International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 14, Issue 12, December 2025)

Review on Cloud Computing and Block Chain Technology for Secured Access

Seema Bapusaheb Saknure[1], Dr. Prashant Laxminarayan Chintal[2]

[1]*Assistant professor, Computer Applications Department, Maharashtra Institute Technology*
[2]*Head and Assistant professor, Computer Applications Department, Maharashtra Institute Technology*

***Abstract*—The issue of achieving safe access to cloud data has become a current research hotspot due to the cloud computing technology's rapid development. Technology based on attributes for encryption makes it possible to accomplish the stated objective. Nevertheless, the majority of current solutions come with hefty trust and computational costs. Furthermore, it may be challenging to ensure data search security and access permission fairness. We suggest a unique blockchain- based access control system that uses attribute-based searchable encryption in a cloud environment to solve these problems. Our proposed method supports policy concealment and attribute revocation and implements proxy encryption and decryption to provide precise access control with little computing overhead. Data integrity and secrecy are guaranteed by storing the encrypted file in the IPFS and the metadata ciphertext on the blockchain. Concurrently, the plan facilitates the safe exploration of ciphertext keywords inside a transparent and open blockchain setting. Furthermore, in order to dynamically manage access permission, an audit contract is made to control user access behavior. Security study demonstrates that our method is immune to keyword guessing and chosen-plaintext attacks.**

***Keywords*—IoT, FAR, BCT, CP-ABE**

I. Introduction

With the introduction of cloud computing, storage outsourcing has become a growing trend, making safe remote data audit a prominent problem that has arisen in the study literature. Some recent research has focused on the issue of safe and efficient public data integrity audits for shared dynamic data. However, in a practical cloud storage system, these approaches are still not safe against the cooperation of cloud storage servers and revoked group users during user revocation. In this research, we analyze the existing technique's collusion attack and propose a successful public integrity auditing scheme with secure group user revoking based on vector

commitment with verifier-local revocation group signature. Based on our scheme specification, we create an actual scheme.

Cloud computing is seen as a feasible architecture for deploying uses, software, and data via the Internet; in addition, hardware, applications, data, including software in data centers offer services. It is technology that provides several services to people. Processor, memory, storage, use, database, software, graphical utilization, and analysis over the internet are examples of services.

Depending on the user needs, resource sharing delivers quicker, more flexible, inventive, and economically scalable hardware components and software distributions. The benefit of having access to a cloud platform is. Users can only pay for the services and time periods that they will utilise. Users may also adjust the hardware, software, and platform utilization based on their needs, and they can switch off the instance when they are not using it.

The technique lowers consumer purchasing costs and builds the infrastructure that they require, as follows:

- Users can build hybrid cloud and multi cloud
- Data storage
- Big data analysis
- Developments and validations
- Disaster recovery
- Archiving and backup
- Social network
- Business infrastructure development

Cloud is the technology and service in which users' network is hosted on cloud. The technology is centralized manage in which multiple computing resources share identical platform and users can enable to operate these resources to specific extent. Various sectors used the technology for speed process and resource management. Based on the cloud service users can improve the communication. The system provides globally positioned servers, and users move among the interconnected servers to save and retrieve the data. Because of the centralized service all the resources are visible to the required users called as tenants, thus, the technology needs utmost performance and security.

The tasks are shared among the cloud environment. Security is given to get enter to the infrastructure, the gateway provides contextual access code and firewall of multi-layer, applications and other services are given to data centers.

The data centers are a massive international cloud network that is continually upgraded with current technology to give cost savings, minimal latency, and scalability. The transactions are safeguarded by the security system, according to the service providers. However, the security system should be upgraded in accordance with current needs and technological improvements. Users can choose to operate the cloud service based on the needed material and time; the servers handle this flexibility and operation. The cloud allows users to preserve their papers and retrieve them from any available device or anywhere by anybody who has authorized it using a web interface. As a result, users may enjoy maximum access speed, data viability, quality security from any location.

