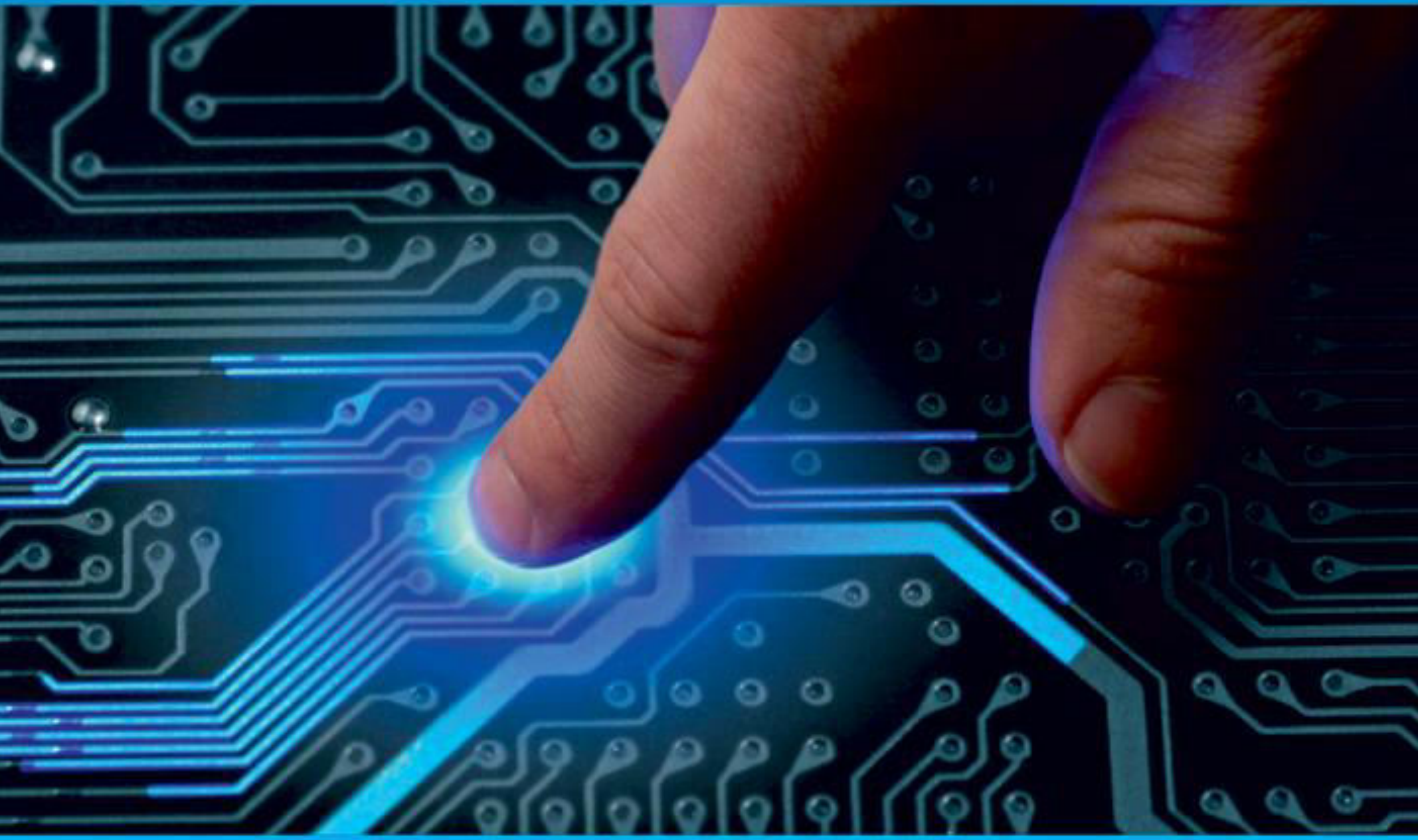
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

A Blockchain-Based Secure Decentralised Storage System

Dr. P. Ravinder Rao, G. Shiva Sai Balaji, K. Rahul, K. Sree Nailu

Assistant Professor, Department of Computer Science Engineering, Anurag University, Hyderabad Telangana, India

Department of Computer Science Engineering, Anurag University, Hyderabad 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, 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 shared 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.

