Blockchain Technology for Data Sharing in Decentralized Storage System

D. Praveena Anjelin and S. Ganesh Kumar

Abstract In Cloud architecture, the storage systems can be centralized and decentralized environments. Centralized storage systems stored data in private cloud, maintained in a single location, can be accessed by one or more user, whereas in decentralized storage system, the data is stored on more than one or multiple servers. Users or companies are being a part of the decentralized cloud storage cloud to host the servers. The data may be stored on any server, i.e., no dedicated server for data storage and which can be accessed easily. In decentralized storage system, the files are stored and protected with the help of blockchain technology. Blockchain is nothing but a chain of blocks (computers or servers), which are connected by using cryptography. Each block contains a set of transactions which has been encrypted and shared in a secured way among multiple servers. Blockchain technology ensures confidentiality and integrity, which can be implemented by using peer-to-peer network. In this paper, we discussed how the technology improves security used by different applications in distributed environment. Further, we proposed adaptive encryption algorithm to improve security and access control.

Keywords Adaptive encryption · Cryptography · Decentralized storage · Blockchain

1 Introduction

In the past few years, most of the organizations have shown concern on outsourcing, it outsources the data and as well as gives functional services to clouds. Actually, the classical cloud storage is a centralized storage system acted as a trusted third-party storage provider to store and transfer the data. This system consumes high operational

D. Praveena Anjelin (✉) · S. Ganesh Kumar
Department of Computer Science and Engineering, SRM Institute of Science and Technology, SRM University, Kattankulathur, Chennai 603203, India
e-mail: pd6231@srmist.edu.in

S. Ganesh Kumar
e-mail: ganeshk1@srmist.edu.in

S. S. Dash et al. (eds.), *Intelligent Computing and Applications*,
Advances in Intelligent Systems and Computing 1172,
https://doi.org/10.1007/978-981-15-5566-4_32

cost, less security, poor performance, and lack of availability to transfer. To overcome the drawbacks of centralized cloud storage, a decentralized storage system (DSS) has been introduced with many features. Blockchain-based cloud storage solutions allow users to store data safely and give access to all participants in digital activities with most effect. Filecoin, storj, ppio, ochain, opacity, bittorrent, neo, and Dfinity are the various platforms of decentralized storage solutions.

Instead of central server, [1] InterPlanetary File System (IPFS) is a distributed file system which stores data on large number of computers that are connected by peer-to-peer networks. IPFS can communicate through Transmission Control Protocol (TCP) which has certain rules for data storage and transmission among connected nodes in the network. Node addressing system identifies nodes and content addressing system constructs the index of the content. Both node address and content address are stored in InterPlanetary Naming System. Files stored on IPFS can be accessed and shared by the users connected to an ipfs node. Files are split into small blocks, those blocks are hashed and distributed to storage nodes in the network. In order to consider privacy and data availability, DSS is better than centralized cloud storage systems, in which operational cost is much lesser than centralized storage. Existing decentralized storage systems supports easy implementation of encryption and storage of data, but the difficulty of data sharing is done secretly. Hence, we proposed a distributed framework to control access and search data using Ethereum Block Chain blockchain technology. Further to ensure security, we used ELGAMAL for encryption which protects the data in cloud storage.

The rest of the paper is sectioned as follows: Sect. 2 consists of literature review of existing technologies that have been used for data sharing in DSS. Section 3 presents reviews storage solutions of blockchain technology. Section 4, elaborate the user access control policy in Blockchain technology. Section 5 presents comparative analysis of various security algorithms in blockchain with DSS. Section 6 presents review of application areas of blockchain. Section 7 concludes the chapter.

2 Literature Review

Decentralized Cloud Storage In Decentralized Cloud storage system, the data is stored on multiple computers or servers connected by P2P network. These servers are hosted by a general user or an organization which can contribute to this decentralized cloud. The files are encrypted by cryptography and protected with the help of blockchain technology. The participants in this system can also earn money in cryptocurrency by sharing their unused space. Each computer in this network stores encrypted form of user data, the user is the only authenticated person to access and manage the files through their own public or private key. There are so many advantages in this technology,

- No dedicated servers for data storage.
- Peer-to-peer system network.

