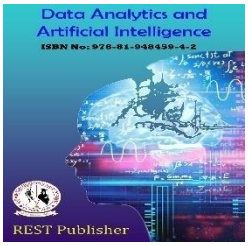
Data Analytics and Artificial Intelligence

Vol: 4(3), 2024

REST Publisher; ISBN: 978-81-948459-4-2

Website: http://restpublisher.com/book-series/daai/

DOI: https://doi.org/10.46632/daai/4/3/2



Intrusion Prevention in Cloud Computing Using Blockchain

***K. Thenmozhi, R. Sabin Begum**

B.S.Abdur Rahman Crescent Institute of Science and Technology, Chennai, Tamil Nadu, India.

*Corresponding Author Email: arasiammu100@gmail.com

Abstract. *The integration of blockchain technology with cloud computing to establish a more secure and transparent Intrusion prevention mechanism. The limitations of traditional Intrusion prevention methods, including security, transparency, and scalability challenges. Blockchain technology has emerged as a promising solution to enhance Intrusion prevention and permissions in a tamper-proof and transparent ledger in cloud computing environments. Blockchain technology has the potential to revolutionize Intrusion prevention in cloud computing by providing a more secure, transparent, and scalable framework. Scalability is an issue since processing many Intrusion prevention transactions on the blockchain might cause network congestion and sluggish processing. Transactions take time to upload to the blockchain, which can delay realtime access choices. It takes skill to integrate and manage blockchain and cloud technologies together. Choosing the correct consensus mechanism affects system efficiency and security. Consider the costs of establishing and maintaining such a system and the difficulty of fixing faults owing to blockchain immutability. In this paper we highlighted the importance of Intrusion prevention in cloud computing, emphasizing the need for secure and transparent management of sensitive data and resources. It also underscores the limitations of traditional Intrusion prevention methods, which can lead to security breaches and unauthorized access. In conclusion, this paper presents a compelling argument for the integration of blockchain technology with cloud computing to establish a more secure and transparent Intrusion prevention mechanism. Keywords: Blockchain, Cloud Computing, Intrusion Prevention, Scalability, immutability*

1. INTRODUCTION

Large-scale, distributed computer technologies gave rise to the clearly defined field of cloud computing. Cloud computing lessens the amount of processing that consumers must do. There are several benefits, such as less hardware and maintenance expenses, global availability, and adaptability with simple scaling capabilities and a highly automated procedure. Numerous big businesses have embraced cloud computing, including IBM, Google, Microsoft as well as Amazon. Prototypes make up a lot of applications. that have emerged, such as Google Cloud and App Engine platform, the Elastic Computing Platform, the Amazon Cloud, and so forth. It offers us the pay-per-use policy feature and adaptable IT architecture that is available online from portable electronics. Despite the cloud's numerous beneficial services, corporations are reluctant to use them because of their privacy issues.

The future of industries aiming to better security and privacy lies in blockchain technology. Blockchain technology a distributed ledger that, in the absence of a central authority, stores tamper-evident data as a chain. The devices or players in the blockchain technology are referred as nodes. Blockchain offers a decentralized system where every network node actively participates in order to verify and check the information. The information that the blockchain will hold will be cryptographically encrypted. Each block has an date, hash, and encrypted hash of the preceding block in the chain that joins the blocks together. Thus, the blockchain is resistant to tampering. Blockchain offers the data with security, and users that are involved will be confirmed in the network, removing the data's privacy concern.

With the great development in information technology, storing data in huge quantitie and sharing it through cloud computing has become easy. As cloud environments grow in complexity, traditional Intrusion Prevention methods face challenges in maintaining the desired level of security, transparency, and scalability. This is where the convergence of blockchain technology with cloud computing emerges as a compelling solution to address these limitations and elevate Intrusion prevention mechanisms to any level of robustness and efficiency. In the

subsequent sections, we will delve into how blockchain can revolutionize Intrusion prevention in cloud computing, offering enhanced security, transparency, and adaptability in an increasingly interconnected digital landscape.

The Blockchain method evolved with the notion of consecutive blocks for data storage, based on the expected continuance of this evolution. The field of blockchain technology has advanced digital informatics and offered several answers to the problems of data sharing flexibility. This technology's main feature, which highlights its principal usage benefits, is its ability to convey any quantity of data in the form of a block and adapt to various use cases efficiently thanks to its hashes, one of its main components. One other noteworthy feature of this technology is that its code is publicly available to everybody with access, eliminating the possibility of a backdoor being created within the system. Consequently, this technique has the potential to increase the level of safety in information sharing in business with various application areas such as commercial, financial, sales export, and banking transactions.

