Blockchain Security in Cloud Computing

Rithika Lal
Department of Science and Technology
Bournemouth University
Bournemouth, England, UK

***Abstract* - Blockchain has been labelled the "next-generation financial technology" for the information age because of its security. It provides security by authenticating peers who share virtual money, encrypting data, and creating hash value, among other things. According to the global financial industry, the market for security- Cloud computing has become widely employed in all IT environments due to its efficiency and availability. This article discusses the idea of blockchain technology, its research developments and blockchain- enabled security in healthcare cloud and electronic vehicles cloud.**

***Index Terms* – Blockchain Security; Cloud Computing; Healthcare Cloud; Electronic Vehicles Cloud**

I. INTRODUCTION

Blockchain is a common data structure used for making and distributing transactions in the form of a distributed ledger across a network of computers. There is no centralized entity that generates and validates transactions throughout the network, which is a common feature of blockchain approach. There are a number of reasons why information security systems have been breached. The systems save data, the traceability of these malevolent acts is tough, and if someone gets access to the data, he or she has power and may therefore use that power to create money. Interfering with information systems does not necessitate the attacker's physical presence near the data centre, which is a benefit. There are several sorts of attacks against information systems. Web robots are used maliciously to organise and automate attacks on networked information systems, such as a botnet's denial-of-service assault or the internet bolt. Phishing, malware, online threats, spams, viruses, and data-stealing malware are among the most common assaults on computer systems. They're also socially engineered assaults that target highly valuable information, and they're carried out by duping the victim into believing he or she is in a safe place by using a familiar notion. The process's major goal was to collect detailed information on the target. This danger offers a significant risk of data loss or inference in data systems. The blockchain security technology proved quite effective in resolving issues brought on by the danger to information systems.

A. Cloud Computing and Security Risks

In general, **cloud computing** may be defined as a distributed architecture aiming at providing any form of computing service via the internet. If the service is provided via shared hardware, it is called as infrastructure as a service (IaaS). It is also possible that the habitat or platform will be shared through the internet, which is known as platform as a service (PaaS). There is also dispersed software that is distributed through the internet, which is known as software as a service (SaaS). Cloud computing distinguishes itself through characteristics like the service on demand, which means that consumers or clients only pays for the amount of service utilised.

Despite the success of employing cloud computing services, there remains a rising security and privacy concern. Several global corporations continue to focus on the security rules and processes implemented in the cloud system before adopting them for their enterprise solutions. As a result, it is critical for cloud vendors to instil trust in their clients regarding the security and privacy of data floating in the cloud environment [9]. Cloud security encompasses a wide range of rules, techniques, control mechanisms, and technologies that are incorporated into the cloud computing system to safeguard cloud-related data, platforms, software, and infrastructure. To safeguard cloud data, update frequent compliance, and provide privacy for implementing the authentication rules that prevent unlawful access, each security measure is connected with a previous data set. From access verification to traffic filtering, cloud security may be tailored to fit the specific demands of the organisation. Administrative expenses are reduced, and IT teams are free to focus on other elements of the business since these rules can be set and handled in a single location. Cloud security will be provided in a variety of ways, depending on the cloud provider or cloud security solutions in use. On the other hand, the implementation of cloud security measures should be a collaborative effort between the business owner and the solution provider [10]. A number of research initiatives are underway to improve cloud security strategies and solutions. One such increased security solution employed across cloud-based systems is the block chain technology [12]. It features a well-organized list for storing information, and it's built in such a manner that no changes can be done at randomly since the information is kept and validated in the blockchain. There are two pieces to each block in the BC: a header and a body. The hash value of last, present, and nonce is stored in the header. The index value is used to search the database for the block data. Blockchain security is a widely known, high-end, and rapidly evolving solution for securing critical transactions like banking [13].

