When Intrusion Detection meets Blockchain technology

2019.03.19
SeoulTech
Mikail Mohammed Salim

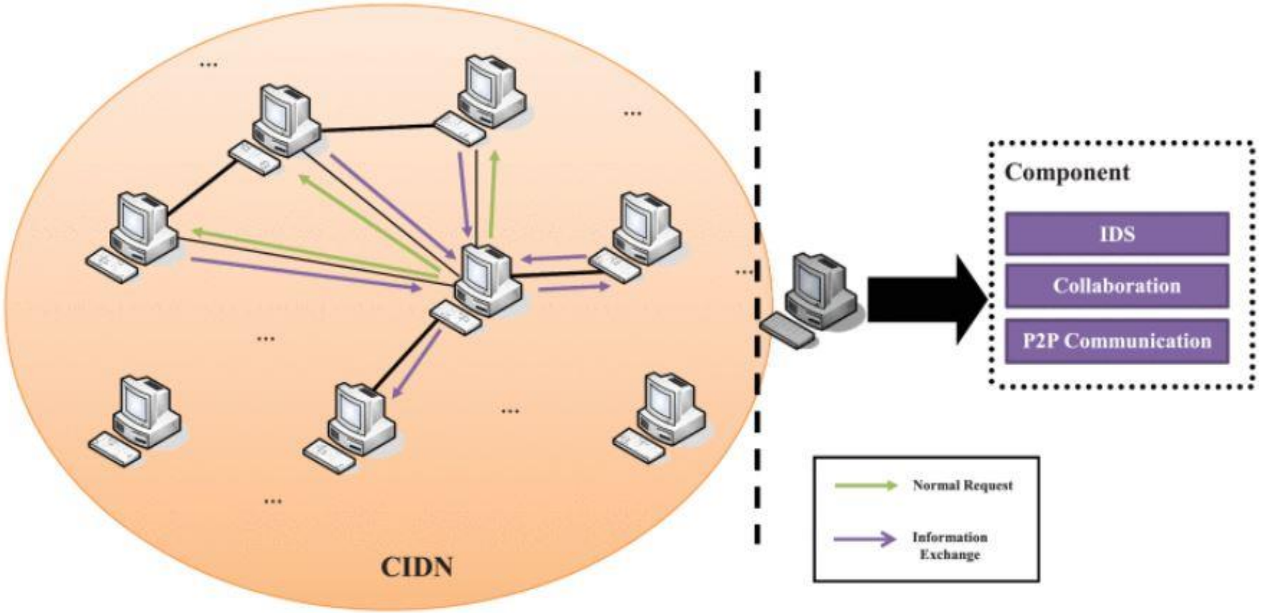
Introduction

- Intrusion detection systems are responsible for detecting anomalous traffic within a network.
- Single IDS are unable to defend against all cyber threats and collaborative IDS system are the solution.
- Traditionally a central server is used to support collaborative intrusion detection systems. They are however susceptible to cyber attacks and are the weakest link themselves.
- Blockchain is described as a means of sharing private data such as financial records without the need for a trusting 3rd party.
- A blockchain is a growing list of records called blocks. Data in a block cannot be altered without modifying data in other blocks. To successfully modify, an attacker needs to control majority of the blocks, which is very difficult.
- This paper aims to combine blockchain technology with intrusion detection systems.

Intrusion Detection

- Intrusion detection system is an application that enables the process of detecting malicious intrusion attempts on the network. It performs two main functions, a) Information recording, and b) Alert generation.
- Collaborative intrusion detection systems combine both Host and network based detection system which strengthens the detection system and provides a more thorough protection.
- Intrusion detection systems are known to employ either
  a. Signature based detection approach – Effective in detecting known exploits but are ineffective in detecting ground zero threats or unknown threats. It can be easily bypassed by an attacker.
  b. Anomaly based detection approach - Possess the ability to detect unknown attacks. Establishes a normal profile by monitoring the system or network. Identifies any deviation in behavior from the established normal profiles. Machine Learning is often used in anomaly based detection approaches.