Incorporating blockchain into cloud computing is only done through two methods. Blockchain can be incorporated into this traditional technology to facilitate business networks such as replication, storage, and transactional base access. Cloud computing is a technical meansfor storing a data to be controlled remotely that will benefit from the network facilitation of blockchain. Additionally, blockchain can be incorporated with other cloud security concepts between user, task, and data management. This showcases its identity and access management capabilities in this sector. There are transparency issues with cloud computing, such as users' lack of management of data use and movement within this system, which can be addressed by leveraging blockchain data security capabilities. Hence, blockchain can be leveraged to address the limitations of cloud computing and enhance its performance. Furthermore, these two technologies have been applied in diverse areas and environments, making it crucial to leverage their advantages for the effectiveness of these areas. Therefore, leveraging these technologies create a more secure approach to controlling access to data and identity in cloud computing.

2. RELATED WORK

In[8],the authors provided are view of the application of blockchain in the cloud computing system by analyzing relevant previous papers and studies and accessing the gap in each study separately to reveal ideas that researchers and interested parties can refer to provide more secure solutions in the future. By reviewing previous studies based on the application of the blockchain in cloud computing, the researchers found that the proposed models lack more features and suffer from data security problems, in addition to the fact that communication between multiparty accounts in light of a large number of users works to disrupt networks.

In [9], authors proposed a blockchain-based access control framework with privacy protection by using the account address of the node in the blockchain as an identity and redefining the access control permission of data for the cloud, which is encrypted and stored in the blockchain. Allaccess control, authorization, and DE authorization processes are through the Auth Privacy Chain.

In [11], it was found that blockchain can be a suitable and powerful tool for providing security in a cloud computing environment after analyzing the overall structure of the blockchain and the characteristics of the security requirements of blockchain and cloud computing. Cloud storage used by blockchain is accessible and open and can view all sorts of services provided by theusers can view the same version/copy. Blockchain coupled with smart contract technologies, enables more trust and transparency.

In [12], the authors provided a platform for those interested in developing their programs by providing a decentralized and transparent means based on public/crowd-based computing resources. So that it provides the ability to run application files in a decentralized environment similar to cloud computing resources in storage and sharing, but in some cases, it lacks the distributed infrastructure. It is interrupted during an unlimited no of nodes assessment.

In [14],the authors proposed a Proxy Chain architecture as an example of a blockchain-based data generation model in a cloud environment by gathering and validating the data source. In the presence of a good level of security and data transparency, the proposed environment needs to fill in some cases where the file size increases, which generates an increase in the load that requires an increase in the computational complexity in data protection.

[15]proposed a new approach to access data without the participation of the provider through the ciphertext- policy attribute-based encryption scheme with dynamic attributes by taking advantage of the idea of the blockchain that depends on the ledger so that the model idea is based on building a record to generate the key, or set the access policy, or change or cancellation, or request access is not subject to change, and hence the degree of security in access to data in the computerized cloud is achieved.

Reference [19] suggests a blockchain-based digital certificate-based data access control system. 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. highlighting a scenario in which a third party is crucial to the standard IoT data exchange methodology.

3. INTRUSION PREVENTION IN CLOUD SYSTEMS

Intrusion prevention is designed to detect and prevent cyber threats in real-time, preventing unauthorized access to sensitive data and systems. IPMs can be integrated with blockchain-based access control systems to enhance security and prevent potential breaches. The vulnerabilities of the computer systems that are being moved to cloud infrastructure are shared by the entire platform. This section will go over ideas and current work on blockchain in the cloud, collaborative IPS, and IPS systems and the ways in which this technology may be used to address issues in managing data trust. There are several current security methods, at various technological phases are intended to address issues with cyber security as magnitude. Applications whitelisting and multi-factor system patching, net-based authentication, privilege restriction, and work monitoring using blockchain, IPSs, and firewalls. But when it comes to intricate cloud systems, there isn't single method to address every kind of security risk. Consequently, in order to guarantee a safe cloud infrastructure, several mechanisms have to be integrated for security. Proxy encryption and decryption are also introduced to reduce user computation consumption. In addition, the solution implements a secure search of encrypted keywords on the blockchain, while monitoring user access behavior and time limits through smart contracts to prevent unauthorized access.

