JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Blockchain Security in Cloud Computing and data integrity protection mechanism

Annu Kumari Singh[1], Tushar Giri[2]
[1]M. Tech Scholar, Department of CSE, Institute of Technology& Management Lucknow UP India
[2]Assistant Professor, Department of CSE, GCRG. Group of Institutions, Lucknow, UP, India

Abstract: Due to its security, blockchain has been dubbed the "next-generation financial technology" for the information era. Through peer authentication, it offers security. among other things, virtual currency, data encryption, and hash value creation. The worldwide financial industry claims that the market for security is huge and that cloud computing, because of its accessibility and efficiency, is now widely used in all IT environments. The concept of blockchain technology, its advancements in research, and blockchain-enabled security in healthcare cloud and electronic vehicles are all covered in this article. cloud The virtual machine agent mechanism handles the dependable data storage, monitoring, and verification responsibilities. In order to construct a blockchain integrity protection mechanism, this is also a prerequisite. The foundation for integrity protection based on blockchain is constructed using the virtual machine proxy model, and the data is owned on time. The unique hash value corresponding to the file created by the Merkel hash tree is used to track changes in the data via the blockchain's smart contract. A blockchain-based cloud data integrity verification system is built using the "block-and-response" mechanism, and the user issues a warning message for data tampering.

Keywords: Blockchain; Cloud Data; Integrity Verification; Merkel hash tree Blockchain Security;

INTRODUCTION

A popular data format called blockchain is used to create and distribute transactions over a network of computers in the form of a distributed ledger. Nothing is centralized. that creates and verifies network-wide transactions, a characteristic shared by blockchain approaches. Information security systems have been compromised for several reasons. The systems save data, it is

difficult to track down these malicious activities, and if someone gains access to the data, they have the capacity to exploit that ability to make money. One advantage of interfering with information systems is that the attacker does not have to be physically present close to the data center in order to do so. Information systems can be attacked in a variety of ways. Malicious web robots are used to plan and carry out coordinated attacks on networked information systems, like denial-of-service attacks using a botnet. attack or the internet's sudden shutdown. Attacks on computer systems that occur most frequently include phishing, malware, online threats, spams, viruses, and malware that steals data. These attacks are also socially engineered, aimed at extremely valuable information, and they are executed by employing a well-known concept to trick the victim into thinking they are in a secure environment. The primary objective of the approach was gathering comprehensive data about the target. This threat presents a serious risk of data loss or data system interception. The problems caused by the threat to information systems were effectively resolved by the blockchain security technology. on this work, mobile agent technology is used to implement the distributed agent model on the cloud. Multi-tenants can collaborate with one another through the virtual machine agent to accomplish the responsibilities of dependable data storage, monitoring, and verification using the mechanism of the virtual machine agent. This is also a prerequisite for developing a blockchain integrity safeguard. The virtual machine proxy model constructs the blockchain-based integrity protection framework, and the smart contract on the blockchain uses the unique hash value corresponding to the file created by the Merkel

hash tree to monitor the change in data and ensure that it is owned on time. The user sends out a cautionary note about altering data;

Cloud Computing and Security Risks

Generally speaking, cloud computing may be described as a distributed architecture that aims to offer any kind of online computing service. If the service is rendered It is referred to as infrastructure as a service (IaaS) because it uses shared hardware. Another possibility is that the platform or habitat will be shared online under a concept called platform as a service (PaaS). Software as a service (SaaS) is another term for distributed software that is made available online. Features like service on demand—which lets customers or clients only pay for the quantity of service used—are how cloud computing sets itself apart.Even if using cloud computing services has proven successful, Because of this, it is essential for cloud providers to provide their customers confidence about the security and privacy of data stored on the cloud. surroundings [9]. To protect cloud-related data, platforms, software, and infrastructure, a variety of laws, practices, control mechanisms, and technological advancements are integrated into the cloud computing system and collectively referred to as cloud security. Each security measure is linked to a prior data set in order to protect cloud data, update compliance often, and give privacy for executing the authentication rules that prohibit unauthorized access. Cloud security can be adapted to meet the unique needs of the company, from traffic filtering to access verification. Administrative costs are decreased, and IT professionals have more time to concentrate on other aspects of the company since Depending on the cloud provider or cloud security solutions being used, cloud security will be offered in a variety of ways. Regarding the On the other hand, the business owner and the solution provider should work together to establish cloud security measures [10]. Several study projects are in progress to enhance cloud security tactics and remedies. Block chain technology is one such enhanced security measure used by cloud-based systems [12]. It is designed so that no modifications can be made at random because the information is stored and verified in the blockchain. It has an orderly list for keeping information. Every block in the BC consists of two parts: a header and a body. The header contains the hash values for the last, present, and nonce. To find the block data in the database, utilize the index value. Security on blockchain is a generally a well-known, upscale, and quickly developing method for protecting important transactions, such as banking [13].

