INTERNATIONAL RESEARCH JOURNAL ON ADVANCED SCIENCE HUB
e-ISSN : 2582 - 4376
Open Access
RSP SCIENCE HUB
(The Hub of Research Ideas)
Available online at www.rspsciencehub.com

A Survey Paper on Cloud Security Based on Distributed Ledgers of Blockchain

Neetha S.S[1], Michel Rwibasira[2], Dr. Suchithra R[3]

[1]Asstant Professor, Dept. of Computer Applications, Sivananda Sarma Memorial RV College, Bangalore, Karnataka, India.

[2]PhD Scholar, Computer Science and Information Technology, Jain University, Bangalore, Karnataka, India.

[3]Head of Department of MSc IT, Jain University, Bangalore, Karnataka, India.

ssneetha.kala@gmail.com[1], kananura25@gmail.com[2], suchithra.suriya@gmail.com[3]

Abstract

Technology grows up, day to day to facilitate human beings' lifestyle, in order to protect them and their properties. Cloud computing is a platform that one hardware is shared by different clients in the virtual ways and works as standalone physical hardware, is accessed everywhere at any time through the internet. Security is an essential and a vital point to all customers is belonged in the same physical component. This survey paper discusses about cloud computing challenges, types of attacks, and currently solutions in the details. Furthermore, cloud security of models as application, network, and deployment and also services. Cloud security based on a distributed ledger helps the clients to operate within transparency manners and is decentralized to enhance cloud computing information security principals, cloud security requirements, cloud security control, and security design of cloud computing.

Keywords: Cloud Security, Blockchain, distributed ledgers.

1. Introduction

Cloud Computing is one of the fastest emerging technologies in data processing. Most are using cloud computing in one or the other way. There are many advantages of using cloud computing like anytime-anywhere approachable, good area coverage, less contribution on system and so on. But there also are difficulties using cloud computing like data security, lack of resources and expertise and so on. Among the difficulties data security stands large and this paper explores the Different Types of Attacks in Cloud Security and provides methodologies to overcome the data security difficulties and provides possible solutions for security attack on Cloud Computing. Cloud Computing presents many unique security issues and challenges. In the cloud data is stored with a third-party provider and accessed over the internet. This means the visibility and control over the data is limited. It also raises the question of how it can be properly secured. It is imperative everyone understands their respective role and the security inherent in cloud computing. Cloud service providers treat cloud security issues and risks as a shared responsibility. In this model, the cloud service provider covers security of the cloud itself, and the customer covers security of what they put in it. In every cloud service from software-as-a-service (SaaS) like Microsoft Office 365 to infrastructure-as-a-service (IaaS) like Amazon Web Services (AWS)—the cloud computing customer is always responsible for protecting their data from security threats and controlling access to it. The security of cloud users by applying the encryption of data storage techniques. And the clients may use the others' storage about those are on the same blockchain network. Rather than adopting, a traditional method on a single third party as a central database. Data storage has smart contract verification, authentication, based on the

consensus agreement between nodes. This allows the payment operation to be performed. Unfortunately, this paper does not handle the issues of the nodes that are not taking part in the computing of the data mining at downtime mode. The work of this paper is dedicated to the work of integrity and blockchain technology in solving current cloud security issues [1]. This paper theoretically proposes blockchain technology based on software network distributed ledger cloud technology. That controls the fog miner; to handle the issues of the traditional approach is used. Furthermore, the internet of things is the new age of technology, and managing its storage becomes a critical issue. The software-defined network offers the low-cost of the internet of things storage. And also, high performance and security of the real-time computation. But this technique does not protect the network from self-mining attackers [2]. The traditional security of cloud storage has based on attribute-based encryption, its issue, and the new approach to blockchain decentralized storage. Cloud storage is increased the number of advantages to the users. The combination of attribute-based encryption and Ethereum blockchain-based on smart contract to enhance security. But this approach does not protect from double-spending attacks through blockchain networks [2][3]. The importance of having a sharing electronic healthy record between medical data centers may improve the researches across the diseases in the medical field to heal them. Hence the security issues of a centralized data center and a cloud uncovers attackers, unavoidably to data security and privacy protection. Also, it adopts blockchain technology with distributed ledgers rather than using a single data center that might cause fail issues often when it goes down, the entire system fails. Besides, it adopts proxy re-encryption that may cause trouble in the database's security to reveal the information due to it alters of ciphertext. Therefore, the security problems might appear as a denial of service (DoS) and active man in the middle attacks and even though users blockchain with distributed ledgers in exchanging the data [4]. Authors consider blockchain technology and it is so attractive in resolving the security of cloud computing in terms of data privacy, auditing, and management of the digital variables. As well known that blockchain offers peer-to-peer to establish a tampered proof field. Verification of security, at any digital information, is done by miners on the network. Once it is approved immediately, added to the unblocked chain. Alas, this technique every node mine for it is in the best interest. This approach has the drawback of creating a private chain and hidden one that may lead to cause a 51% attack [2][5]. This paper discusses how to maintain the data privacy unblocked manners. It adopts blockchain to secure the cloud storage to offer a distributed ledger within the data centers as block-cloud. To implement the proof of stake method and Kubernetes Securing the entire operation of the data is taking place in a cloud environment. But this technique of proof of stake has a big issue of whoever invested higher, profits much too. And own the control of the entire system. Furthermore, Kubernetes often, when interacted with decentralized cloud storage gets, a significant problem of fractured depends on is the architecture of tools that may cause an injury and also, leads to revealing the information from authorized users [6]. This paper details on cloud computing are increasing day today and the security of the people with their properties. And to do so, it has used blockchain with distributed ledgers to protect the data through the internet. It reduces cloud computing security issues by analysing confidentiality, integrity, and access control. However, integrating blockchain technology through cloud computing security issues like double-spending and self-mining attacks [2][7]. cloud computing is secured by introducing the blockchain with distributed ledgers, in order to protect the information and confidentiality through distributed data storage, of blockchain and strongly cryptography of cloud miners, and various application of blockchain. Yet, it is not focused on the blockchain's serious storage and unused blocks during the computing of blocks that may rebuild a private chain side of the main one that is published after and cause a double-spending attack [8].

