Transforming Cloud Security Paradigms via Blockchain Implementation

Sridhar Kontham[1] **and Dr. Pawan Kumar**[2]
Research Scholar, Department of Computer Science & Engineering[1]
Research Guide, Department of Computer Science & Engineering[2]
NIILM University, Kaithal, India

Abstract*: Cloud computing has been widely used in many facets of the IT industry as a means of meeting infrastructure and data service needs at a cheap cost, with little effort, and with a high degree of scalability. Although there has been a noticeable increase in the use of cloud computing, information security issues have not yet been completely addressed. To some degree, information security issues continue to impede the development of cloud computing and must be addressed. In addition, blockchain has become a major player in the security space, particularly with regard to confidentiality, integrity, and authenticity. This article examines the several security facets of blockchain technology and cloud computing, as well as the use of blockchain in cloud computing security.*

Keywords: Cloud Computing, Blockchain, Security, Information security

I. INTRODUCTION

Cloud service providers are contacted by cloud users to seek services. CSPs are independent companies that provide their customers cloud storage services. Attribute Authority and Third-Party Auditor are two more third-party service providers that are meant to provide cloud security features. As it is known to us that security and trust are the most significant and vital problems when helping the companies and institutions with cloud. There are several causes, some of which are cloud customers' data is very vulnerable to loss, leakage, or assault, and they lack any way to escape this untenable circumstance. Users of cloud computing sometimes have no idea who they are exchanging data with or communicating with. Another major issue is transparency; cloud customers are unaware of who is accessing their data or how it is being used inside the cloud.

Blockchain is a new and developing technology that cloud users may utilize to increase data security and trust while outsourcing and purchasing services from the cloud. Compared to centralized database security, blockchain may provide enhanced security. Blockchain keeps track of all the data that are related to the preceding block and safeguarded by a cryptographic hash function on an ongoing basis. A distributed ledger that can record transactions and thwart manipulation is called a blockchain. Blockchain is usually controlled by a peer-to-peer network and is intended to prevent manipulation by outside parties. Blockchain technology may provide security comparable to that of central database data storage. Attacks and harm to data storage may be avoided from a management perspective.

Furthermore, when used to an area where data disclosure is required, the Blockchain's openness feature may enable transparency in the data. Owing to these advantages, it may be used in a variety of contexts, such as the financial industry and the Internet of Things environment, and its uses are anticipated to grow and Because cloud computing is efficient and readily available, it has been used in several IT systems. Furthermore, key security considerations have been used to explore cloud security and privacy problems.

Structure of Blockchain

In a blockchain, a block typically has the primary data, which includes a timestamp, current and historical hashes, and other information.

- **Main data** Typically, it depends on the services the block offers, such as financial transaction information, contact records, clearing records, or Internet of Things data records.

ISSN 2581-9429 IJARSCT

- **Hash:** The transaction is broadcast to other nodes when it has been completed and hashed to code. Because each node block in a blockchain has hundreds of transaction records in addition to the final hash of the block header, the Merkle tree function is used to decrease data transmission and computation resources.
- **Timestamp:** Block generation time.
- **Other Information:** Block signatures, user-defined data, and nonce values fall mostly within the category of other information.

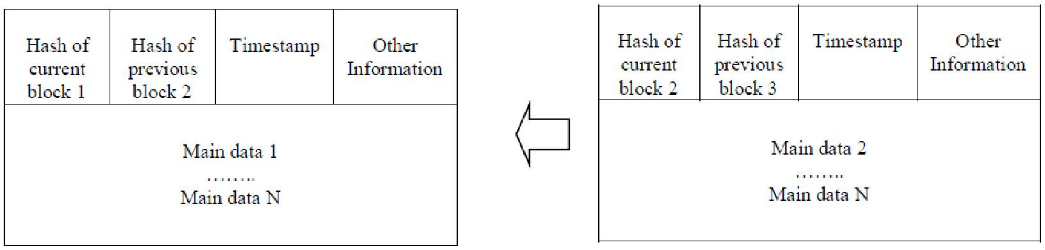

Figure 1: Blockchain structure

A blockchain block is made up of a block header and a block body, as shown in table 1. Block version, Parent block hash, Merkle tree root hash, timestamp, n Bits, and Nonce value make up the block header. A block is made up of a header that contains the list of valid transactions, the key hash of the previous block together with its own, and information about the block contents. A block comprises 500 transactions, and the phrase "Block Height" refers to the height of each block. The block header is 80 bytes, although the average size of a single transaction is 250 bytes.

