2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA) | 978-1-6654-9707-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICIRCA54612.2022.9985510

Reliable Data Storage and Sharing using Block chain Technology and Two Fish Encryption

S. Sivanantham
Assistant Professor
Dept. of Computer Science and Systems Engineering
Sree Vidyanikethan Engineering College
Tirupati, Andhra Pradesh, India
sivanantham.s@vidyanikethan.edu

M. Sakthivel
Professor
Dept. of Computer Science and Engineering
Sree Vidyanikethan Engineering College, Tirupati,
Andhra Pradesh, India
sakthivel.m@vidyanikethan.edu

V. Krishnamoorthy
Assistant Professor
Dept. of Computer Science and Engineering
Bannari Amman Institute of Technology
Sathyamangalam, Tamilnadu, India
krishnamoorthy.v@bitsathy.com

N. Balakrishna
Assistant Professor
Dept. of Computer Science and Engineering
Sree Vidyanikethan Engineering College Tirupati, Andhra Pradesh, India
balakrishna.n@vidyanikethan.edu

V. Akshaya
Assistant Professor
Dept. of Computer Science and Engineering
Sree Vidyanikethan Engineering College Tirupati, Andhra Pradesh, India
akshaya.v@vidyanikethan.edu

***Abstract*— Digital data that has been certified by a respected institution is valuable and can be saved or transmitted over the internet. However, the issues are ensuring the security and reliability of stored and shared data, as well as ensuring a secure, transparent, and fair data sharing process. As a result, The schemas for data production, storage, and sharing is suggested. A group signature scheme in the data production schema for a collection of respected organisations that provide similar services is used. A member of the group develops precious digital data from RD (raw data) provided by a DO (data owner) and then provides a certification based on the encipher of that data. The system saves the data's access address in the database after data owner uploading his or her data to the system in the data storage schema. Before submitting a data sharing proposal to the DO, every person on the system might validate the quality of shared data. The data sharing mechanism is carried out via a smart contract to incentivize honesty. The schemas assure the security properties of data storage and exchange, which include confidentiality, integrity, privacy, and non-repudiation.**

Keywords— Block Chain mechanism, Two Fish algorithm, Data Storage, Data Sharing, Interplanetary File System, Decentralized Storage.

I. Ease of Use

Data has grown at an exponential rate around the world, and individuals and organisations consider trusted data to be one of their most important assets. By 2025, the amount of data created and stored on the planet is expected to reach 175 petabytes. As a result, there is a huge need for important data storage and sharing, which raises data security difficulties in the data storage and sharing procedures. For data storage and sharing, there are currently two basic architectures: centralized and decentralized structures.

Organizations can store the data on their data centre system in a centralized architecture. These systems, on the other hand, have substantial operational costs and limited scalability [1]. Cloud storage services can save money and provide for more flexibility in system growth, making them ideal for IoT systems. It's still a work in progress to combine IoT and cloud storage services. The Murat et al. [2] presented a system with the intention of protecting sensitive data that's saved in databases, encryption techniques and to guarantee the privacy and security of data storage and sharing access control mechanisms are proposed. The centralised architecture, on the other hand, has two drawbacks: one of them is data security; without authorisation, system administrators or hackers could see, modify, or withdraw stored data who have gained access to the system. Users are unable to access services when centralised systems fail owing to system overload or network faults.

Most decentralised architecture solutions leverage block-chain (BC) technology as the main component in the systems to provide attributes such as anonymity, transparency, decentralisation, and auditability. [3]. How accurate and dependable is the data shared on the BC network? Meaningful data is defined as data that has been validated and certified by a reputable organisation (RO). In the medical field, for example, a diagnosis report from a recognised medical organisation with highly qualified doctors publishes an electronic medical record. A data owner (DO) can sell or entirely share his or her meaningful data with other people or organisations on the network, but his or her meaningful data must be kept safe on the system. Before opting to implement a data-sharing contract, requesters could be able to check the trustworthiness and quality of shared data as part of the data-sharing procedures. The security of shared data is based on mutual trust between the two parties involved in the traditional data sharing technique. Doctors and hospitals, for example, have a strong belief in the integrity of medical records obtained from their patients. Furthermore, the identities of everyone engaged in the sharing process should be kept private, and submitted data must be validated for reliability while respecting the privacy of the material.

