Journal of Information Technology and Digital World (ISSN: 2582-418X)
www.irojournals.com/itdw/

A Novel Framework for Cloud Data Security with Blockchain Technology and Distributed Virtual Machine Agents

Oyyappan Duraipandi[1], Thesnath A/L Velayudhan[2],

[1]Associate Professor, Faculty of Business, Lincoln University College, Malaysia.

[2]Faculty of Computer Science and Multimedia, Lincoln University College, Malaysia.

E-mail: [1]oyyappan@lincoln.edu.my

Abstract

Even though cloud computing has advanced over the years, the two major challenges currently faced by cloud computing are data security and trusted computing. In cloud computing applications, blockchain technology can enhance data security and trusted computing when paired with virtual machine agents and mobile agent technologies. A decentralized new framework for distributed computing is blockchain. A potential area of study is the integration of blockchain technology with cloud computing, leveraging the former's security mechanisms to enhance the latter's secure computing and storage capabilities. The usage of the proposed framework builds on the inherent security features of blockchain technology in an effort to secure data and information integrity, confidentiality and authentication in cloud environments. Through the introduction of distributed virtual machine agents, the framework increases the scalability and effectiveness of data protection mechanisms for virtual data environments that can be used to store information protected by cloud security measures. Thus, the proposed study substantiates the applicability and efficiency of the existing and emerging problems of cloud data security and this approach develops satisfactory data protection solutions.

Keywords: Cloud Computing, Blockchain Technology, Data Security, Virtual Machine Agent

DOI: https://doi.org/10.36548/jitdw.2024.2.008
Received: 13.05.2024. received in revised form: 02.06.2024, accepted: 18.06.2024, published: 29.06.2024

1. Introduction

Cloud computing provides scalable internet-based resources and services, it also poses serious security risks. The need for better application and data security is growing along with the creation and hosting of cloud-based applications. Virtual machines are used to host cloud-based applications, and these machines also house the data that these apps create or utilize. Therefore, the only way to secure the data and applications is to secure the virtual machines. Big data security measures processes and data to prevent theft, unauthorised use, hacks, breaches, and other destructive actions. The emergence of cloud computing has significantly changed the traditional model of data storage and processing, providing scalable, adaptive, and, most crucially, cost-effective solutions to an equally diverse range of businesses. Cloud services provide consumers with nearly limitless computing power and storage on demand, which can innovate by clearing up resources that would otherwise be constrained in traditional IT. On the other hand, it facilitated the easy movement of sensitive data to the cloud while also introducing significant security concerns, which have since made cloud data security a top priority for organizations worldwide [11-15].

Cloud computing has become the new standard in modern IT architecture, providing scalable and adaptable resources for storing and processing data at a low cost. Although cloud computing is extensively used by researchers and practitioners, there are some serious security risks that may arise, particularly with data integrity, confidentiality, and availability. Its centralised design can lead to single points of failure and vulnerabilities, making the traditional security solutions insufficient [16-20]. The proposed study suggest a new technique to enhance cloud data security by leveraging blockchain technology and distributed VM agents to address the aforementioned concerns. Figure 1 depicts the cloud data with blockchain infrastructure

