Rehman et al LGURJCSIT 2019

ISSN: 2521-0122 (Online)
ISSN: 2519-7991 (Print)

LGU Research Jounral for
Computer Sciences & IT

Vol. 3 Issue 4, October - December 2019

Cloud Storage Security Using Blockchain Technology

Areeba Rahman, Dr. Muhammad Rizwan, Dr. Fahad Ahmad

Department of Computer Science, Kinnaird College for Women, Lahore, Pakistan

Abstract:

Data is increasing with increasing Internet technology. To handle the large data, more applications choose to enlarge storage capacity via Cloud plate form. It will not a surprise if we say most organizations have moved towards the cloud. While using the cloud, we have to keep our trust for our sensitive and private data in third parties and the data is usually not encrypted. But we need to implement nearly procedures for the assurance of our reserved data. This will be occupied by blockchains. Blockchain has been a center of attention as a next-generation goal because of its security. A comprehensive approach is used in this paper by signifying diverse blockchain methods to protect cloud computing.

Keywords: cloud storage, Trusted Third parties, Blockchain

1. Introduction

Blockchain-based research had been done on the safety and security of bank money between peer groups and any third party. Blockchain is a ledger for transactions and saves from hacking. Services for remote cloud storage have increased over the past few years. The real problem is transferring data into an outside environment that no one can access that specific data other than the owner.

Many ways can be found to secure data. Services that gives storage for data, to access that data and backups the data are easy to use. They also make life easy but here is a problem of trusting the third party. We handover our data to the third party. To overcome this problem, one way is to encrypt the data or any record. Cloud security provides this defensive approach. But encryption is difficult to handle. Encrypted data becomes secure

In the blockchain, all the transactions are kept encrypted according to the rule that is defined in its software. Bitcoin that is electronic money uses blockchain knowledge. It provides transparency to the whole network. Usually, data is stored in core databases that are less secured as compared to the blockchain because it gives more security and safety of data. Even if the database gets damaged because of attacks, it can be overcome with blockchain. Because of these facts and figures, this technology can be implemented not only in bitcoin but also in cloud computing, the Internet of things (IoT), healthcare and much more. The healthcare industry is incorporating IoT based solutions swiftly. Basically, blockchain is the future of cloud storage. It has been applied in many IT atmospheres also because of the efficiency and availability of cloud computing. Blockchain is a decentralized data structure. Many companies and industries provide their stowage substructure and cloud storage in a decentralized manner. They use servers on their own hosts in their offices that are quite costly and expensive. It is not easy to manage in-house servers because of so many facts one is their cost and management. But a convenient solution is Amazon S3. Services like amazon are totally different. It is unbelievable. These accessibilities keep us safe from the downsides. To secure our very personal, private and

sensitive data we have to keep our trust in these third-party tools. In other words, we are dependent on them just to secure our data. It can be stolen or hacked as well. In blockchain technology, the data is encrypted first and divided into fragments and then distributed among distributed nodes in many countries.

Blockchain provides these incredible features that are not possible before.

- Complete redundancy and true decentralization
- Complete privacy
- Cost Deduction

2. THE BLOCKCHAIN DEFINED

The blockchain is considered the next big revolutionizing technology after the Internet, as it reinvents our way of working and living. In 2008, a scholar who applied the numerical cryptocurrency known as Bitcoin primary presented the impression of a blockchain. The blockchain is fundamentally an important slice of the process of Bitcoin.

Since then there have been many cryptocurrencies with very advanced features, such as Ethereum, which introduces intelligent contracts. The main features of the blockchain are shown in Figure 1.

From the exchange of information to money transfer and other belongings that require online transactions, everything involves a reliable intermediate. This trusted mid-way is accountable and takes all the responsibility in case of any failure and handles all the glitches that are related to security.

The need for a central authority between different companies or parties to carry out multiple functions like data transaction and financial processing has been eliminated by blockchain technology via using straight, undisputable and distributed open accounts [1].