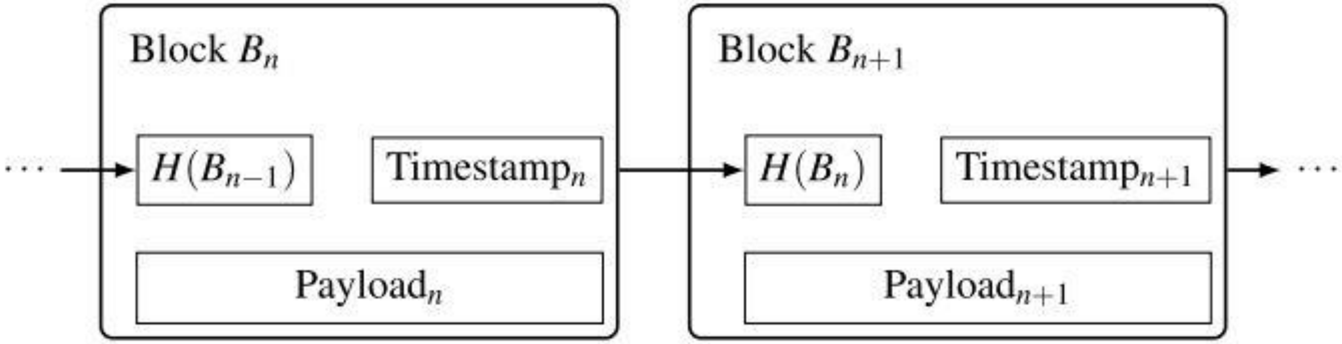
Collaborative intrusion detection architecture



A typical architecture of a collaborative intrusion detection architecture

- A single node, Node A can exchange required information with nodes B,C and D.
- A node comprises of 3 modules,
  a. IDS - IDS module can perform the intrusion detection functions including monitoring network traffic and recording events.
  b. Collaboration - The collaboration component is responsible for assisting a node to exchange required data with other nodes and conduct certain operations like trust computation.
  c. P2P communication - P2P communication component aims to help establish physical connection with other IDS nodes.

Background on Blockchain Technology



Schematic view of Blockchain

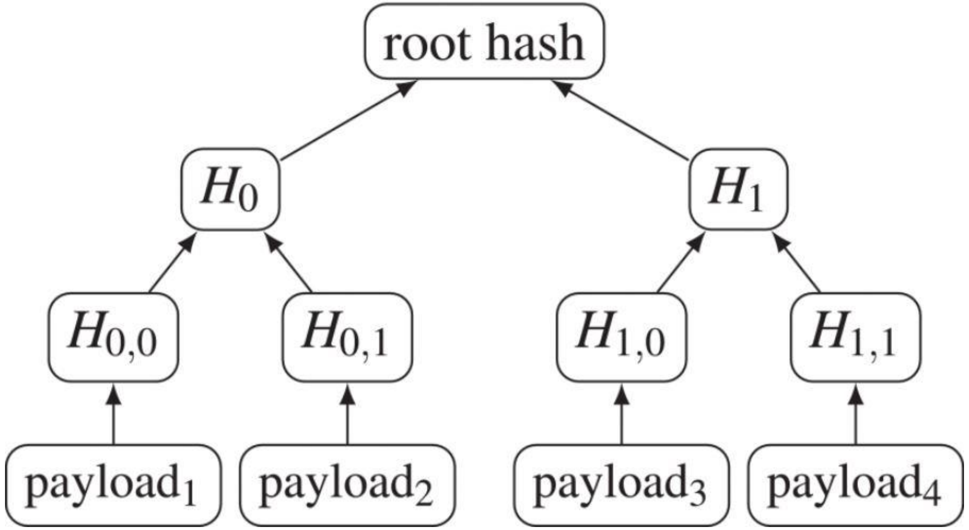
- The basic functionality provided by a blockchain is a cryptographically secure mechanism for obtaining a publicly verifiable and immutable sequence of records (referred to as blocks) chronologically ordered by discrete time stamps.

- Blockchain cryptography security is based on the following concepts,

  a. **Preimage resistance** - Preimage resistance refers to the hash function's ability to be non-reversible. Imagine if you could generate the likeness of a whole person from their fingerprint, it can be very dangerous.

  b. **Second Preimage resistance -** Second preimage resistance refers to a given hash function's ability to be unique. Forensic fingerprinting would be a gross waste of time if any number of individuals could share the same fingerprint

Background on Blockchain Technology



Compact representation of a Merkle Tree

- A Merkle tree summarizes all the transactions in a block by producing a digital fingerprint of the entire set of transactions, thereby enabling a user to verify whether or not a transaction is included in a block.
- Merkle trees are created by repeatedly hashing pairs of nodes until there is only one hash left (this hash is called the Root Hash, or the Merkle Root). They are constructed from the bottom up, from hashes of individual transactions (known as Transaction IDs).

