A SURVEY ON CLOUD SECURITY ISSUES AND BLOCKCHAIN

S.Pavithra
Dept of Information Technology,
Sri Sairam Engineering College,
Chennai, India.
spavithrasai@gmail.com

S.Ramya
Dept of Information Technology,
Sri Sairam Engineering College,
Chennai, India.
sramyasatya@gmail.com

Soma Prathibha
Dept of Information technology,
Sri Sairam Engineering College,
Chennai, India.
prathibha.it@sairam.edu.in

Abstract:-The need for cloud computing is gradually increasing day by day. The cloud computing security is the major difficulty. Since the data in the cloud has to be transferred through internet, the security of data becomes a major concern. The key mechanisms for data protections like integrity, accountability, privacy, access control, authentication, authorization must be maintained. Blockchain is a technology which makes cloud computing better. Blockchain overcomes the security issues in cloud computing. This survey aims at analyzing and comparing various issues in the cloud environment and security issues using blockchain.

Keywords- Cloud computing, Blockchain, Security, Data protection.

I.INTRODUCTION

Security in cloud computing is important to protect the data, applications and infrastructure of cloud computing. Security is provided by policies and different technologies. Cloud computing is an important domain in network and information security. Organizations make use of cloud environment with the different service models of cloud and deployment models of cloud. Cloud security issues are of two types namely issues faced by the cloud provider and issues faced by the consumer of the cloud [20].

Provider is responsible for both their infrastructure security and their client's data and application is protected, while user uses strong passwords and authentication measures. Hence an efficient cloud security architecture is needed which provides control to protect our application by reducing attack. Blockchain is the new technology in the information era with an excellent security. Security is provided by the authentication of peers, encryption, and hash value. Cloud computing is used in all IT environments because of the efficiency and availability [20].

Today, many organizations are hosting their applications on cloud. Hence more Datacenters are created and managed, thereby saving a huge amount of cost. Accessibility is also improved as it can be accessed from anywhere. There is no need of the customers to own their infrastructure and to maintain them. Some cloud vendors include Amazon, Microsoft and IBM [19].

Cloud computing has many characteristics namely availability of large amount of resources, pay for only what you use, flexibility and service from any broad network can be accessed easily [22]. Figure 1 shows some of the advantages and disadvantages of cloud computing.

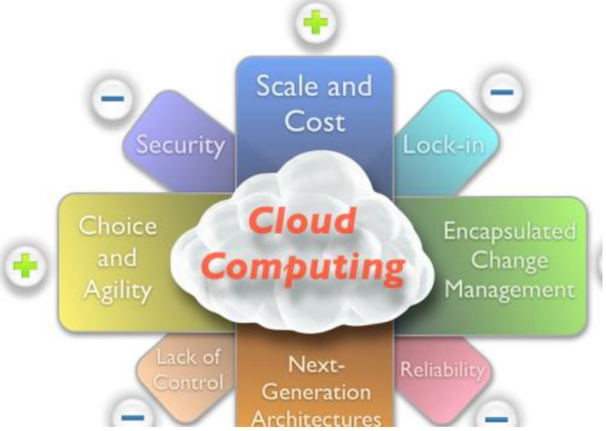

Figure 1. Advantages and, disadvantages of cloud computing[Source: https://sourcetech411.com/]

A. CLOUD SERVICE MODELS

There are three Service models in Cloud Computing. They are SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service).

Software as a Service (SaaS) is a type of service provided over the internet. It is highly scalable internet based application and can be availed from any part of the world. The Platform as a Service (PaaS)is used to design and build applications provided in cloud infrastructure. The Infrastructure as a Service (IaaS) model is pay per use model. The services are offered on demand [18].

B. CLOUD DEPLOYMENT MODELS

978-1-5386-9371-1/19/$31.00 ©2019 IEEE

Cloud deployment models are of four types. They are Private cloud, Public cloud, Community cloud and Hybrid cloud.