Data storage and sharing for verified digital data is vital, demanding solutions to satisfy all of the following conditions:

In data storage: Certificate authorities on stored data, anonymity and DO's privacy must be maintained; Confidentiality and integrity of stored data in the system should be ensured.

For data sharing: That everybody in the system may evaluate the reliability of shared data before sending a sharing request to data owner. It's worth noting that anyone can only verify the accuracy of the shared data. Accessibility, security, and scalability are all requirements for data storage and sharing systems.

Currently available options, on the other hand, do not match all of the above criteria. In this paper, we offer data-producing, data-storage, and data-sharing systems. We regard reputable organization to be a DP, and data providers who provide similar services form a group. A GM puts up a group of data providers that deliver same sort of service in the data producing scheme. A specific DP in the group converts DO raw data into MD. Then, using a symmetric technique, DP encrypts MD. DP then creates a certificate based on the meaningful data cipher text. Finally, DO will receive electronic meaningful data, certificate, and data provider's details. DO saves electrical meaningful data on the Inter-Planetary File System (IPFS) as part of the data storage strategy. The GM uses a smart agreement for data-sharing, which assures that procedure is secure, transparent and reasonable for all members. Before completing the data-sharing smart agreement, the Data User (DU) can check up and verify the quality and correctness of shared data.

The following is an overview of our contributions to this paper:

We offer a data production strategy that ensures MD received via DP is 100% correct and reliable. This approach could secure DP's anonymity while also ensuring DO's privacy.

We propose a data storage technique that combines BC and IPFS to create a safe storage system.

II. RELATED WORK

The present block chain based data storage and sharing options are characterised by the use of block chain technology to store tiny data such as policies for access control, shared data access addresses and management information. Meanwhile, centralized or decentralized systems are used to store shared data.

Before being delivered to the provider of data storage services, data is encrypted using a cryptographic technique for the centralized storage options given. Data privacy can be kept in this preserved, however data availability is dependent on the service provider. A decentralized storage network called IPFS is proposed in [4] to alleviate the shortcomings of the centralized storage approach.

A mechanism for sharing personal health data based on block chain, machine learning and cloud storage approaches was presented by Zheng Xiao hen et al [5]. Before being shared, personal health data is reduced and encrypted being stored on the cloud, and clients can search for data they are interested in purchasing. Secret keys are transferred over an authenticated communication channel from key keepers, or key keepers to consumers. However, because the processes of sharing rely on a middleman, such as key keepers, verifier the abovementioned solutions are still manual.

Researchers [6] developed a block chain based data sharing service that respects users privacy and the privacy of EMRs sharing, in which medical data access control policies are established by owners using smart agreements. However, before requesting patients' EMRs, in this system there is no way for anyone in the block chain network to validate the correctness and trustworthiness of medical information.

Smart agreements are utilised to provide access information to participants and IPFS is used for the peer to peer data transfer methods outlined. A buyer, on the other hand, cannot evaluate the data's reliability before filing a data access permission or completing a smart contract escrow payment [7].

III. BACKGROUND

A. BLOCKCHAIN

A block chain [3] is a continuously expanding list of data chunks that are connected together via encryption. Each data block contains the cryptographic hash code of the previous block, as well as a timestamp and the contents to be delivered. A block chain's data structure varies from that of a normal database. A block chain splits data into chunks, each one holds a set of information. When a block's storing capacity is exceeded, it is closed and connected to the preceding block, creating the block chain, which is a data chain. After the freshly inserted chunk is filled, total additional information is combined into a new chunk, which is then inserted to the chain. The block chain does not allow for data modification. When data in a block is altered, it impacts subsequent blocks, and hence the entire block chain.

