Block Chain Technology to Analyse a Cloud Computing Security Framework

Mr.K.Anil,Assistant Professor, Department of Information Technology, CMR Engineering College, Hyderabad, Telangana,

E-Mail-id kesavareddyanil@cmrec.ac.in

Dr.X.S.Asha Shiny,Professor,Department of Information Technology,CMR Engineering College,Hyderabad,Telangana

Abstract:

The phrase "cloud computing" is in flux right now. It is a business strategy that offers services that are supplied and consumed instantly, anywhere, at any time, over any network that is accessible, utilising computing devices that use cloud computing technologies. Although cloud is advantageous because it offers controlled, tailored, and on-demand resources, it also presents the biggest challenge.

The security risk to the cloud system, particularly the user group, must be overcome in computing. These days, cloud security is a significant privacy challenge for both users and cloud service providers.

The cloud security framework issues are discussed in this study. Most of the time, new technologies enter our lives in ways we never could have predicted. One such technology is blockchain. . In this article, we offered an architecture and framework for cloud security and its problematic areas. Based on that, we had visualised the main cloud security issue areas and showed how the combination of blockchain and cloud computing had a significant impact on cloud security features.

Introduction:

As the foundation for addressing the problems that cloud computing providers and users are encountering, it is crucial to grasp what cloud and cloud security genuinely imply so that we may comprehend the necessity of cloud security and the significance of the cloud security framework. Cloud computing is advantageous because it offers on-demand, appropriate performance management, and tailored resource availability; however, the main difficulty is overcoming the security risk to the cloud computing system, particularly to the user group. When it comes to cloud security, it is well-defined as a collection of practises and procedures that ensure security in an environment utilising cloud computing. Cloud security framework is applied against these security challenges and significant privacy threats and is clearly characterised by procedures that are taken in a well-defined manner.

A key component of the cloud security framework is the mutual authentication framework, and many cloud service providers will also introduce many other terms that are closely linked. Security concerns related to physical and logical security are addressed by cloud computing across all service models. End-users and cloud service providers are primarily concerned with the security policy, how data is kept, where it is stored, how data is accessible, and who is accessing that data. Cloud security covers a wide variety of security constraints from both of these perspectives. The vulnerabilities of cloud computing are addressed by the cloud security framework for a secure and safe computing environment. Because cloud service providers are probably most concerned about cloud security, it is crucial to address this issue. The standards and methodology for establishing security in a cloud-based executing environment have been developed by a group known as the Cloud Security Alliance (CSA). A framework for authentication has been developed to ensure the security of data since, using this method, any system can validate and confirm the identity of a person attempting to access it. A user's identification is checked and confirmed by an authentication service using a secret code, such as a password, which also confirms whether the user's provided information is accurate or not. The main goal of authentication is to increase security, eliminate unauthorised access to data, and reduce attacks like password theft committed by attackers. Data Loss Prevention (DLP) is also a crucial essential in the process of safeguarding data. It recognises and keeps track of the data to make sure that only authorised clients may access it and to prevent data leaks. If data is discovered to be in an unsafe region, it can be transferred to a secure location, and it also reduces the need for manual data examination. It is crucial to understand the fundamental advantages of using the mutual authentication architecture in cloud security as we have already introduced it.

Each system that uses the authentication method validates, examines, and confirms the identity of a user before allowing them access. A user's identification is checked and confirmed by an authentication service using a secret code, such as a password, which also confirms whether the user's provided information is accurate or not.

There are numerous types of authentication methods, which we will examine in more detail. Mutual authentication's main goal is to improve security, eliminate unauthorised user access to services, and reduce assaults like password theft carried out by attackers since it offers robust security measures.

Before granting access to a user, any system that makes use of the authentication mechanism verifies, examines, and confirms their identity. An authentication service uses a secret code, like a password, to check and validate a user's identity and determine whether the information they have provided is accurate.

We will look more closely at a variety of authentication technique kinds that exist. Since it provides strong security measures, mutual authentication's major objective is to increase security, stop unauthorised users from accessing services, and lessen attacks like password theft committed by attackers.

