International Journal of Scientific Research in Science and Technology
Available online at : www.ijsrst.com
OPEN ACCESS
Print ISSN: 2395-6011 | Online ISSN: 2395-602X
doi : https://doi.org/10.32628/IJSRST52411137

Secure Cloud Computing using Blockchain with Verkle Tree Hash algorithm

Imran Shahid Shaikh
Computer Engineering, AI ARKP, Maharashtra, India

ARTICLEINFO

Article History:

Accepted: 15 Jan 2024
Published: 30 Jan 2024

Publication Issue :
Volume 11, Issue 1
January-February-2024
Page Number :
345-351

ABSTRACT

Cloud computing permits you to avoid the need to install your own dedicated servers machines, run your own software, and manage your own databases. You can access data, applications, and computing hardware resources from anywhere in the world, rather than needing to be installed in office. As a result, the cloud offers faster innovation, flexible resources, and economies of scale. A rapid growth in Cloud Computing adaption observed but, still, the data security concerns in cloud are not addressed. In parallel Blockchain, technology is an emerging technology makes it impossible or difficult for the system to be changed, hacked, or manipulated. This paper enlightening the various aspects of security in Blockchain and Cloud Computing.

Keywords - Cloud Computing, Blockchain, Security, Information security, Hash values.

I. INTRODUCTION

Cloud users always worried about data, which can be lost, intercepted or attacked, but they do not have any remedy to come out of this subnormal situation. Cloud users do not even aware of to whom they are dealing with or sharing data. Transparency is also a very serious, cloud users do not have any information about the users of their data and how the data is roving inside the cloud.

In the new generation of information technology, blockchain technology will be the key to breaking the problem. At present, blockchain technology is becoming a frontier field of high value with its unique technological advantages, innovative value concepts and wide application scenarios.

Blockchain technology offers a strong data storage base. Unlike a traditional centralized server operated by a single power, blockchain data storage offers a technology that divides the data into fragments and scatters them across many cloud-based storage devices. Cloud computing generally deals with a big amount of data. Therefore, there is always a feel of data insecurity as cloud computing works on a centralized architecture, due to this there is a possibility of the central server being hacked and in that case, the whole system will collapse and also there will be no backup of data so lost data can't be recovered.

Therefore, there is the scope of using blockchain in cloud computing for solving these issues.

II. LITERATURE REVIEW

Information security splits into three main objectives, such as integrity, confidentiality, and availability. Security threats to these security goals include a long-term confidentiality issue because one considers that present and past encryption schema are not secure. Information leakage vulnerability is another concern, as data is outsourced. Tampering with data also poses threats to data confidentiality.

Organizations continue to experience security-related incidents at the same rate year over year. 24% of users reported experiencing a public cloud related security incident in the 2023.4

Different types of security incidents are happens, The top three types of incidents reported among cybersecurity professionals are wrongly configured resources or accounts (19%), account compromises (16%), and exploited vulnerabilities (16%).4

Storage of data on the cloud in the field of IoT is a big challenge. IoT stored data is related to personal information of the house owner like their video footage, their voice recordings, their household items, their property, their personal habits, and leak of these data can harm the personal security including robbery, attacks, and illegal selling of the personal details for money. These conditions pose a threat to the cloud infrastructure. The solution to this problem is the use of blockchain in cloud computing, which has the potential of providing enhanced security to the whole architecture.

Cloud service users, either clients or attackers, must have users' authentication privileges to access the cloud services. Communication between users and cloud resources seeks the secured channel that keeps the users' login information more secure than hypertext transfer protocol (HTTP) users. Secondly, communication between cloud services and users must be ensured with synchronization.

III. Blockchain Architecture

3.1. Types of Blockchain architecture

There are four types of blockchains - public, private, consortium, and hybrid.

3.1.1. Public Blockchain

Public blockchains are open to everyone and are not restricted by permissions. They can employ a variety of consensus mechanisms, although scalability can be challenging due to the increasing demands of a broad user base. Bitcoin and Ethereum are classic examples.

3.1.2. Private Blockchain

Private blockchains are created for enterprise needs. It is a permissioned blockchain that is only accessible to a selected few, typically for business organizations. Hyperledger Fabric is one of the most prominent private blockchains.

3.1.3. Private Blockchain

A blockchain that combines the features of both public and private blockchains. Examples are Dragonchain, EWF Baseline.

3.1.4. Private Blockchain

A blockchain that is governed by a consortium of organizations. Example are R3 Corda, Hyperledger Fabric.

3.2. Layered structure of Blockchain architecture

3.2.1. Application Layer

Provides blockchain-based applications for the end user.

