

Optimizing blockchain technology using a data sharing model

Israa Nazeeh¹, Teeb Hussein Hadi², Zainab Qahtan Mohammed¹, Shaymaa Taha Ahmed¹,
Qusay Kanaan Kadhim³

¹Department of Computer Science, College of Basic Education, University of Diyala, Diyala, Iraq

²IT Department, Technical College of Management, Middle Technical University, Baghdad, Iraq

³Department of Computer Techniques Engineering, Bilad Alrafidain University College, Baqubah, Iraq

Article Info

Article history:

Received Jul 12, 2022

Revised Sep 13, 2022

Accepted Sep 30, 2022

Keywords:

Blockchain technology

Data sharing model

Network

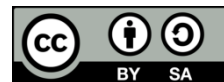
Optimization

Security

ABSTRACT

The improvement of different data-sharing technology has increasingly permeated many industries as technology continues to improve. As a result, for the value of the data to be realized, data sharing and security are essential. However, a fundamental data sharing mechanism is difficult to check for electronic data usage traces. Furthermore, data providers' unwillingness to provide their data is a challenge. Taking use of the dispersed ledger, smart contract, data trust, and traceability aspects of blockchain technology. This research presents a data-sharing model based on blockchain technology optimizing to overcome the challenges in terms of security and control, of conventional centralized data sharing and management, enabling safe access to the data as a result. Moreover, the research assesses the prototype's usefulness and security. Additionally, this paper suggests a method for using blockchain technology to optimize the efficiency of data sharing. This study showed that data sharing via the blockchain technology paradigm proposed in this work is feasible, secure, controllable, and efficient. This was demonstrated in a novel way employing blockchain technology.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Shaymaa Taha Ahmed

Department of Computer Science, College of Basic Education, Diyala University

Diyala, Iraq

Email: mrs.sh.ta.ah@gmail.com

1. INTRODUCTION

In recent years, data have played a crucial part in both peoples' social lives and scientific study, due to the ongoing growth of big data and the internet technologies, and documents dissemination and sharing require increasingly grown in importance as a tool for advancing both social and scientific advancement. Promoting the national big data plan requires secure data interchange. In today's culture, tremendous societal shifts have occurred as a result of the massive infusion of resources into production and living that the convergence of knowledge has produced. Businesses that utilize big data to significantly help society and the economy include those that employ medical data [1], [2], financial documents [3], [4], power data [5], as well as meteorological data [6], [7]. While the development of big data technologies has made life more convenient for people, various data security issues have also been brought up [8], [9]. The constant occurrence of security events like data management security borders and resource theft is one of the most significant issues [10], [11]. Resource hurdles that have been created as a result of data security, and realizing the value of data can be challenging due to business considerations and privacy issues, additionally, the financial benefits of comparing various forms of data do not fully materialize. However, due to technical limitations, the majority of current options for sharing data cannot maintain data security [12], [13]. Common sharing data practices rely on a centralize store and server, which has several weaknesses. First off, central administration gives managers a

lot of control, which might result in internal data breaches. Additionally, centralized servers can be hacked; creating a single point of failure, and the entire system becomes inaccessible when the server goes down. However, due to poor administration, the centralized service may be discontinued, all user data was lost, and there was no guarantee of data protection. Finally, customers are forced to use a third-party platform, which is incredibly hazardous and insecure, under the outdated data sharing approach. To sufficiently secure data security.

The majority of conventional data-sharing methods demand offline transmission. The disadvantage is that it lacks realism and is vulnerable to severe issues such as loss of data. With the current advancements in technology and the internet, the most common method of data transport is now through online sharing of data [14]. Online data transfer offers clear advantages in terms of timeliness when compared to offline data transmission techniques [15]. Furthermore, as the volume of data mostly on internet increases, data security storage will become more important, sharing data with security, and sharing data effectively. As a result, traditional data transmission methods struggle to fulfill the needs of today's data privacy and security. The decentralized, auditable system in this regard blockchain is an intriguing technology to research for data sharing due to its immutability and tamper-proof features. On the other hand, the prerequisites for secure and effective data exchange are not met by simply combining blockchain with data sharing.

Blockchain-based data-sharing and distribution has been the subject of numerous studies, but they have produced many intriguing results. It searches encrypted data on a malicious server while disregarding perfectly alright data constraints [4], [16]. For the goal of exchanging electronic medical records, Zhang and Lin created combined private and federation chain topologies, however, cross-chain behavior and the usage of searchable public key-based encryption are ineffective in practice [17], [18]. A trustworthy data sharing platform was developed by Su *et al.* [19] such as off-chain communication and on-chain storage, where the actual data is delivered securely and for shared data, the request and responses records are open [19]. To some extent, this design can relieve the issues of system execution and privacy preservation. To overcome the challenge of blockchain huge data storage, A two-chain structured infectious illness data sharing architecture was presented by Qiu and Zhu. This employs interplanetary file system (IPFS) storing and, to some extent, safeguards data security and privacy [20]. Blockchain might be used to communicate personal health data, by Li and Sato [20] ensures that personal data is made public and provides privacy protection while encouraging users to provide relevant data [21]. To protect data privacy [21]. recommended using blockchain and fine-grained access control, employing an interplanetary file system for data content storage, and executing key management and authorization checks on blockchain nodes [22].