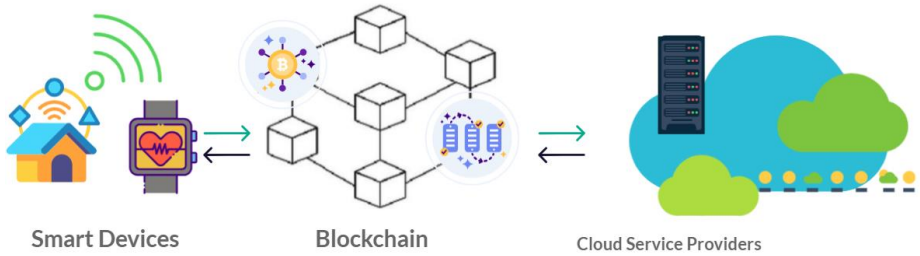

Figure 1. Cloud Data with Blockchain Infrastructure

2. Related Work

2.1 Blockchain

Blockchain refers to a distributed open database that stores multiple records across various nodes in a network while maintaining the integrity and transparency of the records. Every transaction under goes validation and becomes a block of data that is connected to the previous block, forming a continuous chain [21,22]. This structure can make it virtually impossible to change any single transaction without changing all subsequent blocks, which provides enhanced data security. It uses consensus protocols such as Proof of Work (PoW) or Proof of Stake (PoS) whereby the nodes in the network must reach a consensus on the authenticity of the transactions. These mechanisms ensure that only authorized transactions are processed and establish the reliability of data stored in the blockchain. Moreover, blockchain works on a decentralized mechanism, which means that there is no central authority that acts as a single point of failure. Figure 2 depicts the blockchain with authentication system .

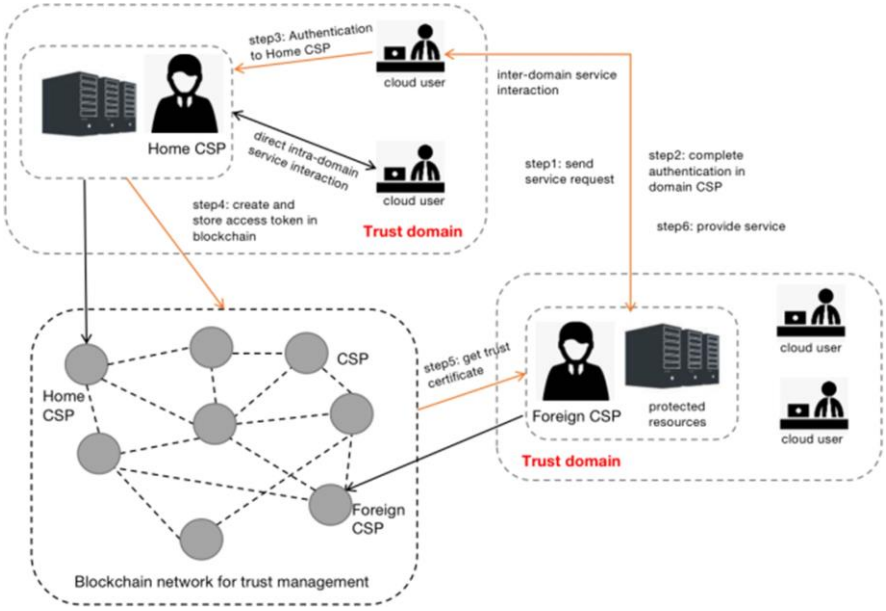

Figure 2. Blockchain with Authentication System [8]

2.2 Cloud Computing

Cloud technology has significantly transformed the traditional model of data storage and processing, enhancing the flexibility in data administration. Businesses profit from cloud services because they allow them to harness large-scale compute in an adaptable, flexible, and

cost-effective manner without having to pay for expensive hardware upfront. Most of these developments have encouraged innovation and flexibility in remote solutions for organisational operations across a wide range of sectors. However, while cloud computing has provided several benefits, it has also introduced a number of security risks that must be managed properly in order to assure information security.

2.3 Distributed VM Agents

Distributed VM agents are progressing autonomy nodes that are established in the cloud environment. These agents work autonomously but can exchange information between themselves and with the use of the network to maintain security as well as manage data. VM agents also improve security as they manage the control and monitor the processes, thus minimizing the dependency on centralized systems.

VM agents that can be located and distributed across geographical locations can perform security tasks such as encryption, user access, and other security services like intrusion. To achieve this level of security, the functions are divided among multiple parties or agents to ensure that an attack or failure of one agent does not bring down the entire system. Every VM agent can be a checkpoint, never forgetting to retain secure data and to recognize any improper activity.

[1] The suggested distributed virtual machine agent approach enables a unique and believable monitoring of virtual machines for each cloud user, preventing the cloud administrator from accessing or interfering with the user's sensitive information. The study uses a data integrity mechanism to assure user data availability and integrity. Security study demonstrates that the suggested protocol can protect against three forms of cloud service provider attacks.

[2] The study offers a blockchain-based cloud data integrity protection mechanism that employs a distributed virtual machine agent paradigm as well as blockchain-based methodologies to verify, monitor, and protect data integrity. The system employs a Merkel hash tree and smart contracts to track data changes and notify users to data manipulation. It also employs a "block-and-response" mode to create a blockchain-based cloud data integrity verification system.

