Block Chain-Powered Cloud Data Integrity Verification System with Excellent Effectiveness

Name – Vaishali Sisaudia[1]
Assistant Professor
Department of Computer Applications
Noida Institute of Engineering & Technology
Greater Noida - 201306
Email – vaishalisisaudia23@gmail.com

Name – Dr. Anil Agarwal[3]
Associate Professor
Noida Institute of Engineering & Technology
Greater Noida - 201306
Email –manikopalkeshav@gmail.com

Name – Ajit Kumar[2]
Assistant Professor
Department of Computer Applications
Noida Institute of Engineering & Technology
Greater Noida – 201306
Email – ajitjnvassam@gmail.com

Name – Jitendra Kumar Sonkar[4]
Assistant Professor
Department of Computer Applications
Noida Institute of Engineering & Technology
Greater Noida - 201306
Email –computer2021zone@gmail.com

***Abstract*— The "next-generation financial technology," or blockchain, is praised for its peer authentication security features, which include virtual money, data encryption, and hash value creation. Cloud computing is widely used due to its efficiency, and the global financial sector sees a vast market for security. Blockchain technology is examined in this article along with its developments and application to cloud computing in healthcare and electronic vehicle security. Verification, oversight, and dependable data storage are made possible by the virtual machine agent mechanism, which is crucial for maintaining blockchain integrity. The Merkel hash tree's unique hash values are used by blockchain smart contracts to keep track of data modifications. Users are notified of data manipulation through a "block-and-response" procedure. Data security and trustworthy computing are still issues in spite of the growth of cloud computing. Different approaches, such as data integrity tests and secure multi-party computations, have been proposed by researchers; however, these frequently encounter problems related to complexity and scalability. This paper investigates the ways in which blockchain technology can help with these issues by providing a decentralized method for improving cloud computing security and storage.**

Keywords*— *Blockchain, money, security, cloud service, technology, big-data, data, healthcare ;

I. INTRODUCTION

Computer systems are frequently attacked by phishing, malware, viruses, spam, and data-stealing malware. These socially engineered attacks aim to steal sensitive information by deceiving victims into believing they are in a secure setting by employing well-known ideas. The primary objective is to compile comprehensive information about the target. This threat has a high potential to cause data loss or system interception. The problems brought on by attacks on information systems have been successfully resolved by blockchain security technology. This study implements the distributed agent model on the cloud using mobile agent technology. Tenants can work together to use the virtual machine agent's mechanism to guarantee dependable data storage, monitoring, and verification. In order to create blockchain integrity protection, this is also necessary. Using the virtual machine proxy model, the integrity protection framework based on blockchain is constructed. The file's distinct hash value, produced by the Merkel hash tree, is used by the blockchain smart contract to monitor modifications to the data and guarantee ownership. The user sends out a warning whenever data is modified. Security Issues with Cloud Computing: A distributed architecture designed to offer a range of online computing services is what is meant by cloud computing. Talk about cloud computing's notions of Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Emphasize to customers using cloud services how crucial it is to protect their data and privacy. In order to protect data, platforms, software, and infrastructure, cloud security refers to the set of regulations, procedures, best practices, technological advancements, and security measures incorporated into cloud computing systems. The necessity of customizing cloud security features, like traffic filtering and access verification, to the particular needs of businesses must be emphasized.

Cloud Healthcare Utilizing Block chain Security

As a big-data industry, the healthcare sector regularly generates, shares, stores, and retrieves massive volumes of data. Data must be forwarded to the radiographer and doctor upon completion of specific tests (such as computed tomography or computerized axial tomography scans). In the event that a physician from a different hospital in the network needs access to the consultation results later, the hospital will retain a copy of them on file. Staff, equipment, and more resources are all easily accessible, and there is the potential for cost savings through more efficient resource allocation and improved patient care (for example, through the use of data analytics to make informed medical decisions). For instance, the high cost of data input errors in paper-based data collection makes it difficult to create, store, and enter into systems that are available when needed. These issues could lead to, among other things, treatment decisions that are not accurate, the need for additional testing due to missing data, or the storage of data at a different hospital in a different state or nation (at an additional cost to the patients). Because of the nature of the industry, data security, confidentiality, and accuracy are crucial. This highlights the significance of having a reliable and secure information management system.