Background on Blockchain Technology

- Blockchains are typically classified into two categories,
  a. **Permissionless blockchain** – Cryptocurrencies such as Bitcoin and Ethereum allow entities to freely participate as both readers and writers. They can read or analyze data record contents and take part in the consensus process as writers.
  b. **Permissioned blockchain** – A central entity has the decision making ability to allow access or the ability to transact with the network. It may also delegate this decision making ability to a group of users resulting in a consortium blockchain. The difference between a public and a private permissioned blockchain is that a public one allows reading the transaction data while a private restricts both read and write access to the public.
- Blockchain consensus protocols are essential to establish a trust between entities or participants. Both Private Permissioned and Permissionless blockchains use consensus protocols to verify transactions.
- Following are three consensus algorithms that help address the problem of universal lack of trust between different participants.
  a. Proof of Work.
  b. Proof of Stake.
  c. Proof of elapsed time.

Background on Blockchain Technology

- Applications of Blockchains,

1. **Cryptocurrency** - Blockchain based digital cash system ingeniously combines the distributed consensus protocol, point-to-point communication techniques to prevent double-spend attacks and remove the need for a trusted party. Cryptocurrency economy is by now the most popular application of blockchain technology and also the most controversial one since it enables a multibillion-dollar global trading of market essentially anonymous transactions without government control.

2. **Smart Contracts** - A smart contract is a computer code running on top of a blockchain containing a set of rules under which the parties to that smart contract agree to interact with each other. If and when the pre-defined rules are met, the agreement is automatically enforced. The smart contract code facilitates, verifies, and enforces the negotiation or performance of an agreement or transaction.

Blockchain based Intrusion Detection

- Challenges in Collaborative Intrusion Detection –

  a. **Data Sharing** - Data sharing is a major issue for a collaborative detection system, as it is not a trivial task to let all participating parties trust each other. Due to privacy concerns, some parties are not willing to share the data. Without enough data, it is unable to optimize detection algorithms and to build a robust model for identifying suspicious events.