[3] Cloud computing delivers on-demand, controlled, and customised resources, but also poses significant security and privacy risks. To solve these difficulties, the article presents a cloud security architecture and framework that makes use of blockchain technology. The combination of blockchain with cloud computing is expected to have a significant influence on cloud security characteristics.

[4] A new system is described that use machine learning to identify attacks by analysing connection attributes and prevents attacks by selectively encrypting virtual machines.This framework detects new and old attack types with almost 98% accuracy. The virtual machines are extremely susceptible during the transfer since they are moved as basic text data within the data centre networks.

[5] Blockchain technology's distributed ledger, consensus-based confirmation, and immutable data storage have the potential to improve cloud computing security. However, blockchain technology has issues in security, compliance, and dependability. The study's major goal is to analyse prior research on merging blockchain with cloud computing in order to better understand the security concerns and build cloud-based threat mitigation solutions.

[6] The research proposes utilising Ethereum blockchain to protect, track, and manage virtual machine images (VMIs) in cloud architecture. The blockchain-based solution is intended to improve the proposed scheme's reliability and provide system auditability by preserving the whole VMI history.

[7] An Ethereum-based blockchain network and a specific smart contract are used to monitor and secure the virtual machine images (VMIs) kept by cloud service providers. Blockchain technology precludes any one administrator or outside party from managing or updating the system, maintaining the integrity of the VMIs. The suggested approach is said to be more efficient than previous methods intended for the same objective.

3. Proposed Framework

The open-source business blockchain technology Hyperledger Fabric is extensively utilised in modern applications; the addition of virtual machines (VMs) agents has the potential to improve cloud data security. In order to preserve data integrity, confidentiality, and access

control while providing auditable features in cloud environments, this integration leverages the distributed ledger and consensus aspects of blockchain technology in conjunction with the distributed and self-governed control feature of the virtual machine agents. Hyperledger Fabric and virtual machine agents together provide a complete security architecture for cloud data protection. Data integrity, confidentiality, access control, and auditability are all improved by this combination.

The integration of Hyperledger Blockchain with cloud computing and VM agents as a proposed framework would allow to take use of the capabilities of the technologies stated above in developing a strong, scalable, and secure framework for varied applications.

The cloud infrastructure extends the scalability option that enables the network to either expand the resources available or reduce them depending on the current network load. Some cloud platforms, such as AWS, Azure, and Google Cloud, allow you to construct or instantiate virtual machines. These are the virtual machines that will host the various components of the Hyperledger Fabric blockchain network.

Every VM may contain the necessary OS, libraries, and services (CPU, memory, and discs) to execute Hyperledger Fabric components. VMs provide enclosed worlds to individual portions of the blockchain network that would otherwise have the capacity to impact one another. It also helps to fulfil the goals of security and stability since isolation minimises susceptibility. Figure 3 shows the proposed blockchain framework

