Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

BCSA: BLOCKCHAIN-BASED SECURE ACCESS CONTROL WITH INTRUSION DETECTION MECHANISM

[1]T. Sanmathi, ME., Department of Computer Science and Engineering, Angel College of Engineering and Technology, Tirupur, Tamilnadu
[2]Mr. M. Kumaresan, ME, Assistant Professor, Department of Computer Science and Engineering, Angel College of Engineering and Technology, Tirupur, Tamilnadu

Abstract

Cloud storage administrations provide customers with the best data storage management for massive amounts of data. Regardless, the data in the outside storage leads cloud storage expert co-ops to cope with the data. As a result, our job should consider ensuring data security and maintaining data trustworthiness while benefiting from beneficial services. This article suggested the BCSA Method, a blockchain-based intrusion detection and firewall safety, through a study on the cloud storage administration model and blockchain innovation. Furthermore, associated conventions are based on arrangement-based engineering. In our approach, the decentralized model addresses the sole purpose of the trust in the traditional data assessing administration architecture through aggregating trust. An open understanding enables reviewers to generate proof of data honesty without constructively touching data. According to security analysis and performance assessment, the suggested technique offers a greater security guarantee than current schemes at the price of acceptable computational costs.

Keywords: Cloud Storage, BlockChain, Access Control, Intrusion Detection, Security

I INTRODUCTION

Cloud Storage Service (CSS) provides unparalleled benefits such as on-demand self-service, omnipresent network connectivity, location-independent resource pools, and quick and flexible resource use regulations. It is transforming the character of corporate storage resources as a disruptive technology with far-reaching implications. Data is centralized and kept on the cloud is a fundamental change in this strategy. Users may alleviate the burden of local data storage and maintenance with remote data storage in the era of big data and service ecosystems. On the other hand, external data storage allows cloud storage service providers to take control of their data, posing security concerns for data and private information. The following factors may contribute to this kind of occurrence that jeopardizes data security: Even if the data saved by the user is totally or partly destroyed, the cloud storage provider may nevertheless persuade the user that it owns the data. Misconduct on cloud storage servers may range from recovering storage space by intentionally destroying data that users have not yet or seldom accessed to concealing data loss occurrences (due to management errors, hardware failures, external or internal attacks).

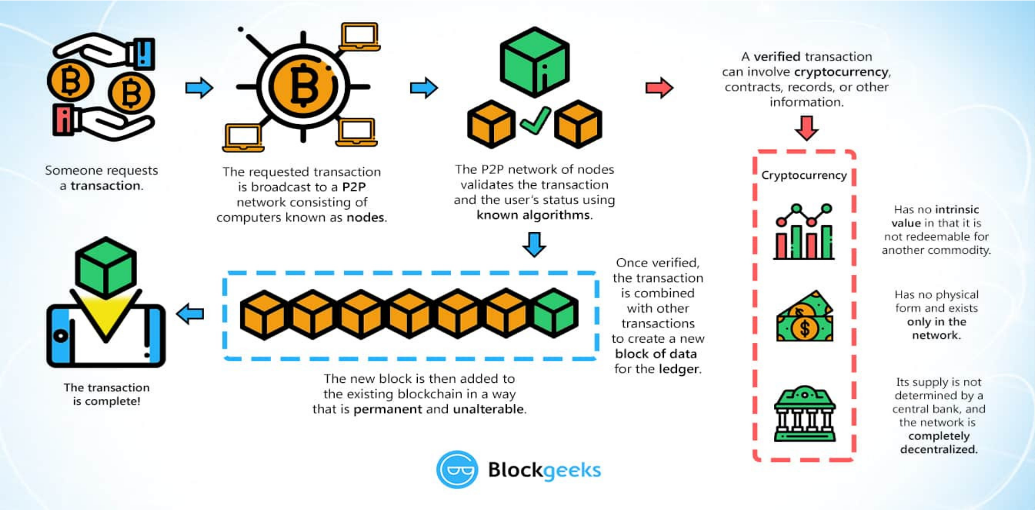
Someone requests a transaction.
The requested transaction is broadcast to a P2P network consisting of computers known as nodes.
The P2P network of nodes validates the transaction and the user's status using known algorithms.
A verified transaction can involve cryptocurrency, contracts, records, or other information.
Cryptocurrency
Has no intrinsic value in that it is not redeemable for another commodity.
Has no physical form and exists only in the network.
Its supply is not determined by a central bank, and the network is completely decentralized.
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.
The new block is then added to the existing blockchain in a way that is permanent and unalterable.
The transaction is complete!
Blockgeeks

Figure 1: Block Chain Architecture

In general, access control in systems is implemented in three steps: identification, authentication, and authorization. Aside from allowing only authorized users to enter a system, access control guarantees accountability: the ability to trace which user performed what action in a system. Traditional access control systems allow security managers to identify which users have access to a certain piece of information. Today's systems are more prone to hackers and anonymous invasions.