The application layer is the end product of the entire system offering specific products for the users, i.e., wallet, lending, staking, etc.

The application layer starts with a smart contract, a programmable code that governs state transitions. It can function as an escrow, payment channel, or vault and is known by different names in various ecosystems, like “programs” in Solana and “chain code” in Hyperledger. Smart contracts are a frequent target for hackers, as any critical error in its code can be exploited for illegal gains.

Usually, users don’t interact with the smart contract directly. Instead, they rely on a front end of a Web3 application or an API. The Uniswap website is an example of a decentralized app combining UI and smart contracts.

3.2.2. Services and Optional Components

Amplifies blockchain capabilities with additional features.

The services layer creates Web3 interconnection, removing barriers and enabling smooth interactions. Optional elements include Decentralized Autonomous Organisations (DAOs), aiding administration and communication in networks like Arbitrum and Polygon, but absent in Bitcoin and Ethereum. Oracles bridge Web3 applications with real-world data on asset pricing, aiding off-chain computations. Hot wallets store on-chain assets but also serve as access points, for example, Metamask or Kaikas – a native wallet for Klaytn. Lastly, block explorers track chain health, helping detect technical glitches and security breaches and mitigate issues early.

3.2.3. Protocol (Consensus) Layer

Set rules for node agreement on the state.

The protocol layer sets the rules for blockchain participation, with the consensus mechanism being its key component. Consensus ensures agreement among nodes for block mining and processing and outlines validator requirements, varying across proof-of-work, proof-of-stake, and other consensus mechanisms. Propagation protocol broadcasts decisions, while protocol audits ensure security against threats like 51% attacks.

Blockchains can be permissioned (limiting access) or permission less (open to all). Sidechains, operating parallel to main chains with separate consensus mechanisms, offer enhanced capabilities. An example is the Polygon-Ethereum relationship.

3.2.4. Network Layer

Provides for peer node interaction.

The network layer enables effective discovery and interaction among peers called nodes. Typically, a node locates a bootnode, which scans for available peers and initiates bonding. As information circulates, it is safeguarded through a Trusted Execution Environment (TEE) to maintain integrity. Node session maintenance varies across networks; for example, Ethereum employs Recursive Length Prefixes, defining the time nodes take to locate, authenticate, and share data.

3.2.5. Data Layer

Ensures secure and confident message transmission.

The data layer of blockchain technology is primarily concerned with data storage and structure. It houses the blockchain, a linear succession of blocks that store transaction information. Depending on the specific blockchain, the data structure can range from a simple transaction list, such as the one used by Bitcoin, to a more intricate structure, like Ethereum’s state trie, which stores contract state information.

While the specifics of transaction addition and hashing used are not the focus here, it is important to note that the data layer does play a role in maintaining integrity and privacy. This is the layer where most cryptographic primitives used in the protocol – signature algorithms, cryptographic libraries, and public-private key pairs — are defined and should be tied to high-security standards.

Asymmetric encryption is a critical component, with a public-private key pair keeping the data confidential. The public key is associated with a wallet address, and the private key grants control over assets tied to that address.

A digital signature accompanies every transaction, is a cryptographic mechanism that avoids impersonation and validates the control of the correct private key without revealing it, thus ensuring security. Signature algorithms such as The Elliptic Curve Digital Signature Algorithm, Rivest–Shamir–Adleman, and so on generate digital signatures.

3.2.6. Hardware/Infrastructure Layer

Provides the necessary capacities to host a blockchain. Blockchain architecture extends to hardware and infrastructure. In this layer—In Proof-of-Work consensus protocols—miners and validators operate, with miners creating new blocks using specialized equipment (GPU, ventilator, stabilizer) and electricity, and validators running nodes for block mining. As for data storage, some blockchains opt for third-party decentralized data hosting's, such as Filecoin, IPFS, Arweave, or Firebase, due to capacity limitations.

Nodes, or clients, come in three types: full, light, and archive nodes. Full nodes store the entire chain's state, participate in consensus processes, and provide data upon request. Light nodes host only block summaries, while archive nodes store transaction data from the genesis block to the present, available for user queries.

IV. Cloud Security

Cloud security is the security measures taken and designed to protect cloud-based information and data. The measures that ensure the security features like user and device authentication, data and data privacy protection, and resource access control.

Identity management, privacy, and access control are especially important for cloud security because cloud systems are typically shared and Internet-facing resources. As more and more organizations use cloud computing and public cloud providers for their daily operations, they must prioritize appropriate security measures to address areas of vulnerability.

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. Concerned issues for users of cloud computing are Eavesdropping should not be happen, Data stored at cloud should have a complete data integrity protection scheme, data should not be discard by service provider for economic benefit, data should not be abused or processed by cloud servers.