Secure data storage and data security management are two crucial research areas for blockchain-based sharing studies. In order to establish a secure data storage system for peer-to-peer transactions that is transparent and safe. Blockchain technology was employed by Nuss *et al.* [23]. To prevent the host from tampering with the data on the blockchain, this design leverages proof of storage, however, the data isn't encrypted or decrypted before being uploaded to the storage component, putting user data's secrecy and privacy at risk. To safely and openly share health-related data, [23] employed blockchain technology. To verify the dataset's integrity, they employed pointers to the dataset's location and a cloud server to store the data in an encrypted fashion [24], [25]. A centralized access control system that makes use used to confirm a user's system access is legitimate, employ ciphertext policies attribute based encryption and a blockchain was proposed by Zhang and Lin [26] used distributed attribute ciphertext encryption and blockchain technology to protect user privacy, blockchain transactions contain data relating to algorithms, and associated algorithms are run on a blockchain networks [27]. Because it concentrates the control of feature administration in the control the skilled attribute authority and decentralizes the authority of a single attribute responsibility, this method of privacy protection is preferable for attribute management, preventing a scenario where one authority has too much power and makes unlawful decisions. Furthermore, because of how attribute-related data is provided through transaction data, this method is limited and prevents the identification of dynamic environmental characteristics at the moment of user request. Throughout their life for different IoT devices, a security management approach built on blockchain technology was developed by [27] By fusing blockchain platforms and input devices as network technology [26]. created backends that replace conventional backend systems while providing high availability, security, and anonymity.

Finally, based on current study on blockchain data sharing, the key issues are the limitations of being non-scalable when employing centralized storage as additional storage, due to blockchain's limited store capacity; it has poor disaster tolerance and expensive human maintenance expenses. Furthermore, the information provided to the supplemental blockchain store is not protected from disclosure, may be used to establish shared security access to data, but the data's confidentiality cannot be maintained. To address the security concerns with the standard data-sharing method. The study proposes replacing the current architecture for data sharing using network servers with a blockchain-based sharing data security paradigm.

2. BLOCKCHAIN TECHNOLOGY

Blockchain technology is built on a shared distributed database with a chain data structure. Figure 1 illustrates the block data structure. A block head and a block body are the basic components of a block, with hash pointers in sequence forming blocks [28].

Smart contracts, peer-to-peer networks, distributed consistent protocols, and cryptography, among other technology are used to construct the blockchain public ledger, which is decentralized, tamper-proof, traceable, and visible. It's distributed, track able, and available to the public. The issues with centralized data sharing, such as the common occurrence of single points of failure, may be efficiently addressed by integrating blockchain technology with data dissemination and sharing. This approach also offers a wide range of possible applications.

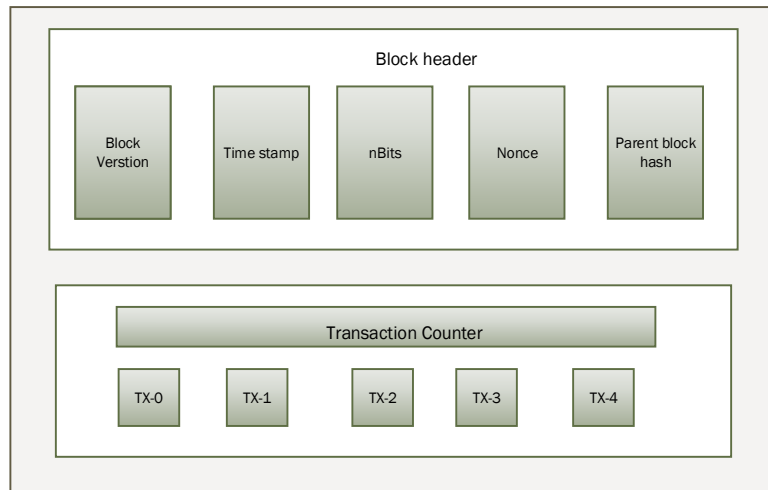


Figure 1. The block data model

Public chains, private chains, and coalition chains are the three types of blockchains that are currently available. Public chains are a type of blockchain that involves public involvement, is decentralized, and does not have a single body in charge of the network. Furthermore, in several cases when blockchain applications, it is unlikely that every user would have equal access to every piece of data, and a private chain is a blockchain topology where only authorized Nodes are permitted to take part and obtain information. Several firms create partially decentralized private chains in which just the majority of the power is spread among a select few nodes that are used to achieve consensus. As a result, the permission chain is a sort of blockchain in which the block chain's administration is centralized. As a sort of blockchain that falls between public and private chains, collaboration chains are designed to alleviate the disadvantages of private chains. Some organizations and nodes can engage in consensus thanks to the coalition's chains' partial decentralization, compared to the centrally-controlled private chain network, where a consensus is determined by a section of the organization that decides to join.

Table 1 depicts the three main forms of blockchain message pairings. A public chain's consensus is reached by all nodes, whereas a private chain's consensus is established internally by the organization, and a coalition chain's consensus is reached by a specified group of nodes. Public chains can freely access transaction information with regard to reading permission for block information, whereas private chains and coalition chains have the option of restricting or granting authorization based on their own application requirements. By means of performance, because there are so many nodes on the consensus between a large many of nodes on a public chain, it takes longer for the public chain to broadcast blocks and transactions, and private chains and coalition chains are more effective and include restricted data of participants into blocks.

