Cloud Security Issues and Blockchain Technology

Mr. Shaikh Rais F.
P.G. Student
Computer Engineering Dept.
S.N.D.C.O.E. Rc. Yeola
shaikhrails9@gmail.com

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.

1. 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. 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. 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. 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.

2. ARCHITECTURE OF CLOUD COMPUTING
Cloud architecture, the system architecture of the software systems involved in the delivery of cloud computing, comprises hardware and software designed by a cloud architect who typically works for a cloud integrator. It typically involves multiple cloud components communicating with each other over application, programming interfaces, usually web services. This closely resembles the UNIX philosophy of having multiple programs each doing one thing well and working together over universal. At the same time, the concept of utility computing became a focus of IT design and operations. Cloud computing takes the utility model to the next level. It’s a new and evolved form of utility computing in which many different types of resources (hardware, software, storage, communications, and so on) can be combined and recombined on the fly into the specific capabilities or services customers require.

Prof. Dhakane Vikas N.
Asst. Professor
Computer Engineering Dept.
S.N.D.C.O.E. Rc. Yeola
vikasdhakane@gmail.com

Resincap Journal of Science and Engineering
Volume 4, Issue 4, April 2020
ISSN: 2456-9976
no capital costs of any kind — and no hidden costs. Just a metered, per-use rate or a fixed subscription fee. Use only what you want, pay only for what you use.

3. CLOUD SECURITY ISSUES

3.1 Privacy Preservation In Cloud

In 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.

3.2 Data Integrity In Cloud

In this 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. In the author survey various researches about data integrity proofs for the cloud systems. Various approaches like Provably Data Possession (PDP), Proof of Irretrievability (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. In 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.

3.3 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 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 outsourcing key updates for auditing the cloud storage in addition with key revelation resilience. In the author proposed a new idea of Identity based RDIC (Remote Data Integrity Checking) protocol. The protocol makes use of key-holomorphic 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

4. BLOCKCHAIN

Blockchain can be defined as a decentralised and distributed digital ledger that is used to record transactions across many computers. In simple terms, we can consider any record within Blockchain technology as a document shared with a group of people (computers/servers that also known as blocks). The document is distributed instead of copied or transferred. This creates a decentralised distribution chain in a way and the involved record cannot be altered retroactively without the alteration of all subsequent blocks.

Fig No 2: Working of Blockchain

4.1 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 block chain’s data is spread out like a chain instead of putting together on one storage space.

5. APPLICATIONS

- **Blockchain in digital advertising:** In today’s world, one of the biggest problems in digital advertising is challenges such as domain fraud, bot traffic, lack of transparency and long payment models. Blockchain can provide solutions to these problems as the technology will only allow the right companies to succeed. It will decrease the number of bad players in the supply chain and minimizing the case of fraud and others.

- **Blockchain in cyber security:** The innovative cryptography feature of the Blockchain Technology will help in encrypting and verifying the data. In this manner, the data is less likely to be attacked or altered without authorization.

- **Blockchain in Forecasting:** The Blockchain technology is set to alter the complete methodology for research, consulting, analysis and forecasting. Most of the global distributed prediction markets are created with the help of online platforms.

- **Blockchain in cloud storage:** The distributed/decentralised security feature of Blockchain will make cloud storage more protected and robust against hacking as the data on a centralized server is exposed to hacking, loss of data, or human error.
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.

REFERENCES