KEYWORDS: IPFS, CSP, CP-ABE, BSSPD

I.INTRODUCTION

In the era of AI-driven data governance, safeguarding privacy while enabling open data sharing is paramount. Traditional data-sharing practices often entail uploading data to centralized cloud servers,relinquishing users' absolute ownership, and raising concerns about security and privacy. While encryption and access control technologies offer partial solutions,they still rely heavily on the credibility of third-party Cloud Service Providers (CSPs). To address these challenges,this paper proposes a Blockchain-Based Security Sharing Scheme for Personal Data (BSSPD). By integrating blockchain, ciphertext-policy attribute-based encryption (CP-ABE), and the InterPlanetary File System (IPFS), BSSPD offers a user-centric approach. Data owners encrypt and store their data on IPFS, ensuring maximum decentralization. Access addresses and decryption keys are encrypted using CP-ABE, allowing data owners to publish information and distribute keys via blockchain. This fine -grained access control mechanism enables only authorized users to download and decrypt data, with support for attribute-level revocation. To enhance privacy, ciphertext keyword search is employed during data retrieval. Security analysis and simulation on the EOS blockchain confirm the feasibility and performance of BSSPD, promising a revolutionary approach to secure, decentralized data storage and sharing across digital platforms.

II. RELATED WORK

This section will discuss previous research and solutions related to data security and privacy in decentralized storage systems. It would likely cover existing methods such as traditional encryption techniques, access control mechanisms, and blockchain-based solutions. It would also highlight the limitations and challenges of these approaches in fully addressing the privacy and security concerns associated with data sharing and storage**.**

III. EXISTING METHOD

Traditionally, data owners often resort to outsourcing their data to cloud servers for sharing and dissemination. However, this approach raises concerns about data security and privacy. While data encryption and access control technologies are utilized to mitigate these concerns, they still rely heavily on the credibility of third-party Cloud Service Providers (CSPs). Once data is uploaded to the server, the data owner loses absolute ownership, making security and privacy vulnerable.

This method involves users uploading their data to cloud servers, where it is stored and disseminated. However, this centralized approach poses risks to data security and privacy, as users relinquish control over their data to third-party CSPs. Despite efforts to implement encryption and access control mechanisms, reliance on CSP credibility remains a challenge.

IV. PROPOSED METHOD

The proposed method, named BSSPD (Blockchain-Based Security Sharing Scheme for Personal Data), aims to address the issues of data security and privacy in existing data-sharing solutions by leveraging blockchain technology, ciphertext-policy attribute-based encryption (CP-ABE), and the InterPlanetary File System (IPFS). Below are the key components and steps involved in the BSSPD scheme:

Decentralized Storage with IPFS:

- Data owners encrypt their sharing data and store it on IPFS, maximizing decentralization and ensuring data availability.
- Attribute-Based Encryption (ABE):
- The address and decryption key of the shared data are encrypted using ciphertext-policy attribute-based encryption (CP-ABE) based on specific access policies defined by the data owner.
- Fine-Grained Access Control:
- Data owners have fine-grained control over access to their data, specifying access policies based on attributes.
- Only data users whose attributes match the access policy can download and decrypt the shared data.
-