B. TWOFISH

Twofish is a block cipher technique that uses a single key to encode and decrypt data and information [8]. It accepts both the key and the textual information. After that, the data is turned to ciphertext, which can't be read without decryption. The encrypted data is given to the recipient, either before or after the ciphertext, together with the encryption key [9]. The user can use this key to decrypt the information that has been encrypted.

Twofish is distinct from other cryptographic algorithms in that one of its fundamental aspects is the use of key-dependent, pre-computed substitution boxes (S-boxes). The S-box hides the key's ciphertext link.

C. IPFS

The IPFS [10] is a collection of distributed file system with peer-to-peer communication protocols that keeps track of everything using a DHT (distributed hash table). The IPFS preserves data regardless of the size, resulting in a unique hash. IPFS could save hash, it can be used afterwards by third parties to data retrieval [11]. When the data is ready to be posted to the IPFS network, it will be split down into multiple small bits [12]. To identify each item, it has its own hash.

IV. THE PLANS PROPOSED

We will present the system model and proposed schemes in this part:

A. SYSTEM MODEL

Our system model is shown in Figure 1. In our project, there are four parties.

(i) Data owner: A data owner (DO) is someone who has raw data (RD) and gives it to a certain DP in order to generate MD. DO has an option to have his information preserved and shared MD.

(ii) A group of DPs: Each data provider in an organisation that has the role and means of producing meaningful data from the data owner's raw data, and each data provider is produced by the group manager. Because DP does not own MD, he has no authority to provide or utilise it without DO's permission. The group's DPs all offers similar services.

(iii) Data user: A data user is a person or organisation who wants to utilize DO's meaningful data.

(iv) Decentralized storage (DS): Decentralized storage is responsible for storing electronic meaningful data and returning the address to data user. As a DS, we use a public IPFS.

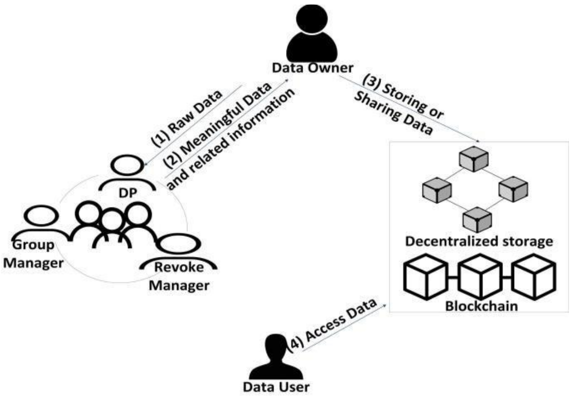


Fig 1 General System Model

. As shown in fig.2 our system offers Data Producing, Data Storage, and Data Sharing defined as follows: •

- Data Producing: This is a procedure that is done manually that takes RD from DO as input and outputs meaningful data as well as some related data (generated by data provider) to data owner.
- Data Storing: It stores electrical meaningful data on interplanetary file system and a store access address of electronic meaningful data and as input, the relevant data from data owner.
- Data Sharing: It checks MD's trustworthiness and performs the smart contract allowing DU to acquire MD with DO.

V. SECURITY ANALYSIS

A. *Confidentiality*

Meaningful data is encrypted for uploading to IPFS in the data storage mechanism using the secret key provided by data provider [13]. To get MD's content, requestors must have the secret key to decode it. As a result, determining the confidential key needed to decode and extract meaningful data from interplanetary file system is incredibly challenging.

B. *Integrity*

The EMD is verified by DP so its integrity is verified in the data-sharing scheme. DO can thus alter meaningful data to generate a new kind of meaningful data, but it will be unable to secure a valid certificate for it since it lacks a group manager key [14].

C. *Privacy*

Through data stored on the IPFS, anybody can evaluate the correctness and integrity of MD, but no one can analyse its content or determine which DP in the DO's group utilised the service [15].

