# Cloud Blockchain Ensuring Data Integrity

Mr.Ashish Mittal[1], Ms.M.Sheetal[2]
[1,2]*Presidency College*

***Abstract -*** In today's world, the most important thing to any organization or company is its data, it's the most valuable asset which a company owns. Threats to data integrity can be deadly for any institution so as to protect that from attackers we are using the blockchain technology with the cloud. Blockchain is an emerging technology which has compelling properties about data integrity. Blockchain technology was invented in 2008 by Satoshi Nakamoto, yet today, no one knows who Satoshi Nakamoto is, whether an individual or a group of people. Since its existence, Blockchain has evolved into something very powerful technology. And by integrating it with Cloud we can secure the which usually gets compromised in the current scenarios where the owners of the data do not have any control over the fundamental aspects, like the physical storage of data and the control of its accesses.

## I. INTRODUCTION

As we're upgrading ourselves at a very high pace and converting all the human-assisted work to automation, we are relying more and more on data. On the other side, the vitality of data has made it a very appealing target for cyber-attacks. Attackers aim to exploit the fundamental CIA properties (Confidentiality, Integrity, Availability) that data should evince in order to be trusted.

The proposed technology can be termed as Cloud Blockchain as it is developed implementing cloud and blockchain together as a whole. The use of blockchain ensures integrity by storing distributed replicas of databases. The processes are first logged by the first-layer chain and then they are executed on the distributed database replicas. The first-layer blockchain is restricted and has one miner on each cloud. They rely on public/private key pair to achieve consensus through mining rotation consensus mechanism in which time is divided into rounds and a miner is elected as a leader. The leader then becomes an in-charge for receiving operations, signing them with the private key and broadcasting them to other miners. When all the miners have signed it, they add these operations to their local ledger and apply them to their local replica. The second layer blockchain interaction is realized via the anchoring technique. It is a settled operation that allows association of a specific part (hashes) of the first-layer to the second-layer. This data in the second-layer is stored as an irreversible transaction which can be very useful as forensic evidence for verifying the integrity of the data stored in the initial layer of the blockchain. If the data is present only in the first-layer, an attacker with required effort may be able to break in gaining access to all the replicas in the first-layer, but as the hashes will be stored in the second-layer as irreversible operation, he is needed to manipulate the values on both layers, thus the data integrity measure would be higher.

## II. BLOCKCHAIN

Blockchain is a disruptive technology we came across in 2008, initially used as a public ledger for Bitcoin cryptocurrency which was composed of consecutive chained blocks containing records, which were replicated on the nodes of p2p network. These nodes witnessed transactions occurred in pseudonyms. And transactions can feature any cryptocurrency like, e.g., Bitcoin, Litecoin, Ethereum or any other kind. The transactions are collectively enclosed in a blockchain is carried out in a decentralised network composed of miners who apply methods like opportune block construction, to achieve consensus among all the miners on the new blocks. Permission less networks include Bitcoin, i.e., any one can be a miner on Bitcoin network. If a network is applied with authentication and authorization layer for miners, then it becomes permissioned. Miners do the job of mining which consists of computationally intensive task of hashing which is regulated according to the blockchain difficulty, the mean time taken by the miners to complete a task and create a new block. Once a node creates a new block, it gets broadcasted to all other miners, that is said to be the newest block and they start mining other blocks to be appended.

When a block is a part of blockchain, all the miners have verified its contents, and it is practically persistent and correct unless an attacker who has the majority of mining powers than the miners and is able to create a fork of chain). Taking an assumption that the majority of the miners are legit, the probability of fork will be $O(2^{-n})$. This gives users high confidence on the network for their transactions. Although this network has some drawbacks too: performance. Due to the process of broadcasting latencies of the blocks on the network, we face major delays on the confirmations of the transactions. In Fact, each block stored in the chain has high confirmation latency of average of 10 minutes.

## III. AN EFFECTIVE BLOCKCHAIN-BASED CLOUD

Blockchain technology is precisely exploited to maintain the integrity of the databases. By its usage, we are able to ensure integrity as well as fully distributed control of the data in database. The proposed model is feasible for the operations under cloud data distribution providing prevention from attackers and decreases all the chances of data theft or loss. By integrating the technologies like cloud and blockchain, we can mould something new which can be even better as the two separately. The cloud blockchain network is governed by the three cloud members who issue operations through the database interface. First the

operations make their way into the chain via suitable evidences from the first-layer, and then they are executed into the network chain nodes. In specific words, anyone cannot enter the first-layer blockchain as it requires permission to become a miner and on each layer one miner is present. The miners make use of the public/private key to sign the messages and maintain consensus. Through this model, we look forward to achieve maximum security and prevent data theft. In simple words, any registered user can upload their important files or data onto the network and get a respective key against it. Once the data gets through, it reaches the miners and after they verify that it's a legit transaction and the sender is legit, they authorize it and then that data is broken down into smaller pieces and is sent to all the nodes across the chain by broadcast. In current scenarios, the data that we upload to cloud is stored in a centralized server and is prone to theft, but in this proposed model, at every node (miner), a small chunk of data is stored so that even if some attacker manages to break-into the network chain, he will only be getting a tiny part of the data uploaded by the user. Also, all the data stored in our network is encrypted by advanced secure algorithms which are very hard to break. Even if the attacker knows how to decrypt the data, he has to gain access to all the nodes present in the network, combine it and then decode the entire dataset which is practically not possible. This technology can be used to store any data which might be valuable to any organization or by any individual trying to remember something very important. The users get a key to their locker (uploaded data) through which they can retrieve it back to their system in one piece. The key can be anything based on the value of the data and the user like a hashed value, secure pin, biometrics etc.

## IV. CONCLUSION

In this paper, we discerned the current Cloud and blockchain technologies, their working and drawbacks and we can use them both combined. By integrating Cloud and Blockchain, a secure network can be casted which ensures data integrity, stability and prevent all the malicious activities which are performed by attackers. This work can further be examined by a working prototype to verify the effectiveness of the solution, as far as achievable latency and throughput are concerned. On the path of its complete deployment, there are parts which needs to be stressed like, violation of a single miner can affect the network. To overcome these problems, the system needs to have an algorithm which is resistive and fault-tolerant that allows combination of availability and integrity. Also, the Cloud-Blockchain network will be feasible enough to realize stable blocks in network chains to make itself a reliable storage option and will lead to adoption by all the major corporations and the individual users.