Using Blockchain Security in Healthcare Cloud

The healthcare sector is a big-data industry that regularly creates, shares, saves, and retrieves enormous amounts of data. Upon completing specific tests (e.g., Data is created (also known as computed tomography or computerized axial tomography scans), and it needs to be given to the radiographer and then the doctor. The results of the consultation will be kept on file at the hospital, and at a later time, a doctor from one of the network's other hospitals might require access to them. It is clear that technology can both potentially reduce costs by more effectively allocating resources and enhance the quality of patient care (e.g., by using data analytics to make informed medical decisions). personnel, apparatus, and more resources. For instance, data collected on paper is challenging to store, create, and enter into systems due to the high cost of data input errors. accessible as required. These issues could lead to incorrect medical decisions, the need for more testing due to missing data, or data being stored at a separate hospital in a different nation or state (at the expense of higher costs). and discomfort for the sufferers), to name a few. Because of the nature of the industry, healthcare data accuracy, confidentiality, and security are vital. This highlights the necessity of an information management system that is both dependable and secure [11]. Electronic medical records, or EMRs, are retained by the accountable healthcare provider and contain clinical and medical data pertaining to a single patient [14]. This facilitates the retrieval and assessment of medical records. Health Information Systems (HIS) in their early generationsare made with the ability to generate new instances of EMRs, store them, and search for and retrieve stored instances of interest in order to enhance EMR management [15]. HIS is comparatively simple, graphically represented solutions, such as web services or graphical user interfaces. They are frequently the front end of a distributed or centralized system, with a database acting as the back end. It became evident that many stand-alone EMR solutions needed to be made interoperable in order to allow for the sharing of healthcare data across different providers, even across national boundaries, as patient mobility (both within and outside of a country) became more common in today's culture [16]. For example, the demand for real-time healthcare data interchange between providers in medical tourism destinations like Singapore .. For instance, EHRs are designed to make it possible for a patient's medical history to follow them or to be shared with other medical professionals. In contrast with EMRs, EHRs have an elaborate data structure. The widespread use of smart technology (such as wearables and smartphones running iOS and Android) has recently caused a dramatic change in the healthcare industry [17]. Healthcare practitioners may provide or give users (such as patients) access to these devices in order to monitor and measure their well-being as well as to notify and facilitate medical treatment. Other devices with built-in sensors are available for more sophisticated medical tasks, including glucose self-testing gadgets or heart rate wristbands for workouts. Despite these difficulties and possibly complex legal considerations, having an HIS built on an ecosystem of solutions that can interchange data seamlessly HIS built on an ecosystem of products that can interchange data effortlessly between them and abstract away the need for a single health data storage system for every given All users, including patients, healthcare providers, and governments, will profit from patient data (e.g., physically spread among various actual software instances at multiple healthcare providers and mobile apps). Because cloud

computing can handle big data (e.g., hosting big data analytical tools) and provide resource flexibility when needed, it is a potential solution for facilitating real-time data sharing regardless of location and obtaining valuable insights from big healthcare data analysis for research and policy decision-making [18] [19]. Hackers may find personal and sensitive information in healthcare data to be enticing. Thus, safeguarding the EMR/EHR/PHR ecosystem's security as well as the auxiliary systems and components that make up the ecosystem are vital, yet because of their interdependence and complexity, they are challenging to manage [11]. Moreover, healthcare data security and authenticity need to be protected against unwanted access attempts from within the network or ecosystem in addition to malevolent people. Techniques include using cryptographic primitives based on public key infrastructure and public clouds are used to preserve data confidentiality and privacy [20]. For instance, before being transferred to the cloud, data is encrypted. Nevertheless, this limits the searchability of the data because medical professionals have to decode the (potentially vast) data. prior to doing a search on the decrypted data, which increased the time and expense of data retrieval and diagnosis (download, decrypt, and search, for example) [21]. An open and distributed online database made up of several linked data structures, commonly referred to as blocks, can be created using the blockchain technology. These blocks are not stored centrally; rather, they are distributed among numerous infrastructure nodes. Each block contains transaction data, the hash of the previous block, the creation date, and, in this example, the client's medical information and healthcare provider details. A new block is created and distributed whenever new medical information is generated for a particular patient (such as after a consultation or an operation). to every peer in the network of patients. Once the new block has been approved by the majority of peers, the system will add it to the chain. This allows us to quickly, accurately, and permanently get a thorough picture of the patient's medical history. If a consensus cannot be achieved, the chain splits, and the block is labeled as an orphan—it is not a part of the main chain.