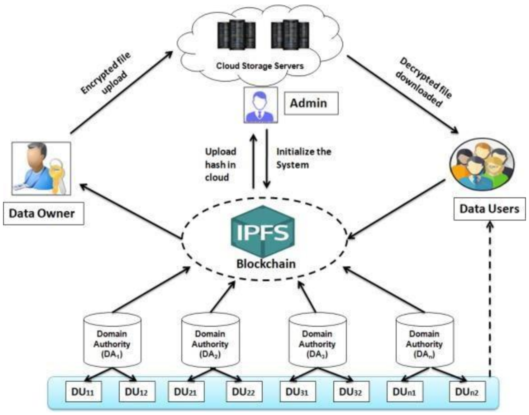
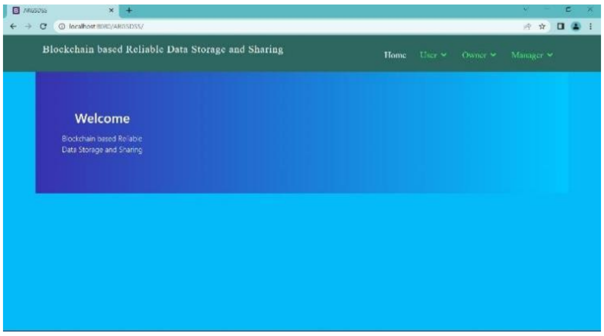


Fig 2. IPFS based decentralized system.

VI. RESULTS

The implementation results for reliability data using block chain technology concept is as follows: Fig.3 shows the frontend webpage of it. In data owner side as shown in Fig.4 have an option to upload files and which are encrypted in backend[16].


Blockchain based Reliable Data Storage and Sharing

Welcome

Blockchain based Reliable Data Storage and Sharing

Fig. 3. Web design of system

After uploading the data file to the system the cipher text of encrypted file and hash value of the data file is stored in the cloud for security. And also data provider will certify the reliability of data [17].

Data owner needs to accept the user requests if user need to access the data file as shown in Fig5.

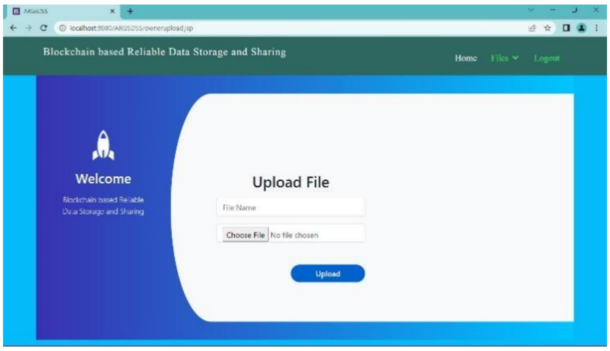
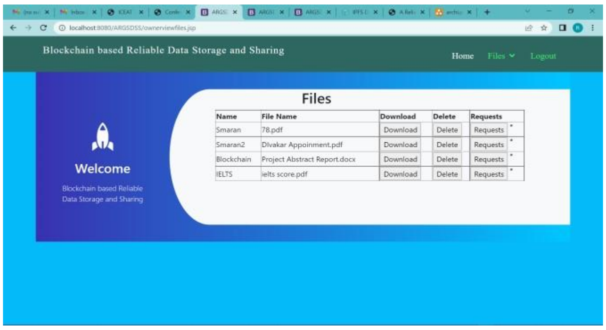

ARGSDSS
localhost:8080/ARGSDSS/ownerupload.jsp
Blockchain based Reliable Data Storage and Sharing
Home
Files
Logout
Welcome
Blockchain based Reliable Data Storage and Sharing
Upload File
File Name
Choose File
No file chosen
Upload