The mutual authentication architecture addresses a variety of security concerns, including:

1. Traditional security issues
2.Issue with availability.
3. Concerns with third-party data control.

The majority of the issues stated above and others are resolved by these security features.

Authorization plays a significant part in the mutual authentication process by allowing users to access systems based on their true identities.

The following are some fundamental authentication procedures:

1. Authentication with passwords and pins.
2. Authentication via SMS.
3. Authentication using symmetric keys.
4. Authentication using public keys.

5.Biometric identification
6. Electronic signature.

Methodology:

While discussing the security domain of the applications we are running, it is crucial to have specific knowledge of the service model, different cloud (deployment model) kinds, and the security domain's goal. Input validations under this open API, SSH, are taken into account when we talk about client level security. While logging, alarm systems, and reporting are taken into account when discussing the monitoring domain. Security measures for the communication medium include VPN, SSL, and IPSEC. Data and storage security is the most crucial area of security, and it includes data encryption, key management, cloud disaster recovery, garbage management, digital signatures, and data masking. SSO, ACL, Authorization, and Directory service are taken into consideration in identity and access management. Registry security, picture encryption, and virtual image security are taken into account. In the security realm, where firewalls are frequently evaluated, network security also plays a crucial role. Last but not least, we discuss physical security, which is a very important aspect of security, and is related to CCTV, access log registers, and data centre setc. The thyroid is a butterfly-shaped gland that may be located in our necks just below the Adam's apple. It is in charge of our body's metabolic processes. It generates Triiodothyronine (T3) and Thyroxine, two hormones, when it is functioning normally (T4). T3 and T4 hormones are also produced by a hormone called Thyroid Stimulating Hormone (TSH), which is released by the pituitary gland. The human body's TSH, T3, and T4 levels determine wellness.

The security framework architecture of the cloud varies depending upon the different service model–
Infrastructure-as-a-service(IaaS),
Software-as-a service(SaaS),
Platform-as-a-service(PaaS).
IaaS is the base of all cloud services.

IaaS cloud security framework architecture:

This model offers the networking and storage parts of cloud architecture. The APIs are mostly used to maintain and communicate with the cloud.
The infrastructure security is handled by the cloud service provider, who also increases cloud computing's adaptability. Network Packet Broker makes security problems in a cloud computing network transparent.
IaaS offers a variety of capabilities for cloud architecture, some of which are covered here. A virtual web application firewall is offered by IaaS to shield websites from male-violent programming. Moreover, IaaS offers network-based firewalls to secure the network edge. For the cloud network, it also offers virtual routers. Moreover, there are IaaS-supported intrusion detection and prevention systems, also known as IDS and IPS. IaaS also offers network segmentation to give users effective services.

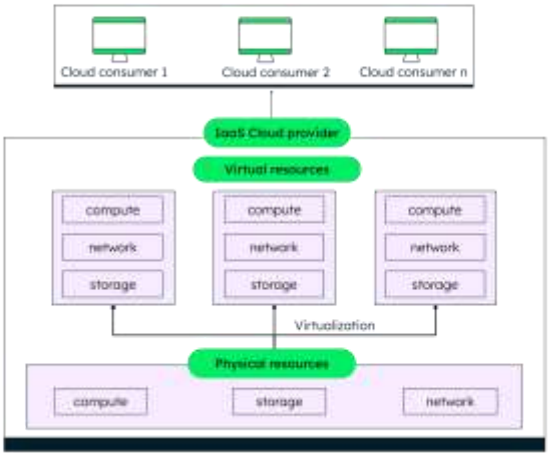

Fig 1: IaaS architecture

SaaS cloud security framework architecture:

The SaaS service model hosts data and software centrally so that it may be accessed through a browser. Due to its ability to provide access control and frequently incorporate encryption capabilities, Cloud Access Security Brokers (CASB) play a crucial role in identifying security concerns within a SaaS service architecture.

