5.4 Blockchain

Blockchain is a shared, decentralized, and digital ledger that records transactions in the form of blocks. This ledger helps to store information transparently due to its property of immutability and access to allowed members only.

Key Blockchain Features:

1. Distributed shared ledger.
2. Immutable records.
3. Decentralized consensus mechanisms.
4. Smart contracts.
5. Cryptographic key pair.
6. Identity and access management.

Possible Blockchain Use Cases For Cybersecurity

1. **IoT security:** With the increasing application of AI and IoT, the security of data and systems from hackers has always been a major concern. Usage of Blockchain for improved security by using device-to-device encryption to secure communication, key management techniques, and authentication is a potential use case to maintain cybersecurity in the IoT system.
2. **The integrity of software downloads:** Blockchain can be utilized to verify updates and installers to prevent malicious software from infecting the devices. Here, hashes are recorded in the blockchain and new software identities can be compared to the hashes to verify the integrity of the downloads.
3. **Data transmission protection:** By using encryption, the data in transit will be protected from unauthorized access.
4. **Decentralized storage of critical data:** With the exponentially increasing data generated every day, blockchain-based storage solutions help achieve decentralized storage thus protecting digital information.
5. **Mitigating DDoS Attacks:** One of the most popular cyberattacks today is DDoS attacks where hackers aim to generate a flood of Internet traffic and thus disrupt the flow of services. The properties of immutability and cryptography help Blockchain prove to be an effective solution for these attacks.

6. **DNS security:** The Domain Name System (DNS) is similar to a public directory that links domain names to their IP addresses. Over time, hackers have tried to access the DNS and exploit these links thus crashing sites. Due to Blockchain's properties of immutability and decentralized systems, the DNS can be stored with enhanced security.

Application of Blockchain in Cybersecurity

In cybersecurity, the CIA triad model acts as a reference to assess the security model of an organization. The triad consists of-

1. **Confidentiality**
2. **Integrity**
3. **Availability**

Blockchain helps us ensure all these policies are satisfied.

1. Confidentiality: It means to ensure that only interested and authorized parties access the appropriate data. Full encryption of blockchain data ensures that the data will not be accessible by unauthorized parties while flowing through untrusted networks. Security measures such as access controls should be implemented directly at the application level so as to prevent attacks from within the network. Blockchain can provide advanced security controls by using public key infrastructure to authenticate parties and encrypt their communication. However backup storage of private keys in secondary storage poses theft of private keys as a high risk. To prevent this, key management procedures such as IETF or RFC and cryptographic algorithms based on integer factorization problems should be implemented.

2. Integrity: Blockchains built-in characteristics of immutability and traceability help organizations ensure data integrity. Consensus model protocols can further help organizations to implement mechanisms to prevent and control ledger splitting in the event of a 51% cyber control attack. In Blockchain, with every new iteration, the previous state of the system is stored thus providing a fully traceable history log. Smart contracts can be used to verify and enforce rules between parties preventing miners from mining blocks of data.

3. Availability: In recent times, cyberattacks attempting to impact technology services availability are on the surge with DDoSs being the most common types of attacks. However, in blockchain-based systems, DDoS attacks are costly as the attacker attempts to overpower the network with a great number of small transactions. Blockchains have no single point of failure which decreases the chances of IP-based DDoS attacks disrupting the normal operation. Data remains available through various nodes and thus full copies of the ledger can be accessed at all times. The combination of multiple nodes and distributed operation makes the platforms and

systems resilient.

Pros of Using Blockchain in Cybersecurity

1. **User confidentiality:** The public key cryptography in a Blockchain network helps maintain the confidentiality of the users.
2. **Data transparency and traceability:** A history of all these transactions is maintained and thus can be traced anytime. The transactions data is digitally signed by members of the Blockchain network thus maintaining transparency.
3. **Secure data storage and processing:** Blockchain's major feature of immutability and records of any changes to the data help store the data in a safe and secure manner.
4. **No single point failures:** Blockchain systems are decentralized and thus a single node failure doesn't affect the entire network. Thus even during DDoS attacks, the system is not compromised due to the maintenance of multiple copies of ledgers. This advantage is not possible for Private blockchains.
5. **Safe data transfers:** The Public Key Infrastructure (PKI) in Blockchain maintains authentication during data transfers. Smart contracts help with the automatic execution of agreements between two parties during a transfer.