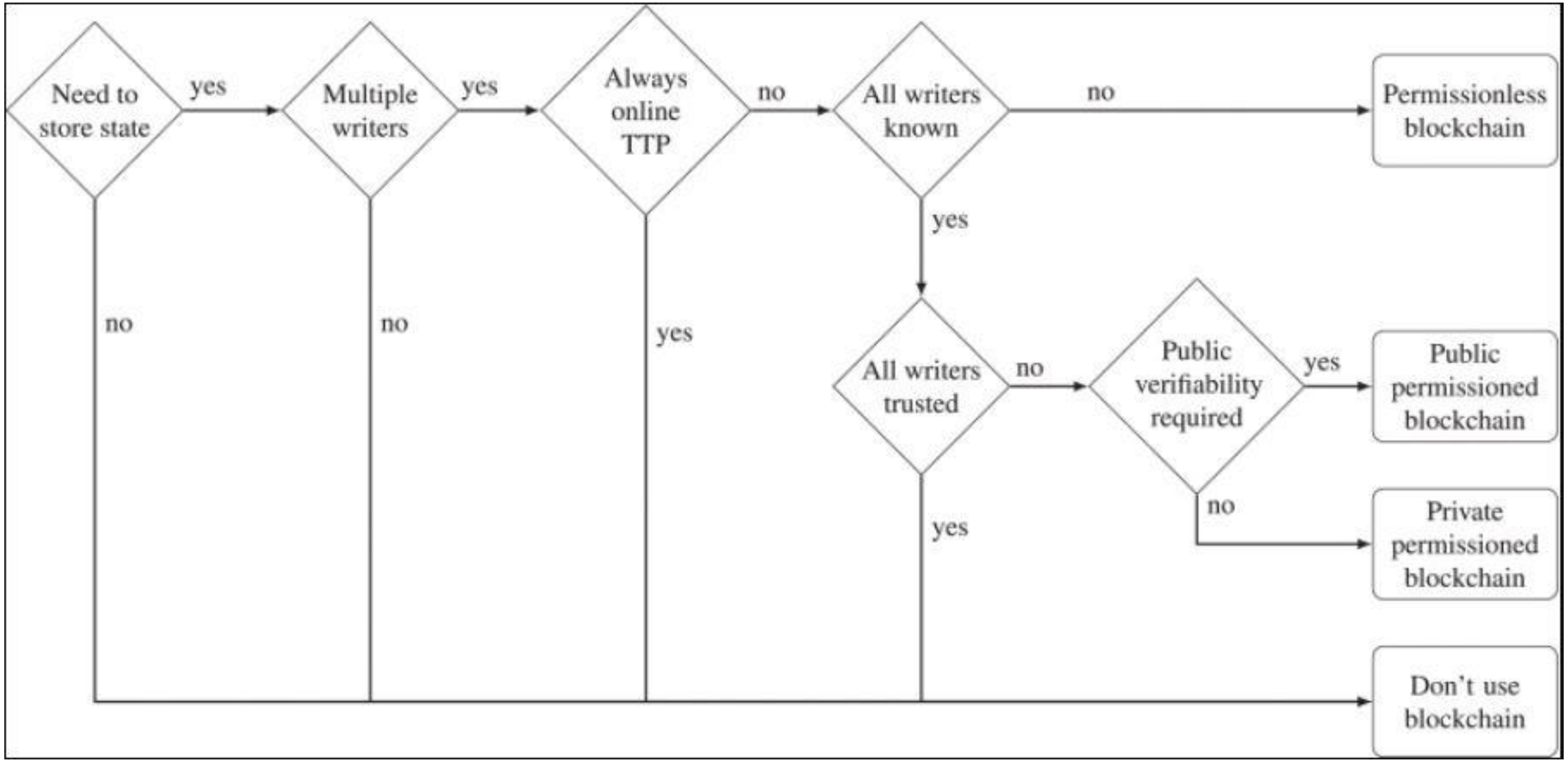
  b. **Trust Management** – Collaborative Intrusion Detection Networks and Systems are vulnerable to attacks where intruders have access to the network. A central server monitors and gathers traffic and behavioral data from different nodes to determine the trust value of the node. However, as the organization grows, the trust factor will decrease as the Intrusion Detection System has to monitor a greater number of nodes and determine which node is trustworthy. A central server may get compromised.

Blockchain based Intrusion Detection

- Blockchain based solutions addressing the challenges of Collaborative Intrusion Detection systems
  - **Data Sharing** – Data sharing between two entities can be treated as a series of transactions. Parties can come to a data sharing agreement to not share each other's data and record it as a transaction in a blockchain block. The transaction is public and cannot be altered.

    Another solution using blockchain between collaborating parties is where Party A wants to verify the performance of their designed Machine learning algorithm. They can send the algorithm as a blockchain transaction to Party B where it will be locally run on available data and the results sent back to Party A. The data belonging to Party B remains with them and data privacy is maintained.
  - **Trust Computation** – To establish trust in a network with its nodes, alert exchange is required to help detect any anomalous traffic. A solution by a researcher, Alexopoulos, proposed that each alert generated by a node should be treated as a transaction. These transactions are recorded and stored with each node in the network. All collaborative nodes adopt a consensus algorithm to guarantee the validity of the transactions before putting them in a block. Recorded transactions in a block ensure that the generated alerts are tamper resistant.

Blockchain based Intrusion Detection



Schematic decision diagram to determine whether a blockchain (and if yes, which type of blockchain) to use in which application scenario.

Challenges and Future Trends

- Challenges pertaining to Intrusion Detection Systems.
  1. **Overhead traffic with limited handling capability**– In a heavy network traffic environment, overhead packets can greatly degrade the performance of a detection system. If the traffic exceeds the maximum processing capability of an IDS, a large amount of network packets have to be discarded.
  2. **Limited Signature coverage-** The detection capability of signature-based detection depends heavily on the available signatures. Knowledge of known attack signatures are usually limited and unable to cover all known attacks and exploits
  3. **Inaccurate Profile Establishment**– For anomaly-based detection, it is difficult to build an accurate normal profile due to the dynamic nature of traffic. More specifically, an anomaly-based IDS often leverages machine learning techniques to build a profile. However, training data, especially labelled attack data, is very limited in practice, resulting in an inaccurate machine learning classifier.
  4. **Massive False Alerts-** It is very important for an IDS to generate accurate alerts to notify security administrators about network anomalies. However, false alarms are a big challenge during detection because of immature signatures and inaccurate profiles, which may significantly degrade the detection performance and increase the workload of security analysts. For instance, a large company may generate more than 10,000 false alarms each day.