Table 1. Evaluation of various blockchains

Category	Compromise	AnalysisApproval	Effectiveness
Public chain	Consensus is reached by all nodes	All have free access	Lower effective
Private chain	Some organizational nodes get at agreement	Open access rights inside a company	Very effective
Coalition chain	a subset of partial nodes agree	limited authorizations	Very effective

3. DATA SHARING

3.1. Interplanetary file system (IPFS)

The interplanetary file system (IPFS) is a distributed file system that is open-source. IPFS works on a peer-to-peer network, as opposed to standard centralized file systems, which only use servers to receive the material, preventing typical centralized networks' single point of failure and attack vulnerabilities. The central server's performance remains unaffected when files are sent from one user to another, considerably improving file transfer efficiency. Furthermore, because resource waste from traditional location-based addressing is a common occurrence, interplanetary file system offers a content-based distribution mechanism. Every file has a distinct hash value; this is no less impenetrable to tampering, but also stops enormous duplication of material from being uploaded and enhances the efficiency of the network. Finally, IPFS provides a number of significant advantages [17]. To begin with, IPFS offers the advantage of being both quick and decentralized. The user's computer houses all IPFS data, data can be retrieved from the closest IPFS user node by other IPFS users. Furthermore, better blockchain integration with IPFS [29]. This can compensate for the distributed ledger storage capacity limitations of the blockchain by creating by publishing using an IPFS connection to a data source and the blockchain, high-capacity data, and the blockchain are connected through a junction gateway.

3.2. Searchable encryption technologies

Encrypted data may be searched using searchable encryption technology without giving any information to an unsecured network. i) By examining the encryption text alone, the plaintext cannot be determined by the untrusted server in any way; ii) A unsafe server can only search with the legitimate user's authentication; iii) When submitting a search request to the server, the user is not required to provide the exact meaning of the keyword; iv) The unauthorized server is unable to receive any unencrypted data about the inquiry results. The server's searchable encryption enables providing cipher text files in response to valid users' query requests while preventing the server from accessing users' data, preserving query speed without compromising the security and privacy of consumers' data.

4. METHOD

4.1. Blockchain based secure data storage

Data owners and data requesters are the two parties involved in the exchange of data, and data is sent from data owners to data submitters. The research leverages technologies like IPFS, smart contracts, blockchain, and others to connect on-chain and off-chain data securely. The two parties involved are the data owner who uploads resources and the data requester who requests resources most crucial procedures in the data safe sharing process [26]. Following are the specifics of data sharing from the data user to the data requestor.

4.1.1. Data upload stage

Data users choose a data they want to part encrypts it with a symmetric key K , after which it decrypts the data EI . The system settings and attribute per mission public key are used by the data user to encrypt the symmetric key, which is created by the licensed policy tree M [27]. As shown in (1) and (2) can be used to illustrate this process.

$$\text{Encryption Data } (L, K) \rightarrow EL \quad (1)$$

$$\text{User Encryption } (M, K) \rightarrow EL \quad (2)$$

4.1.2. Data request stage

To determine the target data, data retrieval is the first thing the data requester does, referring to the data management contract's data list acquisition and data retrieval processes [28]. An encrypted information EI may then be retrieved. The data requester can then receive the symmetric key K by requesting the user key UK from the organization X . In (3) and (4) can describe this process.

$$\text{Decryption } (UK, XL) \rightarrow K \quad (3)$$

$$\text{Decryption Data } (XL, K) \rightarrow L \quad (4)$$

4.2. Access control using blockchain

In implementing a blockchain-based distributed data security access architecture that allows for the secure transmission of symmetric keys and data, based on the results of the requirement analysis, this research

provides for this approach. A fine-grained dynamic access control mechanism based on blockchain technology is proposed [29]. The following is the detailed procedure.

4.2.1. Initialization stage

The M the order bilinear group D must be built in the early phases of system development, as illustrated in (5).

$$M = n1 \times n2 \times n3 \quad (5)$$

Where the integers n1, n2, and n3 are prime.

Following that, one may determine the created unit d of D's subgroup Ds. The authorization authority X invokes the authorization initialization function during the startup phase to choose in the feature set G, for each feature I, there are two random indices, I and β_i . The authorization key SK and the authorization public key PK is acquired. Using input for the public parameter P and the attribute space G. This procedure may be described as shown in (6).

$$(SK, PK) = \text{Authority Key Gen } (G) \quad (6)$$

4.2.2. Controlled request stage

The current access timestamp is an example of a dynamic characteristic that varies based on the date, time, or location of the data requester. A managed requester's current internet protocol address, and other dynamic information AF can be written as (7).

$$AF = \langle af1, af1 \dots afn \rangle \quad (7)$$

4.2.3. Stage of data decryption

If the data request authority has decided, the authorized requester can obtain the key and relevant details. To retrieve the user system key K, the decryption process is initially conducted locally. The decryption algorithm is used by the controlled requester utilizing the user key K, to decrypt the encrypted data E [5].

