International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 1, December 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

An Analytical Survey on Data Access Control Mechanism in Cloud using Blockchain

Rushabh Rajendra Desarda, Nishant Ganesh Chavan, Amit Gunaji Chaure, Pankaj Ramanlal Gandhi, Prof. S. E. Ingale

Computer Department, MES College of Engineering, Pune, Maharashtra, India

ABSTRACT

Cloud storage is known for its huge infrastructure, this property of the cloud inevitably invites attackers. However, to overcome this data stored in encrypted form, this security measure is not enough to handle the issue of data privacy. The other threat to the data arises during the process of accessing these data through various forms like by auditors, other users, data owners and some time by cloud owner itself. To handle these issues quite effectively strict access control mechanism is deployed at cloud end. However, this is not enough to make sure the data is safe, as now a day's data is accessed in multiple tiers by the users, so the block chain is used to effectively to monitor the data sharing between the owners and users. This paper working towards the analysis of the attacks and handling of these attacks using block chain. As the bit towards this paper also proposed to handle data integrity effectively by the usage of block chain and bilinear pairing mechanism together to provide the best solution for data access control mechanism incloud inevitably.

KEYWORDS: *Cloud Computing, Data Security, BiLinear Pairing, BlockChains*

How to cite this paper: Rushabh Rajendra Desarda | Nishant Ganesh Chavan | Amit Gunaji Chaure | Pankaj Ramanlal Gandhi | Prof. S. E. Ingale "An Analytical Survey on Data Access Control Mechanism in Cloud using Blockchain" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-1, December 2019, pp.875-878, URL: www.ijtsrd.com/papers/ijtsrd29724.pdf

IJTSRD29724

I. INRODUCTION

Cloud storage is outlined as "the storage of knowledge on-line within the cloud," whereby a company's knowledge is held in an accessible from multiple distributed and connected storage resources that comprise a cloud.

Cloud storage will offer the advantages of larger accessibility and reliability; speedy deployment; sturdy protection for data backup, repository and disaster recovery purposes; and lower overall storage prices as a result of not having to get, manage and maintain expensive hardware. There are several advantages to the victimization of cloud storage, however, cloud storage will have the potential for security and compliance considerations that don't seem to be related to ancient storage systems.

Also referred to as mobile cloud storage, personal cloud storage may be a set of public cloud storage that applies to store somebody's information within the cloud and providing the individual with access to the information from anyplace. It conjointly provides information syncing and sharing capabilities across multiple devices. Apple's iCloud is an example of non-public cloud storage.

Public cloud storage is wherever the enterprise and storage service supplier are separated and there are not any cloud resources held within the enterprise's data center. The cloud storage supplier absolutely manages the enterprise's public cloud storage.

It is a variety of cloud storage wherever the enterprise and cloud storage supplier units are integrated at regular intervals at the enterprise's knowledge center. In private cloud storage, the storage supplier has an infrastructure at intervals the enterprise's data center that's typically managed by the storage supplier. personal cloud storage helps resolve the potential for security and performance issues whereas still providing the benefits of cloud storage.

Hybrid cloud storage may be a combination of public and personal cloud storage whenever some vital data resides within the enterprise's private cloud whereas alternative knowledge is kept in an accessible form a public cloud storage supplier.

Cloud security is the protection of data held on online platforms from thieving, leakage, and deletion. ways of providing cloud security embody firewalls, penetration testing, obfuscation, tokenization, virtual non-public networks (VPN), and avoiding public net connections. Major threats to cloud security consist of data breaches, data loss, account hijacking, service traffic hijacking, insecure programmer interfaces (APIs), poor selection of cloud storage suppliers, and shared technology that may compromise cloud security. Distributed denial of service (DDoS) attacks is another threat to cloud security. These attacks finish off service by overwhelming it with data in order to stop users from accessing their accounts, like bank accounts or email accounts.

Cloud security is crucial for the various users who are involved with the security of the info they store within the cloud. They believe their knowledge is safer on their own native servers wherever they feel they need additional management over the info. However, data kept within the cloud is also safer, as a result, the cloud service suppliers have superior security measures, and their workers are security An analytical Survey on Data Access Control mechanism in cloud using blockchain specialists. On-premise data is often additional at risk of security breaches, counting on the kind of attack. Social engineering and malware will build any knowledge storage system vulnerable, however, on-the-scene data are also additionally vulnerable since its guardians are less skilled in sleuthing security threats.