The accountable healthcare provider maintains electronic medical records, or EMRs, which contain the clinical and medical data related to a single patient. This simplifies the process of obtaining and assessing medical records. Enhanced Prompt: Create an improved Health Information System (HIS) with an emphasis on enhancing the administration of Electronic Medical Records (EMRs) by facilitating the creation, storing, searching, and retrieving of EMR instances. Web services and graphical user interfaces, which act as the front end of a distributed or centralized system with a database acting as the back end, should be incorporated into the system. The interoperability of stand-alone EMR solutions should be emphasized in light of the growing patient mobility both within and between countries. This will make it easier for healthcare providers to share data, even across international borders. Examine situations like the sharing of medical data in real time in medical tourism destinations such as Singapore. Make sure the system can efficiently track patients and provide medical professionals with their medical history. Electronic Health Records (EHRs) are more complex than EMRs, even though EMRs have a simpler data structure. Use wearables and iOS and Android-powered smartphones, among other smart technology, to give patients the ability to track their health, communicate with doctors, and receive better treatment results. By incorporating sensor-equipped gadgets like heart rate bracelets and glucose self-testing devices, you can overcome the difficulties associated with complicated medical tasks. To improve accessibility for patients, healthcare providers, and governments, design the HIS as an ecosystem of products that interchange data seamlessly. To manage massive volumes of healthcare data and facilitate real-time data sharing across geographic borders, put cloud computing capabilities to use. In order to shield private medical data from hackers and illegal access attempts, emphasize data security measures. To protect privacy and encrypt data, use public key infrastructure and cryptographic primitives. To build a dispersed online database for patient medical records, think about implementing blockchain technology. Make sure that every time a new patient enters their medical history, a new block is created and added to the chain upon peer consensus, allowing for a safe and thorough patient medical history. To preserve data accessibility and integrity, deal with issues like orphan blocks and chain breaks.

Digital Car Security in the Cloud Sponsored by Block chain

A potential network model termed cloud and edge computing for electric cars (EVCE) can integrate distributed electric vehicles (EVs) into a shared resource pool and use them for locally adaptive purposes by combining seamless connectivity in a range of vehicle scenarios. Provide a comprehensive analysis of the security risks associated with automotive applications, with a particular emphasis on the dynamic information and energy exchange that takes place in vehicle-to-anything connections, including those between a vehicle and its surroundings, a grid or other infrastructure, or another vehicle. (V2V). Consider the intricate nature of these relationships and the sensitivity of the data at stake. Discuss potential strategies and instruments that can be employed to fortify the security of these links, ensuring efficient energy distribution and seamless data collection. Apart from providing feasible measures to mitigate these hazards, your examination ought to center on the specific dangers presented by the ever-changing transfer of energy and data in automotive settings. In the future, edge and hybrid cloud computing applications will begin to leverage all three of the following benefits: attributes. Data sharing happens in peer-to-peer communications in the absence of a central node and without prior trust relationships. This is in line with the idea of "center less trust.". ". The limited human interaction capabilities of an electric vehicle (EV) can be leveraged to address crowd intelligence solutions.

A data provenance criterion is satisfied when an EV exchanges sensitive data with different spatiotemporal properties. Energy and knowledge are included in this. The EVCE comes with serious security issues because it treats

attackers and legal entities as equal actors with comparable privileges. The consensus processes and decentralization of block chain technology have been suggested as potential solutions for these security issues. Use of cryptographic techniques to build trust relationships between two or more parties is how the coordinated EVs will contribute to particular processes. The motivation for mass collaboration is collective self-interest, with data ambiguity being a secondary factor. A receipt is stored in each block along with a record of its predecessors. New blocks are added solely to the ledger. assuming the accompanying message's majority authentication process is successful. In case of a single point of failure, this distinct data format is more resilient and impervious to manipulation. The same characteristics apply to the block chain, where users co-validate new blocks for cooperative management. Timingstamps and Merkle hash tree algorithms are employed by the participating teams. PoW and stake-proof PoS content. The PoW is solely dependent on processing power, so players try to enter accurate data with the lowest probability of success. Picking PoS accounts involves deterministic algorithms based on likelihood and total stakes. Provide a thorough explanation of blockchain technology in relation to the introduction of new cryptocurrencies into automobiles. Specifically, explore the concept of data coins and energy coins within the context of vehicle records stored in a consortium blockchain during information and energy transfers. Explain how distributed consensus processes based on blockchain technology are used, and how known distributed consensus techniques are used to separate and encrypt vehicle record blocks. Examine and add data to the blockchain chronologically for validation, taking into account the roles of RSUs and LAGs. Just describe how mobile EVs function as network operators to create V2V connections and take cooperative actions with nearby EVs. For data sharing and swapping among mobile EVs, take into consideration implementing data-coin-based anonymous data confirmation and access control. The creation of temporary session keys via lightweight symmetric encryption is emphasized in the discussion of the use of peer-to-peer networks for key negotiation and distribution during the initialization phase. Examine the possibility of group key agreement using multi-path key mode and shortest path tree routing, as well as the creation of RSU-to-RSU communication and the movement of EVs through access challenges and responses. As EVs work together to exchange data using homomorphic encryption and secure multi-party computing, emphasize the significance of mutual authentication. Evaluate.