3.1 Blockchain

Initially, Bitcoin's underlying enabling technology was blockchain. Essentially, it is a dispersed shared database that is extensively utilized for resource sharing, data traceability, and access control and acts as a ground-breaking low-cost credit technology solution. Scripting languages can operate in an Ethereum virtual machine (EVM) [16] environment, which is provided by Ethereum, a decentralized application 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. Codes created in compliance with transaction rules are known as smart contracts. Smart contracts are operated indefinitely on the blockchain and are unchangeable once created.

By contacting the associated address or interface in the contract, users can communicate with smart contracts that are distributed on the blockchain [17]. The code 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 safe transactions 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.

3.2 Cloud Computing

There are millions of websites hosted on the web in this era of the Internet. The hosted site must be maintained using an expensive stack of servers. These servers need to have a steady flow of traffic and continual maintenance and monitoring. To maintain and arrange these servers, more employees will need to be hired. All of the data will be kept in data centers. Thus, persistent efforts to fix the server problem and the staff might prevent us from reaching our corporate objectives. We are implementing "Cloud Computing" in order to prevent this demanding upkeep.

Using a network of distant computers to store, manage, and analyze data from anywhere in the globe is known as cloud computing. Cloud provides many services, and they are classified mainly into three delivery models. The first service is Software as a Service (SaaS), which is like an application hosted to customers provided across the internet. The Cloud Service Provider delivers the complete applications or projects as a single platform of the software running in the cloud, offering multiple services for many users. Cloud customers do not have control over the cloud infrastructure. Amazon web services, SalesForce.com, Google Mail constitute a significant example of SaaS. The second service is Platform as a Service (PaaS). The cloud service provider allows us to deploy our application and suites of programming languages within the platform. The difference between SaaS and PaaS is that SaaS hosts the whole application in the cloud, where PaaS provides the platform for the application. Google search engine is the best example for PaaS. The third service is Infrastructure as a Service (IaaS), in which it offers the user to directly access the storage, processing, and other resources over the network. Virtualization is used in IaaS to distribute the physical resources to meet the resources demand from cloud customers. The best

virtualization method is to set up independent virtual machines separated from the underlying hardware and other VM's. To provide security, they provide servers with a unique IP address. Amazon EC2, Go Grid, is the best example of IaaS.

3.3Attribute-Based Encryption

A strong cryptographic technique for offering granular access control and confidentiality security services is Attribute-Based Encryption (ABE). For cloud-based applications where one-to-many encryption is essential, ABE is a good fit. By defining relationships between a collection of attributes7 used to encrypt data, ABE presents an expressive method of controlling access to private data. The Key Generation Server (KGS) in the ABE system creates a public key that is used to encrypt data in accordance with predetermined policies and a private key for each authorized user depending on their qualities. Data can only be decrypted by a valid user if it possesses the necessary qualities to comply with the policy.

By implementing robust data encryption strategies in Cloud and Blockchain, organizations can protect sensitive data from unauthorized access, tampering, and theft. Fig 1 shows the layers of Blockchain and Cloud to make the intrusion prevention mechanism by proposing a new approach to access data without the participation of the provider through the ciphertext- policy attribute based encryption scheme with dynamic attributes by taking advantage of the idea of the blockchain that depends on the ledger so that the model idea is based on building a record to generate the key, or set the access policy, or change or cancellation, or request access is not subject to change, and hence the degree of security in access to data in the computerized cloud is achieved.