2. Security Challenges And Threats In Cloud Computing

2.1 Security issues:

Cloud technology is among the trending new-age technologies. In today’s world, a blockchain with distributed ledgers are adopted in cloud technology to facilitate data confidentiality, integrity, and availability. Furthermore, the combination of cloud

technology and blockchain technology are still critical issues. The Threats and challenges are detailed across this paper. Therefore, cloud users may be kept safe through the internet, and cloud service providers might have all means to the data recovery with transparency manners.

3. Cloud Security Based On Distributed Ledgers

This section discusses four main aspects of cloud security are information security principles, cloud security requirements, cloud security control, and lastly security architecture. Moreover, the table1 below, details security perspective within various four elements that are model, challenges, attacks, techniques in cloud security based on distributed ledgers.

Table 1: challenges, threats, and techniques in cloud security

Model	Challenges	Attacks	Techniques
Application	-Links hypervisor -Denial of service -Hiding field attacks -Data immigration -CAPTCHA malfunction -Brute force guesting -Side channel attacks -51% attacks -self-mining attacks	-Data availability and solidarity issues -Security and privacy problems	-Information breaches to malicious -Ledger and service snatching
Service	-Data unveil issue -Hostile attacks -Recovery and storage -Multitenant technological problems -Virtual sys overflow -Man in the middle attacks	-Cloud technology Security defiance -Rules and standards acceptance	
Network	-Session hijacking -Ip spoofing -Replay -Cross site script -Whole fishing -Spear attacks -Pharming	-Defeat in vendor security and leads customers in breaches -Side channel attack	
Deployment	-Shared resource issues -Human errors -Mismatch configuration issues -key management issues -Data immigration issues	-Accepting data blindly from untrusted resource and proceeds	

3.1 Information Security Principles

The information security principles are based on the three main pillows in cloud security and these aspects that comes on the picture, when discussing the establishment of a secure communication channel. The cloud security is overlaying on CIA triad [9] as confidentiality, integrity and availability, those grant the users to identify the problems that could appear under security network and the same way how to resolve the issues to a certain level.

I. Confidentiality is the best approach that offers online data protection from unauthorized users. Its main aim is to secure data through communication and does not allow information to be accessed by unauthorized people. It is well known that in this technology world, everything comes online, in order to facilitate the human being lifestyle, as

well as the attackers and malicious acts are increasing day to day. Therefore, confidentiality is a key in cloud security.

II. Integrity is the model of verifying the transferred data, to ensure that there is no modification of through a network that has taken place from the attacker. It is to ensure that data from the authorized sender to the receiver are genuine, and data are not altered in the transit. III. Availability is the best approach to ensure that the genuine data are always available to the user. Whenever are required, in real-time during an operation, and storage that should be available to the authorized users at every time, everywhere, and whatever.

3.2 Cloud Security Requirements

With the immigration of the data into the cloud platform, security data is not the stand lone point to be stuck on. It is well known that infrastructure is not based only on security [10]. But the healthy Security can be supervised and trusted through distributed ledger. Therefore, to secure the users and their properties across the cloud technology. It is for this regard; security might be strong.

I. Robust security it yields to go further better than a traditional approach of security, even though the multitenant framework. It offers data security to avoid side-channel attacks, nobody can be able to read, access someone else data unless there is an authorization or mutual agreements between the users. It involves the mechanism of confidentiality, cryptography, logs archives, and access control of the entire system.

II. Trust and Self-assurance company remains the positiveness in the integrity of the entire platform. And this focuses on the integrity of the hardware, software, data-centers, and processes of the system. The cloud service provider offers a reliable level of trustiness as well the policies in the transparency manners, reporting ability, and even to identify the vulnerabilities. Moreover, it provides an audit mechanism to the service provider to deal with clients' existing issues.