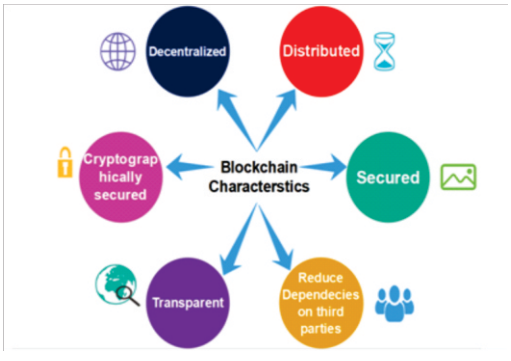

Figure 1. Blockchain Characteristics

The network users use the public ledger which is a distributed and shared database. The public ledger is a kind of record that cannot be interfered with and very secured via cryptographic key distribution and it keeps the records of all of the transactions that have been done among the network users. The property that makes blockchain technology permanent, unchallengeable and irretrievable is that users can view the transactions which are related to them any time they want, but there is a process of validation and once the data or transaction is validated and authenticated, then it can't be deleted nor modified and revised.

There is already a defined criterion for the network users to verify their transaction without confirmation and validation of any significant authority which includes validation, confirmation, agreement, and consensus. It has a great impact on the charge because it reduces the cost. Moreover, it also reduces the chances of data loss that usually happen because of a single point of failure and synchronization have already been done among all of the network users. Therefore, blockchain even assures privacy and security along with other noticeable features in which authentication, validation, decentralization, transparency and much more [2].

The evolution that came along with blockchain technology is high security. It also provides an innovative idea of software-defined parameters. The main thought behind this idea is, before starting the communication, it creates a secure and strong channel first. This channel is associated with a centralized controller. The idea of the software-defined parameter is getting a lot of attention and consideration.

A problem that provoked from the dependency on the third-party authorization which resulted in a single point of failure has also been solved by blockchain. It permits all the associates and network users to maintain a ledger. This ledger contains all of the transaction data and other material. Other than maintaining the ledger, blockchain also allows the users to update the ledger so that the correctness and integrity can be maintained whenever there is new data or a transaction is made.

Recently used research spaces such as cloud, Internet of Things (IoT), edge computing, cloud computing and much more, are based on those entities that are centralized. Whereas, blockchain provides the opportunity to eliminate these centralized controller entities if

these research areas directly apply the blockchain technology. Therefore, the blockchain will benefit several developing technologies, comprising smart cities, banking, and the Internet of Vehicles

The blockchain has broker-free (P2P-based) features. P2P means peer to peer or person to person transactions. The needless fee can be eliminated without having the permission of the third party. Therefore, with blockchain, many people can own the transaction information which makes it difficult to hack. Ultimately, security expenditures are saved. All of the transactions are approved spontaneously and logged by maintaining a record. Hence, reliability, swiftness, and promptness are guaranteed. In this way, transparency can be increased because of the open access and source to the transactions. It can also reduce supervising cost. It also provides a feasibility to the system so that it can be simply applied, linked and Furthermore, the scheme can be effortlessly applied, connected, and long-drawn-out.

There are numerous continuing lessons to reinforce safety by means of these features of blockchain. The utmost significant slice of the blockchain is safety and security connected to the private key cast-off in encryption and here is training on how to defend the private key. An assailant tries a "reuse attack" and additional bouts to get the private key stowed in an aristocrat's scheme in command to menial the bitcoin. The assailant can hack the bitcoin meanwhile the data may have seeped if the assailant can get the private key. To resolve this difficulty, pieces of training on smearing together hardware and software safeties for favorable connections are continuing.

In adding, Blockchain guarantees no dual expenditure occurs.

Transactions are comprised, that is, here are no two transactions that apply the similar even of coins. This is understood by business authentication work in Blockchain. Some approaches and models have been discussed in this paper to secure cloud storage with different blockchain models.

3. BLOCKCHAIN SECURED CLOUD STORAGE USING CHAINFS

This exertion boons ChainFS, a bridge scheme that safeguards cloud storing facilities by means of a slightly reliable Blockchain. ChainFS toughens the cloud storing safety in contradiction of splitting rounds .