Cloud security could be a key concern for cloud storage suppliers. They not solely should satisfy their customers; they additionally should follow restrictive needs for storing sensitive knowledge like Mastercard numbers and health data. Third-party audits of a cloud provider's security systems and procedures facilitate to make sure that users' data is safe.

Maintaining the safety of knowledge within the cloud extends on the far side securing the cloud itself. Cloud users should shield access to the cloud that may be gained from data kept on mobile devices or carelessness with login credentials. Another cloud security issue is that data kept on a cloudhosted in another country is also subjected to totally different laws and privacy measures.

When selecting a cloud supplier, it's necessary to settle on an organization that tries to shield against malicious insiders through background checks and security clearances. the majority suppose outside hacker's are the largest threat to cloud security, however, workers also offer even as massive of a risk. These workers aren't essentially malicious insiders; they're usually workers who unwittingly build mistakes like employing a personal smartphone to access sensitive company knowledge while not the safety of the company's own network.

The blockchain was fabricated in 2008 by a programmer referred to as Satoshi Nakamoto. To date, nobody is aware of who Satoshi Nakamoto is, and whether or not he's someone or whether or not the name represents a bunch of individuals. Blockchain has evolved into one thing terribly powerful since then.

Blockchain technology is made by taking advantage of peer-to-peer networking. Anyone can be a part of the network and ther 's no central authority to manage it. it's operated by individuals, referred to as miners, who lend their computing power to the network so as to unravel advanced algorithms. Machines used by miners perform the mandatory functions to make the transactions, and for that, they're rewarded with a fee (for loaning their computing power). within the case of Bitcoin, that advanced formula is SHA-256.

In a blockchain, every block stores the info of the action, it's hash code and also the previous block's hash code. So, whenever a replacement block is formed, it's valid by a majority of the peers or miners thereon on the network. If anyone tries to vary the info in one block, the whole blockchain is going to be invalidated; thus, it's nearly impossible for an individual to vary all different connected blocks—and that's, how, a blockchain remains secure and managed. Also, all the information is encrypted for security reasons. Bitcoin works on identical technology. it's a virtual currency that's deep-mined using the blockchain technique and now days, the worth of 1 Bitcoin is Rs 458,609. So, as you'll be able to imagine, it's just about like gold.

This research paper dedicates section 2 for analysis of past work as literature survey and finally section 3 concludes this paper.

II. LITERATURE SURVEY

This section of the literature survey eventually reveals some facts based on thoughtful analysis of many authors work as follows.

S. Wang [1] estimates cloud computing and big data technology has been rapidly developed in recent years most of the enterprises select to deploy the data to cloud service providers. For data management and storage cloud computing provides a low-cost, scalable, location independent infrastructure. Deduplication technique is used to moderate costs by taking advantage of the redundancy of storing data and also keep away from storing the same data multiple times in real life. The proposed paper on blockchain technology presents a decentralized fair payment scheme.

Qiwu Z [2] narrates the popular and new attack incidents e.g., data breaches that are emerging in Cloud security. Blockchain is a trusted third-party framework (TTP) to set the security of cloud storage and also to defend against attacks. The data stored on the cloud is end-to-end encrypted. Thus the attack surface concentrates on the planes of key management about encrypted data. Malicious cloud server attends the different requests to different clients of the same query in a forking attack. In the proposed paper the ChainFS system on Ethereum and S3FS and closely included with FUSE clients and Amazon S3 cloud storage.

K. Wang [3] explains the trend of integrating cyber, physical and social (CPS) systems to a highly unified information society is increasing in recent times because of the huge development in the field of information technologies. There is a huge risk of privacy leakage of data owners because of the increasing amount of personal data, including location information, web-searching behavior, user calls, user preference which is collected by the built-in sensors. The concept of blockchain technologies may be the best way to achieve this aim throughout the network to guarantee data sharing in a tamper-proof manner.