Table 1.

Type	**Size (in bytes)**	**Description**
Block Size	4	Size of the block
Counter	1-9	No of transactions
Block Header	80	Block header information

Characteristics of Blockchain

Requirements are all the qualities and attributes that a Blockchain system ought to have as well as the constraints that must be met for the system to function properly. As a result, they affect the Blockchain system's entire operation and may have a greater impact on its architecture. The following are a few of the blockchain network's non-functional features.

- **Openness:** Because the nodes in a blockchain are compatible, the information may be used and exchanged during a transaction.
- **Concurrency:** Blockchain performance becomes better as more nodes process at once.
- **Scalability**: Blockchain is scalable by new Node additions and deletions.

In terms of scalability, the following three parameters are mostly of interest:

- Distribution of Transaction Processing Rate:
- Dimensions:
- Latency or Handling:

Fault tolerance: The Blockchain network's fault-tolerant feature, which allows any problem at any node to be visible to all other nodes in the network, ensures that the network continues to function even in the event of a fault.

Transparency: Every network node may see the transactions recorded on the Blockchain.

Security: Strong cryptographic techniques, such SHA-255, are employed in the Blockchain network to safeguard data.

Quality of Service: Response time and dependability, the time is taken by the transaction to completion and the promise to offer the needed services, defines the quality of service in the Blockchain network.

Failure Management: A procedure that can both strengthen the Blockchain network and identify the root cause of failure has to exist. It could provide advice on how to bounce back from a setback automatically.

Requirement of Cloud

Some of the essential Requirements of Cloud that might affect different design patterns of the Cloud.

Scalability: Millions of users or nodes that utilize cloud services are managed by Cloud Network. Nodes in the hardware design may scale in and out, and its size is variable.

Elasticity: A proficient blockchain system may adjust workload by systematically assigning and de-allocating resources to ensure that, at all times, all available resources maximally satisfy current needs.

Privacy: Every user should be able to effectively manage their data, and the system should safeguard it as well.

Infinite Computing Resources: It is not necessary for consumers to prepare ahead for the cloud provisioning services.

Pricing: The cost of various cloud applications and services varies, and payment is based on how the resources are used.

Utilization: The resources may be efficiently adjusted to fine-tune the fluctuating load by permitting the best feasible utilizations.

Cost Efficiency: Because the customer does not need to buy software licenses that are appropriate for the hardware, cloud services are easy and need-based throughout the internet. The entire cost of operating and maintaining software will go down as a result.

Performance: Evaluations are often measured in terms of how well the services and apps operating on the cloud system perform.

Flexibility: Flexibility includes the capacity to share data or services over the internet. Users have increased freedom thanks to the cloud.

Challenges for Blockchain Security

As far as we are aware, blockchain technology is directly tied to virtual, computer-generated money that is used by everyone. However, there are still a number of documented Blockchain security issues. These include as follows:

- The blockchain agreement,
- wallet security,
- ransactions security,
- software security,
- blockchain agreement

A blockchain is made up of the sequential connections between the basic blocks that are formed. If two separate peers produce different results while mining at the same moment, a blockchain may split into two. This is because the last two blocks are briefly generated and may be utilized by two different users. If the peers in the Bitcoin network do not choose the block as the most recent block, it will lose significance and mining will cease to be worthwhile. The network will follow peers in Bitcoin that have more than 50% mining potential.

Transaction Security

A versatile programming language may be used to construct a variety of transaction formats, and well-written scripts for inputs and outputs can be used to solve security concerns. Financial services, validation, and verification are provided via Bitcoin contracts. The most popular way to draft a contract is using a script that uses the multisig multiple-signature mechanism.

