph' link to view encryption and decryption time overhead



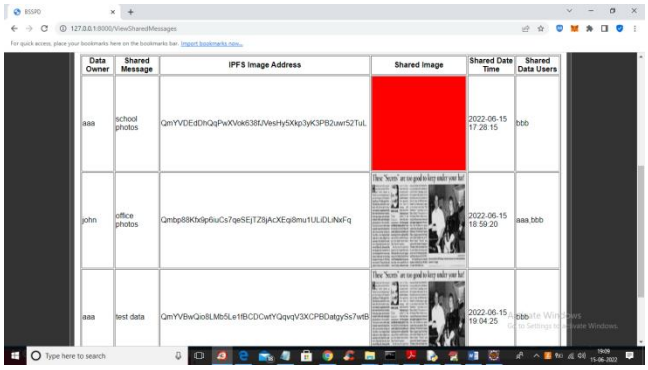

In above screen x-axis represents encryption and decryption and y-axis represents time overhead and now logout and login as 'bbb' user to view shared data.



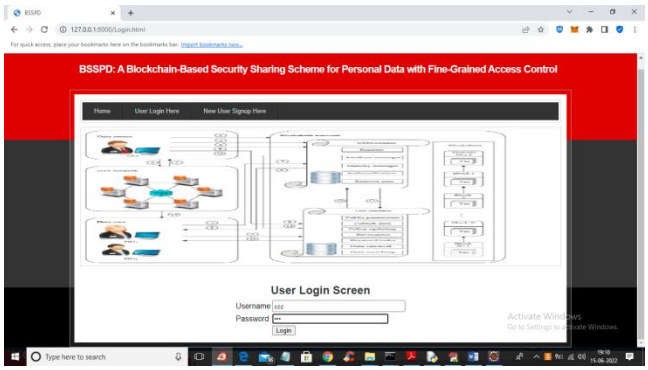

In above screen shared user ‘bbb’ is login and after login will get below output



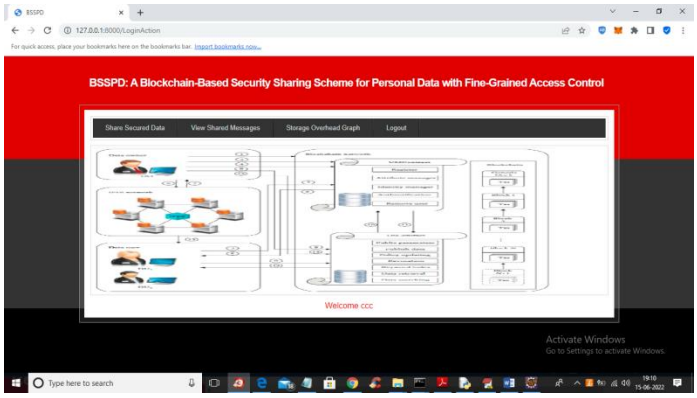

Now in above screen ‘bbb’ can click on ‘View Shared Messages’ link to view all users shared data



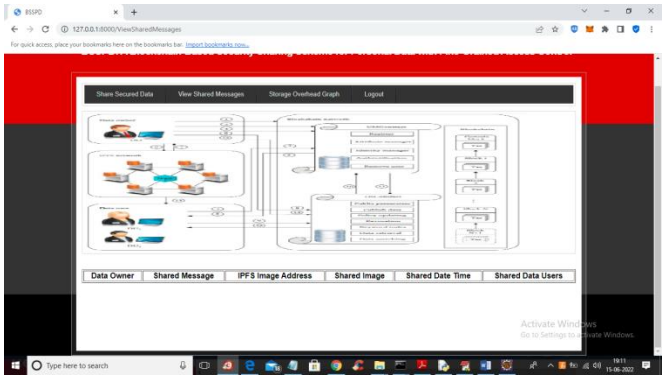

In above screen ‘bbb’ can view shared data from aaa and john and now logout and login as ‘ccc’ and nobody shared data with ‘ccc’ so he cannot access any data




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




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




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

## 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 finegrained 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 complete 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 [38–42]. 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.

## 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.