- Always availability of data.
- User can earn extra money by allowing free space to share.
- Since files are encrypted, it achieves higher rate of data security.
- Operational cost is lesser.
- Load balancing is very flexible.
- It requires less computing power and bandwidth.

Existing Technologies in DSS Distributed storage systems have huge volume of structured data spread over many nodes in the network, which provide highly obtainable service with no distinct end of failure. Some organizations provide distributed storage systems such as Sia, Storj, Maidsafe, and Ethereum, which are based on blockchain technology and a peer-to-peer architecture.

SIA: Sia is a decentralized peer-to-peer cloud storage scheme with blockchain technology. When the user chooses to store data on Sia blockchain. Sia first splits whole data into blocks, encrypts and distributes the data into various nodes connected in the network. The user can retrieve data by making request with a private key. User can get paid in Siacoin by renting out the extra space on their PC to the Sia decentralized network. Similarly, users who wish to use storage space need to pay Siacoins to a host. Sia does this by creating a marketplace for hosts and users via the token economics of Siacoin. Siacoin currency is used to execute a file storage contracts on the Sia blockchain and aim to reduce the cost of cloud storage. A host in this network puts a file contract agreement for keeping files, space required, and to invest Siacoins as collateral. A host can be punished if he does not serve to the user who made the data request. Once the agreement is over, the sum will be credited to the host in Siacoin account by the file contractor.

Storj: This storage platform is built on the Ethereum network best suite for cryptocurrency, store data in decentralized in asecure manner. [2] The user can upload the file with their own private key in order to ensure authenticate person and file is encrypted before sharing in the network. It separated the files from the user and stored in decentralized storage model. When user wants to access the file, he has to make a request, then storj uses distributed hash tables to locate all the shards and piece them together. Storj rents its own network to many users and puts charges for those who had used the network. This technology creates revolution in file sharing due to availability of data among connected nodes. Storj has partnerships with Microsoft Azure and Heroku to deploy its own development tools which creates great initiative for the open-source developer ecosystem. User authentication with direct payment is a major success in storj.

Swarm: Swarm is another decentralized storage system built on Ethereum network. It is one of the best content distributor and provides redundant store for web application. It provides various base layer services for web3 such as media streaming, none-to-node messaging, database services, etc. Actually the content is hosted on peer-to-peer network instead of individual computers or servers. This network is responsible for user authentication and allows them to access resources with payment. It directly integrated with Ethereum blockchain for service payments and data availability.

Cassandra: Cassandra is a distributed storage system used for storing and running a huge volume of structured data across various commodity servers. Cassandra supports dynamic control over data layout for clients with a simple data model [3]. The major distributed system techniques used in Cassandra are partitioning, scaling, replication, creating membership, and failure handling. To handle, either read or write requests, all these modules work under synchrony mode. Partitions the data dynamically, encodes it by hashing method, and assigns it to all nodes in the network. This distributed system uses replication algorithm to improve data availability and durability. Among multiple nodes, one can act as coordinator node which is responsible for keeping redundant data files whenever failure takes place in the network. It provides various replication polices such as Rack Aware, Rack Unaware, and Datacenter Aware to their clients stating that how and when data needs to be replicated. In Bootstrapping module, whenever a node wants to join in the group, first that node has to read its configuration file and membership identity card will be issued. The configuration file contains a list of linking points in it, with the help of this a node can join in the group and share files. It achieves high throughput, high performance, and providing better scalability.

Data Storage systems

Meta Product manufacturers always use their own private cloud to store data due to lack of security and privacy issues. Manufacturers can't trust another network and avoid data sharing [4]. Shrestha, A. K. and Vassileva, J proposed decentralized storage platform for Meta products, such as smartphones, wearable sensor devices, and smart cars. Meta Products must store group user data, later these data can be reused. It is a trusted system for sharing user information across various domains deployed by different organizations. It maintains distributed file account which holds the following information, who can contribute with sharing systems, what file may access, when that file retrieved, etc. This storage system has inbuilt trust mechanism, so it easily identifies the threat whenever a user tries to access an unwanted file. It supports personalized and content-oriented services to their clients.