Wallet Security

Encrypted with a combination of personal and public keys the Bitcoin address uses the hash value of a public key. So, the Bitcoin transaction locking script address cannot be unlocked without an unlocking script that contains the value generated from the combination of a public key and the personal key. Information such as the personal key of the address, which is used for the generation of the unlocking script is stored inside the Bitcoin wallet. That means if we lose information inside the wallet leads to a loss of Bitcoin, as we know to use Bitcoin the information is required and important. Consequently, the Bitcoin wallet turns out to be the prime focus of Bitcoin attack via hacking.

Software Security

The software utilized in Bitcoin is a significant concern due to the potentially critical nature of software bugs. While the official developer documentation of Bitcoin purports to provide comprehensive explanations of all Bitcoin-related processes, the core software remains highly proficient and effective. This is due to the fact that the software developed by Satoshi Nakamoto directed and executed the intricate processes of the initial Bitcoin software.

Secure Blockchain Solution for Cloud

Disclosure of confidential user information within a cloud computing system could potentially lead to both financial and psychological consequences. The examination of data integrity and privacy throughout transmission and storage in a cloud computing environment is our principal objective. When blockchain is integrated into a cloud computing environment and its service level has been upgraded appropriately, it can ensure security. On the Blockchain, a secure electronic wallet is implemented. Improperly deactivating the electronic wallet could potentially lead to the unauthorized access and use of user data. The remaining information of the user may be used to extract the aforementioned data.

A substantial barrier is posed by the prevalence of double transactions on the Blockchain and the possibility of the Bitcoin ledger being forged. It is essential to utilize a trustworthy and secure electronic wallet in order to mitigate these security concerns. E-wallets are predominantly employed on personal computers; nevertheless, the prevalence of mobile devices necessitates the implementation of more rigorous security protocols for e-wallets on mobile devices. A transaction is deemed finalized when its security is guaranteed by employing a time stamp produced by a mobile device, which authenticates its precision and soundness. To develop a secure electronic wallet, it is essential to reduce, validate, and verify issues that may arise during each phase of planning, requirements analysis, implementation and testing, and maintenance.

It is critical to guarantee a reliable and secure restoration of the electronic wallet in the event that its security is compromised or compromised via malware. It is accountable for ensuring the security of the user's transaction data, which is stored in the electronic wallet, in addition to the configurations required for the wallet's administration and operation. The e-wallet should incorporate a feature that enables the secure and efficient removal of any remaining user data when it is not in use. Any such data should then be disposed of.

Blockchain use Cases of Cloud

Open Ledger

Blockchain-enabled cloud storage is accessible and transparent to all users, allowing them to observe all types of cloud services, including service level agreements. Each user is able to observe the security level that the cloud provides and offers. Due to the Cloud's transparent nature and open specifications, users are able to conveniently select the services they need without the need to prepay.

Distributed Ledger

All copies of the ledger are identically synchronized, allowing all cloud users to access the same version/copy. The ledger documents the services utilized by each individual cloud user, as well as policies and SLAs pertaining to service utilization in general. By employing the theory of Bitcoin miners, Cloud users standardize their ledgers, according to the author in.

Decentralized Smart Contract

A smart contract, which is defined as software that stores the terms and conditions of a contract, verifies those terms, and executes them, is utilized in Blockchain, per reference. The combination of blockchain and smart contract technologies increases the transparency and confidence of CSP, TPA, and AA parties. A copy of the Smart Contracts is maintained on the Blockchain, which is accessible to all cloud users. Upon confirmation of payment, the service is contracted out. For future access, the Blockchain records all contract transactions in chronological order, accompanied by a comprehensive audit trail of events. Any attempt to modify a contract on the Blockchain is detectable and preventable by all other cloud users.

II. CONCLUSION

The overall architecture of Blockchain has been examined in this article. Furthermore, an analysis has been conducted on the security requirements of Blockchain technology and cloud computing. On the basis of this analysis, it has been determined that Blockchain may serve as a viable and potent security instrument for cloud computing environments. Additionally, a review of the various extant blockchain implementations for cloud security was provided in this paper.