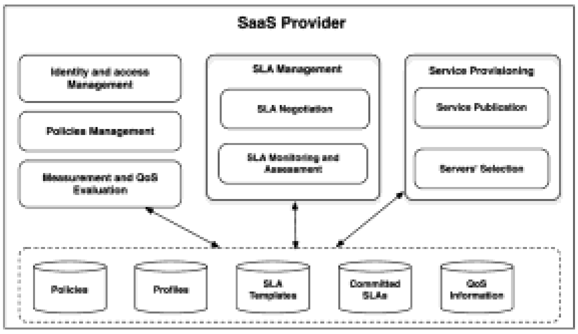

Fig 2: SaaS Architecture

PaaS cloud security framework architecture:

PaaS cloud service model is described as the deployment of online applications without the expense and complexity of purchasing and managing the infrastructure and software, as well as the provisioning capabilities of hosting, by Cloud Service Provider. The bulk of cloud service providers secure the PaaS cloud service model.

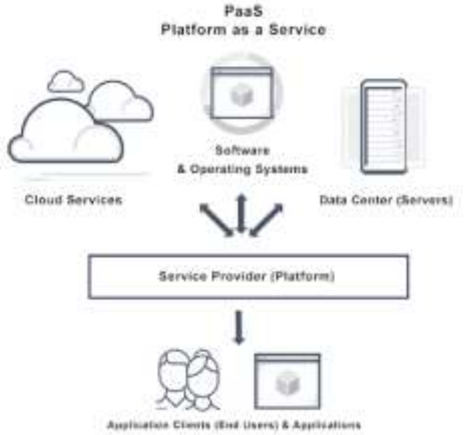
PaaS
Platform as a Service
Cloud Services
Software & Operating Systems
Data Center (Servers)
Service Provider (Platform)
Application Clients (End Users) & Applications

Fig 3: PaaS Architecture

Attacks on cloud computing:

1. Zombie attack: By introducing applications into the system without the user's consent, it makes the system unstable in terms of efficiency, performance, and security. For DoS and DDoS attacks, it is done.

2. Service injection attack: The attacker injects errant services and virtual machines that impair the systems' functionality.

3. Attacks against virtualization include attacks on the hypervisor that stop it from working.

4. Spoofing: This is when a malicious party attacks a network host by attacking its systems.

5. Phishing: In this type of attack, the attacker calls and texts users to obtain sensitive information such as usernames, passwords, credit card numbers, and many more.

6. Backdoor channel attack: Refusal of the standard authentication process for system access. This is done by data thieving, server hijacking etc.

The security model of cloud computing serves as the foundation for this security architecture. Every component in this design is dependent on every other component, either in terms of functionality or operating behaviour, and each component calls for a different technology. On each component, access control processing (ACP) is completed in order to provide consumers with flexible services.

Security aspect of blockchain technology :

The three sub-divisions of the security features of blockchain technology are as follows:
1. An introduction to cryptocurrencies and blockchain technology.
2. The development of commercial sectors using blockchain technology.
3. Barriers to blockchain technology adoption.

1. An introduction to cryptocurrencies and blockchain technology:

Bitcoin is a digital asset created to function as a medium of exchange that secures transactions using the process known as cryptography.

A subset of digital currencies, such as bitcoins, is referred to as cryptocurrencies. Nobody controls bitcoin, a sort of currency (digital cash) that is created and held electronically. The first decentralised digital currency was introduced by it. created by individuals and organisations utilising computers to solve mathematical problems globally.

2. The development of commercial sectors using blockchain technology.

Blockchain technology has the potential to transform many industries, including commercial sectors. Here are some ways that blockchain can be used in commercial sectors:

Supply Chain Management: Blockchain can be used to track the entire supply chain of a product, from its origin to the end consumer. This can help in increasing transparency and accountability, reducing fraud and counterfeiting, and ensuring ethical practices.

Payment and Transactions: Blockchain can be used to streamline payment and transaction processes, making them faster, more secure, and cheaper. It can also eliminate intermediaries like banks, reducing transaction costs.

Identity Management: Blockchain can be used to create a decentralized identity management system, where individuals can control their personal data and share it securely with others. This can reduce identity theft and fraud.

Digital Rights Management: Blockchain can be used to manage digital rights, such as copyrights, patents, and trademarks. This can reduce infringement and ensure that creators are properly compensated for their work.

Insurance: Blockchain can be used to automate insurance processes, making them faster and more efficient. It can also reduce the risk of fraud and improve the accuracy of claims processing.