The private cloud infrastructure operates for a particular organization and serves it completely. The private cloud is preferred because of the security it offers. The public cloud base operates for general public and it is owned by cloud service provider. This infrastructure provides cloud service to all of its customers. Community cloud exclusively operates for specific community of consumers from organization. They are shared by group of organizations of similar industries with similar requirements. The hybrid cloud is made up of two models or more than that. These models holding separate entities are combined through a standard technology enabling portability of data [20].

II.SURVEY ON CLOUD SECURITY ISSUES

Cloud security refers to maintaining the confidentiality, integrity and availability of data stored in cloud. The requirements of cloud security include robust security, trust, assurance, monitoring and governance.

Proper scheduling of tasks is required in cloud environment. Vijayalakshmi and Prathibha proposed one of the algorithm to prioritize the tasks based on the importance before executing the tasks [19].

Computations and data in cloud are associated with number of security risks such as loss of governance, failure in isolation, data protection, service availability, compliance and legal risk, authentication and authorization etc.

This section includes survey on various methods on privacy preservation, data integrity preservation and issues in auditing and storage in the cloud environment.

A.PRIVACY PRESERVATION IN CLOUD

In [9] the author proposed an idea of providing secure cloud ecosystem which makes sure that the security of data and privacy of data is concerned right from user authentication to data being stored on the cloud. The algorithms used in their work are RSA and AES for data encryption and decryption, SHA512 and bcrypt functions for hashing and HMAC (keyed Hash Message Management System) for key management. Their work provides Hybrid Cryptographic System (HCS) that has benefits of both symmetric and asymmetric encryption [9].

In [11] the author summarizes various security measurements including privacy data access processing, encoding data searching and encoding data computing. In privacy data access processing usage of combination of public cloud and private cloud deals with cloud computing security and privacy. The sensitive data must be managed by private cloud whereas insensitive data must be managed by public cloud. For encoding data searching, a better public key encryption scheme must be constructed for protecting the privacy. Homomorphic encryption algorithm is used with encoding, which conducts the cipher text and plain text concurrently and directly[11].

In [1] the author introduced a comprehensible privacy preservation scheme based on Identity-Based Encryption. Their work presents various concepts of privacy and a mechanism for preservation of privacy. The scheme introduced in their research has many advantages but contains some drawbacks too. The IDE scheme requires a channel which must be secure for transmission [1].

Table 1: Survey on Privacy Preservation in the Cloud environment.

Reference number	**Problem addressed**	**Techniques used**
[9]	Cloud Ecosystem with data security and privacy.	SHA 512,bcrypt function and HMAC algorithm
[11]	Levels of security for sensitive and insensitive data.	Homomorphic encryption algorithm.
[1]	Privacy preservation	Identity Based Encryption

B.DATA INTEGRITY IN CLOUD

In [6] the author checks the integrity which is based on MAC scheme. There is no third party in this condition. Their work withstands replays attacks and Man-in- the-Middle attacks. The redundant data is not eliminated in their work[6].

In [15] the author survey various researches about data integrity proofs for the cloud systems. Various approaches like Provable Data Possession (PDP), Proof of Retrievability (POR), hashing, signature methods, encryption are used. The accuracy, fidelity, consistency and validity of the data must be maintained in order to achieve data integrity [15].

In [8] the author proposes an idea of efficient auditing scheme to verify the data's integrity that has been stored in the cloud environment. Their work suggests usage of SHA-2 algorithm for integrity checking and for encryption it uses AES algorithm. Their work doesn't support updating or insertion or deletion of data[8].

Table 2: Survey on data integrity preservation in cloud.

Reference number	Problem addressed	Techniques used
[6]	Replay attack and Man-in- the-Middle attack.	MAC based integrity checking.
[15]	Comparison of various Data integrity schemes.	PDP,POR, Hashing, Signature methods, Encryption.
[8]	Auditing scheme for checking data integrity	AES for encryption and SHA-2 for checking the data integrity.

C.ISSUES IN CLOUD STORAGE AND CLOUD STORAGE AUDITING

Various issues in cloud storage include data leakage, cloud credentials, key management, performance etc. These issues must be addressed when using cloud storage and file sharing in cloud.