REFERENCES

[1]. Alam, S. Siddiqui, S. T. Masoodi, F. and Shuaib M. 2018. Threats to Information Security on Cloud: Implementing Blockchain, 3rd international conference on SMART computing and Informatics (SCI), 21-22 December 2018, Kalinga Institute of Industrial Technology, Odisha. Springer. SPRINGER-SIST series.

[2]. Antonopoulos, Andreas M. 2014. Mastering bitcoin: unlocking digital cryptocurrencies. O'Reilly Media, Inc.

[3]. Bamert, T. Decker, C. Wattenhofer, R. and Welten S. 2014. BlueWallet: The Secure BitcoinWallet. In Security and Trust Management; Mauw, S., Jensen, C., Eds.; Springer International Publishing: Cham, Switzerland, 65–80.

[4]. Beikverdi, A. and JooSeok. S. 2015. Trend of centralization in Bitcoin's distributed network. In Proceedings of the 2015 16th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), Takamatsu, Japan.

[5]. Bonneau, J. Miller, A. Clark, J. Narayanan, A. Kroll, J.A. and Felten E.W. Sok. 2015. Research perspectives and challenges for bitcoin and cryptocurrencies. In Proceedings of the 2015 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA.

[6]. Christidis, K. and Michael, D. 2016. Blockchains and Smart Contracts for the Internet of Things. IEEE Access 2016, 4: 2292–2303.

[7]. Haber, S. and Stornetta, W.S.1990. How to time-stamp a digital document. In Proceedings of the Conference on the Theory and Application of Cryptography, Sydney, NSW, Australia. https://en.wikipedia.org/wiki/Blockchain.

[8]. Huang, H. Chen, X. Wu, Q. Huang, X. and Shen. J. 2016. Bitcoin-based fair payments for outsourcing computations of fogdevices. Future Gener. Comput. Syst.

[9]. Huh, S. Sangrae, C. and Soohyung. K. 2017. Managing IoT devices using blockchain platform. In Proceedings of the 2017 19th International Conference on Advanced Communication Technology (ICACT), Bongpyeong, Korea.

[10]. Hur, J. and Noh, D.K. 2011. Attribute-based access control with efficient revocation in data outsourcing systems. IEEE Trans.Parallel Distrib. Syst. (TPDS) 22(7): 1214–1221.

[11]. Kaskaloglu, K. 2014. Near zero Bitcoin transaction fees cannot last forever. In Proceedings of the International Conference on Digital Security and Forensics (DigitalSec2014), The Society of Digital Information and Wireless Communication, Ostrava, Czech Republic.

[12]. Li, J. Jia, C. Li, J. and Chen, X. 2012. Outsourcing encryption of attribute-based encryption with MapReduce. In: Chim, T.W.,Yuen, .H. (eds.) ICICS 2012. LNCS, vol. 7618: 191–201.

[13]. Omohundro. S. 2014. Cryptocurrencies, smart contracts, and artificial intelligence. AI Matters 1 (2): 19–21.

[14]. Shuaib, M. Samad, A. Alam S., and Siddiqui. S. T. 2019. Why Adopting Cloud Is Still a Challenge? A Review on Issues and Challenges for Cloud Migration. Ambient Communications and Computer Systems: Advances in Intelligent Systems and Computing, vol 904. Springer, Singapore: RACCCS-2018, 387.

[15]. Shuaib, M. Samad, A. and Siddiqui. S. T. 2017. Multi-layer security analysis of hybrid Cloud. In 6th international conferenceon system modeling & advancement in research trends, 526-531.

[16]. Singh, S. Jeong Y.-S. and Park. J.H. 2016. A survey on cloud computing security: Issues, threats, and solutions. J. Netw.Comput. Appl. 75: 200–222.

[17]. Vasek, M. and Moore. T. 2015. There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams. In Proceedings of the International Conference on Financial Cryptography and Data Security, San Juan, Puerto Rico, Springer: Berlin/Heidelberg, Gemany.

[18]. Verizon 2015: 2015 Data Breach Investigations Report (2015). http://www.verizonenterprise.com/DBIR/2015/. Accessed 20Sept 2017

[19]. Zhang, J. Nian, X. and Xin. H. 2014. A Secure System For Pervasive Social Network-based Healthcare. IEEE Access 2016, 4: 9239–9250.