Replication is a key technology of DSS [5] Yijie wang and Sijun Li proposed indirect replication algorithm. In the proposed model, the data is split into different data blocks, these blocks are encoded and distributed among several storage systems. Since data is redundant among data blocks, bipartite graph is used to encode the data blocks. The major advantage of using this algorithm is it provides security, durability, and availability of data. This model can be implemented with less operational cost and storage cost.

3 Blockchain Technology

Cloud storage is a centralized database system, in the extension of a centralized one, a decentralized storage framework is designed with blockchain technology. As we know that blockchain is a distributed database, a user can store any kind of information across different blocks (personal computer or server) connected in the network. Blocks are connected in chronological chain model, hence it is named as blockchain. It can be divided into three categories.

- Cryptocurrency bitcoin
- Smart contracts
- Application.

Cryptocurrency bitcoin: It is nothing but digital cash and as well as currency paid through online modes. It was established in the year 2008 with a group of people under the pseudonym Satoshi nakamoto, effectively solved the Byzantine (cryptographic research) problem. It is the most useful tool for value transfer underlying blockchain technology. The blockchain technology replicated all transactions done in the Bitcoin network. Bitcoin uses proof-of-work mechanism to prevent double-spending in the network; i.e., one who may spend same funds twice. The proof-of-work solved by miners in the bitcoin. Miners are the bitcoin nodes which checks its blockchain history and verifies all transaction made in the network. If anyone in the network tries to change the history, it takes more computational power in the network in order to verify. Actually proof-of-work mechanism is very expensive but, it is the only prevention method against Sybil attack. Sybil attack means, a node in network claims multiple fake identities and gain resources without spending currency. This attack highly influenced on following applications, voting systems, location-aware routing, data aggregation, and reputation evaluation.

Smart contracts: Smart contract is nothing but crypto contract, maintained by peer-to-peer network. In 1994, smart contracts idea was first proposed by Nick Szabo in 1994. He was interested in starting digital currency. Then later, in 2008, the cryptocurrency bitcoin was developed via a blockchain platform, this technology enabled smart contract. This tool can provide some coordination and assigned agreements among nodes who participate in the network. This tool can directly control digital payment, currency transfer, or sharing assets between nodes in the network. It enforces the contractor to follow all rules and obligations related to the agreement as the same way what traditional contract did by generating tokens. Blockchain managed the self-enforcing agreement which is embedded in some other computer code. The code contains smart contract agreement policy which parties need to interact; what file needs to be shared and cost details. The agreement is enforced automatically when the rules are met, i.e., it unlocks the access and manages tokenized assets. In technical aspects, the merit of the smart contract is self-verifying, self-executing, and tamper resistant. In economic aspects, decentralized ledger initiated transactions. So, low expenses and maintains higher transparency. In legal aspects, security is the major issue that needs to be resolved.

Blockchains: In general, blockchain requires a huge computational resource to run, since it has been available in public and accessed by many nodes in the network. So, the system is almost utilized its maximum potential but the user should have limitations to access. Sometimes an unauthorized user may access the network, he can download the file, i.e., confidentiality of data, secure sharing, and redundancy are major issues in blockchain. In distributed systems, private data must be shared by all nodes connected on the network. So, data may be completely exposed. In centralized storage systems, data can be stored securely with less transparency. This is one of the primary contradiction between centralized storage system and decentralized public blockchain. Based on access mechanism, blockchain can be classified as,

Public blockchain: A blockchain grants permissions to issue transactions and to read access for all data of the chain to all users.

Private blockchain: A blockchain is available for a predefined list of entities to access stored data and create a transaction on the chain. There are two types of blockchains.

Permissionless blockchain: This type of blockchain does not restrict the identities of transactions.

Permissioned blockchain: This type of blockchain accepts only the predefined entities performed transactions with known identifications [6, 7].