The chains Bridge delivers the end workers through a file scheme border. Within, ChainFS supplies information records in the cloud and spreads to the blockchain negligible and essential functioning for key delivery and cataloging of file operations. We organize and carefully assimilate the ChainFS scheme on Ethereum and S3FS with FUSE patrons and Amazon S3 cloud storing. We amount the presentation of the scheme and display little overhead.

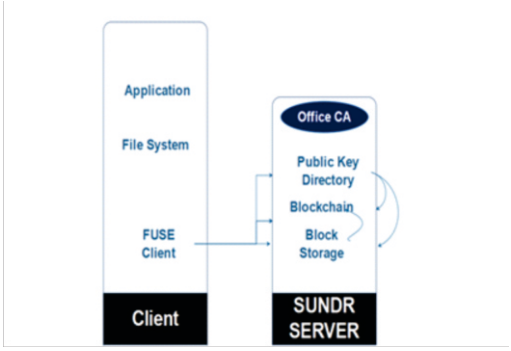

Figure 2. System Overview

A. SECURITY ANALYSIS WITH CHAINFS

ChainFS influences the Blockchain to add forking-attack pliability to an encoded file scheme on the cloud. For equal open key almanac and file scheme processes, it upholds a lined record of application-dependent entrances and charts the record to Blockchain.

Forcing attacks in the open almanac means that the cloud has dissimilar key terms (of the same person) for dissimilar customers. For the customer to receive the requisite, recall that it forms the presence of the compulsory in the almanac snap with abridgment as a checked log entrance in the blockchain. Two record entrances must be checked in the blockchain at the similar time to let two patrons to receive two cleft bands. .

For the SUNDR attack (SUNDR is a network file system designed to safely store data on untrusted servers) the stowage server can extant two encoded and dissimilar files to two diverse customers. These two measures are logged in the native logs of these two customers. In adding, the cloud server records its own global log version in the Blockchain. Native records will be likened to the worldwide record

during log certification and auditing to exam whether the native record is a subsection of the worldwide record and if there is a fissure of the steadiness of the storing. In order to avoid the attack, Blockchain must be forced to fork itself. It is difficult in a large community blockchain to divide chunks that are established (e.g. after 6 times).

B. PERFORMANCE

We take three kinds of machineries in this experimentation system. Mainly, we create an Amazon S3 AWS account and route cloud cases. Furthermore, we route our FUSE patrons nearby. The customer mechanism has an Intel(R) Xeon(R) CPUE5-2680 v3 CPU with a memory of 2.50GHz and 10 GB Then, the Blockchain is a track on three server engines with the subsequent requirement: 2.70GHz and 8 MB hoard Intel8-core i7-6820HK microchip, 32 GB Ram and 1 TB Disk.

File Create/Write Performance: In tests, we primary usage LFS minor file standards to produce 1000 small files of 1 KB to 100 KB sizes. We practice the Linux dd value to produce files and ration phase. Regular time and standard deviation are stated. In this situation, the files are produced by means of arbitrary content so that the abridgments to be placed on Blockchain alteration and ChainFS has no partial advantage.

The consequences of the minor file experiment are shown in figure 2. Our ChainFS has up to 35 percent overhead presentation (with 10 KB files) to parallel the best situation that turns an S3FS without a Blockchain. As the files produce large, the overhead shrinkages. The routine becomes unbalanced, particularly when files are too minor. The participation of Blockchain does not upsurge much standard deviation, and we are unsure that this is for the reason that the actual cloud connection is rather undefined.

We also convey out experimentations with big files following a related process. Files with a file mass of amid 1 MB and 1 GB are created. We degree the period of implementation and state metrics in a similar method as the minor file situation. The outcome is shown in Figure 3. The overhead of the Blockchain upsurges as the file produces greater and spreads a supreme of 28 percent (1 GB). In the outsized file arrangement, the blockage scheme handovers data above the Internet .