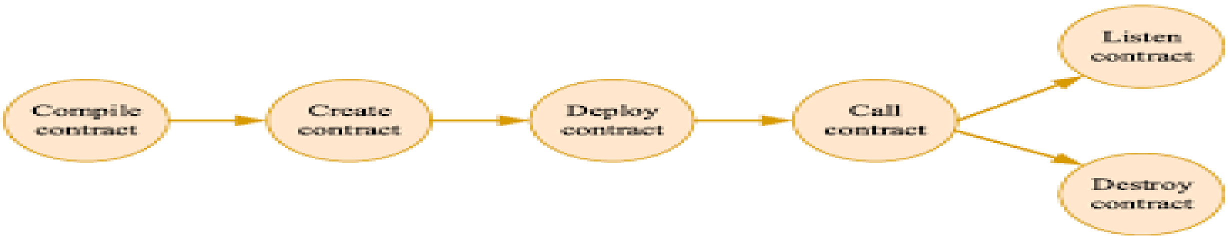


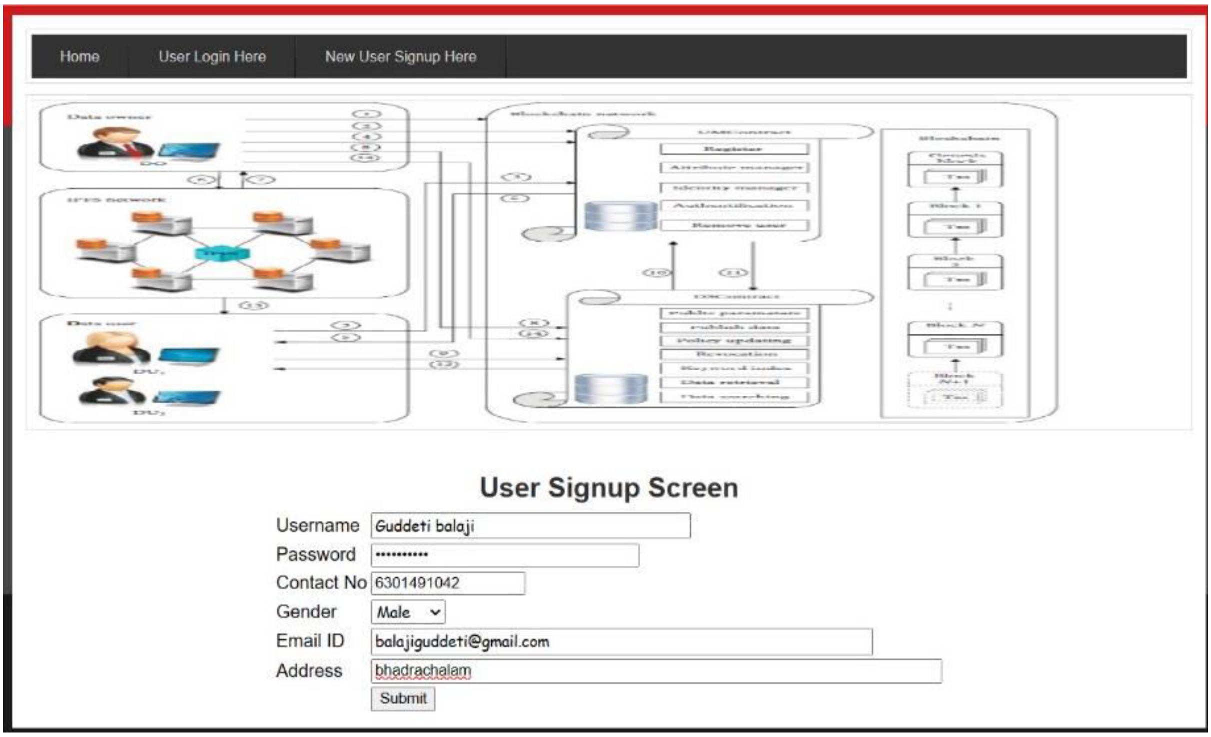
Fig 1: Flow Chart

V. SIMULATION RESULTS

The simulation of the BSSPD (Blockchain-Based Security Sharing Scheme for Personal Data) was conducted on the EOS blockchain to evaluate its feasibility and performance. The following are the key findings and results obtained from the simulation:

1. Feasibility Assessment:
   - The simulation confirmed the feasibility of implementing the BSSPD on the EOS blockchain.
2. Security Analysis:
   - The security analysis of the BSSPD revealed robust protection mechanisms against unauthorized access and data breaches.
   - The combination of blockchain, CP-ABE encryption, and IPFS storage provided a secure and decentralized platform for storing and sharing personal data.
3. Performance Evaluation:
   - The performance of the BSSPD was evaluated in terms of storage and computing overhead.
   - Results indicated that the scheme incurred reasonable overhead, demonstrating good performance in real-world deployment scenarios.