Blockchain-Enabled Security in Electronic Vehicles Cloud

Cloud and edge computing for electric vehicles (EVCE) is a promising network paradigm that involves smooth connections in various vehicle scenarios to combine distributed electric automobiles (EVs) into a common resource pool and use them for locally adaptable use [1]. In order to facilitate cooperative data sensing, information analysis, and energy sharing, information and energy flow are dynamically shared in EVCE computing during vehicle-to-anything connections, such as vehicle-to-grid (V2G), vehicle-to-infrastructure (V2I), and vehicle-to-vehicle (V2V). Because of the intricacy of the scenario and the sensitivity of the data, vehicular applications confront significant security risks [7]. Future automotive applications are starting to use the coexistence of hybrid cloud and edge computing, which has the following three advantages: qualities. Without a central node, peer-to-peer communications include data sharing without previously established trust relationships. This is known as centerless trust. Interpersonal Intelligence, In order to solve problems related to crowd intelligence, an EV works in restricted conjunction [2]. Spatial-Temporal Sensitivity: The energy and information that an EV exchanges are sensitive data that clearly have spatiotemporal characteristics in order to meet the data provenance criterion [3]. The EVCE has serious security issues since attackers and legal entities are equal participants with equal privileges. The decentralization and consensus mechanisms inherent in blockchain technology have been suggested as potential remedies for these security issues. contribution to particular processing; the EVs that are coordinated will Cryptographic procedures are used to establish trust relationships between two or more parties. Mass collaboration is driven by collective self-interests, and data ambiguity is A small thing to think about. Every block keeps track of previous blocks and saves a receipt to link with them. A new block is only added to the ledger when the messages that go with it pass majority authentication [4]. In the event of a single point of failure, the robustness and protection against manipulation of this special data format are enhanced. Similar characteristics apply to the blockchain, where all users cooperatively validate new blocks for cooperative management. Participating teams execute it using Merkle hash tree techniques and timestamps. Proof of work and consensus are the two most used algorithms. (PoW) and stake proof (PoS). The PoW is totally dependent on processing power, and players fight to enter accurate data with the lowest possible chance of success. A PoS account is selected using a deterministic algorithm based on probability and total stakes [1]. Data coins and energy coins are new cryptocurrency for use in automobiles that are defined here. During information and energy exchanges, vehicle records are kept in a consortium blockchain, and distributed consensus processes based on blockchain technology are put into place. The car records will be divided into blocks and encrypted using pre-established distributed consensus techniques. consensus processes, wherein RSUs and LAGs verify the records by auditing them and appending them to a block chain in a sequential chronological sequence [4]. The mobile EVs act as network operators to create V2V connections. EVm connects with its neighbors EVm1, EVm2,..., EVmi (iN) for cooperative actions. These moving EVs should take data-coin-based anonymous data confirmation and access control into consideration for data swapping and sharing.The moving EVs employ peer-to-peer networks for key negotiation and distribution during the initialization phase; lightweight symmetric encryption could be used to generate temporary session keys. Multi-path key mode

and shortest path tree routing could be used to obtain group key agreement. Next, via access challenges and responses, the RSU and the moving EVs establish communication. In this scenario, the moving EVs cooperate to communicate data, mutual authentication can be used, and the signed data can be broadcast to surrounding EVs. be produced using secure multi-party computing and homomorphic encryption. The distribution of resources among moving EVs is directly impacted by the encrypted data coins. Moreover, spatial-temporal features may be utilized for data sharing and data concealment issues amongst EVs, and conditional proxy re-encryption may be utilized for access control.

Proposed method

Introduction to blockchain

Block chain (Block chain) is an open, decentralized database that is distributed. Its data blocks are frequently arranged according to the generation of connections from cryptographic algorithms. A novel distributed computing paradigm is blockchain. Its core concepts for designand benefits are spread without requiring confidence in nodes thanks to incentive systems, consensus procedures, time stamping strategies, encryption algorithms, and incentive systems. Peer-to-peer based point-to-point coordination, cooperation, and information transfer are implemented by network technology. A blockchain is made up of a series of chronological blocks that together provide a comprehensive record of all network transactions that are currently valid. Every piece of dataA blockchain block typically consists of a block body and a block header. The transaction counter and comprehensive transaction data are the primary contents of the block's block body. Information like the Merkle root hash, parent hash value, time stamp, and calculation are all contained in the block header. intricacy and arbitrary figure. The size and block size of each transaction determine how many transactions a block may hold at most.