Both private and permissioned blockchains are not the same based on storage mechanism. For example, a permissioned blockchain can be available to the public to read the data from blockchain, but the general users might not have permission to create transactions. It has distributed ledgers to maintain storage details, access details and protocols can be used to provide security and increase the availability of data. But, in private blockchains may have full permission to access the blockchain by preconfigured entities. Moreover blockchain may be any type, must have multi-level permissions such as connection establishment, create storage block, send and receive transactions, read data from decentralized storage systems. All these technologies support security, data consistency, and easy access. The following table shows comparison among various blockchains (Table 1).

Blockchain-based storage solutions: Blockchain technology provides decentralized storage structure with a secure manner when compared to traditional cloud storage. There has been significant growth in technology with respect to storage, security, authentication, and access control. Whenever a node in network wants to upload a file, first that must be encrypted before sharing and also ensure availability

Table 1 Comparisons among public blockchain, consortium blockchain and private blockchain [6]

S. No	Property	Public blockchain	Consortium blockchain	Private blockchain
1	Consensus determination	All miners	Selected set of nodes	One organization
2	Read permission	Public	Could be public or restricted	Could be public or restricted
3	Immutability	Nearly impossible to tamper	Could be tampered	Could be tampered
4	Efficiency	Low	High	High
5	Centralized	No	Partial	Yes
6	Consensus process	Permissionless	Permissioned	Permissioned

of data [8]. Metadisk is an open-source software to provide decentralized storage system which is more secure and efficient. Its main objective to establish a constant platform for P2P cloud storage network (Storj). This application provides an interface for nontechnical users also. Using this API, users can upload and download files in a secure way. Client-side encryption has taken place on it. Users can generate private key and assign to files while uploading files on the network. Multiple nodes in a network may have the same file according to data availability.

Once the file has been encrypted, the SHA-256 hash serves a unique identity and way to detect file tampering. [9] In blockchain distributed storage, first data storage provides decentralized platform where, ana organization can register in order to access distributed data and further it can be shared. Anonymous access control component ensures the client access is provided by data owner itself. The data owner may not aware of who will be the data user and how many times the data consumer has to show the credential proof. Private keyword search mechanism helps a data user to recognize the encrypted information. The consumer can directly interact with blockchain node by giving a single keyword to get the fingerprint of specific data content. At last, data consumer retrieves encrypted documents from decentralized storage system. Keyword search cryptosystem consists of KeyGen, Trapdoor, Encrypt, and test algorithms. KeyGen generates private search key, encrypt algorithm produces ciphertext for keyword which are performed by the data owner. KeyDerieve algorithm is used by the owner to produce secret search key for data consumer. Trapdoor is run by data user for keyword. Test algorithm is executed by smart contracts on blockchain.

4 Access Control Mechanism in BlockChain Technology

Samarati and de Vimercati [10] defined Access Control as "The process of mediating every request to resources and data maintained by a system and determining whether the request should be granted or denied." The primary goal of access control mechanism is to verify and limit the actions that authorized users can perform within a computer system. Access control has set certain limitations to users, as what a user could perform directly with the system, what programs can be executed on behalf of the users who are permitted to execute those programs with approval. An access control community should have an object, subject, operations, permissions, control list, and matrix.

Access control Models: The access control system has been developed based on security policy and security model. Security mechanism is a model which comprises of low-level implementation of both hardware and software. Access control models can be categorized as,

1. Mandatory Access Control
2. Discretionary Access Control
3. Role-based Access Control

4. Organization-based Access Control
5. Attribute-based Access Control
6. Centralized and Decentralized Access Control.

Laurent et al. [11] They proposed a new access control method. In that, a smart auditable contracts deployed in blockchain infrastructures which is a transparent one and provides controlled access to outsourced data, i.e., Malicious entities should not access data without the knowledge of the data owner. They would implement this proposed new solution on Ethereum blockchain network. The proposed access control mechanism has four entities which are defined as Data Storage Provide (DSP): It is not an active client having read access alone and governs distributed remote servers and hosts application services. Data Owner (DO): Ensures authorized entities and makes uses of resources provided by data storage provider in order to store and share data in network. Data retriever (DR): DR is a client of blockchain, he can access the content stored in remote servers. Blockchain Infrastructure (BC): It is a mediator, permits to authenticate DRs. It ensures authenticated access control with respect to efficient whitelist definitions and preserves privacy among entities. Unlinking properties can support one-time access control which ensures unlinkability between different access sessions by users.