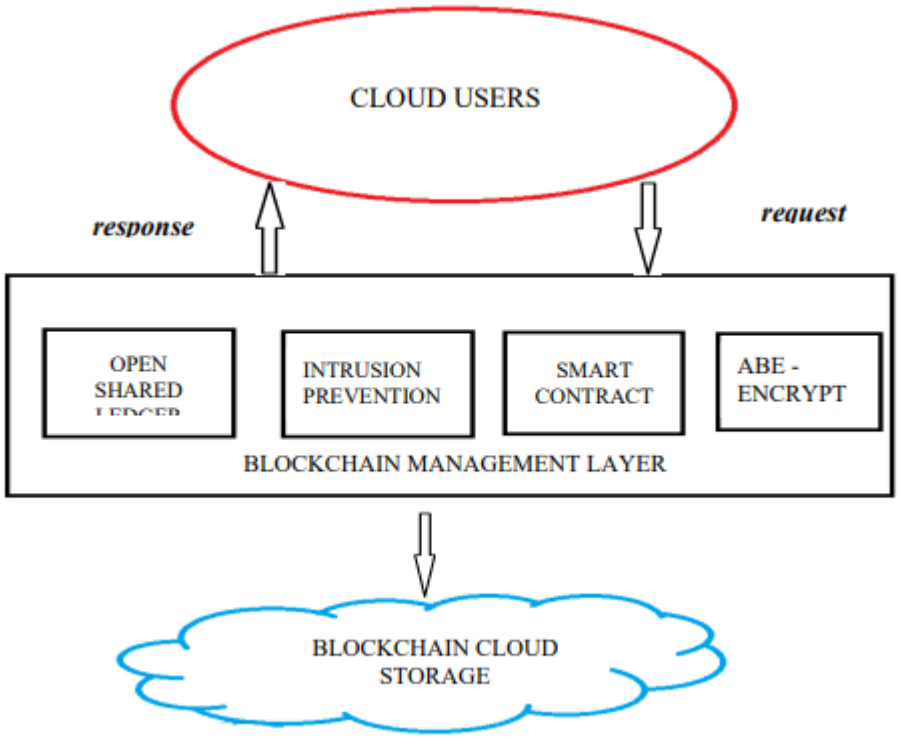


FIGURE 1. Layers of blockchain in Cloud Framework

The aforementioned difficulty was initially put up by Sahai et al. in 2005, and it was later resolved with the introduction of Attribute-Based Encryption (ABE) [1], which led to the development of Key Policy–Attribute-Based Encryption (KP-ABE) [2] and Ciphertext Policy–Attribute-Based Encryption (CP-ABE) [3]. In CP-ABE, data owners may personalize access controls and include them into ciphertext. In addition to achieving flexible and fine-grained access control, this method addresses the shortcomings of traditional access control, which finds it difficult to uphold the minimal authorization principle and adjust on the fly to changing environmental conditions. Nonetheless, there are still certain issues with conventional CP-ABE systems in real-world settings. For instance, in the majority of CP-ABE schemes, all user attributes must be managed by a single authorization authority with the assistance of a completely trusted attribute authorization authority.

The distributed ledger technology known as blockchain has gained popularity and is a viable option for trustworthy access control because of its programmability, traceability, nonfalsification, decentralization, and data tampering capabilities. However, a number of difficulties arise with regard to the security and control of data kept in blockchain due to its open and transparent character. The cryptographic method of CP-ABE, when paired with blockchain technology, may guarantee the security, privacy, and confidentiality of data stored on the blockchain. On the other hand, blockchain technology can support the current CP-ABE-based schemes with features like efficient audits and trusted authority verification. For instance, using CP-ABE and blockchain technology, the programs in reference establish privacy protection and enable the accountability of past protocols.

The most popular blockchain application platforms are Hyperledger Fabric, Ethereum, and Bitcoin. The blockchain technology's prototype, Bitcoin, does not have smart contracts or privacy protection. It cannot be applied in intricate circumstances as a result. The public blockchain is called Ethereum. On Ethereum, though, every transaction has to be paid for. Additionally, there are no limitations on users of the public blockchain, who typically engage in anonymous participation, which makes it challenging to govern. Moreover, Fabric's modularization of rights management, authentication, consensus mechanisms, and other technologies offers significant flexibility, pluggability, and scalability.

4. CONCLUSION

Cloud computing is a well-known technology as it has existed for many years. But people are still struggling to overcome some challenges of cloud computing like data security, data management, interoperability, etc. Blockchain technology is an emerging technology well known for its security and authenticity, which are the main characteristics that are making the world turn to its side. By integrating blockchain with cloud computing, there will be many advantages in usability, trust, security, scalability, data management, and many other advantages. In this paper, we briefly introduced cloud computing, blockchain technology. We discussed the benefits of integrating the blockchain network with a scalable cloud environment to enhance confidence, data security, and user data management. In this research, we present an attribute-based searchable encryption and blockchain-based data security intrusion prevention mechanism for cloud computing environments. By providing policy concealment and attribute revocation, our system enables safe search and fine-grained access to cloud data. In order to lower users' processing costs, proxy encryption and decryption are deployed concurrently. When combine with blockchain technology, it guarantees a fair keyword search and the safe dissemination of metadata ciphertext and keys. Furthermore, dynamic monitoring of user access behavior is realized through the use of smart contracts. This approach offers improved computing and storage performance while maintaining data security and equitable user access, according to security, performance comparison, communication, and computing analyses.