In [16] the author proposes idea to deal with key exposure problem. Their work tries to make the key as transparent as possible to the clients. In their work the cloud stores the files uploaded by the client. The Third Party Auditor (TPA) holds the encrypted secret key and updates in each time period. Their work provides information on outsource key updates for auditing the cloud storage in addition with key revelation resilience [16].

In [13] the author proposed a new idea of Identity based RDIC (Remote Data Integrity Checking) protocol. The protocol makes use of key-homomorphic cryptographic primitive thereby it reduces the system complexity. There is no leakage of information in stored data. The security model suggested in their work achieves robustness and complete data privacy [13].

In [14] the author proposes an idea that deals with key exposure problem. The Third Party Auditor is assigned with two tasks. The first is to provide the auditing service and to check the file's integrity that is stored in the cloud server by the client. The second is to provide messages to the client to update their secret key. The update messages are provided to client in different time periods. The strong key-revelation resilience auditing scheme for storage of cloud data makes the system efficient and secure [14].

In [10] the author proposes a idea to minimize the computational burden caused by user revocation. Their work depends on identity-base cryptography. The group manager makes sure that the removed user must not be capable of sending any data to cloud. In this scheme the non-removed users will not be able to re-sign any of the file sections of the revoked user. Their work achieves secure and efficient user revocation [10].

Table 3: Survey on issues addressed in cloud storage and cloud storage auditing.

Reference number	Problem addressed	Solution provided
[16]	Key Exposure problem	1. Third Party Auditor (TPA) updates the encrypted secret key. 2.Client can download the key from TPA.
[13]	Complex Key Management and checking the Data Integrity.	Identity-based RDIC (Remote Data Integrity Checking) protocol.
[14]	Key Exposure problem	1. Third Party Auditor (TPA) updates the secret key. (Here the secret key is not encrypted). 2. TPA checks the integrity of files.
[10]	Computation overhead caused by user revocation.	Identity-base Cryptography and auditing scheme.

III.BLOCKCHAIN

Blockchain is the collection of blocks which are linked together by cryptograph, hence they keep on growing. Figure 2 shows the collection of blocks in Blockchain. The blocks contain Cryptographic hash of the previous blocks, a timestamp and transaction data. Blockchain cannot be modified. It records the transactions taking place between different parties efficiently. In this section, some of the papers related to block chain technology in movement, management and storage of data in cloud are surveyed [23].

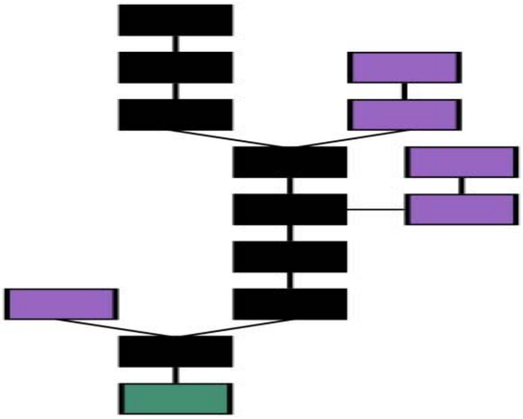

Figure 2: Diagram of Blockchain [source:https://en.wikipedia.org/wiki/Blockchain#/media/File:Blockchain.svg]

In [4] the author proposed a system for cloud trust a new technology called for cloud trust using a new technology called blockchain in which transparency is increased, depending on trusted third party's problem is reduced. Ethereum supports smart contracts which are used as an intermediate among different parties without the need of third party which is trusted. A cloud trust framework is proposed with the model of Belief and Recommendation with five degrees of recommendation. Vendor Threshold of trust is calculated where trust is based on evidence and experience. Smart contract is accessed by one Ethereum address which is public. A white list algorithm which uses key called customer address in structure of hash storage [4].

