Cyber Security in Blockchain Based System

– **Vinod Kumar Mishra**,
Blockchain Consultant with Natanedu & VegoilChain
vkumar201415@gmail.com
Linkedin- https://www.linkedin.com/in/vinodkumarmishra

The technological advancement in the last 3 decades has impacted almost all the industries like Banking, travel, insurance, supply chain, medical, communication, etc. just to name a few. All the advancements have made the life of human beings more comfortable

But, an equivalent amount of risks is also prevalent along with easy accessibility to products and services. Every individual is generally tagged to a specific user credential which discretely identifies and authenticates the individual the access of a product or service. Few statistics related to the number of user actions and transactions in major web-based product or services is given below. A large amount of data is generated on the internet every day.

- Google processes around 40,000 search queries in one second which is around 3.5 billion searches per day.
- Amazon processes around 306 transactions per second which translates to about 26M transactions per day.
- More than 4 million blogs are posted on the internet daily.
- More than 500 tweets are shared every day.
- There are more than 4 billion internet users in the world.

There are different kinds of data which is linked to the transactions for various services. Some of the data is highly confidential. Imagine a user credential of a bank being stolen on the network in which the user is authenticating in the application. The impact of such data and security breaches is irreversible and huge. Some of the significant security breaches in recent times is mentioned below:

- In Sept 2016 around 3 billion user accounts of Yahoo was hacked.
- Information of around 145 million users of Equifax (*one of the largest credit reporting agency in the US) was leaked.
- Accounts and data of more than 20 years for 412 million accounts of Adult friend finder was hacked.

Most of the security breaches have occurred since the data, and the credentials existed in a single centralised server for all the users. The data in the server is exposed when the hacker gets access to the server along with all the credentials. Another common reason for most of the security breaches is human error or the poor security of data/ credentials.

Blockchain technology seems to be a better choice to prevent cyber-attacks which is prevalent in solutions build on a centralised architecture. Blockchain promises to protect the data from manipulation or tamper by its inherent decentralised nature in the peer to peer network. All changes in the assets are recorded in the form of transactions which is protected by a complex hashing algorithm. Also, there is no single server containing all the data and the credentials with all nodes maintaining a copy of the record in the network. But the distributed decentralised systems are also vulnerable to multiple risks and attacks. The public blockchain based systems have also faced threats and attacks and have eventually recovered.

Characteristics of Blockchain in Cyber security

- **Data Integrity:**

Blockchain can help in preventing tamper and manipulation of data and ensure data integrity. Many techniques are already used like hashing, encryption and digital signature. But, the inherent characteristics of Blockchain like sequential hashing and asymmetric cryptography provides immutability and tamperproof provenance for data integrity.

- **Non repudiation:**

The cyber security property of non-

repudiation which means that the validity of something cannot be denied by anyone. It is ensured by Blockchain by the use of cryptographic timestamp and digital signature embedded in every transaction in the linear chain of records. The chain of records in the distributed network is shared among all the nodes and is cryptographically secured with automatic audit trials.

- **Prevention of DDOS attack:**

The distributed denial of service is one of the most common cyber attack in traditional systems. The traditional Domain Name Services (DNS) which relies on caching was attacked in 2016 which cut off the access to major websites like twitter, Paypal, Netflix, etc. The decentralized and peer to peer characteristics of Blockchain based system makes it difficult to attack multiple servers at the same point.

- **Secured storage:**

The data which is stored in the Blockchain ledger is replicated on all the nodes in the network which makes it very difficult for the hacker to change it simultaneously on all the systems. Any tamper in the block will change the root hash of the block which is referred in all the subsequent blocks.

Cyber security attacks in public blockchain based systems

But, the Blockchain based systems are also prone to uncertain dangers due to its decentralised distributed nature. The risk team needs to react and respond very effectively in minimum time when the blockchain based systems are attacked. The blockchain based public networks have been attacked by different kinds of cyber-attacks like DAO attack, Liveness attack, eclipse attack and distributed denial of service attack.

- **DAO Attack**

The Decentralized autonomous organisation smart contract was released on 28th May 2016 and it collected around $150 million in about 20 days. It was attacked by the attackers when a vulnerability in the smart contract was discovered. The attack known as re-entrancy vulnerability was exposed to the decentralised smart contract. More precisely the attacker deployed its smart contract with a function withdraw () into the DAO smart contract code. The DAO code would invoke the withdraw () function every time the DAO contract executed, stealing more than 6-million US dollars.