Ronghua and Chen[12] A blockchain-enabled decentralized access control (BlendCAC), is suitable for decentralized storage in a secured manner. Its major aim is to provide effective access control mechanism to devices, services, and information especially in large scale IoTs (Internet of Things). It efficiently does process related to IoT and also provides granularity, scalability, and dynamicity of AC strategies for IoTs. The proposed system, IoT devices acts as a master, controls all the resources used in the network instead of centralized authority. The operations are carried out in Ac as listed below. Registration: Entities that participate in blockchain network must create an account with a pair of keys for authentication purpose. Smart Contract Deployment: Domain owner developed and deployed capability tokens on blockchain network, those tokens are managed by smart contract. Capability Propagation: Initially, an entity sends access rights request to the domain owner to get the capability token. Then the system checks for authorization, if it is found to be right entity, then capability token is issued by data owner. Capability token encodes the access rights, then initiates transactions in order to update token data in the smart contract. Authorization Validation: Service providers performed authorization validation on receiving service request from an entity.

Steichen et al. [13] IPFS uses Ethereum smart contract to provide access-controlled file sharing. The proposed mechanism allows users to do all financial transactions in its own cryptocurrency area and custom currencies called tokens. Access control system has some privileges regarding addition, modification, and removal of permissions that are recorded on blockchain. The access control contract contains four functions such as, AMIOwner, MIOwnerMultiple, CheckAccess, and CheckAccessMultiple. AdBlock function used to register an IPFS file chunk in control list. Cryptographic hashes identify IPFS file chunks. This hash value is used as a key stored along with file chunks. GrantAccess function accepts request given by data owner, check for hash value. If value exists, then it sends the key to owner. Remove access function used to remove the user whenever hash value mismatched or different being posted by data owner. AMIOwner: It accepts the request and checks the hash value of file chunks. If it has the same value what a data owner already registered, then it gives access rights to data owner to get access of file chunks of storage blockchain. Its values are mismatched, then it returns false message. DeleteBlock function reverts if the hash value is empty, soon it removes files from data storage since the file has not been requested so far from the owner's side. *f* hash value resides, it knows that file may be accessed and retrieved soon.

Thwin and Vasupongayya [14] Personal health record system (PHR system) stores individual health-related information. This system allows data owners to share and manage data among selected individuals. Information stored in database may be incorrect because of immutability, irreversibility properties, and originality of content may be inequitable. Fortunately, blockchain technology gives potential solutions to solve this issue. The proposed system supports tampering resistance feature which includes fine-grained access control, auditability, tamper resistance, and revocability of consent. To preserve privacy, proxy reencryption and cryptographic techniques are used. Proxy reencryption scheme is an asymmetric cryptosystem; enables its users to share their decryprion capabilities with others. The ciphertext is encrypted with user public key, that file can be decrypted by another user by using their own private key but the content cannot be retrieved fully during transactions. Since the encrypted file can be constructed in such a way, ensure secure data sharing scheme. The data owner must send reencryption key to proxy in order to share data. The reencryption key is generated with the combination of owners secret key and users public key. Moreover the proxy cannot read any information from original data with the help of reencryption key.

5 Privacy/Security in Blockchain

(i) **Existing Algorithm**:

Decentralized storage solutions create massive attraction among storage providers. Data can be stored in different nodes in the network and being shared with entire network. However, uploading, downloading, and sharing of files may not be secure in a distributed platform. Since, authentication and security can be a big challenge in distributed architecture. Existing decentralized architectures are constructed to support huge volume of data storage and shard, but, still there are no effective solutions for security issues. P2P network has been widely implemented over the distributed systems. We compared different blockchain technologies so far that had been implemented, security algorithms used, and their performance with evaluation metrics. The comparison of different blockchain platforms along with network performance has been shown in Table 2.