4.3. Data-sharing technology based on blockchain

The blockchain-based distributed data security share method may be divided into two parts depend on its intended use: access control and data management. Figure 2 shows the layers for user access, the blockchain engine, and data storage, which are the system's three primary implementation layers. A user-oriented operational layer called a user access level enables the model's main functions to be executed logically. The layer is equivalent to the data-sharing model's functional modules, identical access control component, in terms of logical implementation, and the data management module. To perform duties related to consistent access control and data management, utilizing data from the blockchain engine level and data storage layer, these three crucial implementation components will connect with the user. The blockchain engine layer serves as the user access layer's backend implementation support layer. As a vital repository and operational auditing tool for the construction of systems, in the paradigm of data sharing, the blockchain is essential. For shared information, the user data storage layer provides safe data storage. The storage technique has been accredited as IPFS storage to ensure the security of the data.

4.3.1. Access control modules

Figure 3 depicts the structure of the access control module. There are three groups of functions in the access control module: Encryption and decryption, individuality management, and feature management. Because the encryption and decryption module's aim information and ciphertext decoding functionalities don't require blockchain-related storage and auditing, a user access layer is where the specific implementation is carried out. The encryption and decryption module's identity management, attributes management, and information storage functions, as well as attributes query functions, are finished in the blockchain storage or operational auditing, consequently, the user access layer implements the logical interface, while the blockchain level implements the practical interface.

4.3.2. Data management modules

A next three modules abstract the functions that were necessary for the data organization component: Data management, data storage, and encryption and decryption are all examples of data as shown in Figure 4. A data contented is kept by IPFS in the data access level. Whereas the blockchain engine layer stores the data meta-information in the blockchain for data conservation and inquiry.

4.4. Data sharing blockchain engine

By implementing smart contracts, the data-sharing blockchain engine may implement customized features. As this solution for data sharing activities is being developed, the interface and returns values, a variety of software design principles are used in the blockchain engine developed in this study, and layered, modular design concepts are used to make sure the systems design is understandable then simple for explaining. Furthermore, the blockchain satisfies the security and suitability criteria of the regulations. According to its role, the data sharing blockchain engine is separated into three layers: three layers: the interface layer, core layer, and storage layer. Every one of the engines' big function levels has its own set of internal smaller functional modules. Figure 5 shows the architecture of the blockchain engine.