B. Using Blockchain Security in Healthcare Cloud

Healthcare is a big-data industry that generates, disseminates, stores, and accesses a vast quantity of data on a regular basis. When a patient performs certain tests (e.g., computed tomography or computerised axial tomography scans), data is generated, and it must be distributed to the radiographer and subsequently to the physician. The findings of the consultation will be retained at the hospital, and a physician from another hospital in the network may need to access them at a later date. It is obvious that technology has the ability to improve patient care quality (e.g., by employing data analytics to make educated medical decisions) while also possibly lowering costs by more efficiently allocating employees, equipment, and other resources. For example, data gathered on paper is difficult to enter into systems (because to the high cost of data input mistakes), archive, and make available when needed. These difficulties may result in

erroneous medical choices, the necessity for repeat tests owing to missing data, or data being kept at a different hospital in another country or state (at the price of increased expenditures and inconvenience for patients), among other things. The confidentiality, security, and accuracy of healthcare data are critical because of the nature of the sector. This emphasises the need of a reliable and secure information management system [11].

EMRs (Electronic Medical Records) are files that include medical and clinical information on a specific patient and are kept by the accountable healthcare provider [14]. The recovery and evaluation of healthcare data is made easier as a result of this. Early generations of Health Information Systems (HIS) are created with the potential to create new EMR instances, store them, and search and obtain stored EMRs of interest to better enable EMR administration [15]. HIS can be relatively basic solutions, like as a graphical interface or a web service, which can be expressed graphically. In a centralised or distributed solution, they are often the front-end with a database at the back-end. With patient mobility (both within and outside of a country) becoming more common in today's culture, it became clear that numerous stand-alone EMR solutions needed to be made interoperable to allow for the sharing of healthcare data across different providers, even across national boundaries [16]. For instance, in medical tourism hotspots like Singapore, the demand for real-time healthcare data exchange across providers and between countries is growing. EMRs must codify their data structure and HIS architecture to enable data exchange and even patient data portability. EHRs, for example, are intended to allow a patient's medical history to follow them or to be shared with other healthcare practitioners. Compared to EMRs, EHRs have a more detailed data structure. Smart technologies' pervasiveness (e.g., Android and iOS smartphones, as well as wearable devices) has recently resulted in a radical shift in the healthcare business [17]. Users (e.g., patients) can possess or have such devices placed by healthcare providers to measure their well-being and notify/facilitate medical treatment and monitoring. There are other gadgets with incorporated sensors for more complex medical duties, such as heart rate wristbands for exercises or glucose self-testing devices. Even with such challenges and potentially vexing legal issues, having an HIS based on an ecosystem of solutions capable of seamlessly exchanging data among themselves and providing the abstraction of a single health data storage for any given patient (e.g., physically distributed across numerous tangible software instances at multiple healthcare providers and mobile apps) will benefit all users, from patients to healthcare providers to governments. Cloud computing is a potential solution because of its capacity to facilitate real-time data sharing regardless of location, to provide resource flexibility as needed, and to handle big data (e.g., hosting big data analytical tools) to obtain valuable insights from big healthcare data analysis for research and policy decision making [18] [19].

Healthcare data contains personal and sensitive information that may be appealing to hackers. As a result, protecting the security of the EMR/EHR/PHR ecosystem and the supporting systems and components that comprise the ecosystem is critical, but difficult owing to the interaction and complexity of the systems and components [11]. Furthermore, the confidentiality and authenticity of healthcare data must be secured not just from malicious users, but also against unwanted access attempts from within the network or ecosystem. To maintain data confidentiality and privacy, approaches include employing cryptographic primitives such as those based on public key infrastructure and public clouds [20]. Data, for example, is encrypted before being sent to the cloud. However, this restricts the data's searchability in that healthcare practitioners must decrypt the (possibly large) data before searching on the decrypted data, resulting in increased time and costs for data retrieval and diagnosis (e.g., download, decrypt, and search) [21]. Blockchain is a technology that allows for the creation of an open and distributed online database comprised of a series of data structures (also known as blocks) that are connected to one another. These blocks are dispersed across many infrastructure nodes and are not centrally kept. Each block includes a timestamp of its creation, the hash of the preceding block, transaction data, and, in this case, a client's medical data and healthcare provider information. When new healthcare data for a specific patient is generated (for example, from a consultation or a medical intervention such as surgery), a new block is formed and sent to all peers in the patient network. The system will place the new block into the chain after it has been authorised by a majority of the peers. This enables us to obtain a comprehensive perspective of the patient's medical history in an efficient, reliable, and lasting manner. If an agreement cannot be reached, a fork in the chain is formed, and the block is designated as an orphan, meaning it does not belong to the main chain.