Table 2 Comparisons of blockchain technologies, security algorithm used

S. No	Platforms/applications	Business logic	Configuration mode	Encryption	Workload	Transaction data	evaluation metrics
1	Ethereum	Smart contract	Private network	Single public key	Random	Deployment time, completion time	Execution time, throughput
2	Hyperledger Fabric	Chaincode	Private network	Different private key	Random	Completion time	Latency and throughput
3	Smart home systems	Bitcoin	Private blockchain	Signcryption	Asynchronous	Completion time	Execution time
4	Peer-to-peer	Medibchain protocol (smart contract)	Private blockchain	Elliptic curve cryptography			
5	P2P network	Bitcoin	Private	Digital signature algorithm	Random	Transaction time	Latency

(ii) **Adaptive Encryption Algorithm**:

Adaptive encryption techniques can be applied on decentralized storage systems because of data confidentiality. This algorithm permits the cloud server to do a large set of SQL operations over encrypted data. The below listed encryption schemes are used in it.

- Deterministic
- Order Preserving encryption
- Random
- Search
- Plain
- Sum.

Each client can participate in DSS to get services by direct execution of SQL operations. This algorithm guarantees the same level of scalability and data availability. Initially, data is encrypted using key, then it is stored in cloud server. Whenever the client wants to get data, he has to decrypt with key value after downloading a file from the server. This algorithm is well-suited for encryption since it does not allow even a trusted party to manage encryption details. It also simplifies database server configuration because of operation automation.

6 Application Areas

Blockchain technology is very proficient and gives copious reimbursement such as decentralization, persistency, auditability, and anonymity. Cryptocurrency, financial services, Internet of Things, risk management are various sectors where blockchain technology can be applied.

Finance:

(i) **Financial Services**: Bitcoin is one of mostly widely used cryptocurrency method. Blockchain technology can be used for financial transactions, clearing and settlement of financial assets, and reducing cost and risk. Microsoft Azure, IBM are tremendous software companies offering blockchain services to the general public.

(ii) **P2P financial market**: Blockchain builds a P2P financial network to establish financial services among network in a secure and reliable way. Blockchain creates shared computation protocols to create a P2P financial shared computational market. This MPC market allows a P2P network to do computational task in offload mode.

(iii) **Enterprise transformation**: The traditional organization has completed all its transactions smoothly with help of blockchain technology. For example, the traditional postal operators (Pos) acts as an intermediator between customers and merchants. Pos make use of cryptocurrency techniques to extend both financial and nonfinancial services.

(iv) **Risk management**: Blockchain technology provides risk-management framework used to decide the investments plan, collaterals, and analyze investment risk also. Smart contract enables decentralized autonomous organizations to manage with all its business activity collaborations.

Internet of things (IoT): IoT is nothing but integration of objects (electronic devices and smart objects) with internet to provide different services to users. Some of the applications of IoTs as logistic management with Radio-Frequency Identification (RFID), smart homes, smart grids, e-health,maritime industry, etc. Blockchain with IoT potentially improves e-business model. This model has DAC, the people who trade with DAC to get transactions quickly, get coins, and the people can also exchange data with intermediary. Blockchain can improve privacy in IoT applications. Hardjono and Smith (2016) proposed a privacy-preserving method for IoT device into cloud ecosystem. This system ensures security by not allowing unauthorized access of devices. IBM ADEPT system developed to build a distributed platform, where devices are connected.

Public and Social Services: Blockchain can be widely used for public services such as patent management, income tax generation and monitoring system, digital signatures, marriage registrations, etc. Decentralized storage access provided to all users connected in network which reduces hard copy system and easy access to user.

(i) **Education**: Blockchain learning is proposed by Devine (2015) which achieves online educational marketing strategy. In this learning model, the teachers can segregate the learning materials into blocks; those blocks are packed and placed into the blockchain. Any user can access blocks on blockchain by paying coins through cryptocurrecy.

(ii) **Energy saving**: Gogerty and Zitoli proposed solarcoin. Solarcoin encourages the usage of renewable energies by rewarding digital currency to energy producers.