Key characteristics of the blockchain

The following are the main characteristics of the blockchain generally: Decentralization comes first.Every transaction in the heart of traditional trading systems must be verified by a reliable central mechanism, which invariably results in the expense and server for the security center. On the other hand, the blockchain eliminates the necessity for the central mechanism.Secondly, perseverance. Once a transaction is added to the blockchain, it is nearly hard to remove, alter, or reverse it. Effective transaction data can be swiftly confirmed. Additionally, during the verification process, the block containing invalid transaction information will be promptly checked out and deleted. And lastly, privacy. To conceal their actual identity, each user communicates with the blockchain using the generated user address. system, as well as the blockchain network's usersThe fourth is auditability. Bitcoin stores user balance data using the (UTO) paradigm. Every transaction needs to make reference to a few of the previously unsold ones. The status of the quoted transaction is updated once the transaction is registered in the blockchain. Consequently,thetransaction Records are easily trackable and verifiable.

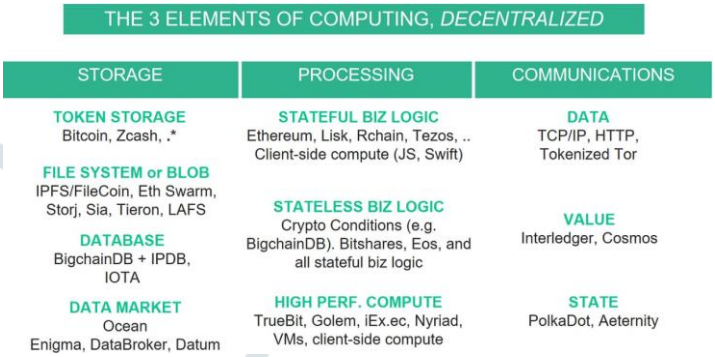

Figure 1 blockchain infrastructure

In cloud computing, data storage is not only the focus, but also the foundation. Data security is also the top priority of cloud computing security protection. Therefore, data information is an important part of the assets of enterprises and individual users. Whether data information stored in the cloud is safe is the most concerned issue for users. A general cloud storage service security model is shown in Figure 2

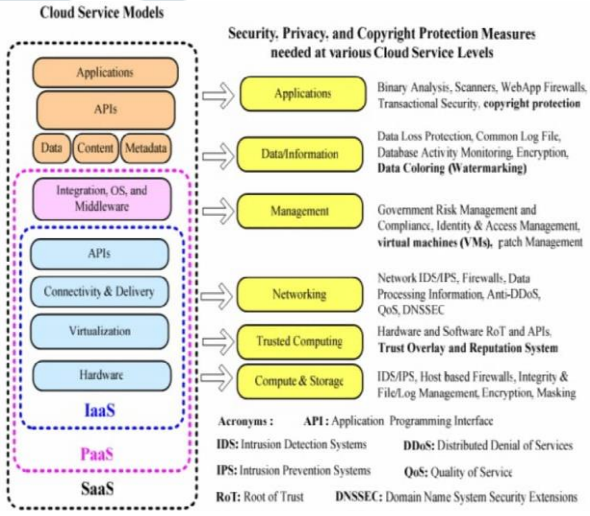

Figure 2 Cloud Storage Service Security Model

(2) **Ciphertext access control technology**

Data confidentiality refers to the idea that no other user may explicitly access or receive data; only data owners and authorized users are able to do so. Encryption is the most widely used method of safeguarding data secrecy.Users usually encrypt data prior to transferring their information to the cloud. One of the key tactics for guaranteeing the lawfulness of information use, network security, and system resource preservation is access control. The topic implements access to its resources in accordance with various policies under various access control models. The user's access to the data becomes a ciphertext access control issue because it is kept in the cloud in a ciphertext state. The technology used for ciphertext access control manages the user's access by encrypting important data and managing access privileges. It is a crucial tool for protecting user data in an untrusted cloud environment. It not only significantly increases user data privacy and confidentiality, but also lower the possibility that user data will be disclosed unlawfully. When attribute-based encryption technology (ABE) and access control technology are coupled, the result is attribute-based ciphertext access control (ABAC), which restricts access to data to users who meet the attribute's decision rules. ABAC is more suited for cloud storage setups with multiple tenants and frequent permission changes due to its greater flexibility and tighter access control granularity. The user can only decrypt in the KP-ABE and CP-ABE schemes when the attribute set fulfills the access tree.