Fig. 4. Owner side interface

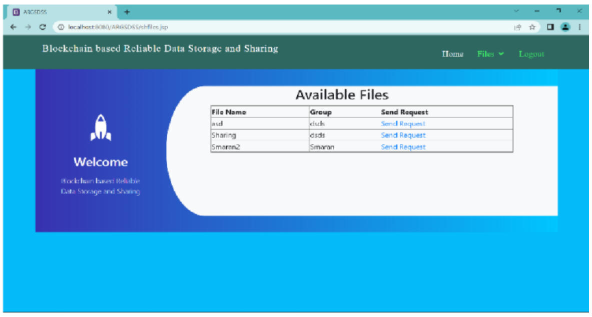
In user side have an option to request shared files as shown in Fig.6 and user can download the decrypted file after the acceptance of the owner [18], [19].


localhost:8080/ARGSDSS/ownerviewfiles.jsp
Blockchain based Reliable Data Storage and Sharing
Home
Files
Logout
Welcome
Blockchain based Reliable Data Storage and Sharing

Files

Name	File Name	Download	Delete	Requests
Smaran	78.pdf	Download	Delete	Requests
Smaran2	Divakar Appoinment.pdf	Download	Delete	Requests
Blockchain	Project Abstract Report.docx	Download	Delete	Requests
IELTS	ielts score.pdf	Download	Delete	Requests

Fig 5 Data file requests from users


ARGSDSS
localhost:8080/ARGSDSS/shfiles.jsp
Blockchain based Reliable Data Storage and Sharing
Home
Files
Logout
Welcome
Blockchain based Reliable Data Storage and Sharing

Available Files

File Name	Group	Send Request
asd	dsds	Send Request
Sharing	dsds	Send Request
Smaran2	Smaran	Send Request

Figure 6 User side interface

VII.CONCLUSION

In this study, we present data-producing, data-storage, and data-sharing methodologies. We consider reputable organization to be a data provider in the data-producing system, and a GM creates a group of data providers that provide the similar services. After receiving raw data from data owner, data provider can build meaningful data and issue an electronic meaningful data certificate.

We guarantee not only the data's security and integrity, but also DO's privacy, which are not currently provided by other solutions.

Before submitting a data sharing request to data owner, everyone on the system can validate the correctness of shared data using the data sharing scheme. It's worth noting that anyone can only check the supplied data's reliability, not read its contents. Existing solutions were unable to meet this requirement. Furthermore, data is transferred directly between DO and DU, with no intermediaries involved.

According to the findings of the security analysis, the proposed schemes fulfil the security attributes of secrecy, integrity, and privacy.

We can use this proposed technology in the future for specialised applications like IoT and electronic medical records.

The schemes will then be evaluated and optimized.

REFERENCES

[1] D. Reinsel, J. Gantz, and J. Rydning, ''The digitization of the world from edge to core,'' IDC White Paper, Nov. 2018.

[2] M. F. Bari, R. Boutaba, R. Esteves, L. Z. Granville, M. Podlesny, M. G. Rabbani, Q. Zhang, and M. F. Zhani, ''Data center network virtualization: A survey,'' *EEE Commun. Surveys Tuts.*, vol. 15, no. 2, pp. 909–928, 2nd Quart., 2013.

[3] L. Jiang, L. D. Xu, H. Cai, Z. Jiang, F. Bu, and B. Xu, ''An IoT-oriented data storage framework in cloud computing platform,'' *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1443–1451, May 2014.

[4] T. A. Phan, J. K. Nurminen, and M. Di Francesco, ''Cloud databases for Internet-of-Things data,'' in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom)*, Sep. 2014, pp. 117–124.

[5] K. Yasumoto, H. Yamaguchi, and H. Shigeno, ''Survey of real-time processing technologies of IoT data streams,'' *J. Inf. Process.*, vol. 24, no. 2, pp. 195–202, 2016.

[6] A. Kumar, N. C. Narendra, and U. Bellur, ''Uploading and replicating Internet of Things (IoT) data on distributed cloud storage,'' in *Proc. IEEE 9th Int. Conf. Cloud Comput. (CLOUD)*, Jun. 2016, pp. 670–677.