N. Tapas [4] presents the increasing popularity of IoT solutions, is progressively on the top, and ever more critical to services and businesses. huge amounts of data are being generated at any time due to smart devices and the Internet of Things. The cloud system is not only popular in enterprises and in the business but also on small scale and individuals. For Infrastructure-as-a-Service, which is supported by giants such as IBM, Dell, Cisco. Blockchain is growing as a potential solution for provable and publicly testable security. Cloud storage presents the problem such as potential server misdemeanor, causing the client to distrust the server, for example falsely claiming a violation of user agreement. By leveraging distributed ledger technologies (DLT) to get auditability and non-repudiation guarantees of a solution.

T. Gabriel [5] proposes the blockchain concept using encryption in order to form a chain. The blockchain is a series of transactions organized logically inside a block, these blocks are wrapped together. Databases maintained information conventionally stored by each organization. CAP theorem describes Database technology in which C stands for Consistency, A stands for Availability and P stands for Partition Tolerance. , Inside the Central Dispatch Center, Energy Management Systems (EMS) are compound systems that are usually developed at a national level. EMS systems help central dispatchers make informed decisions like Automatic Generation Control (AGC), Real-Time Contingency Analysis (RTCA), State Estimator (SE), Economic Dispatcher, Energy forecasting, Balancing Market, Short circuit current calculations.

I. Sukhodolskiy [6] states that the untrusted environment needs the ability to securely share information in a cloud storage system. There have always been some issues regarding security problems and the copyright aspect. A number of facilities provide services for data storage backup files. The Cloud Security Alliance states that encryption is one of the best protective mechanisms suggested. Encryption has some difficulty to utilize the data and creates hurdles to access them. To control access to encrypted data the project uses a decentralized scheme. The proposed paper's results have been demonstrated an acceptable complexity, functionality, and complexity of implementation.

M. Kumar [7] suggests the most important process to keep any organization safe and secure is by auditing network by monitoring and log auditing. As the attacker keeps changing their attacking strategies, security devices also have to be modulated accordingly thus Network security devices can provide adequate security. To spot the complex attack pattern and the attacker's master plan the effective network monitoring and auditing help the administrator. In cybercrime investigation and digital forensic analysis log records also play a significant role. Regulatory compliance such as Payment Card Industry Data Security Standard (PCI DSS) or Health Insurance Portability and Accountability Act (HIPAA) normally approve that log record should be preserved in a forensically sound manner.

H. Zhu [8] explains a trusted distributed audit technique for cloud function scheduling, which is used for the trusted storage of cloud task scheduling information in the cloudcluster. The technique of the distribution solutions includes blockchain technology and combines it with the traditional cloud server to get the solution of problem integrity and task scheduling for the security of the cloud to secure the data. The paper proposes the framework in four parts: cloud cluster, control system, blockchain network, and cloud database. The transparency, authenticity, and validity of the data are verified by the blocks that are generated for each data record. The developed system and evaluated its performance and show the system is accurate and secure.

S. Ramamoorthy [9] narrates the most promising task for any IT operation in the future is Data security and Storage Management. Technology like cloud computing which pools computing resources is very important for businesses and service providers. A major problem among the community cloud users is data security and modification over the data stored on the cloud. Thus the proposed paper aims to protect cloud data by using the new technologies such as blockchain. The data security issue among the community cloud users can be solved by using the Hybrid approach by combining the BlockChain(BC) Technology with the cloud paradigm.

X. Yang [10] introduces an effective online voting system by using advanced security methods. To develop the online voting systems Homomorphic encryption which is a well-known powerful technique with many useful applications is used. To improve security guarantees in future elections in the United States, India and Brazil have highlighted significant challenges in recent experimental online voting. In an online voting system maintaining the privacy and security of the voters is a priority. The following security requirements ensure that an efficient voting system has been implemented, such as Eligibility of Voters, Multiple-Voting Detection, Integrity of Ballot, Correctness of Tallied Result, End-to-End Voter Verifiable.

Keke Gai [11] presents a conceptual model for fusing blockchains and cloud computing for additional value creation. They implement three deployment modes: Cloud over Blockchain (CoB), Blockchain over Cloud (BoC), and Mixed Blockchain–Cloud (MBC). The key concerns in cloud adoption or deployment are privacy. There is an additional role of lockchain in a cloud system. Tamper-resistant performance is supported only in the subsystem or subsystems in which the blockchain is used e.g., traceable data usage. In the proposed system the limitation is that the service conveyance with records requires a large reengineering effort.