A. Problem definition

Large volumes of sensitive data are stored on the cloud by users. In our current system, sharing sensitive data will assist firms in lowering the cost of offering individualized services to consumers while also providing value-added data services. However, secure data exchange is a challenge. Security is one of the most challenging aspects of cloud computing to accomplish. As a result, security is not improved in the current environment. Even with adopting multilayered security, there will remain uncertainty (i.e., the uploaded viruses and Trojans are blocked by the data center, even after the user continuously tries to upload the virus file). A server is kept busy in this situation. We are addressing this problem by creating a notion of malicious user blocking. Safe file sharing is not covered because the cloud is a multi-user accessible source; unwanted access might abuse data. Accessibility permission is permitted in our suggested system, i.e., file accessing permission is supplied through an email address, so an authorized user can only view the files.

II RELATED WORKS

To address the synchronization challenges in conventional distributed databases, the blockchain incorporates distributed consensus and peer-to-peer networking and cryptographic methods, mathematics, and economic models. The connected publications describe the key features of the blockchain and its benefits.

Joshi, Archana et al. [1] discuss blockchain security and privacy concerns, providing extensive data about the blockchain, its principles, the consensus methods utilized, and the blockchain kinds.

Biswas et al. [2] suggest using blockchain technology to protect smart cities from digital disruption and create a secure communication platform for smart cities. Yli-Huumo et al. [3] present a comprehensive review of blockchain research. Halpin, Harry, et al. [4] present an introduction to blockchain security and privacy concerns "Including peer-reviewed publications to collect unresolved topics related to blockchain security and privacy. The report also discusses the blockchain research problems ". Lin et al. [5]

emphasize the existing regulatory concerns, integrated cost problems, and the blockchain's fork problem that produces security issues and obstacles. Suma and colleagues [6] blockchain, as a fundamental technology influencing and attracting a broad variety of applications, has emerged as a dominating solution to the challenge of privacy preservation and security across a wide range of sectors controlled by the government and the private sector. To increase blockchain security, the author suggests a blockchain with an RSA digital signature ".. Bhalaji, N et al. [7] advocated using blockchain to improve the quality of service and defense in wireless networks that are built on the fly. I. J. Jacob et al. [8] offer a biometric recognition system for safe information exchange. Sivaganesan, D. et al. [9] discuss the security of the internet of things as it is controlled via the blockchain. S. Smys et al. [10] explain and propose "Prevention of inference attacks for private information on social networking sites." Karthiban, K. et al. [11] present privacy-preserving cloud computing techniques. Dinesh Kumar et al. [12] offer a unique wireless body network assault detection approach. Though the articles emphasized the different applications available to secure transactions using the blockchain, many people are still unaware of the linking-inability issue that causes security breaches in the blockchain and its solutions. The paper's suggested technique combines homomorphic encryption [13] as well as game-based smart contracts [14] [15] to protect the blockchain from privacy issues induced by unlinkability.

III SYSTEM MODEL

This system suggested a new secure decentralized cloud storage solution with access control using blockchain technology. The possible single-point failure of the central authority in the original concept is mitigated to some degree in this scheme by integrating blockchain technology. At the same time, the addition of a blockchain to the access control scheme is equal to adding a logging system to record all access operation records. In our system, Smart Contract will hold information about the encrypted file. More crucially, smart contracts are used by data consumers and owners to store and retrieve ciphertext data to perform encryption and decryption algorithms. Every contract call is recorded on the blockchain. As a result, the information sent between data users and owners is non-tamperable and non-repudiable.

1) GenKey - When an entity connects to the network, the system generates account information such as a password. The protocol algorithm's output is the user's key pair (pk, sk).

2) SigBlock - Extract the file label of a data block.

3) SigOps - This event will be recorded when user data is migrated from one account to another.

4) TraceEvent - Retrieve the details of the data block transfer event from the blockchain-based on the file label of the data block.

3.1 System Methodology

Cloud server: Responsible for storing encrypted files uploaded by data owners;

Ethereum blockchain: Deploy smart contracts on Ethereum, the smart contracts is of interfaces to store data and get data;

Data Owner(*DO*): Responsible for creating and deploying smart contracts, uploading encrypted files, defining access control policies, assigning attribute sets, and appending valid access periods to data users;

Data User(*DU*): Accessing an encrypted file stored in the cloud server. When its attribute set satisfies the access structure embedded in a given ciphertext, it can decrypt the received ciphertext to obtain the content key to decrypt the encrypted file.