Challenges and Future Trends

Challenges pertaining to Blockchain Technology-

1. **Energy and Cost**– High energy costs are a concern in a growing blockchain network.
2. **Security and Privacy-** Many existing blockchain-related applications require smart transactions and contracts to be linked to known identities, which raise the privacy and security concerns of the data stored on the shared ledger. Moreover, blockchain technology itself could be an attractive target for cyber-criminals, and thus suffer from various attacks like distributed denial-of-service attacks (DDoS).
3. **Latency and Complexity**– Due to the distributed nature, blockchain-based transactions may spend several hours to finish until all parties update their corresponding ledgers. This latency would create much uncertainty for transaction participants and open a hole for cyber-criminals.
4. **Awareness and Adoption-** One of the major challenges regarding blockchain technology is the lack of awareness and adoption. For example, many people are short of understanding of how it works. The future development of blockchain depends upon how many parties adopting the technology, but now it is still a question.
5. **Regulations and Management-** Regulations imposed are often behind existing advanced technologies Bitcoin cryptocurrency is an example of blockchain technology which has bypassed existing regulations for better efficiency. However, blockchain applications are expected to work within regulations

Challenges and Future Trends

Future Directions-

1. **Data sharing**– Blockchain is suitable for recording data as transactions which offers greater security than other networks. Data management is a big issue among collaborative intrusion detection systems, the evolving blockchain technology has the potential to improve performance by enforcing trust and data privacy between parties.
2. **Alert exchange-** We discussed the research work done by Alexopoulos who introduced how to use blockchains to secure the alerts generated by various nodes and ensure only truthful alerts would be exchanged. Due to the lack of real system applications, it is an interesting and important direction for future research studies.
3. **Trust computation**– Some collaborative detection approaches utilize alerts to evaluate the trustiness of others, blockchains can thus provide a solution to enhance the process of trust computation.

Opinions on implementing Blockchain technology for Intrusion detection systems

1. **Accurate data sharing** – Intrusion detection systems require sharing of accurate data between organizations for detection of malicious traffic in anomaly based detection methods. Blockchain can be used to help make sure the data entered as a transaction remains unaltered or tamper resistant. Permissioned private blockchains will be ideal for such data sharing.
2. **Data security** – Data stored in blocks cannot be altered by foreign intrusion. Transactions approved are stored in other blocks which verify the validity of any malicious information injected by an attacker. Intrusion Detection Systems rely heavily on unaltered data received from the network to successfully prevent attacks.
3. **Latency issues**– Blockchain suffers from the problem of slow approval of transactions. For example, Bitcoin and Ethereum based blockchain process only 7 and 15 transactions per second, respectively. The delay caused by new data captured from nodes to be recorded as a transaction can leave the intrusion detection system to respond slowly. Blockchain may not be the best solution for intrusion detection systems.

Proposal

1. A custom built private permissioned blockchain network is essential for an intrusion detection system. They will offer the valuable existing advantages of maintaining data security and accurate data sharing advantages present in current blockchain models.
2. Latency in blockchain can be reduced by using other blockchain technologies which offer quicker transactions per second. Unlike bitcoin based blockchain networks which support 7 to 15 transactions per second other light blockchain networks allow between 13 and 1500 transactions per second such as IOTA.
3. IOTA blockchain is ideal for blockchain based intrusion detection systems which gather data flow from devices in the form of transactions which can be done in real-time. With no delay in receiving data from device nodes, an intrusion detection system can perform accurately as a detection and prevention system.
4. While there are many other lightweight blockchain based systems, I feel a custom blockchain similar to IOTA among the existing systems is a good alternative as it is specifically built for blockchain based IoT device networks. It retains the security and privacy of data and resolves the critical issue of latency in approving transactions.

Thank you