Fuzzy Systems and Soft Computing
ISSN : 1819-4362

REVIEW ON THE EFFECTIVENESS OF USING BLOCK CHAIN IN CLOUD SECURITY

Ms.Fatema Ranapur Research Scholar, Shri JJTU University, Rajasthan
Dr.Archana Tukaram Bhise

ABSTRACT:
Cloud computing is emerging as a key technology in providing on-demand scalable and elastic infrastructureandstorageservicesthroughasharedpoolofvirtualizedresourcesforalongperiod. These services are low-cost and involve minimal effort. Cloud has a centralized service architecture that works in real-time providing ubiquitous computing. Though it has many advantages ensuring reliability and security to users, their outsourced data is a key problem. Block chain technology with its public and distributed peer-to-peer ledger is emerging as an attractive solution for this problem. In this paper, we studied the available literature on security aspects of block chain technologies and cloud computing and further analyzed the effectiveness of block chain in cloud security.

Keywords
Cloud Computing, Block chain, Security, Encryption

INTRODUCTION:
Cloud computing is an operational and economic model rather than a specific infrastructure technology. It offers a flexible, on-demand network of shared computing resources that can be accessed any time, any whereby leveraging this model, users benefit from cost efficiency, as they only pay for the resources they consume rather than maintaining an entire infrastructure. The shared nature of cloud services enhances scalability, allowing users to adjust computing capabilities in real-time based on their needs. This adaptability ensures that businesses and individuals can optimize performance while minimizing costs. Additionally, cloud computing provides seamless access to computing power, storage, and applications, making it a highly convenient and efficient solution for modern digital needs. The ability to configure resources dynamically ensures that users can scale up or down as required, improving overall operational efficiency. This makes cloud computing an essential tool for businesses and individuals seeking agility, cost savings, and reliable access to technology services.

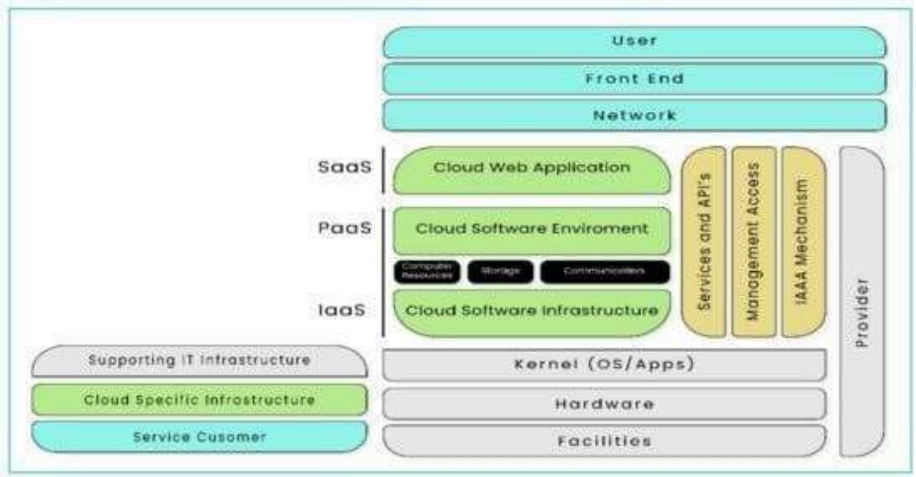

Figure1.Cloud Reference Architecture(Uddinetal., 2021)

Cloud computing infrastructure primarily provides three main service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These services are accessible worldwide at any time through high-speed internet. As businesses increasingly rely on cloud technology, many are transitioning to cloud-based data storage. Given that data is a critical asset, ensuring its security is a top priority. Encryption techniques play a key role in protecting data from unauthorized access by converting it into ciphertext before storage and decrypting it upon retrieval.Since cloud-stored data can be distributed across multiple locations, securing it requires a shift from traditional infrastructure-focused security models to data-centric cloud security frameworks. This approach prioritizes the protection of the data itself rather than just the underlying infrastructure. By implementing robust encryption methods and advanced security protocols, cloud computing enhances data security, fostering greater trust and reliability among users and businesses.

Blockchain has emerged as a widely adopted technology for managing digital transactions (Rathod & Motwani, 2018) and is considered a promising solution for addressing cloud computing vulnerabilities. It enables the development of a secure and reliable authentication system, allowing participating peer nodes to securely share data (Uddin et al., 2021). This paper explores common vulnerabilities in cloud computing and evaluates the effectiveness of blockchain technology in mitigating these security challenges.

SECURITY IN CLOUD COMPUTING:

Cloud service providers are responsible for managing security risks to ensure data protection. This is achieved through the implementation of policies and procedures based on industry best practices, maintaining a balance between business and IT objectives (Carroll et al., 2011). To support its flexibility, cloud computing primarily relies on virtualization and network infrastructure. It follows a Service-Oriented Architecture (SOA), where services are delivered as web services that can be accessed through API calls.

According to Wang & Cao (n.d.), cloud computing involves three key network entities:

1. **User** – An individual or enterprise that depends on the cloud for data storage and computational needs.
2. **Cloud Server** – Managed by a cloud service provider, it offers storage capacity and computing resources.
3. **Third-Party Auditor** – An independent entity with expertise in cloud security, entrusted by users to assess and identify potential risks.