In [2] the author presents a system named Saranyu, in which smart contracts runs on ledger which is distributed, which is used for the management of tenant account and service account in data center of cloud computing, containing 4 services namely identity management, authentication, authorization and charging. Saranyu system is implemented on the Quorum blockchain system highly suitable for developing distributed cloud architectures. Saranyu is just like Ethereum. Quorum accounts are of two types – externally owned and smart contract. Saranyu is like Dapp based on blockchain and available on Quorum. Tenants establish accounts with *Saranyu*. Public/private key pair has public part which is used to identify the accounts for tenants and services. Services of Saranyu can also be done with other registered services and payment for services is paid to developers when used. Here tenants and services are made using contract accounts. Saranyu authenticates on every tenant logging into using private/public key of tenant. *Saranyu* represents delegation as a smart contract, including any quotas specifying the service attributes consumed maximum by the receiving member, charging schedules for the attributes of the service, and revokers who are allowed to suspend the delegation. Authorization request and grant operations are done in saranyu. After grant two times of operations are mentioned here they are *Authorization Grant Suspension and Revocation.* Payment processor is used when many charging credentials given by the tenants or services. Saranyu does not support crypto currency which is one of the settlements means [2].

In [5] the author uses ChainFS system which protects storage of cloud using blockchain, is a middleware system. ChainFS is implemented on Ethereum and S3Fs with Fuse based clients also cloud storage using Amazon S3 also performance is measured in the ChainFS system and also low overhead is demonstrated. ChainFS system comprises of a client, a server which is managed and hosted by untrusted cloud and blockchain. Fuse clients interact with remote parties in two planes. Read operations are carried after verifying using Merkle proof and then new root hash is used in place of local state generated before sending it. In ChainFS interaction between FUSE-blockchain is done having an intermediatary web_server process where the fuse client CURL request to webserver.SHA256 algorithm is used in implementing a hash function here. System Performance is checked after creation of the file and using the file read performance [5].

Table 4:Survey on cloud security issues using Blockchain

Referenc e number	**Problem solved**	**Techniques used**
[4]	Transparency increased, problem of depending on TTPs is reduced	White list policy Smart contract, Ethereum
[2]	Manage tenant and service accounts in data center	Quorum, smart contract
[5]	Preventing against forking attacks	Ethereum S3FS

IV.BLOCKCHAIN AND CLOUD COMPUTING

Cloud computing has many challenges and one of the key challenges of cloud computing is overcome by blockchain is cost. Cloud computing can be decentralized with the blockchain technology.

Even though cloud computing tend to be cheaper but when used with variety of elements it is quite expensive. Decentralizing eliminates the risk of data breaches. Blockchain enables to directly connect to massive GPU mining firms and leverage their computation power. Blockchain powered cloud solutions rely on idle computational power from a pool of providers includes individual computer users also. Blockchain storage accounts cannot be targeted or got easily. Even for a potential hacker it is very difficult to access large amount of data via blockchain because unlike traditional storage blockchain's data is spread out like a chain instead of putting together on one storage space.

V.IMPLEMENTATION

Our proposed system is developed for Healthcare systems. All data are transferred in file format within the groups, those files are encrypted using AES algorithm and integrity is maintained by MD5 or SHA algorithm. The MD5 or SHA algorithm is used to check for the modifications in the data being stored in the cloud storage. The particular user who makes modifications can be removed to have a secured data transfer and storage in cloud. In addition Blockchain improves the security issues in cloud computing.

VI.CONCLUSION

Cloud computing is considered to be the future of computing and storage technology. The works carried out using next generation technology like blockchain are surveyed in this paper. Considering these security issues we have proposed a model which increases the integrity of the data. The increase in connected devices and increase in computation is the need for cloud computing in now-a-days trend.

VII.REFERENCES

[1].Hongbing Cheng, ChunmingRong, ManyunQian, and Weihong Wang (2018), “Accountable Privacy-Preserving Mechanism For Cloud Computing Based On Identity-Based Encryption”, IEEE.

[2].SambitNayak, Nanjangud C Narendra, Anshu ,JamesKempf (2018), IEEE 11th International Conference on Cloud Computing, Saranyu: Using Smart Contracts and Blockchain for Cloud Tenant Management.