Encrypt $(PK, ck, \Gamma) \rightarrow CT$. The encryption algorithm takes the public key PK , access structure Γ and the symmetric encryption key ck as inputs, and outputs the ciphertext CT . The ciphertext CT is stored by DO in smart contract.

KeyGen $(MSK, S) \rightarrow SK$: The key generation algorithm is still executed by the data owner DO . DU sends a access request to DO , then DO assigns attributes set to DU and adds the effective access period to DU .The algorithm sets the attribute set S of DU , the master key MSK as inputs, and outputs the private key SK of DU . After DO and DU share the common key (the Diffie-Hellman key exchange protocol generates the common key), SK is symmetrically encrypted by the AES algorithm with the common key as encryption key. The ciphertext *SK*, the encrypted private key, is stored in the smart contract to ensure its privacy.

Decrypt (*PK*, *SK*,*CT*) →*ck*: The decryption algorithm is executed by *DU*. The *DU* obtains an access period from smart contract. Then *DU* performs the decryption algorithm if the time is within the valid access period. *DU* obtains *CT* and the private key's ciphertext *SK*' from smart contract. The *SK* is decrypted as the private key *SK* by the symmetric encryption algorithm AES by using the common key as the decryption key. The algorithm inputs the public key *PK* , private key *SK* and ciphertext *CT*. If and only if *SK* satisfies the access policy *Γ* , *DU* can recover the key *ck* of the encrypted document so that the encrypted document is decrypted, otherwise, the decryption will fail. *DU* obtains the encrypted document *Eck* (*M*) from the cloud server, decrypts the encrypted document *M* by using key*ck* , and outputs the document *M* before *DO* encrypts.

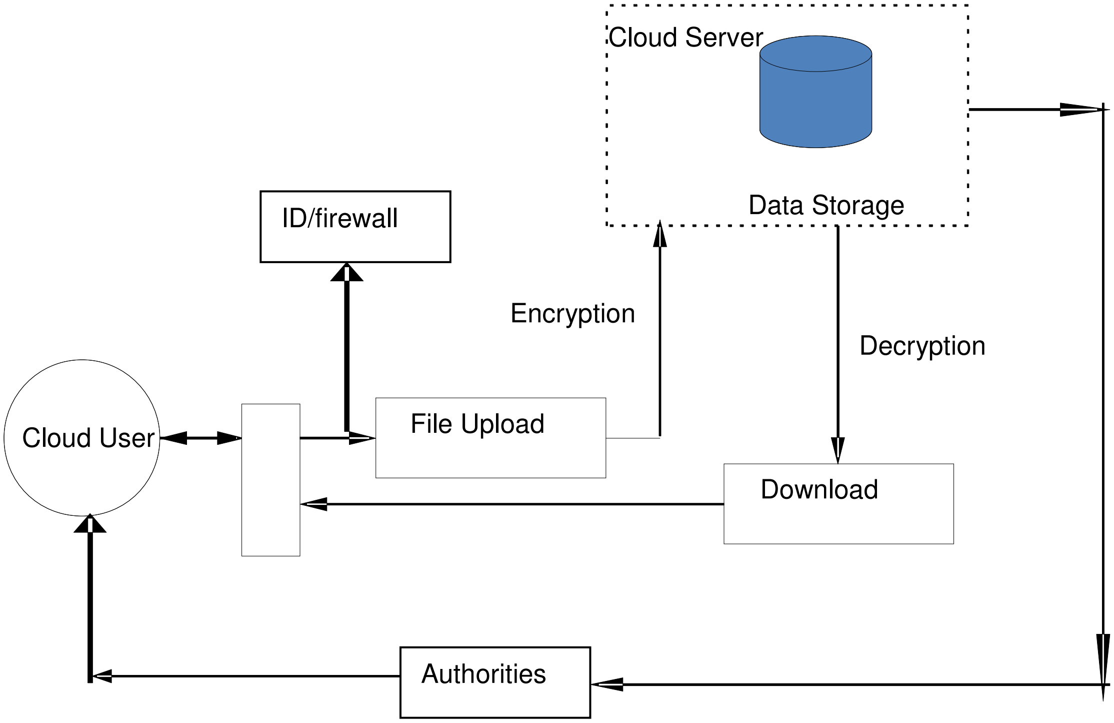

Figure 2: System Architecture

3.2 INTRUSION DETECTION AND PREVENTION

The goal is to detect intrusions and attacks. Identity management is enforced to guarantee that only the appropriate degree of access is allowed to the appropriate individual. The intrusion detection section alerts the cloud management team, data center, data owner, and security pools about intrusions by raising alarms. The threats posed by the incursions are scalable. The rejection and warning emails will be written for the data owner to receive. The process begins with a probable intrusion event (this might be unlawful access to data), which prompts the client process in this model to compose an email/message to the cloud data administrator.