Cloud providers store data across multiple servers in a distributed manner, with these servers operating in parallel. Data redundancy mechanisms are implemented to prevent data loss in case of server failures. Additionally, cloud providers verify the integrity of received files and audit the compatibility of stored content. To maintain confidentiality, all data, processes, and communications are encrypted before being stored on the server.

Identity and access management (IAM) is also employed to associate specific information with a designated entity. Cloud providers adhere to various security standards, including SPML, SAML, OAuth, and XACML, to ensure robust identity management and secure access control.

VULNERABILITIES IN CLOUD COMPUTING:

- **Resource Sharing**

Cloud computing allows multiple tenants to share computational resources, applications, and storage, leading to efficient resource utilization and cost reduction. However, this shared environment increases the risk of information leakage and potential cyberattacks, which may also result in data loss.

Elasticity and Scalability:
Cloud services enable consumers to automatically scale resources up or down based on demand. However, previously allocated resources may have been used by other tenants, creating a risk of confidentiality breaches.

Insider Threats:
Since data is stored on shared storage managed entirely by the cloud service provider, there is always a risk that an insider, such as a cloud employee or third-party vendor, could access, corrupt, or sell sensitive information.

Loss of Control:
Cloud providers maintain location transparency, meaning consumers are often unaware of where their data is stored and the security measures in place. As a result, organizations may lose control over their data and might not even be aware of potential data losses.

DDoS Attacks:
Cloud servers and networks are vulnerable to Distributed Denial of Service (DDoS) attacks, where an attacker overwhelms the system with excessive requests, preventing legitimate users from accessing services.

Malware Injection Attacks:
When data is transmitted from the consumer to the service provider, attackers may inject malicious code into the transmission. Since authentication and authorization are required for data transfers, the malicious code can enter the system through an authenticated user, leading to unauthorized execution of harmful operations.

CHARACTERISTICS OF BLOCK CHAIN:

- **Distributed and Decentralized**

Blockchain removes the need for a central authentication authority. Since every node holds a copy of the ledger, the single-point failure vulnerability of centralized systems is eliminated. Each node participates in the verification process, and new blocks are added once the majority of nodes approve them. This structure eliminates performance bottlenecks, service fees, and waiting times associated with third-party involvement.

- **Immutability**

Once a transaction is added to the blockchain, it cannot be withdrawn or reversed. Data in blockchain is immutable, meaning that any changes to the content of a block will alter the hash of all subsequent blocks. Consequently, any modifications are reflected across all blocks in the network, enabling the tracking of an asset's location and history.

- **Consensus**

Before any transaction can be executed, all participants must agree and verify the accuracy of the data. This process, known as "consensus," involves using various algorithms and processes to make fast and objective decisions. If consensus is not reached, a block will not be added to the network.

- **Anonymity**

Users only need to provide their address to participate in transactions. Communication between users can be done via these addresses, ensuring anonymity.

- **Traceability**

Each block in the blockchain is linked to the preceding one, creating an unbroken chain. Furthermore, all transactions, whether private or public, are timestamped and digitally signed. This ensures that the entire history of a transaction can be traced, from its current state back to its origin.

Blockchain solution for cloud vulnerabilities

Open Ledger:

By using an open ledger cloud service, users can access different levels of security provided by the cloud and select the services that best meet their needs. This approach offers transparency, allowing users to view all available cloud services (Gupta et al., 2019).

Distributed Ledger:

The distributed ledger concept allows the cloud to maintain synchronized copies of the ledger, which all cloud users can access to monitor service usage, policies, and service level agreements. It enables the secure transfer of information through a series of cryptographically secure keys across a distributed system (Tosh et al., 2017). By adopting the mining principles from Bitcoin, cloud users can standardize their ledgers (Gupta et al., 2019).

Decentralized Servers:

Blockchain ensures data ownership by encrypting and storing data, making it difficult to tamper with due to the transaction records being stored on all participating nodes. The decentralization of servers guarantees that they will continue running smoothly in the event of an attack, eliminating the risk of a DoS attack (Habib et al., 2022).

CONCLUSIONS:

While the cloud offers several advantages over traditional data centers, it also has certain drawbacks. Integrating blockchain technology with cloud computing could enhance security, improving both the reliability and security of the cloud computing model. Additionally, the cloud provides the computational power and storage capacity needed for blockchain operations. This paper reviews existing literature to better understand the basic characteristics of blockchain and its potential applications in cloud computing.

REFERENCES:

1 Gupta, A., Siddiqui, S., Alam, S., & Shuaib, M. (2019). **Cloud Computing Security using Blockchain.** *6*, 791–794.

2 Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). **Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing.** *Future Internet, 14*(11), 341. https://doi.org/10.3390/fi14110341

3 Nwokeji, J.C., Coffman, J., Holmes, T., Liu, Y., Irons, G., Diaz, N.M., & Aqlan, F. (2020). **Panel: Incorporating Cloud Computing Competencies into the Computing Curriculum: Challenges & Prospects.** *2020 IEEE Frontiers in Education Conference (FIE)*, 1–3. https://doi.org/10.1109/FIE44824.2020.9274219

4 Rathod, N., & Motwani, D. (2018). **Security Threats on Blockchain and Its Countermeasures.** *05*(11).

5 Wang, J. (2017). **Cloud Computing Technologies in Writing Class: Factors Influencing Students' Learning Experience.** *Turkish Online Journal of Distance Education, 18*(3), Article 3. https://doi.org/10.17718/tojde.328954