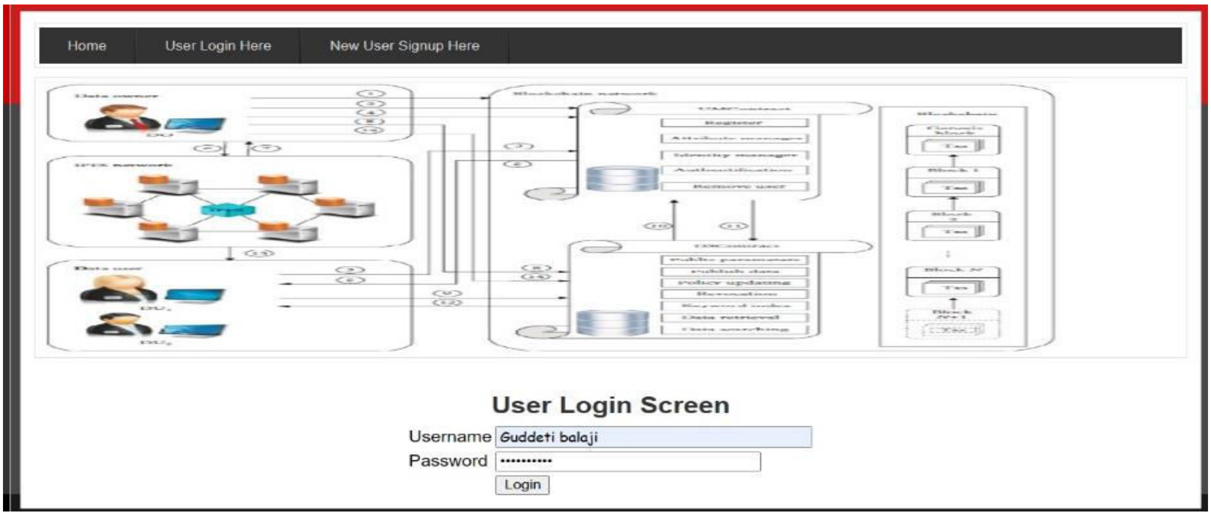
4. Storage Overhead:
   - The storage overhead refers to the additional storage space required to implement the BSSPD.
   - It was found that the storage overhead was manageable and did not significantly impact the overall storage efficiency of the system.
5. Computing Overhead:
   - Computing overhead refers to the additional computational resources needed to execute the BSSPD operations.
   - **The simulation showed that the computing overhead was within acceptable limits, ensuring efficient data processing and access control.**



User Signup Screen

Username: Guddeti balaji
Password: ••••••••••
Contact No: 6301491042
Gender: Male
Email ID: balajiguddeti@gmail.com
Address: bhadrachalam