- **Liveness attack**

The Bitcoin and Ethereum network have been attacked with liveness attack. The liveness attack is aimed to prevent the confirmation of transactions. It is divided into 3 phases with the group of miners colliding in the preparation phase and storing a particular transaction in a privately held block. The attacker will propose the block with the specific transaction to create a separate chain with more loyal miners. The attacker will again select a transaction thus ensuring denial of transaction validation for selected transactions.

- **Eclipse attack**

Eclipse attack is a form of cyber-attack in which the attacker takes control of all incoming and outgoing requests of a node, thus isolating the node from the entire Blockchain network. These types of attackers utilise the computational power of the node and increase its stake on the network. It also demotivates the node since no activities are recorded on the main network. Eclipse attack leads to other attacks like Selfish mining, Engineering block races (Which is wasting the computational power on an orphan block, etc.), etc.

- **Distributed Denial of Service Attack**

The Bitcoin network was struck in March 2016 when a large pool of transactions with a little higher transaction fee flooded the network. If an attacker generates multiple malicious transactions with a higher transaction fee, the miners will pick up the transactions and waste their computational energy in verifying these transactions. The valid transactions will have to wait for a longer time to be validated by the miners in the public network.

The recent advancements in the Blockchain adoption is more inclined towards building permissioned private blockchain for the enterprises. The systems will exist in the enterprise networks with limited access to the participants. The benefits of Blockchain can be achieved with the multiple parties with different access control in the network. The following considerations should be addressed while designing a private permissioned blockchain based system.

Security considerations in Permissioned Private Blockchain network

The security considerations while creating a private permissioned blockchain network are discussed briefly below:

- **Access Control:**It is a security technique that can be used to regulate who or what can view or use resources in a computing environment. (i.e. Restricting individual for specific areas.)
- **Hardening of Server:** It means disabling unnecessary services, software, users, etc. and changing

default passwords which are present in the system which causes security risks. Points to Keep in mind during Hardening of Servers in Blockchain:

- **Network Security:** It consists of the policies and practices adopted to prevent and monitor unauthorised access, modification, misuse or denial of service of a computer network and network-accessible resources.

- **Permission Management:** It allows direct control over the extent to which the permission is granted. Privileges like SEND, RECEIVE, ACTIVATE, MINE should be thoroughly checked while giving. Also, the method to add/delete users should involve multiple parties.

- **Regulating Security Parameters:** Parameters like the mining difficulty and diversity of miners or validators in the network should be ensured. Also, the time interval between the creation of new blocks should be less.

- **Secure Backing up of Keys:** The Node should be backed up in a distributed environment with a real-time image of the disk as a backup to ensure that the node is running in the network.

- **Consensus Mechanism:** The efficiency of the permissioned private blockchain is dependent on the active selection and use of consensus protocols.

The design of the Blockchain based system should also be able to protect itself against future cyber-attacks. Blockchain cryptography is subject to change over time. Cryptography applied to a given block must be correctly identified. Otherwise, relying parties may lose their ability to gain assurance in the integrity and authenticity of stored content, and risk loss of access to any encrypted or tokenised data related to land. The cryptographic algorithms which are used today need to be updated with time because of the:

- Increased computing power can attack the cryptographic systems
- The emergence of better crypto analysis tools
- The advent of new technologies such as Quantum computing

References:

https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1093&context=msia_etds

https://finance.yahoo.com/news/worst-cyber-attacks-past-10-202226243.html

Vinod Kumar Mishra has around 2 years experience as Freelancer Consultant in Blockchain and Cyber Security. He is presently working as Blockchain Consultant with Natanedu & VegoilChain. His qualifications include B. Tech in Computer Science and Engineering (C.S.E) and Bachelor of Laws (L.L.B). He has Completed multiple certifications in Blockchain including ' Introduction to Digital Currencies' from University of Nicosia, 'Blockchain for Business - An Introduction to Hyperledger Technologies' from Linux Foundation, ' IBM Blockchain Foundation Developer' and ' IBM Blockchain Essentials' from IBM , Certified Blockchain Expert (CBE) from Blockchain Council and ConsenSys. He has also completed multiple certifications in Cyber Security from Asian School of Cyber Laws. His contact details are as under:

vkumar201415@gmail.com

Linkedin- https://www.linkedin.com/in/vinodkumarmishra