III. Monitoring and Governance it commits a position that permits the customer to keep eye on their system security, performance, and reliability. With these efficiencies, the client has the capability to act immediately according to the detail of information security received from the cloud service provider into their storage. The client is able to reboot the function, as well as governance the risk management of the system.

3.3 Cloud Security Control

Normally, cloud security control is anticipated within three ways are following front end security layer, middle layer, and lastly back end security layer [10,11].

I. The front-end security layer- it is the initial security point, where the user deals with the security perspective of authentication as the login credibility, and authorization as the permission to access the data to some extent, based on the cloud security service provider policies.

II. Middle security layer - this layer deals with infrastructure's operating system security, hypervisors and the security of virtual machine.

III. Back end security layer as well that security of the system is not a single point alas, it is interoperated chain to ensure the security aspects, after all being done into first two steps as is stated above, this deals with network security, data storage security and securing data by themselves.

3.4 Security Architecture

The good security design, follows the three main points, to keep client's data safe which are isolation of every virtual machine, works as a standalone system; confidentiality data are secured from authorized users and the function of the corporate to maintain security [11].

I. Isolation it surely verifies that in all configurations of virtual machines through the hypervisor, each virtual machine works as a stand-alone system. To avoid side-channel access and malicious acts, this offers security to the clients and their properties in cloud security.

II. Confidentiality it deals with the protection of the users 'information, blockchain with distributed ledgers secure data by applying cryptography to encryption as "signing" process via a private key and decryption as "discovery" via a public key. All those processes deal with security of protecting data from the authorized user to access secured data.

III. Access Control and Identity Management identity management credits that data are accessed by authorized personnel only. As an infrastructure's security key point, identity management verifies the user before granting access to the data into the secured system. And

also, access control and identity management are offered by federated identity management.

Conclusions

Initially, cloud computing remains the platform, where users share the same hardware resources. And works as an independent virtual machine. It is properly recognized that reduces the cost savings, strategic edges, incredible speed, reliable backup, and mobility. Woefully, traditionally, the days, the software developers were unbothered about safety. For instance, this reason, these days everything sets out through cloud technology. Safety concerns become a critical issue because of the malicious behaviours. the most attackers' acts are taken place, throughout the cloud technology sensitive data are exchanged between various clients, and that uses cloud computing data centres. This survey paper discusses safekeeping, challenges, and risks. Within various models of security that offer awareness to the cloud service providers. And the ways of getting hold of their customers from assaults that might be internal and externalattackers, to protect mortal beings and their personal properties.

References

[1]. JingtingXue, Chunxiang Xu, Yuan Zhang, Lanhua Bai, "DStore: A Distributed Cloud Storage System Based on Smart Contracts and Blockchain", spring, 07 july,2018.

[2]. Pradip Kumar Sharma, Mu-Yen Chen2, Jong Hyuk Park, "A Software Defined Fog Node based Distributed Blockchain Cloud Architecture for IoT", IEEE (Volume: 6), 29 September 2017, page: 115-124.

[3]. Shangping wang, yinglongzhang, yalingzhang, "A Blockchain-Based Framework for Data Control in Decentralized Storage Systems Sharing with Fine-grained Access", IEEE Access (Volume: 6), 28 June 2018, pages 38437 – 38450.

[4]. yong. wang, aiqing. zhang1, peiyun. zhang, huaqun. wang, "cloud-assisted ehr sharing with security and privacy preservation via consortium blockchain", IEEE Access (Volume: 7), 23 September 2019, page: 136704 – 136719.

[5]. Deepak K. Tosh, Sachin Shetty, Xueping Liang, Charles A. Kamhoua, Kevin A. Kwiat, Laurent Njilla, "Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack",17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, 13 July 2017.

[6]. Deepak K. Tosh, Sachin Shetty, Peter Foytik, Charles A. Kamhoua, Laurent Njilla. "CloudPoS: A Proof-of-Stake Consensus Design for Blockchain Integrated Cloud", IEEE 11th International Conference on Cloud Computing, 10 September 2018.

[7]. S. Pavithra, s. Ramya, soma prathibha, "A survey on cloud security issues and blockchain", 3rd International Conference on Computing and Communications Technologies (ICCCT), 05 September 2019.

[8]. Shweta Gaur Sharma, Dr. Laxmi Ahuja, "Building Secure Infrastructure for Cloud Computing using Blockchain", Second International Conference on Intelligent Computing and Control Systems (ICICCS), 11 March 2019.

[9]. Muskangupta, "Article", principles of information system security, 15th jan,2020.

[10]. Cloud information center, "cloud security", 3rd December, 2020

[11]. Subra kumaraswamy, "Introduction to cloud security architecture from a cloud consumers perspective", 07th December, 2011.