The cloud is a technology and service that hosts users' networks. The technology is centralized managed, which means that many computing resources share the same platform and users can operate with these assets to a limited extent. Various industries made use of the technology to improve process business resource management. Users can increase their communication by using the cloud service.

The system provides globally distributed servers, and users navigate between them to save and retrieve data. Because of the centralized service, all resources are accessible to the appropriate tenants; hence, the technology requires maximum performance and security. The duties are distributed over the cloud environment. To get access to the infrastructure, security is provided by the gateway, which offers a contextual access code and a multi-layer firewall, as well as applications and additional services to data centers.

An increasing number of communication academics and industry professionals are dedicated to developing a secure and efficient resource sharing mechanism in the cloud environment as a result of the interconnection of the worldwide mobile Internet and the quick growth of cloud computing [1]. Because cloud storage technology is inexpensive and performs well, it has becoming extensively employed. Private data is often encrypted and kept in cloud services to guarantee security. Nevertheless, the present requirements for cloud data privacy security have proven too great for the conventional public key encryption solution.

How to obtain access permission and precise cloud data retrieval in this setting has emerged as a new difficulty.

One essential piece of technology for preserving data security and privacy is access control (AC) [2]. The aforementioned issue is resolved by the AC, which limits user access privileges to guarantee authorized access to sensitive information. In addition to providing fine-grained access control over encrypted data, attribute-based searchable encryption based on ciphertext policy also allows users to retrieve ciphertext using keywords. Data owners can independently create data access policies based on a set of characteristics and link data access policies to ciphertexts using the Ciphertext Policy Attribute-Based Encryption Algorithm (CP-ABE) [3, 4].

This works well in "one-to-many" access scenarios where the user's attribute set complies with the access policy. The ciphertext may be decrypted using the associated attribute private key, but the identity of the decryptor is kept secret. To increase the privacy and security of cloud data, a lot of research has recently used attribute-based encryption technology to cloud data access control [5, 6]. But because the access policy is incorporated into the ciphertext, the security of the policy is frequently disregarded, and the conventional CP-ABE technique is quite computationally expensive. Furthermore, there are pressing concerns that need to be resolved, such as attribute access expiration and permission changes.

The majority of access control techniques in use today primarily employ a centralized administration approach, which leaves them vulnerable to a single malfunction that might bring the entire system down. Furthermore, access choices in traditional systems are made by trusted third parties, which entails paying unfair service fees in addition to a high overhead of trust. Thus, creating equitable and safe searchable access control systems continues to be a difficult task. Blockchain is a distributed ledger system that is open, transparent, tamper-resistant, traceable, and decentralized [7].

Users no longer need to be concerned about the substantial trust and security concerns created by third parties, since it facilitates the safe storage and processing of data without the participation of third parties. This implies that a fair and reliable distributed access control system may be enabled by using blockchain technology in place of conventional third parties for access authorization management. We suggest a unique distributed data-sharing system by combining attribute-based search encryption technology with blockchain technology, which is based on the study of the aforementioned challenges.

This technique considers low computational expenses, policy privacy, attribute revocation, and dynamic permission in order to achieve fine-grained search access to encrypted cloud data.

II. Related Work

In a multi-tenant SaaS architecture fragments are allocated to the sites where they are most frequently accessed, aiming at maximizing the number of local accesses compared to accesses from remote sites. The cost of the read operation can be further reduced by the replication of fragments when beneficial. Fragmentation, Allocation, and Replication will be referred to as FAR in the rest of the paper [2,3].

A cloud uses technology of multitenancy to share IT resources among multiple applications and tenants securely. Virtualization-based architectures is used by some clouds to isolate tenants, and some uses custom software architectures to get the job done. In this paper we have shown the proposed architecture for standing tenant placement for query request with sample HR benchmark design combined both approaches in memory and multitenancy [4].