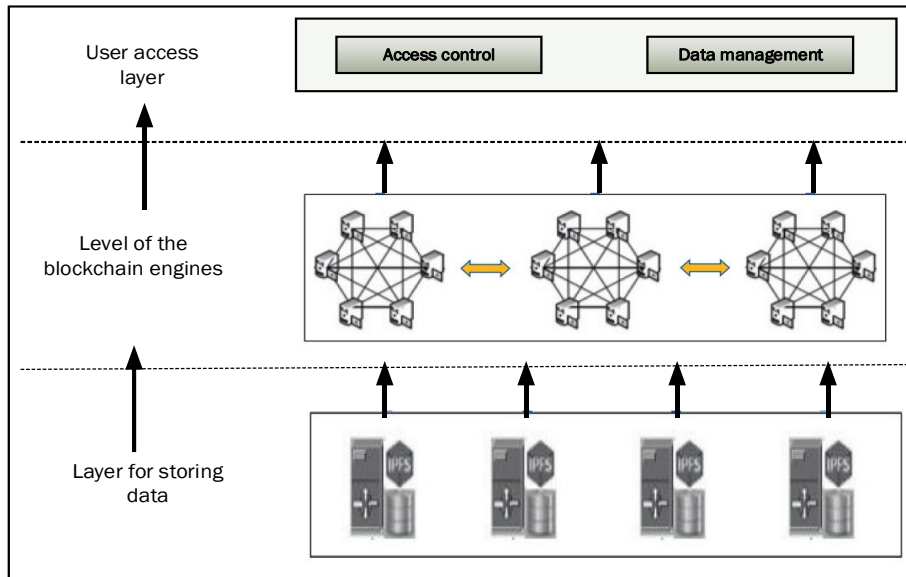


Figure 2. Framework for data sharing model

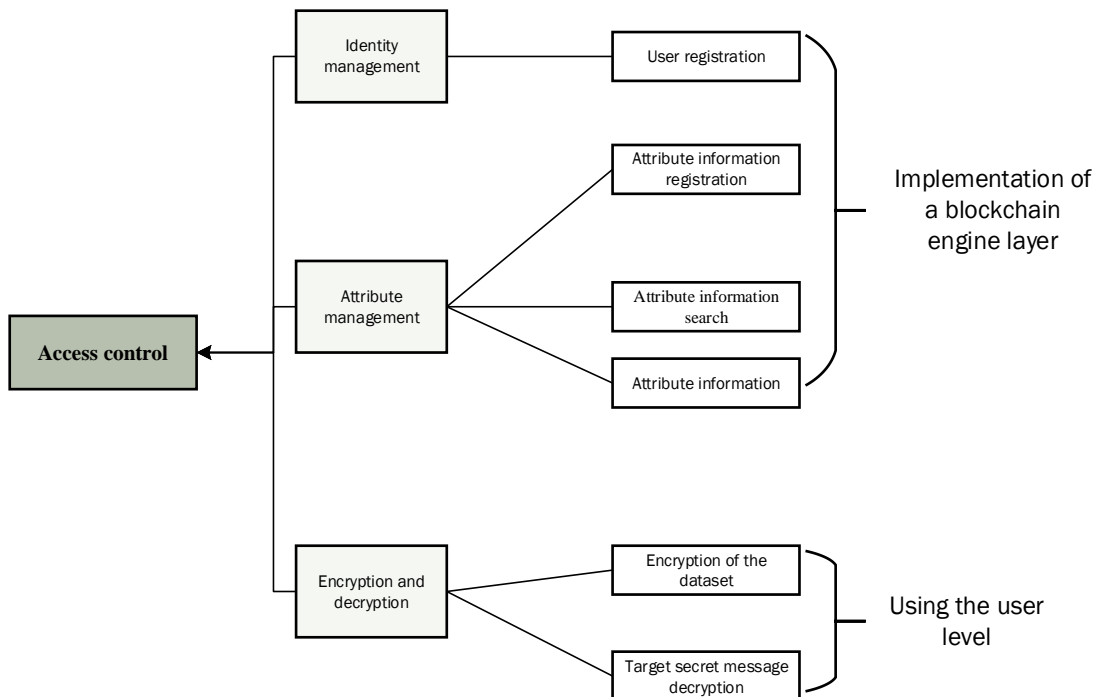


Figure 3. Access control component structure

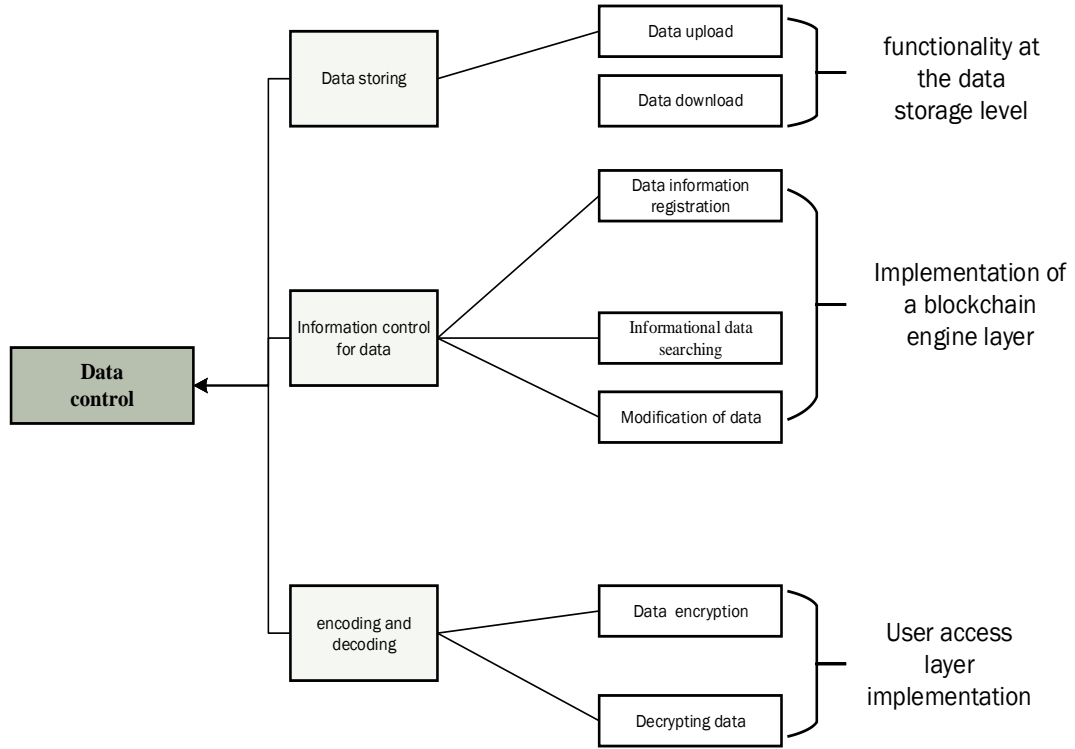


Figure 4. The module's structure for data management

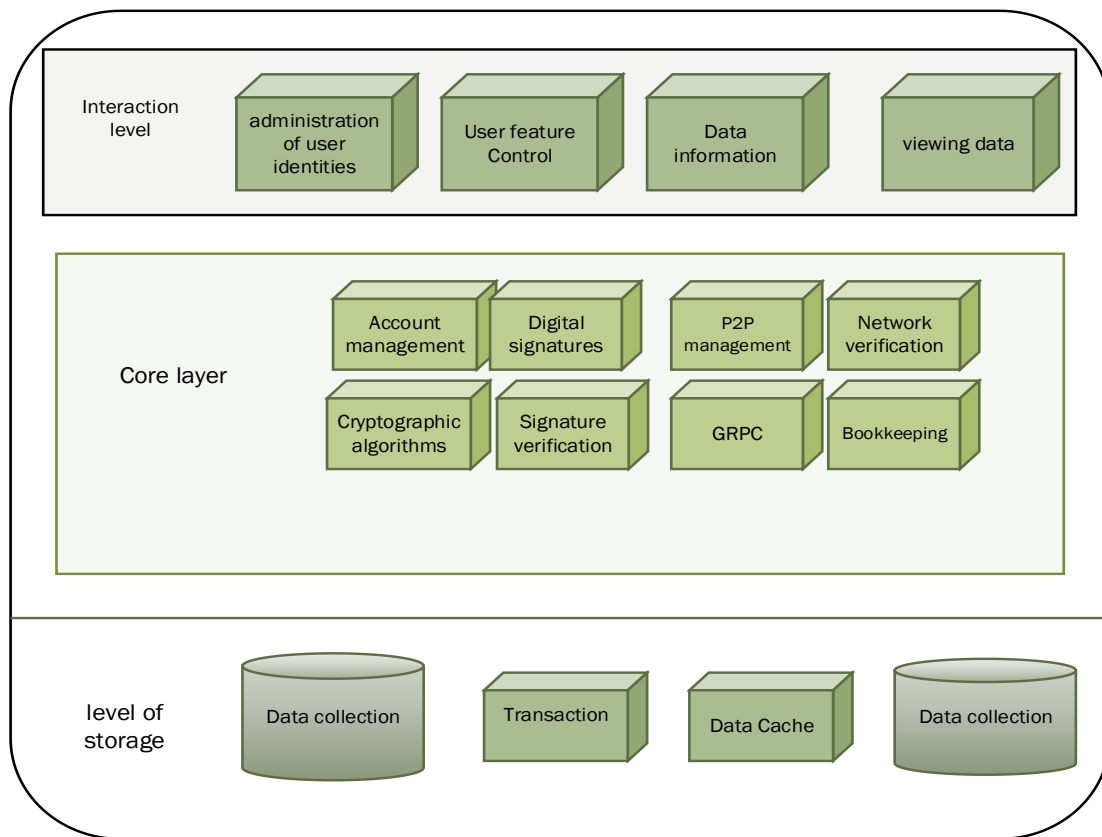


Figure 5. Blockchain engine for sharing data

4.5. Environment for model development using hardware and software

Table 2 shows the setup of the devices. The blockchain software environment is shown in Table 3. The following Tables 2 and 3.

Table 2. A data sharing model's hardware environment

Term	Data
Processor	Intel® Core™ i7-6400H CPU @ 4.40 GHz
Memory	Memory 256
Operating system	MacOS 10.13

Table 3. The data-sharing model's software environment

Term	Data
Advanced instrument	IntelliJ IDEA 2021.3
Simulated mechanism	Virtualization for Oracle Virtual machine 6.1.34
Database	SQL Server

5. RESULTS AND DISCUSSION

5.1. Evaluation of functionality

Identity management of data users is carried out in the study's designed data-sharing paradigm, utilizing user data providing registered users with administrative unique numbers and attribute data, CP-ABE is used to provide fine-grained access control. By separating dynamic from static characteristics and creating distinct accessing control strategies for the two systems, you can protect your data; the determination of dynamic access rights is accomplished in phases, with access policies being updated dynamically. Simultaneously, Smart contracts are employed as a gateway and a means of changing the blockchain's current state, Furthermore, the programmable impact facilitates the development of user interfaces for data retrieval from the chain using keywords to generate categories or searches.

5.2. Evaluation of security

Unlike typical data sharing systems, the approach described in this research takes heavy usage of the decentralized concept, so resolving the difficulty with a single point of failure. To begin, this data sharing strategy's overall architecture is built on IPFS storage devices and blockchain technology. Because IPFS and blockchain are distributed and decentralized technologies, despite any nodes that failed, a system's overall availability is unaffected. Second, this paradigm allows for the control of many attribute agencies. A distribution of characteristic management power efficiently eliminates the possibility for illicit actions generated by centralized power and prevents the solution's functioning from being hampered by a single attribute authority failing. Furthermore, unlike a case where the data owner manages the attributes, this study removes the data owner's attribute management. The only user-managed duties that a data user does are those of a data manager, successfully preventing the issue of data non-availability brought on by the data owner's slow response.