File Read Performance: We perform experimentation to estimate ChainFS' evaluation dormancy. The customer engine primary turns a script in the testing to generate 100 mutable scope records (from 1 KB to 100 KB). It formerly jolts a sequence of Linux CAT instructions to read the files above and over again. We portion the period consumed in the next phase (i.e. CAT commands) in this testing. On usual, ChainFS enhances about 30 percent overhead to the fixed cloud file arrangement read pathway. As the file produces huge, the overhead stays continuous .

4. BLOCKCHAIN-BASED ACCESS CONTROL SCHEME FOR CLOUD STORAGE

In this approach, a multiple worker system prototypes for controlling access is used for data sets to be stored in a cloud atmosphere that is not trusted. Just like any not trusted environment, cloud storage requires the ability to secure information sharing. This approach allows access to data/information which is stored in the secured cloud without the participation of the provider. The main tool which is used to access the control mechanism is a text-policy encryption scheme based on static attributes with dynamic attributes. The proposed scheme delivers an immutable record of all meaningful data security events, such as key generation, access policy assignment, access request, change or revocation, using a blockchain-based decentralized ledger. We suggest a set of cryptographic procedures to ensure the privacy of secret or private key cryptographic operations. Only hash code ciphertexts are transmitted via the blockchain ledger. Our system's prototype is implemented with intelligent contracts and tested on the Ethereum blockchain platform .

The aim of the problem-solving approach is to develop an access control model based on blockchain transactions, data storage in untrusted storage and the implementation of Ethereum smart contracts based on attribute-based encryption. We use a model of access control based on attributes. XACML is the most commonly used standard for access control based on attributes. This standard describes the components, purpose, interaction and use of the access control system.

The system is expected to apply to various types of data, such as multimedia

information, electronic documents, etc. It is not advisable to store this amount of data directly in the blockchain, as increasing the number and the size of the blocks increases the complexity of Ethereum, which mainly affects the cost of transactions. Therefore, data is stored in cloud storage in which the file identifying information is only available .

The Ethereum platform is designed to create a blockchain-based decentralized service. It's a single virtual machine distributed. Smart contracts Unlike Bitcoin, Ethereum supports cycles that, on the one hand, have led to the introduction of fees for their implementation, called gas, and have significantly expanded their applications on the other. Changing the virtual machine status can be written in the full script language of Turing. For each file, the user creates a smart contract that stores owner information, access policy, hash sum of the stored information, cloud identifying information, and any changes to the file. Since the information stored in the blockchain is public, information must be encrypted before it is sent to storage and access controlled.

The interaction scheme between the client, CA and AA is shown on Fig. a contract file is created to store data. It contains information on the location of the file in the cloud storage, access policy and information for additional owners. It is possible to interact with the file using the contract. The system supports four types of interactions: create, edit, read, and delete.

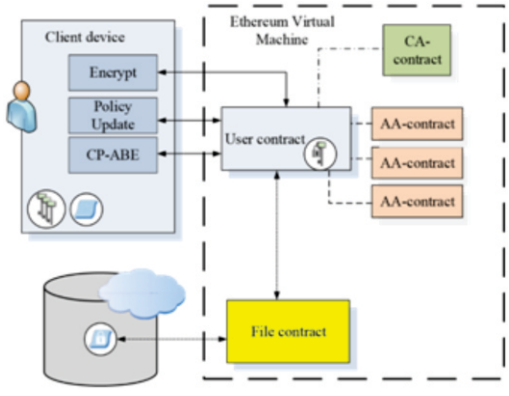

Figure 3. Access Control System

For altering the file's contact strategy, the CD does apprise of the contact environment and mechanisms of the ciphertext. It formerly modernizes the facts in the pact file and substitutes the mechanisms of the ciphertext in the cloud .

When removing a folder or a file, the pact case self-destroys and CD must eliminate it from the cloud. After erasing the file, the connection to it cannot be cast-off all over again in the scheme to eradicate the option of arguments. A worker wanting to read a file must bout the access strategy and have the essential keys to decrypt. After testing for strategy acquiescence, the worker obtains a connection to the file and can copy it, and then decode. If the user does not see access strategy, then the file it is to decode even if he will be capable to tie to it .