V. Blockchain in Cloud Computing

5.1. Decentralization

Problems arise as if a failure of the central server may disturb the whole system and may cause loss of important data, which was stored on a central server. In addition, the central server is prone to attacked by hackers. The blockchain can provide a solution to this problem as in the decentralized system multiple copies of the same data are stored on multiple computer nodes which removes the possibility of failure of the complete system if one server fails. In addition, the loss of data cannot be a problem as multiple copies of the data are present on multiple nodes.

5.2. Scalability

On largescale blockchain applications, the number of transactions in blockchain networks can be huge. Therefore, it is very important to have powerful data processing services to have high transaction execution for enabling scalable blockchain services. In this field, the cloud can give on-demand computing resources for blockchain operations. Due to its scalability capabilities. So, the combination of cloud computing and blockchain can provide a highly scalable integrated system.

5.3. Fault Tolerance

Cloud can help replicate blockchain data across a network of computing servers that are interconnected with each other robustly by collaborative clouds. This will minimize the single-failure risks because of the disruption of any cloud node so they enable uninterrupted services.

5.4. Data Security

Illegal selling of the personal details for money is a big challenge as IoT stored data is generally related to personal information of the house owner, like their video footage, their voice recordings, their household items, their property, their personal habits, and leak of these data can harm the personal security. These conditions create a threat to the cloud infrastructure. The solution to this problem is the use of blockchain in cloud computing, which has the potential of providing enhanced security to the whole architecture.

5.5. Markle Hash Tree

Markle Hash Tree is a tree like data structure comprising the hashes of transactions on same data block- for example consider data block 1, there are four transactions for data block 1, for each transaction a hash is generated, then two hashes are stitched together at a time, and resultant hash is calculated for the pair. This continues until you reach a root hash or Merkle Root, which summarizes the entire ledger.

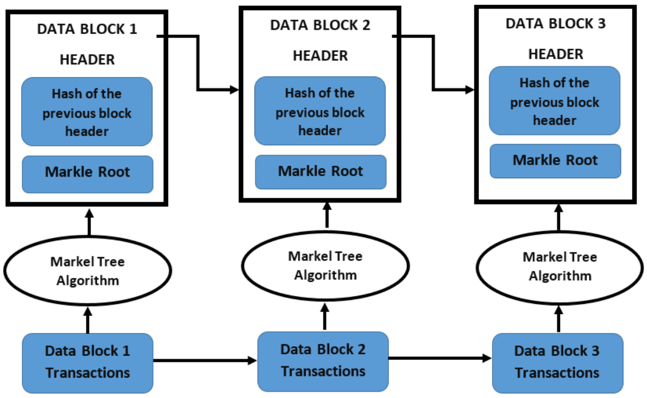
DATA BLOCK 1
HEADER
Hash of the previous block header
Markle Root
DATA BLOCK 2
HEADER
Hash of the previous block header
Markle Root
DATA BLOCK 3
HEADER
Hash of the previous block header
Markle Root
Markel Tree Algorithm
Markel Tree Algorithm
Markel Tree Algorithm
Data Block 1 Transactions
Data Block 2 Transactions
Data Block 3 Transactions

Fig 1. Markle Tree in Blockchain Technology

5.6. Verkle Hash Tree

A Verkle Tree is a tree data structure that uses a novel technique called key prefix encoding to enable more efficient and secure proofs of inclusion and non-inclusion of data items.

Verkle Trees are constructed by dividing the key space into small segments and encoding each segment's prefix in the tree.

This enables more efficient verification of the authenticity of any given data item, as only a small portion of the tree needs to be traversed.

Verkle trees are set to address the scalability problem that blockchain continues to face. For one, they need only 150 bytes of storage for proof for 1 billion data storage points. Since the length of the proof is logarithmic, Verkle trees could greatly impact communication within the network. Unlike Merkle trees, these trees eliminate the need to present proof to each sister node at each entry point.

The key insight of the Verkle Tree is that we can construct a Merkle Tree, but replace Cryptographic Hash functions with Vector Commitments. Before computing a Verkle Tree over some files F0, F1, F2 and so on , we first select the branching factor of the tree, i.e k. We then group our files into subsets of k files and compute a Vector Commitment, C, over each of the subsets of files. We also compute each VC membership proofs πi for each file Fi in the subset with respect to C. We then continue computing Vector Commitments up the tree over previously computed commitments until we compute the root commitment. In Figure 2, we began with 9 files and branching factor of 3. After dividing the files into subsets of size k = 3, a Vector Commitment is computed over each subset along with the corresponding membership proofs. This leaves us with the commitments C1, C2, and C3. We compute the Vector Commitment C4 over these three commitment along with the membership proofs π9, π10, and π11 for the commitments C1, C2, and C3 respectively with respect to the commitment C4. The digest of the Verkle Tree is the root commitment, which is C4 in this case.