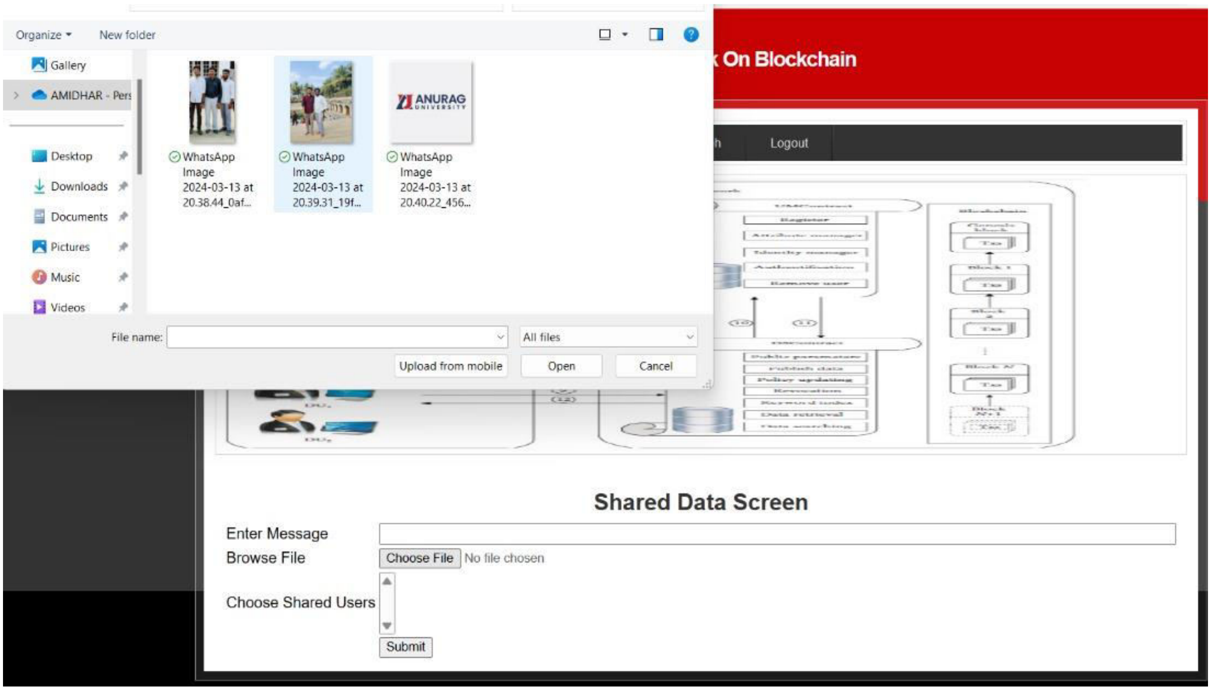
Fig:2.1: Signup Page



User Login Screen

Username: Guddeti balaji
Password: ••••••••••

Fig:2.2: Login Page



Shared Data Screen

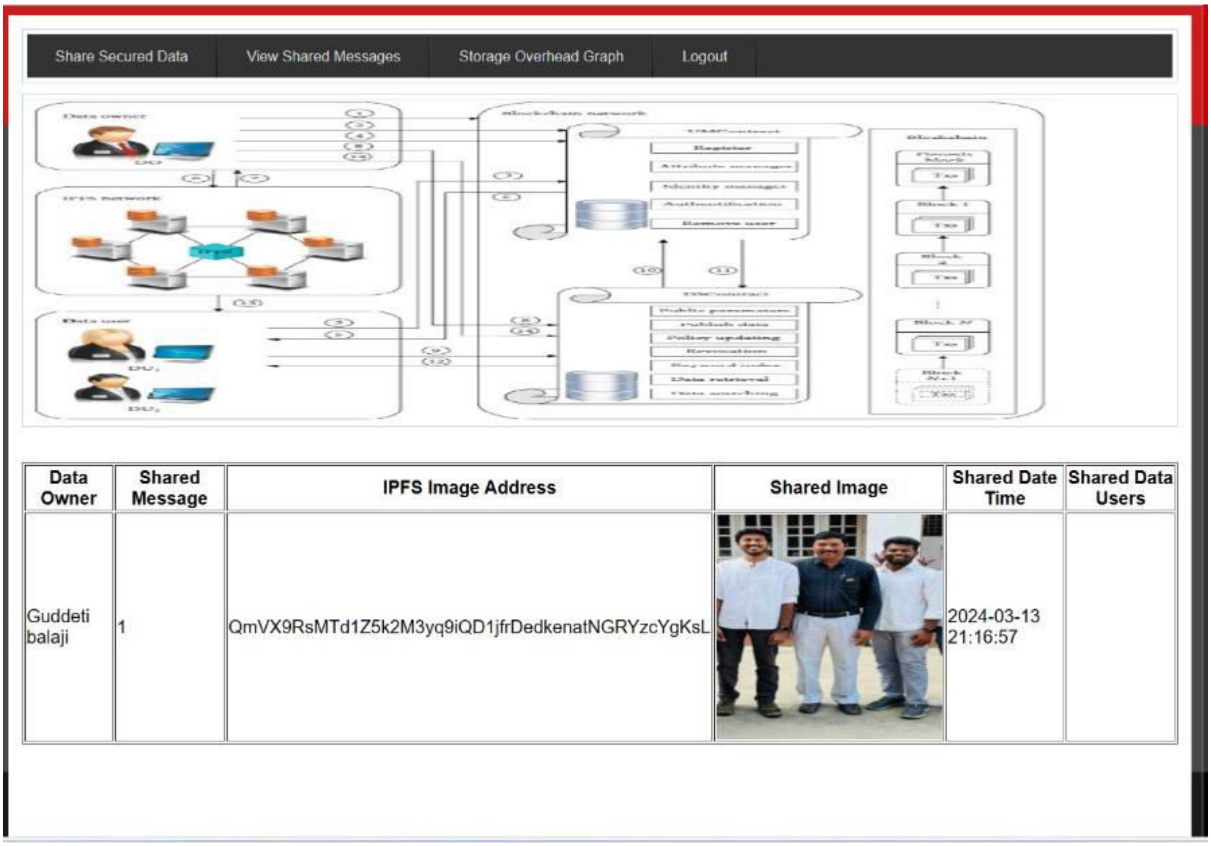
Enter Message

Browse File Choose File No file chosen

Choose Shared Users

Submit

Fig:2.3: Inserting data



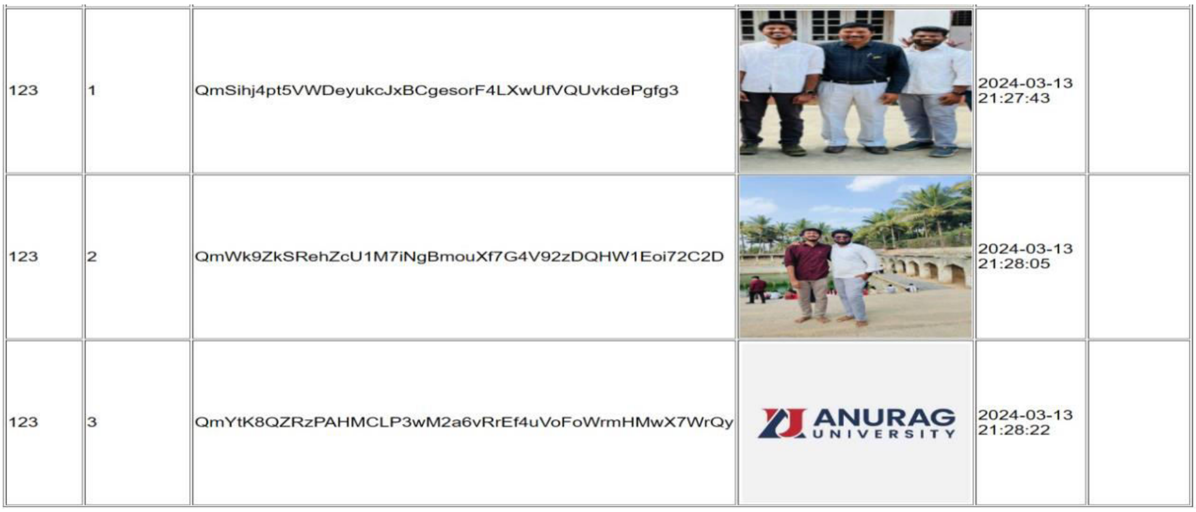
Data Owner	Shared Message	IPFS Image Address	Shared Image	Shared Date Time	Shared Data Users
Guddeti balaji	1	QmVX9RsMTd1Z5k2M3yq9iQD1jfrDedkenatNGRYzcYgKsL		2024-03-13 21:16:57	

Fig:2.4: Uploaded data

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204055 |



123	1	QmSihj4pt5VWDeyukcJxBCgesorF4LXwUfVQUvkdePgfg3		2024-03-13 21:27:43	
123	2	QmWk9ZkSRehZcU1M7iNgBmouXf7G4V92zDQHW1Eoi72C2D		2024-03-13 21:28:05	
123	3	QmYtK8QZRzPAHMCLP3wM2a6vRrEf4uVoFoWrmHMwX7WrQy	ANURAG UNIVERSITY	2024-03-13 21:28:22	

Fig:2.6: Data

VI. CONCLUSION AND FUTURE WORK

The BSSPD (Blockchain-Based Security Sharing Scheme for Personal Data) proposed in this paper offers a robust solution to the critical issues of data security and privacy in the era of AI-driven data governance. By combining blockchain technology, ciphertext-policy attribute-based encryption (CP-ABE), and the InterPlanetary File System (IPFS), BSSPD ensures decentralized storage, fine-grained access control, and attribute-level revocation of data users. Through encryption and decentralized storage on IPFS, data owners retain absolute control over their data, mitigating dependence on third-party Cloud Service Providers (CSPs). The scheme's user-centric approach and support for ciphertext keyword search further enhance privacy protection. Simulation on the EOS blockchain demonstrates the feasibility of BSSPD, while comprehensive analysis confirms its performance and security.