6. CONCLUSION

To protect data security, traditional data interchange has been mostly conducted offline, nonetheless, there are drawbacks including slow real-time performance and data loss. As Internet technology has developed, online data exchange has taken over as the most popular way of data delivery and has definite benefits over conventional techniques in terms of timeliness. Additionally, as Internet data continues to grow, there is a growing need for data management and privacy safeguards. Networking, distributed storage, and encryption technologies are all combined in the technology-integrated system known as a blockchain. Decentralization and the immutability of the chain's information are among the distinguishing qualities, which can provide native solutions to some of the issues with data exchange. In this study, distributed data security sharing solutions based on blockchain are examined and used, it is suggested that blockchain technology has the capacity and key application value in security and control to optimize the effectiveness of data exchange. Considering the state of domestic and international research on blockchain-based data security sharing, the first section of this article suggests a data-sharing architecture based on blockchain. This idea is established on the distributed data security access model and decentralized Blockchain concept for perfectly alright data access, which features symmetric data content encryption to act as the link between the entire architecture and prevent data content leakage. To solve problems like centralized storage with a data loss, a basic IPFS technology is




used as distributed storage. The following ways this study might eventually be prolonged. A data-sharing paradigm presented in this paper could first be enhanced, trying to improve the efficiency of the optimization algorithm by including theft monitoring techniques by the combining the optimization algorithm with the data sharing technique. Additionally, by trying to separate the LAN and WAN components by various application scenarios, to improve transmission performance, the storage layer's architecture and implementation might be changed.