Cons of Using Blockchain in Cybersecurity

1. **Reliance on private keys:** Blockchains rely heavily on Private Keys for encryption of data but these private keys cannot be recovered once lost. This may lead to losing access to encrypted data forever.
2. **Adaptability and scalability challenges:** Blockchain networks have preset block volume and limits to transactions per second so it becomes very important to check the scalability of the network. Integrating Blockchain technology requires a complete replacement of the current systems and thus companies may face difficulties in doing so.
3. **High operating costs:** Blockchain requires high computing power and storage capabilities. This leads to higher costs as compared to non-Blockchain applications.
4. **Lack of governance:** Blockchain concepts aren't regulated globally yet. Regulations and frameworks need to be developed in order to maintain governance in Blockchain applications.
5. **Blockchain literacy:** Learning Blockchain technology requires a profound knowledge of various development, programming languages, and other tools. Thus in spite of numerous applications of Blockchain Technology, enough Blockchain developers are not available in the present scenario.

Real-Life Application Examples

Following are some prominent examples where Blockchain is used for Cybersecurity:

1. **Barclays (London, England), Traditional Banking:** Barclays have filed a patent to use blockchain to enhance security in fund transfers. It aims to stabilize cryptocurrency transfers by using Distributed Ledger Technology (DLT). Thus, blockchain helps the bank store customer information on a secure blockchain.
2. **CISCO (San Jose, California), IoT:** Cisco plans to use blockchain to secure IoT devices as ledger technology eliminates single point of failure and encryption helps secure data.
3. **Coinbase (San Francisco, California), Cryptocurrencies:** Coinbase uses encryption to store wallets and passwords in a secure database. It also undergoes background checks on employees to ensure that their crypto is secured.
4. **Australian Government (Canberra, Australia):** The Australian government has plans to develop a cybersecurity network based on DLT. The government has also partnered with IBM to secure the storage of government documents with the creation of a blockchain ecosystem.
5. **Philips Healthcare (Andover, Massachusetts), Healthcare:** Philips Healthcare has partnered with hospitals all over the world to create a healthcare ecosystem using blockchain and AI. This ecosystem will help discover and analyze various operational, administrative, and medical data.
6. **Chinese Military (Beijing, China), Defense and Military:** China's government and the military are attempting to secure vital government and military information, intelligence information using blockchain cybersecurity.
7. **Founders Bank (Valletta, Malta), Cryptocurrencies:** They aim to be the world's first decentralized bank thus being owned by the buyers and not any central authority. Concepts such as encryption and distributed ledgers will be used to store and secure users' cryptocurrencies.

Blockchain networks can differ in who can participate and who has access to the data. Networks are typically labeled as either public or private, which describes who is allowed to participate, and permissioned or permissionless, which describes how participants gain access to the network.

Publicandprivateblockchains

Public blockchain networks typically allow anyone to join and for participants to remain anonymous. A public blockchain uses internet-connected computers to validate transactions and achieve consensus. Bitcoin is probably the most well-known example of a public blockchain, and it achieves consensus through "bitcoin mining." Computers on the bitcoin network, or

“miners,” try to solve a complex cryptographic problem to create proof of work and thereby validate the transaction. Outside of public keys, there are few identity and access controls in this type of network.

Private blockchains use identity to confirm membership and access privileges and typically only permit known organizations to join. Together, the organizations form a private, members- only "business network." A private blockchain in a permissioned network achieves consensus through a process called "selective endorsement," where known users verify the transactions. Only members with special access and permissions can maintain the transaction ledger. This network type requires more identity and access controls.

When building a blockchain application, it's critical to assess which type of network will best suit your business goals. Private and permissioned networks can be tightly controlled and preferable for compliance and regulatory reasons. However, public and permissionless networks can achieve greater decentralization and distribution.

Public blockchains are public, and anyone can join them and validate transactions.

Private blockchains are restricted and usually limited to business networks. A single entity, or consortium, controls membership.

Permissionless blockchains have no restrictions on processors.

Permissioned blockchains are limited to a select set of users who are granted identities using certificates.