[3].Stephen S Kirkman and Richard Newman, (2018), Regular Paper: A Cloud Data Movement Policy Architecture Based on Smart Contracts and the Ethereum Blockchain IEEE International Conference on Cloud Engineering.

[4].Stephen S Kirkman,(2018) A Data Movement Policy Framework for Improving Trust in the Cloud Using Smart Contracts and Blockchains, IEEE International Conference on Cloud Engineering.

[5].QiwuZou, Yuzhe Tang, Ju Chen, Kai Li, Charles A. Kamhoua, Kevin Kwiat, Laurent Njilla, (2018),IEEE 11th International Conference on Cloud Computing ,*ChainFS: Blockchain-Secured Cloud Storage.*

[6].YindongChen, LipingLi, ZiranChen (2017),“ An Approach to Verifying Data Integrity for Cloud Storage”, IEEE.

[7].S.Rajeswari, R.Kalaiselvi, Proceedings of 2017 IEEE International Conference on Circuits and Systems (ICCS 2017), Survey of data and storage security in cloud computing

[8].Shivarajkumar Hiremath, Sanjeev Kunte,(2017),” A Novel Data Auditing Approach to Achieve Data Privacy and Data Integrity in Cloud Computing”, International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT).

[9].Akshay Arora,Abhirup Khanna, Anmol Rastogi, Amit Agarwal (2017), ”Cloud Security Ecosystem for Data Security and Privacy”, IEEE.

[10]. Yue Zhang, Jia Yu, RongHao, Cong Wang, Senior Member, IEEE and KuiRen, Fellow, IEEE (2017) “Enabling Efficient User Revocation in Identity-based Cloud Storage Auditing for Shared Big Data” , IEEE.

[11].Weiwei Kong, Yang Lei, Jing Ma (2017),”Data Security and Privacy Information Challenges in Cloud Computing”, International Conference on Intelligent Networking and Collaborative Systems, IEEE.

[12].WgCdr Nimi tKaura, LtCol Abhishek Lal, (2017),”Survey paper on cloud computing security”, IEEE.

[13].Yong Yu, Man Ho Au, Member, IEEE, Giuseppe Ateniese, Xinyi Huang, Willy Susilo, Yuanshun Dai, and Geyong Min(2017), “Identity-Based Remote Data Integrity Checking With Perfect Data Privacy Preserving for Cloud Storage”, IEEE

[14].Jia Yu, Huaqun Wang (2016) “Strong Key Exposure Resilient Auditing for Secure Cloud Storage”, IEEE.

[15].KamileNurSeviş, Ensar Şeker, “Survey on Data Integrity in Cloud”, (2016), IEEE 3rd International Conference on Cyber Security and Cloud Computing.

[16].Jia Yu, KuiRen, Senior Member, IEEE, and Cong Wang, Member, IEEE(2015),“Enabling Cloud Storage Auditing with Verifiable Outsourcing of Key Updates”,IEEE

[17].Tunisha Saxenal, Vaishali Chourey, 978-1-4799-3064-7/14/$31. 00©2014 IEEE,A Survey Paper on Cloud Security Issues and Challenges.

[18].Durga Priya G , Soma Prathibha,” Assuring Correctness for Securing Outsourced Data Repository in Cloud Environment”,(2014), IEEE International Conference on Advanced Communication Control and Computing Technologies (lCACCCT).

[19].Vijayalakshmi, R., &Prathibha, S. (2013).A novel approach for task scheduling in cloud. 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT).

[20].Ni Zhang, Di Liu, Yunyong Zhang. "A Research on Cloud Computing Security", 2013 International Conference on Information Technology and Applications, 2013

[21].Mell P. and Granc G., “The NIST Definition of Cloud Computing (Draft),” in Proceedings of the National Institute of Standards and Technology, Gaithersburg, pp. 6, 2011.

[22].D Carrell. "A Strategy for Deploying Secure Cloud-Based Natural Language Processing Systems for Applied Research Involving Clinical Text", 2011 44th Hawaii International Conference on System Sciences, 2011.

[23]. https://en.wikipedia.org/wiki/Blockchain