integrity verification technology

Data integrity, including the integrity of usage and storage, is a crucial criterion for determining whether the data is authentic and trustworthy. In cloud storage environments, data integrity typically refers to cloud storage service providers storing all customer data on cloud servers in accordance with their needs. namely, integrity of storage. Provable storage, another name for cloud storage, uses integrity verification to verify data so that users can obtain a tiny quantity of data with a specificknowledge protocol or to assess the quality of the data kept in the cloud. finished. In the conventional sense, access and challenge-response-based methods are the two primary means of confirming the accuracy of data in a storage system. The latter, however,ismore appropriate for use in cloud storage environments that are distributed. Verifiers and responders are components of the challenge-response-based integrity verification model. Typically, the responder is the cloud server and the certifier is the data owner or a reliable third party. The way it works is that the cloud server receives a challenge information from the verifier, which it then uses to generate and return appropriate answer information based on the information it receives. In the end, the verifier makes decisions and verifies integrity using the response data that was received. Provable data holding (PDP) and recoverable proof (POR) technologies are the two primary technologies utilized.

CONCLUSIONS

This essay defines cloud computing, blockchain technology, and blockchain security. This article also provides an overview of the applications of blockchain security in business and industry. Although blockchain security is theoretically secure by design, there are still certain issues that can be resolved or managed with the development of new methods.

REFERENCES

[1] 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.

[2] 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.

[3] 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 Multi-Signatures, Blockchain and Anonymous Messaging Streams."

[4] "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.

[5] "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.

[6]"Vehicles as Connected Resources: Opportunities and Challenges for the Future," IEEE Vehicular Technology Magazine, vol. 12, S. K. Datta, J. Haerri, C. Bonnet, and R. Ferreira Da Costa

[7] "Vehicles as Connected Resources: Opportunities and Challenges for the Future, S. K. Datta, J. Haerri, C. Bonnet, and R. Ferreira Da Costa, IEEE Vehicular

Technology Magazine, vol. 12, no. 2, pp. 26–35, June 2017, doi: 10.1109/mvt.2017.2670859.

[8] J. Park and J. Park, "Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions," doi: 10.3390/sym9080164, Symmetry, vol. 9, no. 8, p. 164, Aug. 2017.

[9] " Blockchain: A panacea for Healthcare Cloud-Based Data Security and Privacy? C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, IEEE Cloud Computing, vol. 5, no. 1, pp.

[10] "Implementing Blockchain Technology: Way to Avoid Evasive Threats to Information Security on Cloud," S. Tabrez Siddiqui, M. Shuaib, A. Kumar Gupta, and S. Alam, 2020 International Conference on Computing and Information Technology (ICCIT-1441), 2020, pp. 1–5, doi: 10.1109/ICCIT-144147971.2020.9213798.

[11] In IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 2009–2030, third quarter 2020, K. Gai, J. Guo, L. Zhu, and S. Yu, "Blockchain Meets Cloud Computing: A Survey," doi: 10.1109/COMST.2020.2989392

[12] M. Steward, Journal of Legal Medicine, vol. 26, no. 4, pp. 491–506, 2005

[13]. "Electronic Medical Records." In 2006, R. Hauxe published "Health Information Systems—Past Present Future" in the International Journal of Medical Informatics, vol. 75, no. 3-5, pp. 268–281.

[14] K. Häyrinena and colleagues, "A Review of the Definition Structure Content Use and Effects of Electronic Health Records

[15] 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"

[16] 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

[18]. 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.

[19] Blockchain Technique in the Energy Internet: Preliminary Research Framework and Typical Applications[J], Zhang N, Wang Y, Kang C, et al. Csee Proceedings, 2016 33(01):11–12.

[20] Understanding Modern Banking Ledgers with Blockchain Technologies: The Internet of Money's Future of Transaction Processing and Smart Contracts[J] by Peters G. W. and Panayi E. 71(01):1113, Social Science Electronic Publishing, 2016.

[11] Martin J C D, Vetrò A, Conoscenti M. Blockchain Technology for the Internet of Things: An Organized review of literature[C]// Computer Systems & Applications. 2017-07-07.