REFERENCES

[1]. Sahai, A.; Waters, B. Fuzzy identity-based encryption. In Proceedings of the Advances in Cryptology—EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, 22–26 May 2005; Springer: Berlin/Heidelberg, Germany, 2005; pp. 457–473.

[2]. Goyal, V.; Pandey, O.; Sahai, A.; Waters, B. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM Conference on Computer and Communications Security, Alexandria, VA, USA, 30 October–3 November 2006; pp. 89–98.

[3]. Waters, B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In Proceedings of the International Workshop on Public Key Cryptography, Taormina, Italy, 6–9 March 2011; Springer: Berlin/Heidelberg, Germany, 2011; pp. 53–70.

[4]. O.Ali,A.Jaradat,A.Kulakli,andA.Abuhalimeh, "Comparative study: Blockchain technology utilization benefits, challenges, and functionalities," Ieee Access, vol. 9, pp. 12730- 12749, 2021.

[5]. A.Gupta,S.T.Siddiqui,S.Alam,andM.Shuaib, "Cloud computing security using blockchain," JournalofEmergingTechnologiesandInnovative Research (JETIR),vol.6,no.6,pp.791-794,2019.

[6]. W.VentersandE.A.Whitley,"Acriticalreview of cloud computing: Researching desires and realities," J. Inf. Technol., vol.27, no. 3, pp. 179– 197, 2012.

[7]. J.Zhang,X.Nian,andH.Xin,"A Secure System For Pervasive Social Network-based Healthcare," IEEE Access, vol. 4, pp. 9239-9250, 2016.

[8]. Ch.V.N.U.B.Murthy,L.M.Shri,S.Kadry,and S. Lim, "Blockchain Based Cloud Computing: Architecture and Research Challenges," IEEE Access, vol. 8, 2020.

[9]. C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, and K. Yu, "AuthPrivacyChain: A blockchain-based access control framework with privacy protection in cloud," IEEE Access, vol. 8, pp. 70604-70615, 2020.

[10]. Z. Dong, Y. C. Lee, and A. Y. Zomaya, "Proofware: Proof of useful work blockchain consensus protocol for decentralized applications," 2019, arXiv preprint arXiv:1903.09276.
[11]. X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "Provchain: A blockchain- based data provenance architecture in a cloud environment with enhanced privacy and availability," IEEE, 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), pp. 468-477, 2017.
[12]. X. Zheng, R. R. Mukkamala, R. Vatrapu, J. Ordieres-Mere, "Blockchain-based Personal Health Data Sharing System Using Cloud Storage," IEEE, J. Kubicek (Ed.), 20th InternationalConferenceonE-HealthNetworking, Applications and Services (Healthcom) Los Alamos, CA: IEEE, 2018.
[13]. N.Mansourov,and D.Campara, "Knowledge ofrisk as an element of cybersecurity argument," System Assurance, 2011.
[14]. Z. Shahbazi and Y. C. Byun, "Improving transactional data system based on an edge computing–blockchain–machinelearning integratedframework,"Processes,vol.9,no.1,pp.92,2021.
[15]. M.Laurent,N.Kaaniche,C.Le,andM.Vander, "Plaetse, A blockchainbased access control scheme," ICETE, 2018 - Proceedings of the 15th International Joint Conference on e-Business and Telecommunications,vol.2,no.7,pp.168–176,2018.
[16]. Ma F, Fu Y, Ren M, Wang M, Jiang Y, Zhang K, Li H, Shi X (2019) Evm*: from offline detection to online reinforcement for ethereum virtual machine. In: 2019 IEEE 26th International Conference on Software Analysis, Evolution and Reengineering (SANER): 24-27 February. IEEE, Harbin, pp 554–558.
[17]. Oliva GA, Hassan AE, Jiang ZMJ (2020) An exploratory study of smart contracts in the ethereum blockchain platform. EmpirSoftw Eng 25(3):1864–1904.
[18]. Liu S, Yu J, Xiao Y, Wan Z, Wang S, Yan B (2020) Bc-sabe: Blockchain-aided searchable attribute-based encryption for cloud-iot. IEEE Internet Things J 7(9):7851–7867.
[19]. Liu B, Xiao L, Long J, Tang M, Hosam O (2020) Secure digital certificate-based data access control scheme in blockchain. IEEE Access 8:91751–91760