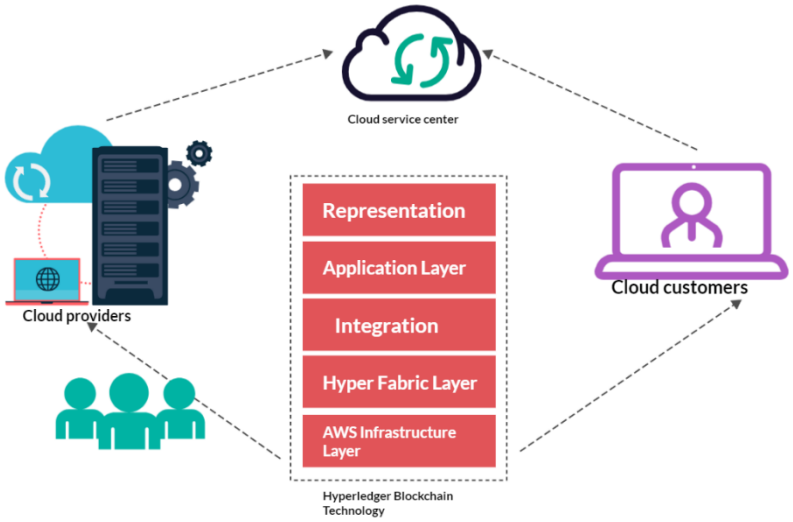

Figure 3. Proposed Blockchain Framework

Virtual machines host peer nodes, which help to maintain ledgers and perform smart contracts known as chain code. It is worth mentioning that any organisation in the network may have one, a few, or no peer nodes. VMs have ordering nodes, which are used to arrange transactions while also contributing in the formation of consensus among the various members. Hyperledger Fabric, for its part, provides for the option of alternative consensus models according on the application's requirements. CA nodes can be hosted on network VMs to control network members' identities. This includes the giving and revocation of certifications required for network access.

Every peer node has a copy of the ledger, which contains a record of all transactions that have gone through validation and consensus. The ledger is made up of two parts: the blockchain, also known as the blocks, which we've heard a much about (the continuous series of blocks), and the blockchain's current state, also known as the global state. Another option for managing ledgers is to use Cloud storage solutions, which allow for multiple copies of ledger data for availability and redundancy.

3.1 Benefits of the Proposed Framework

Data Privacy: Another important problem that must be addressed is privacy. Blockchain offers benefits like data traceability and transparency, but it also raises the possibility of data exploitation and privacy violations. Future studies must strike a compromise between user privacy and disclosure.

Data Integrity: Information exchange within the ordered and peer nodes occurs stochastically while all the data exchange records are stored on Hyperledger Fabric’s blockchain. This again holds the implication of a fairly decentralised log, one that guarantees that once data has been entered into the ledger it cannot be changed without the entire network agreeing on this[9].

Other roles of VM agents are to decide or validate transactions and prevent fraudulent transactions from going through, thus being recorded on the blockchain. They check the accuracy of data before it is written to the ledger before sensitive transactions take place[10].

Data Confidentiality: VM agents along with Hyperledger framework are able to effectively encrypt data prior to storing it in the cloud libraries. This means that only the agents

who are permitted to do so carry the key or code to decrypt the content since its content is sensitive.

4. Conclusion

Hyperledger Blockchain, in conjunction with cloud infrastructure and VM agents, provides a strong foundation for running blockchain applications now and in the future, while also leveraging the inherent capabilities of both technologies within their respective industries and purposes. The integration of distributed virtual machine agents with the Fabric platform to enable Hyperledger Blockchain creates a novel and capable cloud data security environment. It offers another way to secure any sensitive data stored in cloud services and resolves a number of significant issues, including data consistency, non-disclosure, authorization, and authentication. Since the performance of these technologies and their diverse applications need to be assessed, additional uses of these technologies will be implemented accordingly in future.

References

[1] Xu, Xiaolong, Guangpei Liu, and Jie Zhu. "Cloud data security and integrity protection model based on distributed virtual machine agents." In 2016 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 6-13. IEEE, 2016.

[2] Wei, PengCheng, Dahu Wang, Yu Zhao, Sumarga Kumar Sah Tyagi, and Neeraj Kumar. "Blockchain data-based cloud data integrity protection mechanism." Future Generation Computer Systems 102 (2020): 902-911.

[3] Kumar, Sunny, Aditi Singhal, and Ankur Dumka. "Analysis of cloud security framework using blockchain technology." In International Conference on Advances in Engineering Science Management & Technology (ICAESMT)-2019, Uttaranchal University, Dehradun, India. 2019.

[4] Radharani, S., and V. B. Narasimha. "A Novel Framework for Cloud based Virtual Machine Security by Change Management using Machine." International Journal of Advanced Computer Science and Applications 12, no. 12 (2021).

[5] Rani, Meena, Kalpna Guleria, and Surya Narayan Panda. "Blockchain technology novel prospective for cloud security." In 2022 10th International Conference on

Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO), pp. 1-6. IEEE, 2022.

[6] Basu, Srijita, Sandip Karmakar, and Debasish Bera. "Securing cloud virtual machine image using ethereum blockchain." International Journal of Information Security and Privacy (IJISP) 16, no. 1 (2022): 1-22.