Suggested technique Overview of block chain technology

Block chain is a distributed, open, and decentralized database (Block chain). Its data chunks are frequently arranged in accordance with the connections that cryptographic algorithms make between them. A novel approach to distributed computing is block chain. Explain the fundamental principles of blockchain technology's design and advantages without relying on node trust. Describe the ways that consensus procedures, incentive systems, time stamping methods, and encryption algorithms enhance the security and effectiveness of blockchain networks. Describe how peer-to-peer cooperation, coordination, and information sharing are achieved through the use of network technology. Stress the importance of chronological blocks in offering a thorough log of network transactions, along with the composition of a typical block chain block, which consists of a block header and a block body. Examine the variables that affect the maximum number of transactions that can be contained in a block while taking block and transaction size limitations into account. Make sure to stick to the technical terminology and specifics from the original prompt.

Crucial elements of the block chain.

The following are the main characteristics of the block chain as a whole: Decentralization comes first. Conventional trading systems need that each transaction be approved by a trustworthy central authority. This always adds to the cost and complexity of the security center's server. But the block chain eliminates the requirement for the central mechanism. Persistence comes next. Once a transaction is added to the block chain, it is nearly impossible to remove, alter, or reverse it. Quick verification of effective transaction data is achievable. Throughout the verification process, the block containing the incorrect transaction information will also be quickly checked out and removed. And finally, seclusion. In order to conceal their true identities, each user communicates with the block chain and other users on the network through the created user address system. At position four is auditability. Using the (UTO) paradigm, Bit coin saves user balance information. The primary objective and fundamental component of cloud computing is data storage. Data security is given top priority when it comes to cloud computing security protection. For this reason, information data is an important part of user and business assets. Users are most concerned about the security of data stored on cloud platforms.

Access control technology using ciphertext

According to the idea of "data confidentiality," only authorized users and data owners are permitted explicit access to or receipt of data. Encryption is the most widely used method of data privacy protection. Users usually encrypt their data before sending it to the cloud. For network security, system resource preservation, and the lawful use of information, access control is an essential tactic. The subject governs resource access by implementing various policies under various access control models. The user's access to the data becomes a cipher text access control issue because it is stored in the cloud in a cipher text state. Access privileges and critical data are encrypted by the technology used for ciphertext access control, which controls user access. It is a crucial tool for protecting user data in a cloud environment where trust is lacking. User data privacy and confidentiality are significantly enhanced, and the possibility of user data being improperly released is reduced. Attribute-based ciphertext access control, or ABAC, is the outcome of merging attribute-based encryption technology with access control. It restricts data access to users who meet the attribute's decision rules. Cloud storage configurations with multiple tenants and frequent permission changes are better suited for ABAC due to its increased flexibility and tighter access control granularity. The user can only decrypt using the CP-ABE and KP-ABE methods once the set of attributes completes the access tree. Verification technologies for integrity. Data integrity, which includes usage and storage integrity, is a crucial component in determining whether or not the data is authentic and trustworthy. When cloud storage service providers discuss data integrity in their environments, what they typically mean is that they store all of their clients' data on cloud servers in accordance with their specifications. specifically, integrity of storage. Users can assess the quality of data stored in the cloud or obtain small amounts of data using a predetermined knowledge procedure by using integrity verification to verify data. Another term for cloud storage is prove storage, which is the method used here. satisfied. Traditional access- and challenge-response-based methods are the two primary means of confirming the correctness of data in a storage system. On the other hand, the latter is more appropriate for use in distributed cloud storage environments. Responders and verifiers are the two main parts of challenge-response-based integrity verification. Typically, the cloud server acts as the responder and the data owner or a reliable third party acts as the certifier. The way it works is that the verifier sends a challenge to the cloud server, which then uses the information it gets to generate and return pertinent answer data. In the end, decisions are made and integrity is confirmed using the response data that the verifier collected. The pair.