Cloud Computing appears as a computational paradigm as well as distribution architecture and its main objective is to provide secure, quick, convenient data storage and net computing service, with all computing resources visualized as services and delivered over the Internet [5].

In a multi-tenant SaaS architecture, different data layer designs have been proposed and used in different domains. The only difference between these designs is the level of the data separation for all tenants. Regardless of the design used for the data layers, service providers face enormous [6].

Cloud computing provides various facilities for the users like scalability, special computational mean and reducing workload and reducing capital expensive [7]. It consists of large-scale central servers, numerous edge servers deployed at the network edge, and a huge number of distributed end devices. Instead of considering them as separated parts, most applications require all of them to be well orchestrated for providing reliable services over different temporal and spatial scales [8].

Controlling access is a crucial security feature that safeguards private data and system assets [8]. Blockchain is an underlying technology architecture with great value, low cost, and trustworthiness. To address the shortcomings of conventional centralized access control, several academics have attempted to integrate blockchain technology with access control.

The majority of the current blockchain access control systems rely on permission verification and on-chain storage.

In order to make it easier for lightweight IoT devices to be added, updated, and removed from the blockchain, Reference [9] suggests an access control method. Nevertheless, this approach is not appropriate for big file sharing.

Blockchain technology is used by Reference [10] to facilitate the safe exchange of vehicle data. The aforementioned technique computes a vehicle's reputation value using a weight model in order to prohibit unlawful sharing; nevertheless, privacy is not taken into consideration.

A blockchain data access control system based on digital certificates is suggested in Reference [11]. This strategy uses signature technology to safeguard sensitive contract information and user identification information, but it does not take data storage security into account. Instead, it builds an identity authentication protocol that does not need third-party signature verification.

Reference [12] uses blockchain technology to create a trustless sharing paradigm, focusing on a scenario where the conventional IoT data sharing approach is highly dependent on a third party.

However, symmetric encryption is used in this system to achieve fine-grained control. References [13, 14, 15,] implement an access policy in the smart contract and achieve user attribute matching access control in a non-encrypted state. Because of the blockchain's openness and transparency, a user might communicate a smart contract the access rules and characteristics, jeopardizing privacy.

It has been suggested that attribute-based encryption and cloud storage be used in access control methods to improve data access security and reduce blockchain storage bottlenecks. Superior data protection and precise access control for external storage are made possible by the CP-ABE algorithm. According to the plan put forward by [16,17,18], shared data is kept in a cloud service and encrypted using CP-ABE. There is a chance that user data will be lost as data security is directly impacted by cloud service security.

A blockchain-based and secret sharing data-sharing mechanism is implemented in [19] using a distributed storage IPFS. The IPFS technology is used by this approach to store unencrypted data. One clear disadvantage is that any unauthorized user might acquire the associated unencrypted data when an address saved in the IPFS is released.

Proxy computing is used in References [20, 21] to guarantee the traceability of the secret key and lower the computational overhead of CP-ABE. They do not, however, take access policies' privacy into account. Because the access policy is included into the ciphertext in plaintext, attackers can use it to deduce private information.

In order to keep the access structure from being made public, Reference [22] suggests a policy- hiding smart grid data sharing method. Proxy decryption is also included to lower the cost associated with user decryption. In order to thwart keyword-guessing attacks, Reference [23] suggests an attribute-based encryption technique for keyword searches based on policy concealing. Based on the "AND" gate access structure, Reference [24] suggests a cloud storage approach with attribute policy concealing that incorporates obscured features into the original access policy for authentication by users.

Nevertheless, [22, 23–24] do not rely on blockchain technology and do not consider external security risks. A policy-hiding blockchain access control system based on CP-ABE is proposed in Reference [25]. Polynomials are used in the scheme to represent the access structure. Users of the data can utilize homomorphic encryption to verify locally while doing attribute policy matching. However, this approach requires a large amount of computational power.