Overall, blockchain technology can bring transparency, security, and efficiency to commercial sectors, which can lead to cost savings and increased trust among stakeholders.

3. Barriers to blockchain technology adoption.

The difficulties that blockchain technology faces will be covered in this section. Working within an existing framework is one of the most difficult tasks to complete; an easier-to-use framework must be used in its place. The significant costs associated with switching from a centralised to a distributed approach are one of the problems with blockchain technology. One of the factors that must be taken into consideration is security, as blockchain technology may experience issues with accountability and breach. The Payment Card Industry- Data Security Standard (PCI-DSS) payment gateway can be connected to transactions made using blockchain technology, which will benefit the financial sector by ensuring secure transmission. The demand of today is to be concerned about anonymity and security in relation to various applications as the use of applications grows. One of the difficulties that could result in the decryption of highly secure data in the case of an anonymous bitcoin authority is Bitcoin, one of the most recent trending areas to develop in blockchain technology. Concerns with blockchain technology also include throughput, latency, and resource waste.

Conclusion :

In this study, we suggested integrating blockchain technology with cloud computing technology to improve cloud environment security. The experimental results obtained using the Eclipse software and the Java programming language are presented in the study to support the integration of cloud technology with blockchain technology. The following are some of the ways that blockchain integration with cloud security aids in producing results that are more specific and safe for users and clients:

a. Distributed and digital features that utilise powerful, highly specialised computer techniques and cryptographic locking systems to record transactions.

b. Confidentiality, integrity, anonymity, availability, privacy protection, and other attributes are some of the ones to which blockchain has successfully contributed.

c. Bitcoins, cryptocurrencies, and cryptography are the main focuses of the blockchain.

References:

1. Xu M, Buyya R Brownout approach for adaptive Management of Resources and Applications in cloud computing systems. ACM Comput Surve 52(1):1–27

2. Zhu Y, Zhang W, Chen Y, Gao H A novel approach to workload prediction using attention-based LSTM encoder-decoder network in cloud environment. EURASIP J Wirel Commun Netw 247. https://doi.org/10.1186/s13638-019-1605-z

3. Li X, Gui X (2010) Cognitive model of dynamic trust forecasting. J Software 21(1):163–176.

4. Tahta U, Sen S, Can A (2015) GenTrust: a genetic trust management model for peer-to-peer systems. Appl Soft Comput 34:693–704. https://doi.org/10.1016/j.asoc.2015.04.053

5. Sanadhya S, Singh S Trust calculation with ant Colony optimization in online social networks. Procedia Computer Sci 54(2015):186–195. https://doi.org/10.1016/j.procs.2015.06.021

6. Gao H, Huang W, Duan Y The cloud-edge-based dynamic reconfiguration to service workflow for Mobile ecommerce environments: a QoS prediction perspective. ACM Transact Int Technol 21(1):1–23. https://doi.org/10.1145/3391198

7. Zhang P, Kong Y, Zhou M A novel trust model for unreliable public clouds based on domain partition. In Proceedings of IEEE 14th International Conference on Networking, Sensing and Control (ICNSC). IEEE, pp 275–280.

8. Li W, Ping L, Pan X Trust model to enhance security and interoperability of cloud environment. In: Proceedings of CloudCom'09 the 1st International Conference on Cloud Computing. Beijing. Springer, Berlin, pp 69–79.

9. Li W, Wu J, Zhang Q, Hu K, Li J Trust-driven and QoS demand clustering analysis based cloud workflow scheduling strategies. Cluster Comput 17(1):1013–1030

10. Li X, He J, Du Y Trust based service optimization selection for cloud computing. Int J Multimedia Ubiquitous Engineering 105:221–230

11. Yin Y, Li Y, Ye B, Liang T, Li Y A Blockchain-based incremental update supported data storage system for intelligent vehicles. IEEE Trans Veh Technol:1.https://doi.org/10.1109/TVT.2021.3068990

12. Xie L, Ding Y, Yang H, Wang X Blockchain-based secure and trustworthy internet of things in SDN-enabled 5G-VANETs. IEEE Access 7:56656–56666. https://doi.org/10.1109/ACCESS.2019.2913682