REFERENCES




- [1] C. Zhang, L. Cao, and A. Romagnoli, "On the feature engineering of building energy data mining," *Sustain. Cities Soc.*, vol. 39, pp. 508–518, 2018, doi: 10.1016/j.scs.2018.02.016.
- [2] Q. K. Kadhim, R. Yusof, and H. S. Mahdi, "A review study on cloud computing issues a review study on cloud computing issues," *J. Phys. Conf. Ser. Pap.*, IOP Publishing, vol. 1018, no. 1, 2018, p. 012006.
- [3] J. P. Gouveia, J. Seixas, and G. Long, "Mining households' energy data to disclose fuel poverty: Lessons for Southern Europe," *J. Clean. Prod.*, vol. 178, pp. 534–550, 2018, doi: 10.1016/j.jclepro.2018.01.021.
- [4] Y. Sun, F. Haghighat, and B. C. M. Fung, "A review of the-state-of-the-art in data-driven approaches for building energy prediction," *Energy Build.*, vol. 221, 2020, doi: 10.1016/j.enbuild.2020.110022.
- [5] H. Sadeq, M. Alsultani, S. T. Ahmed, B. J. Khadhim, and Q. K. Kadhim, "The use of spatial relationships and object identification in image understanding," *Int. J. Civ. Eng. Technol.*, vol. 9, no. 5, pp. 487–496, 2018.
- [6] T. K. Mackey, T. Kuo, B. Gummadi, K. A. Clauson, G. Church, and D. Grishin, "Opportunities for applications of blockchain technology in the future of healthcare," *BMC Med.*, pp. 1–17, 2019, doi: 10.1186/s12916-019-1296-7.
- [7] S. T. Ahmed, Q. K. Kadhim, H. S. Mahdi, and W. S. A. Almahdy, "Applying the MCMSI for online educational systems using the two-factor authentication," *Int. J. Interact. Mob. Technol.*, vol. 15, no. 13, pp. 162–171, 2021, doi: 10.3991/ijim.v15i13.23227.
- [8] R. Yuan *et al.*, "A system dynamic model for simulating the potential of prefabrication on construction waste reduction," *Environ. Sci. Pollut. Res.*, vol. 29, no. 9, pp. 12589–12600, 2022, doi: 10.1007/s11356-021-14370-y.
- [9] G. Ghiani, "Using blockchain to drive supply chain innovation," *Deloitte*, pp. 04–11, 2017, [Online]. Available: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-blockchain-to-drive-supply-chain-innovation.pdf>.
- [10] S. T. Ahmed and S. M. Kadhem, "Early alzheimer's disease detection using different techniques based on microarray data: A review," *iJOE*, vol. 18, no. 04, 2022, doi: 10.3991/ijoe.v18i04.27133.
- [11] S. T. Ahmed and S. M. Kadhem, "Alzheimer's disease prediction using three machine learning methods," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 27, no. 3, pp. 1689–1697, 2022, doi: 10.11591/ijeecs.v27.i3.pp1689-1697.
- [12] M. Berneis, D. Bartsch, and H. Winkler, "Applications of blockchain technology in logistics and supply chain management — insights from a systematic," *Logist. Rev.*, 2021, doi: 10.3390/logistics5030043.
- [13] S. T. Ahmed and S. M. Kadhem, "Using machine learning via deep learning algorithms to diagnose the lung disease based on chest imaging: A survey," *Int. J. Interact. Mob. Technol.*, vol. 15, no. 16, p. 95, 2021, doi: 10.3991/ijim.v15i16.24191.
- [14] S. Wang, "Improved blockchain technology for performance optimization model design of sports clubs," *J. Electr. Comput. Eng.*, vol. 2022, 2022, doi: 10.1155/2022/4436471.
- [15] A. Moazzami, V. M. Nik, S. Carlucci, and S. Geving, "Impacts of future weather data typology on building energy performance – Investigating long-term patterns of climate change and extreme weather conditions," *Appl. Energy*, vol. 238, no. January, pp. 696–720, 2019, doi: 10.1016/j.apenergy.2019.01.085.
- [16] A. R. Rajput and Q. Li, "A blockchain-based secret-data sharing framework for personal health records in emergency condition," *In Healthcare*, MDPI, vol. 9, no. 2, pp. 1–17, 2021, doi: 10.3390/healthcare9020206.
- [17] H. Saeed *et al.*, "Blockchain technology in healthcare: A systematic review," *Plos one*, vol. 17, no. 4 April, 2022, doi: 10.1371/journal.pone.0266462.
- [18] A. Abdelmaboud *et al.*, "Blockchain for IoT applications: taxonomy, platforms, recent advances, challenges and future research directions," *Electron.*, vol. 11, no. 4, pp. 1–35, 2022, doi: 10.3390/electronics11040630.
- [19] M. Billah, S. T. Mehedi, A. Anwar, Z. Rahman, and R. Islam, "A systematic literature review on blockchain enabled federated learning framework for internet of vehicles," *IEEE Access*, vol. 4, pp. 1–21, 2022, [Online]. Available: <http://arxiv.org/abs/2203.05192>.
- [20] G. Li and H. Sato, "A privacy-preserving and fully decentralized storage and sharing system on blockchain," *Proc. - Int. Comput. Softw. Appl. Conf.*, vol. 2, pp. 694–699, 2019, doi: 10.1109/COMPSAC.2019.10289.
- [21] X. Zheng, R. R. Mukkamala, R. Vatrappu, and J. Ordieres-Mere, "Blockchain-based personal health data sharing system using cloud storage," *2018 IEEE 20th Int. Conf. e-Health Networking, Appl. Serv. Heal. 2018*, 2018, doi: 10.1109/HealthCom.2018.8531125.
- [22] S. Wang, X. Wang, and Y. Zhang, "A secure cloud storage framework with access control based on blockchain," *IEEE Access*, vol. 7, pp. 112713–112725, 2019, doi: 10.1109/ACCESS.2019.2929205.
- [23] M. Nuss, A. Puchta, and M. Kunz, "Towards blockchain-based identity and access management for internet of things in enterprises," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11033 LNCS, pp. 167–181, 2018, doi: 10.1007/978-3-319-98385-1_12.
- [24] J. P. Dias, H. S. Ferreira, and Á. Martins, "A blockchain-based scheme for access control in e-health scenarios," *Adv. Intell. Syst. Comput.*, vol. 942, pp. 238–247, 2020, doi: 10.1007/978-3-030-17065-3_24.
- [25] Z. Qiu and Y. Zhu, "A novel structure of blockchain applied in vaccine quality control: Double-chain structured blockchain system for vaccine anticounterfeiting and traceability," *J. Healthc. Eng.*, 2021, doi: 10.1155/2021/6660102.
- [26] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," *J. Med. Syst.*, vol. 42, no. 8, 2018, doi: 10.1007/s10916-018-0995-5.
- [27] S. Hu, C. Cai, Q. Wang, C. Wang, X. Luo, and K. Ren, "Searching an encrypted cloud meets blockchain: A decentralized, reliable and fair realization," *Proc. - IEEE INFOCOM*, vol. 2018-April, pp. 792–800, 2018, doi: 10.1109/INFOCOM.2018.8485890.
- [28] L. Cai and P. Li, "Research on the optimization of University financial sharing mode based on blockchain technology," *Proc. 2021 Int. Conf. Cult. Des. Soc. Dev. (CDS D 2021)*, vol. 634, no. Cdsd 2021, 2022, pp. 409–413, doi: 10.2991/assehr.k.220109.084.
- [29] J. Yuan, J. Ding, Y. Ma, Y. Zhou, Y. Liu, and Y. Chen, "Optimized design and implementation of testing laboratory based on blockchain technology," *J. Phys. Conf. Ser.*, vol. 2219, no. 1, p. 012037, 2022, doi: 10.1088/1742-6596/2219/1/012037.