5. BLOCKCHAIN CLOUD AND RELATED SUSCEPTIBILITIES

Amongst all the safety matters that occur in the cloud atmosphere, blockchain will be very operative in addressing the tasks and challenges intricate in the application of certain data attribution. We extant the tests related to certain data attribution in the cloud and blockchain competences to report them.

A. Blockchain and Cloud Security

Cloud computing permits users to distantly stock their data into the cloud and delivers on-demand requests and facilities from a shared loch of configurable calculating properties. The sanctuary of the subcontracted data in the cloud is reliant on the safety of the cloud computing scheme and net. Though, cloud's key features, on-demand facilities, continuous network contact, reserve assembling, and fast resistance are vulnerable to vulnerabilities. In adding, the cloud computing's central tools for virtualization, cryptography, and net amenities have susceptibilities, that are consequences of uncertain application. At a similar time, security checks, such as key organizations, in the cloud computing environment have numerous trials. For example, to the appliance, an operative key management scheme in cloud computing substructure needs administration and storing of many types of keys. The trouble in conveying standard key organization twigs from the point that simulated technologies typically have varied and heterogeneous hardware/software, and the cloud-dependent computing and storing are purely distributed.

The problem relies on the cloud substructure is that if some unauthorized entity tries to interfere and change the data, it cannot be detected. It happens because of the PKI based nature of the cloud. Therefore, a very strong attribution structure is required so that this problem can be eliminated and the responsible entity can be detected. Data authority is a thing that delivers information about all the changes and variations accomplished through data exchange between different units. Scholars have projected safety keys, such as PKI signatures, to guarantee the provenance. Whereas the application of PKI signatures normally rests on a central authority, that is not operative in the cloud substructure .

Blockchain claims that it does not require a central system or central authority because its execution is different from the rest of the technologies. There are some ledgers which are distributed, that ledges hold and record all of the transactions and actions that have been done on data. After maintaining the record it shares that with all of the other users who are the participating units. Blockchain provides complete and safe transmission of information via a system of some cryptographically secure keys in a distributed environment. Hence, blockchain and keyless signatures can be the replacement of PKI signatures. The transactions in the public ledger are verified by a consensus of the majority of participating entities.

The record of any transaction cannot be changed in blockchain technology because it is confirmable. Signatures that are keyless are those signatures that are unlike traditional digital signatures. These keyless signatures state an issue of "PKI key compromise". PKI is "Public key Infrastructure" which depends on the distorted phenomenon of key cryptography. It disassociates the reliability and integrity protection and process from identifying the signer. These are those processes that are accountable for keeping the privacy and secrecy of the keys. The asymmetric cryptography and keyless cryptography are the choices from the techniques that are helpful in the identification of signer and protection of integrity. Hashing, publications, and aggregation are the methods of the keyless signature phenomena. One of the examples of keyless cryptography is "One-way Collision-free hash functions"

The understanding of keyless signatures needs a Keyless Signature Infrastructure (KSI) that contains a pyramid of the co-operative aggregation servers which produce the universal hash trees. The authentication in KSI centers on the safety of hash functions then accessibility of a community record (blockchain). The ledger is openly accessible and rules to bringing up-to-date, spreader consent and way of the process are well cleared.

I. DIFFERENCE

Table 1: Different Methodologies and their purpose

Methodologies	***Performance***
ChainFS	Reduces Forking attack. File create/read/write performance is better.
Access Control System	No provider contribution included. No third party presence. Accounts deliver an immutable record of all events.
Keyless Signatures Distributed Information	Deliver cryptographic tools to remove the errors in PKI based signatures. Superior then public key substructure.
PKI based signatures	Public key infrastructure (**PKI**) security technique is used to implement strong verification, data encryption , and digital signatures.
Cipher-text Policy attribute - based encryption	Cipher-text is an encrypted manuscript. A text before encryption is basic text and cipher -text is the encrypted consequence.