C. Blockchain-Enabled Security in Electronic Vehicles Cloud

Electric vehicles cloud and edge (EVCE) computing is an appealing network model that entails seamless connections in diverse vehicular contexts to aggregate distributed electric vehicles (EVs) into a shared resource pool and invoke the EVs for locally flexible utilisation [1]. 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), to enable collaborative data sensing, information analysis, and energy sharing. Vehicular applications face substantial security concerns due to the sensitivity of data and the complexity of the situation [7]. The coexistence of hybrid cloud computing and edge computing is becoming the trend of future vehicular applications, which have the following three characteristics. Centreless trust, there is no center node in peer-to-peer communications, in which data exchange is performed without pre-assigned trust relationships. Collaborative Intelligence**,** An EV makes a limited contribution to specific processing; the coordinated EVs will

jointly address problem solving for crowd intelligence [2]. Spatio-Temporal Sensitivity**,** An EV's exchanged information and energy are sensitive data with obvious spatio-temporal attributes for the data provenance requirement [3]. As legal entities and attackers are equal players with equal privilege, the EVCE faces major security concerns. Using the features of decentralization and consensus algorithms, blockchain technology has been proposed as a possible solution to these security challenges. To build mutual or multi-party trust relationships, cryptographic techniques are used. Collective self-interests drive mass collaboration, and data uncertainty is a minor consideration. Any block records and maintains a receipt to a link with the preceding block, and a new block is only added to the ledger if the accompanying messages pass majority authentication [4]. This unique data format improves robustness and protects against manipulation in the event of a single point of failure.

The blockchain, in which all participants collaboratively validate new blocks for collaborative management, has comparable qualities (e.g., centerless trust and collaborative intelligence) as EVCE computing. Before transaction records are put into a digital ledger, Blockchain generates distributed consensus [3]. Based on timestamps and Merkle hash tree methods, it is carried out by collaborative participants. The two most common consensus algorithms are proof of work (PoW) and proof of stake (PoS). The PoW is entirely reliant on processing power, and participants compete to write correct data with a minimal probability of success. A PoS account is chosen based on its total stakes and is based on a deterministic method and probability [1]. As new cryptocurrency for vehicular applications, data coins and energy coins are defined here. Vehicle records are maintained in a consortium blockchain during information and energy transactions, and distributed consensus procedures based on blockchain technology are implemented. The vehicle records will be encrypted and organised into blocks using pre-defined distributed consensus procedures, with RSUs and LAGs auditing the records and adding them to a block-chain in a linear chronological order for verification [4].

To establish V2V connections, the moving EVs serve as network operators. For collaborative actions, EVm communicates with its neighbours EVm1, EVm2,..., EVmi (iN). For data swapping and sharing, these moving EVs should consider data-coin-based anonymous data confirmation and access control.During the initialization process, the moving EVs use peer-to-peer networks to perform key negotiation and distribution; temporary session keys could be created using lightweight symmetric encryption. Group key agreement could be achieved using shortest path tree routing and multi-path key mode. Following then, through access challenges and answers, the moving EVs and the RSU create contacts. Here, the moving EVs work together to exchange data, the signed data can be broadcast to nearby EVs, and mutual authentication can be created via homomorphic encryption and safe multi-party computing. The encrypted data coins have a direct impact on resource allocation among moving EVs. Furthermore, spatial-temporal features might be employed for access control, and conditional proxy re-encryption could be used to handle data sharing and data concealing difficulties between EVs.