References [26, 27] provide an attribute-based encryption strategy based on keyword search to achieve the searchability of ciphertext. In order to make sure the retrieved ciphertext matches, they search for keywords on cloud services and store encrypted data there. In real-world applications, changes in permissions and other circumstances may cause attributes to be revoked. In order to do this, data-sharing methods that permit attribute revocation are proposed in references [28,29, 30].

A multi-authority comprehensive searchable access mechanism for cloud data is proposed in Reference [28]. This technique readily results in security bottlenecks, even if it requires several authorizations in order to keep user information secret. Building on the work of reference [29], reference [31] introduces policy concealment. Nevertheless, the aforementioned technique leaves users' search activity unpredictable, and it could lead to an unfair search service price payment issue. Blockchain technology is used by Reference [32] to address the aforementioned issues; nevertheless, this plan does not allow for policy concealing.

This study suggests a safe access control system based on blockchain technology and attribute- based searchable cryptography in a cloud environment based on the aforementioned analysis. The plan uses IPFS to store encrypted data, which reduces the strain on blockchain storage and the issue with single points of failure in conventional storage models. Enhancing the security and adaptability of access, the method also includes attribute revocation and attribute policy concealment. Another way to lower user compute usage is to offer proxy encryption and decryption. Furthermore, the system use smart contracts to monitor user behavior and time limitations and conduct a safe search of encrypted words on the blockchain to prevent unwanted access.

By contacting the associated address or interfaces in the contract, users can communicate with smart contracts that are distributed on the blockchain [40]. The coding of smart contracts has advantages over traditional contracts in terms of legality and its ability to run automatically and without interruptions when the necessary circumstances are satisfied. In addition, smart contracts have the ability to carry out secure interactions in a blockchain setting without the need for an outside arbitrator. The agreed-upon monies must be submitted by all parties prior to contract execution. The contract is carried out in accordance with the required automated execution outcome, whether or not it is violated.

Initially, Bitcoin's underlying enabling technology was blockchain. Essentially, it is a dispersed shared database that is extensively utilized for resource sharing, data accountability, and control of access and acts as a ground-breaking low-cost credit technology solution [33, 34]. Scripting languages can operate in an Ethereum virtual machines (EVM) [35] environment, which is provided by Ethereum, an application development platform built on the blockchain. Programming languages like JavaScript and Solidity may be used by users to build and implement decentralized apps and smart contracts in Ethereum, expanding the potential of blockchains [36, 37]. Codes created in compliance with transaction rules are known as smart contracts [38, 39].

Smart contracts are operated indefinitely on the blockchain and are unchangeable once created. A secure operating environment is produced using EVM. A pair of public and private keys make up an Ethereum account, which may be categorized as either a contract account or an externally held account.

An account that is managed by the user's account private key and is not connected to the contract is said to be externally owned. An account linked to the contract code created during contract deployment is known as a contract account.

III. Conclusion

- The information is stored in the database of Blockchain, and each user has a copy of the database so that if one part of the network fails, the data remains safe so that it can be updated later.
- The encryption and decryption have tolerable impact on average response time for accessing & updating record on cloud.
- Blockchain is a distributed shared database used for low-cost credit technology.
- Ethereum, a decentralized application platform, provides an Ethereum virtual machine (EVM) environment for scripting languages.
- Users can write and deploy smart contracts and decentralized applications in Ethereum using programming languages like Solidity and JavaScript.
- Smart contracts are codes written in accordance with transaction rules, running permanently on the blockchain.Ethereum accounts consist of a pair of public and private keys and can be classified as externally owned or contract accounts.

REFERENCES

[1] Q. Chai and G. Guang, "Verifiable symmetric searchable encryption for semihonest-but-curious cloud servers," in IEEE International Conference on Communications (ICC), 2012.

[2] David Berdik, Safa Otoum, "A Survey on Blockchain for Information Systems Management andSecurity," Information Processing & Management, vol. Volume 58, no. Issue 1, 2021.

[3] A. K. Minhaj and S. Khaled, "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395-411, 2018.