According to all directly above deliberated techniques and methodologies of securing cloud storage with blockchain technology, the access control system has been the best approach so far. The Access control system uses the cipher-text policy to encrypt the data. The previously attribute-based encryption system used attributes to present encrypted data. While in cipher-text attributes they are used to define user's credentials. Text is plain before encryption and cipher-text encryption is the resultant data. The access control system also maintains a log of all events as shown in figure6 [5-9].

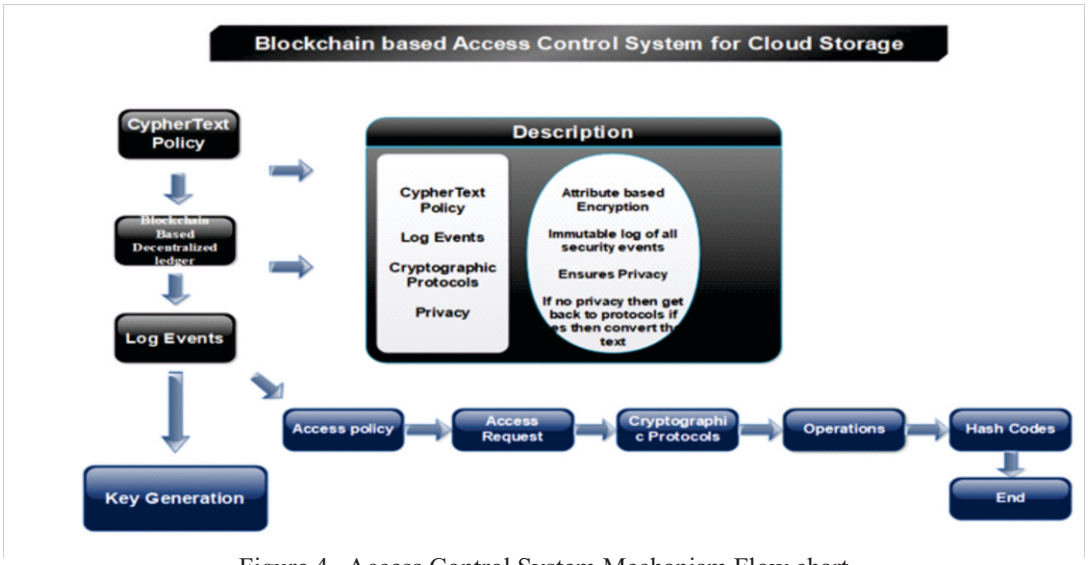

Figure 4. Access Control System Mechanism Flow chart

7. CONCLUSION

This paper presents a comprehensive approach to secure cloud storage using different blockchain methodologies. All the methods result in providing end-users to securely share their data. The best method among all of the above solutions is an Access Control System that provides a model to safe data by making it unchallengeable. The main idea is to adjust the access strategy for the encoded and encrypted data without repeating them to a huge amount of members that makes its presentation improved than ChainFS system and keyless signatures. Even though they have their individual compensations.

REFERENCES

[1] J. C. K. L. C. A. K. K. K. L. N. Qiwu Zou Yuzhe Tang, "ChainFS: Blockchain-Secured Cloud Storage," in 2018 IEEE 11th International Conference on Cloud Computing, New York, 2018.

[2] N. M. S. P. M. E. K. a. C. Y. Deepak Puthal, "The Blockchain as a Decentralized Framework," IEEE Consumer Electronics Magazine, p. 4, March 2018.

[3] S. Z. Ilya Sukhodolskiy, "A Blockchain-Based Access Control System for," 978-1-5386-4340-2/18/$31.00©2018 IEEE, p. 4, 2018.

[4] C. A. K. K. A. K. L. N. D. K. T. S. S. Xueping Liang, "Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack," in 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, 2017.

[5] T. Boxcryptor, 2017. [Online]. Available: https://www.boxcryptor.com/en/.

[6] H. M., "Attribute-Based Encryption Optimized for Cloud," SOFSEM, 2015.

[7] L. B. N. T. Courtois, "subversive miner strategies and block withholding attack in bitcoin digital currency," arXiv preprint.

[8] "Amazon AWS," [Online]. Available: https://aws.amazon.com/..

[9] G. Developers, "Google cloud computing, hosting services & apis.," 2015.