[7] K. Hossain, M. Rahman, and S. Roy, ''IoT data compression and optimization techniques in cloud storage: Current prospects and future directions,'' *Int. J. Cloud Appl. Comput.*, vol. 9, no. 2, pp. 43–59, Apr. 2019.

[8] J. D.Bokefode, A. S.Bhise, P. A. Satarkar,and D. G.Modani, ''Developing a secure cloud storage system for storing IoT data by applying role based encryption,'' *Procedia Comput. Sci.*, vol. 89, no. 1, pp. 43–50, 2016.

[9] W.Wang,P.Xu,andL.T.Yang,''Securedatacollection,storageandaccess in cloud-assisted IoT,'' *IEEE Cloud Comput.*, vol. 5, no. 4, pp. 77–88, Jul. 2018.

[10] M. Rashid, S. A. Parah, A. R. Wani, and S. K. Gupta, ‘‘Securing Ehealth IoT data on cloud systems using novel extended role based access control model,’’ in *Internet Things (IoT)*. Cham, Switzerland: Springer, pp. 473–489, 2020.

[11] Bhalaji, N. "Reliable Data Transmission with Heightened Confidentiality and Integrity in IOT Empowered Mobile Networks." *Journal of ISMAC,* Vol. 2, no.2, pp.106-117, 2020.

[12] Andi, Hari Krishnan. "Estimating the Role of Blockchain, Deep Learning and Cryptography algorithms in Cloud Security," *Journal of Trends in Computer Science and Smart Technology,* vol.3, no. 4, pp.305-313, 2021.

[13] Kitsantas, Thomas Vazakidis, Athanasios & Chytis, Evangelos, “A Review of Blockchain Technology and Its Applications in the Business Environment,” *International Conference on Enterprise, Systems, Accounting, Logistics & Management*, *Greece*, 2019.

[14] Xiaohu Zhou, Antonio Nehme, Vitor Jesus, Yonghao Wang, Mark Josephs, Khaled Mahbub, Ali Abdallah, “AudiWFlow: Confidential, collusion-resistant auditing of distributed workflows,” *Blockchain: Research and Applications,* Vol. 3, No. 3, 2022.

[15] H. R. Andrian, N. B. Kurniawan and Suhardi, "Blockchain Technology and Implementation: A Systematic Literature Review," *International Conference on Information Technology Systems and Innovation (ICITSI)*, pp. 370-374, 2018.

[16] Akshaya V, Sathyapriya M, Ranjini Devi R, Sivanantham, S, “Detecting Credit Card Fraud Using Majority Voting-Based Machine Learning Approach”, *In: Reddy, V.S., Prasad, V.K., Mallikarjuna Rao, D.N., Satapathy, S.C. (eds), Intelligent Systems and Sustainable Computing. Smart Innovation, Systems and Technologies*, vol 289, Springer, Singapore, 2022.

[17] Sivanantham S, Dhinagar S.R, Kawin P, Amarnath J. “Hybrid Approach Using Machine Learning Techniques in Credit Card Fraud Detection*”. In: Suresh, P., Saravanakumar, U., Hussein Al Salameh, M. (eds) Advances in Smart System Technologies, Advances in Intelligent Systems and Computing*, vol 1163. Springer, Singapore, 2021.

[18] Sakthivel M, Sivanantham S, Kamalraj R & Krishnamoorthy V, “An Analysis of Machine Learning Depend on Q-MIND for Defencing the Distributed Denial of Service Attack on Software Defined Network”, *International Journal of Early Childhood Special Education*, vol. 14, no. 05, pp.3769 – 3776, 2022.

[19] Siva Kumar Depuru & K.Madhavi , “Autoencoder Integrated Deep Neural Network for effective analysis of malware in distributed Internet of Things (IoT) Devices”, *The International journal of analytical and experimental modal analysis,* vol.9 , no.8 , pp.226 – 232, 2019.