3.3 SECURED DATA SHARING

It can resolve issues between several user contexts when it comes to sharing. If the person needs to view a file that the data owner has updated, he must first make an access request to the owner; after receiving access confirmation through email alert (access key), he may only access the system. So that only authorized users may access the file system, allowing the data owner to transfer files securely. Unauthorized access may be stopped with the aid of this improved technology.

IV RESULTS AND DISCUSSION

The Asp.Net programming language was used to build the BCSA approach. We focus on information security while meeting a massive increase in information, regardless of whether it is from external sources, such as an attack of viruses or trojans, or internal sources, such as clients or customers gathering several gigabytes of information every day. This is an investigation problem for information security, which is critical for the better management of the server farm to cope with a rapid increase in data. Aside from server farm security administration for quick information creation, the product design technique should be adequately robust to survive assaults and unauthorized access. The whole approach may also be linked with the advancement of a structure to manage the specific plan and utilization, administration, and strategies associated with fantastic practices. This motivates us to create a method, BCSA, to assist organizations in successfully receiving and conveying any cloud services and ventures. This document outline executes and responds to our Cloud security blueprint. We use infiltration testing and related examinations to validate its power and accuracy and review and F-measure to justify favorable circumstances over other methodologies.

V CONCLUSION

We presented the BCSA approach, blockchain-based secure data exchange, and a computerized resource conveyance system. The primary goal of this suggested situation is to provide data legitimacy and quality to the client while also providing a consistent business stage for the proprietor—decentered storage addresses the expansion concern at the proprietor's end. A blockchain-based secure cloud storage access control architecture is presented. The standard ciphertext-policy attribute-based encryption technique is modified by including Intrusion detection and Firewall security features. The distribution key is no longer reliant on the central authority to keep the central authority safe from attack. Our plan is decentralized. Interaction between data owners is used to construct a distributed access control strategy. To increase security and efficiency via the usage of user rights for future research.

VI REFERENCES

[1] Joshi, Archana Prashanth, Meng Han, and Yan Wang. "A survey on security and privacy issues of blockchain technology." Mathematical Foundations of Computing 1, no. 2 (2018): 121-147.

[2] Biswas, K., & Muthukkumarasamy, V. (2016, December). Securing smart cities using blockchain technology. In 2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS) (pp. 1392-1393). IEEE.

[3] Yli-Huumo, Jesse, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander. "Where is current research on blockchain technology?—a systematic review." PloS one 11, no. 10 (2016): e0163477.

[4] Halpin, Harry, and Marta Piekarska. "Introduction to Security and Privacy on the Blockchain." In 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 1-3. IEEE, 2017.

[5] Lin, Iuon-Chang, and Tzu-Chun Liao. "A Survey of Blockchain Security Issues and

Challenges." IJ Network Security 19, no. 5 (2017): 653-659.

[6] Suma, V. "SECURITY AND PRIVACY MECHANISM USING BLOCKCHAIN." Journal of Ubiquitous Computing and Communication Technologies (UCCT) 1, no. 01 (2019): 45-54. [7] Bhalaji, N. (2019). QOS AND DEFENSE ENHANCEMENT USING BLOCK CHAIN FOR FLY WIRELESS NETWORKS. Journal of trends in Computer Science and Smart technology (TCSST), 1(01), 1-13.

[8] Jacob, I. J. (2019). CAPSULE NETWORK BASED BIOMETRIC RECOGNITION SYSTEM. Journal of Artificial Intelligence, 1(02), 83-94.

[9] Sivaganesan, D. (2019). BLOCK CHAIN ENABLED INTERNET OF THINGS. Journal of Information Technology, 1(01), 1-8.

[10] Praveena, A., and S. Smys. "Prevention of inference attacks for private information in social networking sites." In 2017 International Conference on Inventive Systems and Control (ICISC), pp. 1- 7. IEEE, 2017.

[11] Karthiban, K., and S. Smys. "Privacy preserving approaches in cloud computing." In 2018 2nd International Conference on Inventive Systems and Control (ICISC), pp. 462-467. IEEE, 2018.

[12] Anguraj, Dinesh Kumar, and S. Smys. "Trust-based intrusion detection and clustering approach for wireless body area networks." Wireless Personal Communications 104, no. 1 (2019): 1-20.

[13] [n. d.]. Ethereum Project. https://www.ethereum.org. ([n. d.]).

[14] Kalodner, Harry, Steven Goldfeder, Xiaoqi Chen, S. Matthew Weinberg, and Edward W. Felten. "Arbitrum: Scalable, private smart contracts." In 27th {USENIX} Security Symposium ({USENIX} Security 18), pp. 1353-1370. 2018.

[15] Jason Teutsch and Christian Reitwießner. 2017. TrueBit: A scalable verification solution for blockchains. (2017)