[4] H. Péter, Towards Analyzing the Complexity Landscape of Solidity Based Ethereum SmartContracts, vol. 7, Technologies, 2019.

[5] J. Bethencourt, S. Amit and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in IEEEsymposium on security and privacy (SP'07), 2007.

[6] P. Yanji and e. all, "Polynomial-Based Key Management for secure intra-Group communication," Computers and Mathematics with Applications, vol. 65, p. 1300– 1309, 2013.

[7] Z. Yuanyu and K. Shoji, "Smart Contract-Based Access Control for the Internet of Things," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1594-1605, 2015.

[8] J. Mayssa and S. Ahmed, "Decentralized access control mechanism with temporal dimension based on blockchain," in The Fourteenth IEEE International Conference on Business Engineering,2017.

[9] L. Xiehua and J. Jie, "Fully Decentralized Authentication and Revocation Scheme in Data Sharing Systems," in 17Th IEEE international Conference on Trust, 2018.

[10] P. Arman and I. Md Nazmul, "Privacy in Blockchain Enabled IoT Devices," in IEEE/ACM ThirdInternational Conference on Internet-of-Things Design and Implementation, 2018.

[11] I. Md Nazmul and K. Sandip, "Preserving IoT Privacy in Sharing Economy via Smart Contract," inIEEE/ACM Third International Conference on Internet-ofThings Design and Implementation,2018.

[12] S. Wang, Y. Zhang and Y. Zhang, "A Blockchain-Based Framework for Data Sharing with Fine- grained Access Control in Decentralized Storage Systems," IEEE Access, vol. 6, pp. 38437-38450,2018.

[13] Z. Yunru and H. Debiao, "BaDS: Blockchain-Based Architecture for Data Sharing with ABS and CP- ABE in IoT," Wireless Communications and Mobile Computing, vol. 2018, 2018.

[14] Y. Liu and J. Zhang, "A Blockchain-based Secure Cloud Files Sharing Scheme with Fine-GrainedAccess," in International Conference on Networking and Network Applications, 2018.

[15] S. Wang, X. Wang and Y. Zhang, "Secure Cloud Storage Framework with Access Control based onBlockchain," IEEE Access, vol. 7, pp. 112713-112725, 2019.

[16] N. Oscar, "Blockchain Meets IoT: an Architecture for Scalable Access Management in IoT," IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1184-1195, 2018.

[17] S. Ding, C. Jin, L. Chen, F. Kai and H. Li, "A Novel Attribute-Based Access Control Scheme UsingBlockchain for IoT," IEEE Access, no. 7, pp. 38431-38441, 2019.

[18] H. M. Htet and K. T. M. Htet, "Developing a Transparent Tax Data Access Control System Based on Blockchain," in ICCA 2019, 2019.

[19] G. Li and H. Sato, "A Privacy-Preserving and Fully Decentralized Storage and Sharing System onBlockchain," in IEEE 43rd Annual Computer Software and Applications Conference, 2019.

[20] R. Mythili, V. Revathi and T. S. Raj, "An attribute-based lightweight cloud data access control using hypergraph structure," Supercomputing, 2020.

[21] A. Afnan and D. T. Bradley, "Attribute-based Access Control of Data Sharing Based onHyperledger Blockchain," in ICBCT'20: The 2nd International Conference on BlockchainTechnology, 2020.

[22] S. Noh, D. Kim, Z. Cai and K. H. Rhee, "A Novel User Collusion-Resistant Decentralized Multi- Authority Attribute-Based Encryption Scheme Using the Deposit on a Blockchain," Wireless Communications and Mobile Computing, 2021.

[23] L. Guo, X. Yang and W. C. Yau, "TABE-DAC: Efficient traceable attribute-based encryption scheme with dynamic access control based on blockchain," IEEE Access, vol. 9, pp. 8479-8490,2021.

[24] A. A. Kamal, "Cryptanalysis of a Polynomial-based Key Management Scheme for Secure Group Communication," International Journal of Network Security, vol. 15, no. 1, pp. 68-70, 2013.