Future research could focus on enhancing the scalability and interoperability of BSSPD to accommodate larger datasets and integrate seamlessly with other blockchain-based systems. Improvements in the efficiency of attribute revocation mechanisms and optimization of storage and computing overheads could further enhance the scheme's performance. Additionally, exploring the integration of advanced cryptographic techniques and exploring potential applications in specific domains like healthcare or finance could extend the utility and impact of BSSPD. Continuous evaluation and refinement are essential to adapt BSSPD to evolving technological and regulatory landscapes, ensuring its relevance and effectiveness in safeguarding data privacy and security in the digital age.

REFERENCES

[1] SARA ROUHANI AND RALPH DETERS "Data Trust Framework Using Blockchain Technology and Adaptive Transaction Validation"
https://ieeexplore.ieee.org/document/9461755

[2] Z. Su, Y. Wang, Q. Xu, and N. Zhang, "LVBS: Lightweight vehicular blockchain for secure data sharing in disaster rescue"
https://ieeexplore.ieee.org/document/9035635

[3] X. Zheng, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Mere, "Blockchain-based personal health data sharing system using cloud storage"
https://ieeexplore.ieee.org/document/8531125

[4] J. An, J. Cheng, X. Gui, W. Zhang, D. Liang, R. Gui, L. Jiang, and D. Liao, "A lightweight blockchain-based model for data quality assessment in crowdsensing"
https://ieeexplore.ieee.org/document/8956067

[5] B. Shala, U. Trick, A. Lehmann, B. Ghita, and S. Shiaeles, "Blockchain and trust for secure, end-user-based and decentralized IoT service provision"
https://ieeexplore.ieee.org/document/9127445

[6] J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, "A blockchain based privacy-preserving incentive mechanism in crowdsensing applications"
https://ieeexplore.ieee.org/document/8306424

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com