(iii) **Land Registration**: Blockchain technology highly contributes in public services and as a proof land registration is major application of it. The land information such as physical status, registered details, authorized person, landmark, cost details are publicized on blockchains. Whenever there is any changes in details, that are updated lively on blockchains to improve effectiveness of communal services consequently.

Reputation System: Reputation is nothing but trustworthy. Simply saying, an Individual's reputation can be evaluated based on the previous transaction done by him. Individuals overall interactions can be taken place within community. In e-commerce applications, to achieve high reputation, many service providers enrolled large number of fake customers. This creates problem for vendors also. This issue can be solved with the support of blockchain. Reputation is an important thing for an academician [15]. Blockchain-based distributed system is proposed to manage educational record and reputation. In this model, initially each institution and their professionally qualified workers will be awarded (educational reputation currency). An institution also awards the intellectual worker by transferring record status to them. All transactions are stored dynamically. So, changes in reputations can be detected easily. In web community, members can be reputed based on their qualities. Carboni proposed a reputation model based on blockchain, the service providers in web community may be reputed by getting feedback from customers. Reputation values are stored on blocks across a distributed network.

7 Conclusion

Decentralized storage system is created a revolution in storage area where the public can interact with internet. It provides distributed data storage, though there may issues on security, no safe on stored data, trustless environment. In this cyber world, no security, difficult to predict third party access, no privacy of sharing data. Blockchain is emerging technology which gives promising potential solutions for these issues. Data stored on this blockchain is more secure and ensures confidentiality by using cryptographic techniques. It provides high-quality services to all connected in network and set check constraints for third party access. The aim of this paper is to show a comprehensive view of blockchain technology and its merits. This paper includes study of existing technologies in DSS, storage solutions of DSS with blockchain technology, various access control mechanisms implemented for blockchain. In this paper, we have also discussed about security algorithms used in blockchain, and comparisons among various public blockchain used, consortium blockchain used and private blockchain used in network. Further we discussed about various application areas, where blockchain technology could be implemented.

References

1. J. Benet, IPFS—Content addressed, versioned, p2p file system (draft 3), (2014). https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf
2. Storj—A Peer-to-Peer Cloud Storage Network. https://storj.io/storj.pdf
3. A. Lakshman, P. Malik, Cassandra—A Decentralized Structured Storage system, from Facebook Org
4. A.K. Shrestha, J. Vassileva, Towards decentralized data storage in general cloud platform for meta-products, in *Proceedings of the International Conference on Big Data and Advanced Wireless Technologies (BDAW '16)* (ACM, New York, NY, 2016)
5. Y. Wang, S. Li, Research and performance evaluation of data replication technology in distributed storage systems. Comput. Math. Appl.
6. Z. Beaven, D. Neilson, R. Osborne, P. Pacifico, Blockchain for creative industries music on the blockchain (2016)
7. Public versus Private Blockchains Part 1: Permissioned Blockchains (2015)
8. S. Wilkinson, J. Lowry, Metadisk: Blockchain-Based Decentralized File Storage Application. http://storj.io. August 20, 2014

9. H. Giang, W. Keong, Blockchain-based system for secure data storage with private keyword search, in *on 13th World Congress on Services* (IEEE, 2017)
10. P. Samarati, S. De Capitani, D. Vimercati, Access control: policies, models, and mechanisms (2000)
11. M. Laurent, N. Kaaniche, C. Le, M. Vander Plaetse, An access control scheme based on blockchain technology
12. E.B. Ronghua, G. Chen, BlendCAC: a Blockchain–Enabled Decentralized Capability-based Access Control for IoTs (April 2018)
13. M. Steichen et al., Blockchain-based, Decntralized Access Control for IPFS. IEEE conf. Internet of Things (2018)
14. T.T. Thwin, S.Vasupongayya, Blockchain-based access control model to preserve privacy for personal health record systems. Secur. Commun. Netw. Article ID 8315614, (2019)
15. Z. Zheng, H.-N Dai, Bloakchain challenges and opportunities: a survey. Article ID 101504, (Oct2018)