[25] X. Sun, X. Wu, C. Huang, Z. Xu and J. Zhong, "Modified access polynomial based self-healing key management schemes with broadcast authentication and enhanced collusion resistance in wireless sensor networks.," Ad Hoc Networks, vol. 37, pp. 324-336, 2016.

[26] V. Goyal, P. Omkant, S. Amit and W. Brent, "Attribute-based encryption for finegrained access control of encrypted data," in 13th ACM conference on Computer and communications security,2006.

[27] Amazon, "Amazon S3 : Amazon Simple Storage Service," Amazon, [Online]. Available:https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html.

[28] B. Blanchet, M. Abadi and C. Fournet, "Automated verification of selected equivalences for security protocols.," The Journal of Logic and Algebraic Programming,, vol. 75, no. 1, pp. 3-51,2008.

[29] H. Lenstra, A. Willem, K. Lenstra and L. Lovfiasz, "Factoring polynomials with rational coeficients," 1982. [Online]. Available: https://openaccess.leidenuniv.nl/bitstream/handle/1887/3810/346_050.pdf.

[30] Etherscan, "Ethereum Gas Tracker," [Online]. Available: https://etherscan.io/gastracker. [31] Binance, "Binance chain," [Online]. Available: https://www.binance.com. [32] BscScan, "BNB Smart Chain Gas Tracker," [Online]. Available: https://bscscan.com/gastracker

[31] Deepak Kumar Verma, Tanya Sharma, "Issues and Challenges in Cloud Computing", International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 8, Issue 4, April 2019.

[32] Ahmed E. Abdel Raouf, Nagwa L. Badr, and Mohamed Fahmy Tolba, "Dynamic Distributed Database over Cloud Environment", 13 January 2016.

[33] Mohammad Mehrtak, SeyedAhmad SeyedAlinaghi, Mehrzad MohsseniPour, Tayebeh Noori, Amirali Karimi, Ahmadreza Shamsabadi, Mohammad Heydari, Alireza Barzegary, Pegah Mirzapour, Mahdi Soleymanzadeh, Farzin Vahedi, Esmaeil Mehraeen, Omid Dadras, "Security challenges and solutions using healthcare cloud computing", Journal of Medicine and Life. Vol: 14 Issue: 4 July August 2021.

[34] Arpita Shah, and Narendra Patel, "Efficient and scalable multitenant placement approach for in- memory database over supple architecture", Computer Science and Information Technologies, Vol. 1, No. 2, pp. 39, July 2020.

[35] Dr. N. Krishna Murthy, Dr. R. Selvam, "Security Issues and Challenges in Cloud Computing",International Advanced Research Journal in Science, Engineering and Technology(IARJSET), Vol.2, Issue 12, December 2015.

[36] Ahmed E. Abdel Raouf, Alshaimaa Abo-alian, Nagwa L. Badr, "Multi-Tenant RDBMS Migration in the Cloud Environment", International Journal of Intelligent Computing and Information Sciences, Vol.21, No.2, 2021.

[37] A. Stephen, A. Arul Anitha, L. Arockiam, "Cloud Computing: Opportunities and Challenges",ReTeLL, Vol. 21, June 2019.

[38] Ju Ren, Deyu Zhang, Shiwen He, and Yaoxue Zhang, "A Survey on End-Edge-Cloud Orchestrated Network Computing Paradigms: Transparent Computing, Mobile Edge Computing, Fog Computing, and Cloudlet", ACM Computing Surveys, Vol. 52, No. 6, October, 2019.

[39] Alshamaileh Mohammad, Li Chunlin, "Evaluating Mobile Cloud Computing Models", 4th International Conference on Machinery, Materials and Computing Technology (ICMMCT 2016). [40] Trilochan, Anjali Verma, "Cloud Computing: Evolution and Challenges", International Journal of Engineering Science and Computing, April 2017.