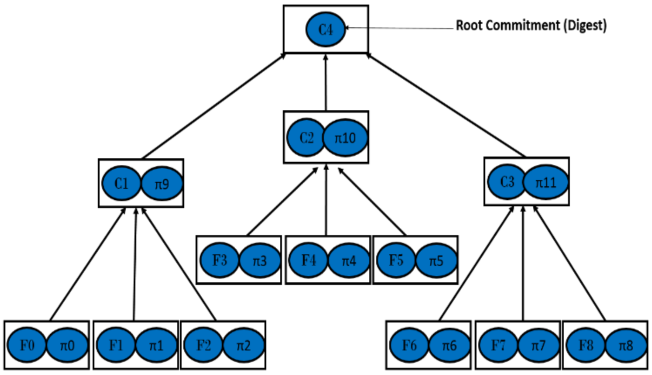

Fig 2. Verkle Tree in Blockchain Technology

5.7. Blockchain Technology with Verkle Tree

Verkle Trees are more scalable than Merkle Trees, making them a better fit for high-throughput applications. Verkle Trees provide increased security by preventing certain types of attacks that are possible with Merkle Trees.

Verkle Trees can be used to prove the inclusion or non-inclusion of data without revealing the actual data, which is useful in privacy-focused applications. Merkle Trees do not provide this feature.

It eliminates the requirement of presenting proof to every sister node at every entry point, like the Merkle tree. Verkle Trees reduce the proof size on a scale of six to eight compared to ideal Merkle Trees.

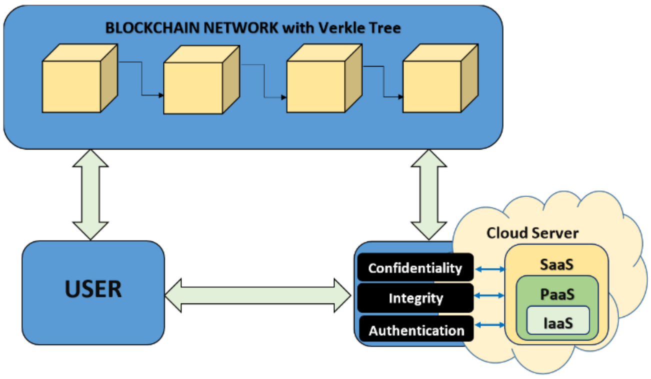

Fig 3. Blockchain Technology in Cloud Security

VI. CONCLUSION

We discussed the differences and advantages of Markle Tree and Verkle Tree data structure techniques to store data on a blockchain platform with immutable scrutiny and security.

We found advantages of Verkle Tree over Markle Tree, following figure shows enhanced security implementation in cloud computing using blockchain with Verkle tree.

VII. REFERENCES

[1]. Yuan Y, Wang F Y. Blockchain: The State of the Art and Future Trends[J]. Acta Automatica Sinica, 2016.22(03):1882.

[2]. Pilkington M. Blockchain Technology: Principles and Applications[J]. Social Science Electronic Publishing, 2015.51(07):121-122.

[3]. Pass R, Seeman L, Shelat A. Analysis of the Blockchain Protocol in Asynchronous Networks[C]// International Conference on the Theory & Applications of Cryptographic Techniques. 2017.(03).

[4]. Cloud Security Report 2023 [online] Available: https://www.cybersecurity-insiders.com/portfolio/2023-cloud-security-report-check-point

[5]. John Kuszmaul, 2019 PRIMES Conference Talk on Verkle Trees.

[6]. S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, 2008, Accessed: 2017-03-08.

[7]. P. Rogaway and T. Shrimpton, “Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance, 2004, Accessed: 2017-9-16.

[8]. R. C. Merkle, A digital signature based on a conventional encryption function, in Conference on the Theory and Application of Cryptographic Techniques. Springer, 1987, pp. 369–378.

[9]. D. Catalano and D. Fiore, Vector commitments and their applications, in Public-Key Cryptography–PKC 2013. Springer, 2013, pp. 55–72.

Cite this article as :

Imran Shahid Shaikh, "Secure Cloud Computing using Blockchain with Verkle Tree Hash algorithm", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 11 Issue 1, pp. 345-351, January-February 2024. Available at doi : https://doi.org/10.32628/IJSRST52411137

Journal URL : https://ijsrst.com/IJSRST52411137