[7] Basu, Srijita, Sandip Karmakar, and Debasish Bera. "Blockchain based Secured Virtual Machine Image Monitor." In ICISSP, pp. 432-439. 2021.]

[8] Nayak S, Narendra N, Shukla A et al (2018) Saranyu: using smart contracts and Blockchain for cloud tenant management. In proceedings of 2018 IEEE 11th international conference on cloud computing. IEEE 2018:857–861]

[9] Aghamohammadzadeh, Ehsan, and Omid Fatahi Valilai. "A novel cloud manufacturing service composition platform enabled by Blockchain technology." International Journal of Production Research 58, no. 17 (2020): 5280-5298.

[10] Kubendiran, Mohan, Satyapal Singh, and Arun Kumar Sangaiah. "Enhanced security framework for e-health systems using blockchain." Journal of Information Processing Systems 15, no. 2 (2019): 239-250.

[11] Alsulbi, Khalil Ahmad, Maher Ali Khemakhem, Abdullah Ahamd Basuhail, Fathy Eassa Eassa, Kamal Mansur Jambi, and Khalid Ali Almarhabi. "A proposed framework for secure data storage in a big data environment based on blockchain and mobile agent." Symmetry 13, no. 11 (2021): 1990.

[12] Li, Zhi, Ali Vatankhah Barenji, and George Q. Huang. "Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform." Robotics and computer-integrated manufacturing 54 (2018): 133-144.

[13] Uddin, Mueen, Anjum Khalique, Awais Khan Jumani, Syed Sajid Ullah, and Saddam Hussain. "Next-generation blockchain-enabled virtualized cloud security solutions: review and open challenges." Electronics 10, no. 20 (2021): 2493.

[14] Nair, Rajit, Syed Nasrullah Zafrullah, P. Vinayasree, Prabhdeep Singh, Musaddak Maher Abdul Zahra, Tripti Sharma, and Fardin Ahmadi. "Blockchain-Based Decentralized Cloud Solutions for Data Transfer." Computational Intelligence and Neuroscience 2022, no. 1 (2022): 8209854.

[15] Hussain, Muhammad Zunnurain, Muhammad Zulkifl Hasan, Adnan Nabeel Qureshi, and Ghulam Mustafa. "Implementation of a Blockchain-Based Secure Cloud Computing Mechanism for Transactions." In Blockchain-based Internet of Things, pp. 146-166. Chapman and Hall/CRC, 2024.

[16] Roopa Devi, E. M., R. Shanthakumari, R. Rajadevi, D. Kayethri, and V. Aparna. "Decentralized, Distributed Computing for Internet of Things-Based Cloud Applications." Automated Secure Computing for Next-Generation Systems (2024): 43-64.

[17] Gousteris, Solonas, Yannis C. Stamatiou, Constantinos Halkiopoulos, Hera Antonopoulou, and Nikos Kostopoulos. "Secure distributed cloud storage based on the blockchain technology and smart contracts." Emerging Science Journal 7, no. 2 (2023): 469-479.

[18] Golightly, Lewis, Paolo Modesti, Rémi Garcia, and Victor Chang. "Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN." Cyber Security and Applications 1 (2023): 100015.

[19] Li, Wenjuan, Jiyi Wu, Jian Cao, Nan Chen, Qifei Zhang, and Rajkumar Buyya. "Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions." Journal of Cloud Computing 10, no. 1 (2021): 35.

[20] Gai, Keke, Jinnan Guo, Liehuang Zhu, and Shui Yu. "Blockchain meets cloud computing: A survey." IEEE Communications Surveys & Tutorials 22, no. 3 (2020): 2009-2030.

[21] Ashraf, Muhammad Usman. "A Survey on Data Security in Cloud Computing Using Blockchain: Challenges, Existing-State-Of-The-Art Methods, And Future Directions." Lahore Garrison University Research Journal of Computer Science and Information Technology 5, no. 3 (2021): 15-30.

[22] Tyagi, Amit Kumar, Saravanan Chandrasekaran, and N. Sreenath. "Blockchain technology: a new technology for creating distributed and trusted computing environment." In 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), pp. 1348-1354. IEEE, 2022.