II. Conclusions

This paper explains what blockchain technology, blockchain security and cloud computing is. This paper also gives an insight on how blockchain security is used in industry and businesses. Conceptually blockchain security is secure by design but still have some challenges which can be mitigated or controlled by evolving techniques.

Acknowledgment

The author would like to extend sincere gratitude and appreciation to the faculty of science and technology at Bournemouth University for guidance and assistance.

References

[1] H. Liu, Y. Zhang, and T. Yang, "Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing," *IEEE Network*, vol. 32, no. 3, pp. 78–83, May 2018, doi: 10.1109/mnet.2018.1700344.

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

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

[4] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017, doi: 10.1109/jiot.2017.2740569.

[5] N. Kshetri, "Can Blockchain Strengthen the Internet of Things?," *IT Professional*, vol. 19, no. 4, pp. 68–72, 2017, doi: 10.1109/mitp.2017.3051335.

[6] H. Li, D. Liu, Y. Dai, and T. H. Luan, "Engineering searchable encryption of mobile cloud networks: when QoE meets QoP," *IEEE Wireless Communications*, vol. 22, no. 4, pp. 74–80, Aug. 2015, doi: 10.1109/mwc.2015.7224730.

[7] S. K. Datta, J. Haerri, C. Bonnet, and R. Ferreira Da Costa, "Vehicles as Connected Resources: Opportunities and Challenges for the Future," *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 26–35, Jun. 2017, doi: 10.1109/mvt.2017.2670859.

[8] S. Nakamoto, "Bitcoin: a Peer-to-Peer Electronic Cash System," Oct. 2008. Accessed: Jan. 10, 2022. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

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

[10] M. Mayuranathan, M. Murugan, and V. Dhanakoti, “Enhanced security in cloud applications using emerging blockchain security algorithm,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. s12652-02002339-7, Jul. 2020, doi: 10.1007/s12652-020-02339-7.

[11] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, “Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?,” *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31–37, Jan. 2018, doi: 10.1109/mcc.2018.011791712.

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

[13] K. Gai, J. Guo, L. Zhu and S. Yu, "Blockchain Meets Cloud Computing: A Survey," in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 2009-2030, thirdquarter 2020, doi: 10.1109/COMST.2020.2989392.

[14] M. Steward, "Electronic Medical Records", *Journal of Legal Medicine*, vol. 26, no. 4, pp. 491-506, 2005.

[15] R. Hauxe, "Health Information Systems—Past Present Future", *Int'l Journal of Medical Informatics*, vol. 75, no. 3–4, pp. 268-281, 2006.

[16] K. Häyrinena et al., "Definition Structure Content Use and Impacts of Electronic Health Records: A Review of the Research Literature", *Int'l Journal of Medical Informatics*, vol. 77, no. 5, pp. 291-304, 2008.

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

[18] A. Mu-Hsing Kuo, "Opportunities and Challenges of Cloud Computing to Improve Health Care Services", *Journal of Medical Internet Research*, vol. 13, no. 3, 2011.

[19] V. Casola et al., "Healthcare-Related Data in the Cloud: Challenges and Opportunities", *IEEE Cloud Computing*, vol. 3, no. 6, pp. 10-14, 2016

[20] S. Nepal et al., "Trustworthy Processing of Healthcare Big Data in Hybrid Clouds", *IEEE Cloud Computing*, vol. 2, no. 2, pp. 78-84, 2015.

[21] G.S. Poh et al., "Searchable Symmetric Encryption: Designs and Challenges", *ACM Computing Surveys*, vol. 50, no. 3, 2017.