BIOGRAPHIES OF AUTHORS






Israa Nazeeh    is a Master at Department of Computer Science, College of Science, Diyala University, Iraq. She holds a Master degree in Computer Science from Diyala University and the Bachelor degree in computer science from Al-Yarmok University College. She can be contacted at email: israamohammed@uodiyala.edu.iq.






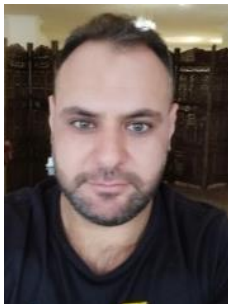
Teeb Hussein Hadi    received the bachelor's degree in Computer and Software Engineering from Engineering Collage, Diyala University, Iraq in 2009 and she received the master degree in 2013 in Software Engineering Science from Iraqi Commission for Computers and Informatics (ICCI), Informatics Institute of Higher Studies, Iraq. She is currently work as a lecturer in IT Department, Technical College of Management, Middle Technical University (MTU). She can be contacted at email: eng.teebhussien@mtu.edu.iq.






Zainab Qahtan Mohammed    received M.Sc. (2016) in India, Department of Computer Engineering, College of Engineering, Acharya Nagarjuna University. She holds a Bachelor degree in 2011 in Computer Engineering from the College of Engineering, University of Mustansiriyyah, Baghdad, Iraq. She can be contacted at email: rahmafaris.2017@gmail.com.



Shaymaa Taha Ahmed    received M.Sc. (2015) in India at University of Diyala Department Computer Science/College: basic of education Specialization: Computer science/information system. Research interests is cloud computing, deep learning, machine learning, AI, data mining. She can be contacted at email: or mrs.sh.ta.ah@gmail.com and Shaymaa.taha.ahmed@basicedu.uodiyala.edu.iq



Qusay Kanaan Kadhim    is a Ph.D. in information technology and communication from Technical University of Malaysia Malacca, UTEM. Department of Computer System and Communication. Specialization: information technology and communication, Bilad Alrafidain University College, Baqubah, Iraq. Research interests: cloud computing, information security, cybersecurity, artificial intelligence, and data mining. He can be contacted at email: qusaykn@bauc14.edu.iq or qusaykn@gmail.com.