Jiaxing Li [12] discusses that the cloud storage platform has gained massive attention in personal and business organizations because it is highly convenient and efficient. P2P network has been mostly developed over distributed systems and we use an unstructured P2P network in our architecture. Bitcoin proposed by the Nakamoto blockchain is a blockchain-based technology. Evaluation of the network performance and security is based on the Number of Users and Network Latency, The Number of Users and File Security. Thus the paper presents the comparative simulation results with outstanding security performance and acceptable network performance.

H. Do [13] narrates that there has been an outstanding growth in the interest to outsource data as well as operational services to clouds. A decentralized cloud storage network has been introduced with many advantages. The most important challenge is data usability in the management of encrypted data. The proposed paper gives rise to a number of shortcomings including the performance, availability, security, and high operational cost. Blockchain is one of the important parts for off-chain data storage access, permission grant and searches token generation. It involves the three major parties such as data storage access, permission grant and searches token generation.

III. CONCLUSION

This paper effectively analyzes some past works on implementation of block chain technologies in order to improve the quality of Access control mechanism in cloud based storage. This paper learnt some facts like most of the works working on the linear model of block chain that is not enough to handle the complex hierarchy of data access control. So this paper decided to use Blockchains in hierarchical ways that effectively handle the data access control mechanism for the stored data in the cloud. And also this me mechanism is adopted by data integrity evaluation using improved bilinear pairing techniques in the public cloud platf rm from a standalone mode of application.

REFERENCES

[1] SHANGPING WANG1, YUYING WANG2, and YALING ZHANG3," Blockchain-based fair payment protocol for deduplication cloud storage system "Digital Object Identifier 10.1109/ACCESS..Doi Number. 2019

[2] Qiwu Zou, Yuzhe Tang, Ju Chen, Kai Li, Charles A. Kamhoua, Kevin Kwiat, Laurent Njilla," ChainFS: Blockchain-Secured Cloud Storage ", IEEE 11th International Conference on Cloud Computing 2018

[3] KAI WANG , JIAQING DONG, YING WANG," Securing Data With Blockchain and AI " Digital Object Identifier 10.1109/ACCESS..2921555 2019

[4] Nachiket Tapas, Giovanni Merlino, Francesco Longo, Antonio Puliafito," Blockchain-based Publicly Verifiable Cloud Storage" IEEE International Conference on Smart Computing SMARTCOMP 2019

[5] Tudor Gabriel, Andrei Cornel Cristian, Madalina Arhip-Calin, Alexandru Zamfirescu," Cloud Storage. A comparison between centralized solutions versus decentralized cloud storage solutions using Blockchain technology " 978-1-7281- 3349-2/19©IEEE 2019

[6] Ilya Sukhodolskiy, Sergey Zapechnikov," A Blockchain-Based Access Control System for Cloud Storage" 978-1-5386- 4340-2/18 IEEE 2018

[7] Dr. Manish Kumar, Ashish Kumar Singh, Dr. T V Suresh Kumar," Secure Log Storage Using Blockchain and Cloud Infrastructur" July 10-12, , IISC, Bengaluru 2018

[8] He Zhu, Yichuan Wang, Xinhong Hei, Wenjiang Ji, Li Zhang," A Blockchain-based Decentralized Cloud Resource Scheduling Architecture " International Conference on Networking and Network Applications 2018

[9] 1S. Ramamoorthy, B.Baranidharan," CloudBC-A Secure Cloud Data acess Management system" 978-1-5386-9371- 1/19/ IEEE 2019

[10] Xuechao yang , Xun yi1, Surya nepal, Andrei kelarev, and Fengling han," A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption" Digital Object Identifier 10.1109/ACCESS..2817518 2018

[11] Keke Gai, Kim-Kwang Raymond, Liehuang Zhu," Blockchain-Enabled Reengineering of Cloud Datacenters" Co published by the IEEE CS and IEEE Com Soc November/December 2018 2325-6095/2018

[12] Jiaxing Li, Zhusong Liu, Long Chen, Pinghua Chen, Jigang Wu," Blockchain-based Security Architecture for Distributed Cloud Storage" IEEE International Symposium on Parallel and Distributed Processing with Applications 2017

[13] Hoang Giang Do, Wee Keong Ng," Blockchain-based System for Secure Data Storage with Private Keyword Search " IEEE 13th World Congress on Services 2017