Conclusions

Blockchain technology presents promising answers to some of the most important problems in cloud computing, healthcare, and electric vehicle systems because of its decentralized architecture and cryptographic security. Blockchain improves the integrity, security, and transparency of data transactions by utilizing virtual machine agents, Merkle hash trees, and decentralized consensus mechanisms. Blockchain technology is being used in cloud computing to help solve issues like data manipulation, privacy issues, and unauthorized access—all of which are crucial in sectors like healthcare that handle sensitive data. Blockchain technology provides novel approaches to safeguard data and dynamic energy exchanges between automobiles in the automotive industry, promoting confidence in communications between vehicles and grids, infrastructure, and other vehicles. Although ciphertext access control and integrity verification, two popular cloud and data security technologies, offer a solid base for safe data transmission and storage, they have drawbacks in terms of scalability, complexity, and flexibility. By offering a decentralized, immutable, and transparent system that guarantees data authenticity and boosts user trust, blockchain solves these problems. Overall, there are a number of security, scalability, and efficiency benefits to integrating blockchain technology with cloud computing and cutting-edge industries like healthcare and electric cars. The ongoing investigation and advancement of blockchain-based systems has the capacity to fundamentally alter the ways in which various industries handle, protect, and exchange data in a decentralized environment.

REFERENCES

[1] D. He et al., IEEE Transactions on Dependable and Secure Computing, vol. PP, no. 99, 2016, "A Provably-Secure Cross-Domain Handshake Scheme with Symptoms-Matching for Mobile Healthcare Social Network"

[2] A. Mu-Hsing Kuo, Journal of Medical Internet Research, vol. 13, no. 3, 2011, "Opportunities and Challenges of Cloud Computing to Improve Health Care Services". on 2016, V. Casola and colleagues published [17]"Healthcare-Related Data in the Cloud: Challenges and Opportunities" in IEEE Cloud Computing, vol. 3, no. 6, pp. 10–14. The article "Trustworthy Processing of Healthcare Big Data in Hybrid Clouds" was published in 2015 by S. Nepal et al.

[3]. in IEEE Cloud Computing, vol. 2, no. 2, pp. 78-84. [21] In 2017, G.S. Poh and colleagues published "Searchable Symmetric Encryption: Designs and Challenges" in ACM Computing Surveys, vol. 50, no.3.

[4]The article "Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing" was published in May 2018 by IEEE Network, vol. 32, no. 3, pp. 78–83, doi: 10.1109/mnet.2018.1700344.

[5] DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks, P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, IEEE Communications Magazine, vol. 55, no. 9, pp. 78–85, 2017, doi: 10.1109/mcom.2017.1700041.

[6] N. Z. Aitzhan and D. Svetinovic, The IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 5, pp. 840–852, Sep. 2018, doi: 10.1109/tdsc.2016.2616861, "Security and Privacy in Decentralized Energy Trading Through MultiSignatures, Blockchain and Anonymous Messaging Streams."

[7] "Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems," A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, IEEE Internet of Things Journal.

[8] "IEEE Wireless Communications published a paper titled "Engineering searchable encryption of mobile cloud networks: when QoE meets QoP," which was written by H. Li, D. Liu, Y. Dai, and T. H. Luan. The paper was published online 10.1109/mwc.2015.7224730.

[9] Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin.

[10] Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and the Application of the Next Internet Technology. Wiley.

[11] Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. 2015 IEEE Security and Privacy Workshops. DOI: 10.1109/SPW.2015.27

[12] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. IEEE Access, 4, 2292-2303. DOI: 10.1109/ACCESS.2016.2566339

[13] Kshetri, N. (2017). Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy. Telecommunications Policy, 41(10), 1027-1038. DOI: 10.1016/j.telpol.2017.09.003

[14] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf