International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

BLOCKCHAIN IN SYSTEM AND NETWORK SECURITY

Mr. Divyesh Vadher[1], Prof. Chandresh Parekh[2]

[1] *Student, School of Information Technology & Cyber Security, Raksha Shakti University, Gujarat, India*
[2]*Dean, School of Information Technology & Cyber Security, Raksha Shakti University, Gujarat, India*

Abstract: *The message passing and communication is basically carried over the wired and wireless medium known as a network. The message and the data originating from a source for a particular address passes though many mediums, logical algorithms and processes. The main concern recently is trust or confirmation of legitimate source and destination address. The packets, data or request received or sent may be from an untrusted source whose intention would be to hack, manipulate or steal the data. Thus, firewalls and secure servers are used to protect and verify the incoming and outgoing packets, but servers and firewalls being a centralized and single system, it can be easily bypassed. Here we introduce blockchain technology for communication amongst the firewalls and servers (cloud / private) of a network or topology to share the banned IP addresses, MAC addresses and signature of attack so as to be updated with recent and past attack patterns as precautionary measures. Blockchain technology here will gather information regarding the IP addresses, MAC addresses and signature of attack using which attacks are performed on any organisation and share among the connected nodes so that they can block the incoming packets from the same malicious IP and MAC addresses and also detect malicious packets of same signature.*

Keywords: **Blockchain, IP address, MAC address, Network, Security, Attack signature, Nodes, Consensus algorithm, Decentralise system, Cryptography, Proof of work.**

1. INTRODUCTION:

Information Technology & Data security has become the most necessary and important aspect of in the recent world of digital transaction, information security and data analysis. The communication process and the data sharing are basically carried over the wired or wireless network with certain topologies and routing mechanisms. The messages / data are transferred using the physical devices and other mediums such as switches, routers, modems, cables, firewalls; moreover, a physical address (MAC Address) & logical address (IP Address) are always associated with the message or data sent over the internet so as to distinguish the sender and receiver. The message sent over the network may or may not be from a trusted source or a legitimate IP Address. Many devices and software such as centralised firewalls and security algorithms are used to filter out the unwanted or malicious data coming from an untrusted IP Address. The most important aspect here in the security mechanism is to identify the IP Address and type of the message coming inbound or going outbound.

The firewalls and software used generally in day to day systems are centralised and with a fixed amount of database to compare with for the unwanted message type and IP, the limited amount of data and records available make it easy to bypass the mechanism and security wall. If only a single firewall or policy is applied then it would be easily cracked or know to the hacker or to the person trying to bypass the security. Here blockchain concept can be implemented so as to make the security high. Basically, blockchain is decentralized, distributed and a public ledger (digital) used to record processes, transactions across many computers / systems so the data cannot be altered without the changing other connected blocks. This helps the nodes and the network to verify and audit the processes and data individually and in cheap manner. The database managed here is autonomous using a peer-to-peer network with a distributed timestamping server mechanism which are authenticated by multiple collaboration by collective nodes or peers in the networks. Now using the concept of blockchain the firewalls of an enterprise, ISP, network, cloud can be configured so as to check the incoming and outgoing packets amongst multiple firewalls which contains the database of past attack or malicious data records, blacklisted IP addresses, doubtful MAC addresses. Here polling method and multiple firewalls interconnected with different protocols and policies make it hard to bypass for data packet received or sent. The interconnected firewalls basically examine the packet (i.e. data), different firewalls would check into their respective databases and logs of blocked or blacklisted IP, malicious codes or banned MAC addresses and share the result amongst themselves, if any banned packet / IP / MAC is found then it would be discarded from the communication and the databases of firewalls would keep a track of it for further blocking. In case of some database error or log error amongst the firewalls, a polling would be done amongst them for the packet verification and processing further. The firewalls would be sharing their databases on regular basis which would include the block contents and packet type to be filtered out. The adjacent nodes or the firewall would always be connected so as to get the new updates and

policies. The polling and interconnection reduce the dependencies which were seen basically in conventional single firewall mechanism. This blockchain-based exchange of logs and banned IP's can be completed quicker, safer and cheaper than with traditional sharing systems which makes hard for a hacker or intruder to attack with a new mechanism every time and totally preventing BOT attacks. Thus, a blockchain when properly set up to detail the exchange and monitor the packets, it provides a record that is genuine, unbiased & most importantly secure.

2. INTRODUCTION TO BLOCKCHAIN

2.1. CONCEPT OF BLOCKCHAIN

A Blockchain is distributed, decentralized and public ledger. This ledger is jointly maintained by multiple nodes, using cryptography. Use of cryptography in ledger is to ensure data storage consistency, security of transmission and access, temper-proof data and prevention of repudiation. As this ledger is distributed it is also named as distributed ledger technology (DLT). A typical blockchain uses units of blocks to store data also it contains cryptographic hash value if prior block in this blockchain, this links the two adjacent blocks. With its unique and trust-building mechanism which is also indispensable, Blockchain changes operation rules and the application scenarios of many industries.

In a typical blockchain system, each party shares information and reaches consensus in accordance with rules agreed in advance. In order to prevent the consensus information from being tampered with, the system stores data in units of blocks which form a cryptographical chain of data structure in chronological order, and the record nodes are selected by the consensus mechanism to determine the data of the latest block and other nodes participate in the verification, storage and maintenance of the latest data block. Once the data is confirmed, it is difficult to delete and modify, and only the authorized query operation can be performed. Depending on the system has a node admission mechanism/control, blockchains can be classified into Permissioned Blockchains and Permission-less Blockchains. The joining and exiting of the nodes in the permissioned blockchain require the permission of the blockchain system. Depending on whether the entities with control rights are centralized or not, Permissioned blockchains can be divided into the Consortium Blockchain and the Private Blockchain. The Permission-less Blockchain, also be called as the Public Blockchain, is completely open, which nodes can join and exit at any time.

2.2. CHARACTERISTICS OF BLOCKCHAIN

2.2.1. BLOCK

Blocks in blockchain are like pages which includes pieces of digital information, it includes four components: a content of transaction, timestamps, reference to a previous block (i.e., hash value of previous block) and Proof of Work for block robustness.

2.2.2. NODES

Nodes in blockchain are distributed computers that built the decentralized network. These nodes possess entire copy of blockchain. The data in the blockchain is synchronized, replicable and shared among all of the nodes. The data is not governed by any single node or network.

2.2.3. MINING

Mining in blockchain is a process to add unconfirmed transactions performed by the nodes as the block in the chain. In mining process, the dump of unconfirmed transactions will be verified and validated and then they will be added to the chain.

2.2.4. IMMUTABILITY

Every block in blockchain contains reference to previous block as a hash value of previous block. Also, every node has replica of entire chain which are frequently being synchronized among all the nodes so information within the blocks cannot be altered or manipulated without affection subsequent blocks as it creates mismatch in embedded digital signatures.

2.2.5. DECENTRALIZED

Decentralization is a most important characteristic of blockchain. Blockchain builds peer to peer network which has no governing authority to control chain. Every participating node will be part of validation and verification of chain.

2.2.6. CRYPTOGRAPHIC HASH

There is cryptographic algorithm in blockchain, that creates a hash value by which blocks are identified. Every block in blockchain contains hash value of previous block as a reference, this sequence of linked hashes produces a secure and independent blockchain.

2.2.7. PROOF OF WORK (POW)

In blockchain the main purpose Proof of Work is to generate a solution that is very difficult to calculate but easy to verify. Proof of Work algorithm is implemented under a network where nodes do not trust each other yet they have to do an agreement. During mining of block

miners perform very complex calculation to validate block and add to the network as a reward by proof of Work algorithm.

3. ARCHITECTURE OF BLOCKCHAIN

The Blockchain technology provides a combination of cryptography, consensus algorithm, distributed ledger and, optionally, decentralized computation capability, to create a decentralized and trustworthy platform

3.1.1. CRYPTOGRAPHIC DIGITAL SIGNATURE

Blockchain uses public key cryptography to generate a fingerprint/signature for Blockchain transactions. When Nodes perform transactions, digital signature will be created using their private keys. Other participant nodes in the blockchain network will verify this transaction using the public key of the sender node to make sure that this transaction is indeed signed by the sender node. Sender node sign the transaction while creating a transaction. There are many different consensus approaches for agreement of chain. This ranges from the permissioned Byzantine fault tolerant to protocol permission less proof of work with longest-chain adoption.

3.1.2. DISTRIBUTED LEDGER

In Blockchain technology distributed storage is used to record the transactions. In this network all the participant nodes in the network store either entire the transaction or portion of the transaction. After this all the node uses the consensus algorithm (An agreement for valid chain) for entering this transaction into ledger, due to this feature of blockchain, it becomes effectively immutable.

3.1.3. CONSENSUS ALGORITHM

Due to its peer to peer architecture, the blockchain consist of multiple nodes. There could be some intentional or unintentional manipulation by some node or any latency in network can differ copy of chains of some nodes. The consensus algorithm in blockchain in which all participant nodes will agree upon some valid chain. This protocol ensures integrity of blockchain as every participant node will verify valid chain.

3.1.4. DECENTRALIZED COMPUTATION

Applications built on top of a blockchain are called “decentralized applications” due to distributed ledger technology. blockchain is peer to peer network. There is no any governing authority that maintains all data set. This chain of block is completely decentralized and managed by all the participating nodes in the network. So, such application tasks may be performed by the all the nodes in the blockchain network by implementation of smart contracts or through off-chain interactions with computational servers following a protocol defined by the underlying blockchain platform.

4. METHODOLOGY:

Using blockchain’s ledger methodology, data can be sent across a network securely. A blockchain technique will ensure that the data is from the correct sources and that nothing is intercepted in the interim. If this technology is more widely implemented, the probability of hacking can go down. Blockchain is more robust than the legacy systems in your organization. Thus, blockchain technology minimizes cyber security risk by simply removing the need for human intervention.

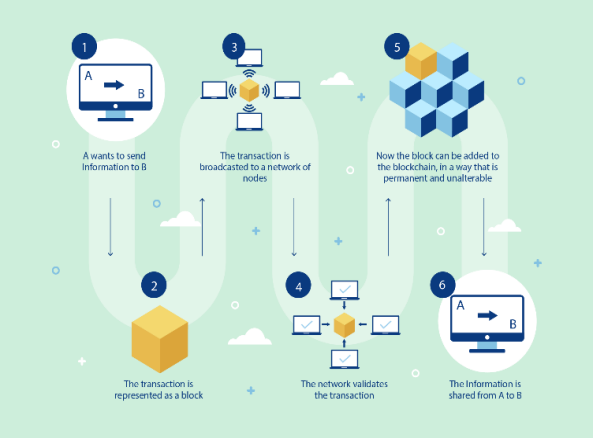


Fig: 1 Node Communication

Above figure represents the whole process of exchanging information about the banned IP addresses, MAC addresses and signature of the attack. As we can see when any request from suspicious IP address come to firewall or secure server it will broadcast that IP in P2P network to each individual node. That node will check the logs generated and verify whether this particular IP or MAC is trustable or not. If more than 51% of nodes agree and define it as a legitimate IP or MAC than it will notify the node to allow traffic else will record it as suspicious IP or MAC and create block of details which contains source IP, source MAC, Type of attack and nature of attack. Add this block into digital ledger. At the end we will find a digital ledger that contains list of suspicious IP and MAC through which attacks can be done. Using this blockchain digital ledger methodology, we can protect networks being vulnerable to attacks and manipulations of data.

To understand and build this system we will use python as a base programming language and develop algorithms for the system.

4.1. TRANSACTION

In this system, transaction is the data retrieved from the reporter node that will be to mined as a block and

added into the blockchain. Here data will be fetched from node and marked it as unconfirmed transaction.

4.2. STORE TRANSACTION CONTENTS AND ADD DIGITAL FINGERPRINT INTO THE BLOCKS

First, we will define the contents that a block will contain. In this system, Block will contain below data,

```
{
"reporter": "IP OF REPORTER NODE",
"IP_address": "malicious IP address to report ",
"MAC_address": "malicious MAC address to report",
"type_of_attack": "Attack description or type of attack",
"timestamp": "Time of content creation"
}
```

Now we will define Block that contains index value of block, content of block, hash value of previous block and some random integer value as nonce. Here we are adding nonce to the Block to avoid conflicts in hash value and this random value ensures uniqueness of block and it makes block more robust.

```
class Block:
  def __init__(self, block_index, transaction_content,
timestamp, previous_block_hash, nonce=0):
    self. block_index = block_index
    self. transaction_content = transaction_content
    self.timestamp = timestamp
    self. previous_block_hash = previous_block_hash
    self.nonce = nonce
```

To calculate hash of block below function returns hash of block, in this way we are adding digital fingerprint to block,

```
  def calculate_hash(self)
    string_b = struct.pack(self)
    return sha256(string_b.encode()).hexdigest()
```

4.3. CREATING CHAIN OF BLOCKS

First, we have to create chain and then create first block in the chain, let's call it the origin block,

```
class Blockcahin:
    def __init__(self):
        self.unconfirmed_transaction_content = []
        self.chain = []

    def create_origin_block(self):
```

This function creates origin block and appends it to the chain. This block has block_index as 0, previous_block_hash as 0, and a valid hash of entire block,

```
    origin_block = Block(0, [], 0, "0")
    origin_block.hash = origin_block.calculate_hash()
    self.chain.append(origin_block)
```

now we have to assign it as previous block as chain will always have at least one block (i.e., origin block), hear origin block will be most recent block,

```
    def previous_block(self):
      return self.chain[-1]
```

4.4. PROOF OF WORK ALGORITHM IMPLEMENTATION

Sometimes if we make change in previous block, it will be easy task to re calculate following block hashes and create a new valid blockchain. To prevent this situation, we should make our hash more robust that calculation of hash should be difficult. As we know we can't change hash without making a change in block, so we add some modifiable data to block that makes hash calculation difficult we can call it as nonce. Nonce is random number that will keep altering until desired difficulty level of hash that satisfies our criteria.

In blockchain class we will define difficulty level of proof of work,

```
pow_difficulty = 3

   def proof_of_work(self, block):
      block.nonce = 0

      calculated_hash = block.calculate_hash()
       while not calculated_hash.startswith('0' *
Blockchain.pow_difficulty):
        block.nonce += 1
        calculated_hash = block.calculate_hash()

    return calculated_hash
```

4.5. CHECK VALIDITY OF BLOCKS BEFORE ADDING TO THE CHAIN

For adding the blocks in the chain, we have to assure integrity and valid order of transaction.

Now we have to verify if block has valid hash difficulty level that satisfies defined criteria

```
    def is_valid_pow(cls, block,hash):

        return (hash.startswith('0' *
Blockchain.pow_difficulty) and
        hash == block.calculate_hash())


    def add_block(self, block, pow):
```

```
        previous_block_hash = self.latest_block.hash

        if previous_block_hash !=
block.previous_block_hash:
            return  False

        if ! Blockchain.is_valid_pow(block, pow):
            return False

            block.hash = pow
            self.chain.append(block)
            return True
```

Now to verify validity of chain,

```
    def chain_validity(cls, chain):
        validity = True
        previous_block_hash = "0"

        for block in chain:
            hash = block.hash

            if not cls.is_valid_pow(block, hash) or \
                 previous_block_hash !=
block.previous_block_hash:
                validity = False
                break

            block.hash=hash
            previous_block_hash = hash

        return validity
```

4.6. BLOCK MINING

When transaction occurs, these transactions are unconfirmed transactions so they are not yet added to block. Mining is a process of putting these transactions to blocks and calculating proof of work. After nonce satisfies criteria of proof of work these blocks will be added in to blockchain,

```
    def mine(self):
        if not self.unconfirmed_transactions:
            return False

        latest_block = self.latest_block

        new_block = Block(index=latest_block.index +
1,

    transactions=self.unconfirmed_transactions,
                      timestamp=time.time(),

    previous_block_hash=latest_block.hash)

        pow = self.proof_of_work(new_block)
        self.add_block(new_block, proof)

        self.unconfirmed_transactions = []

        chain_data = []
        for block in self.chain:
            chain_data.append(block.__dict__)
        with open("./mined_block/blacklist.txt", "w")
as file_:
            print("Block mined!! Mined block
documented sucessfully")
            file_.write(str(chain_data +'\n') )

        return new_block.index
```

4.7. DECENTRALISATION AND NODE REGISTRATION

As we know blockchain is peer to peer network. There is no any governing authority that maintains all data set. This chain of block is completely decentralized and managed by all the participating nodes in the network. For this system we will register new nodes with,

```
    def register_new_node():
            peers.add(node_address)
            return get_chain()
```

4.8. IMPLEMENTATION OF CONSENSUS ALGORITHM

As the blockchain consist of multiple nodes there could be some intentional or unintentional manipulation by some node or any latency in network can differ copy of chains of some nodes.

There is consensus algorithm in blockchain in which all participant nodes will agree upon some valid chain. This algorithm ensures integrity of blockchain as every participant node will verify valid chain. In this system we implement consensus algorithm in a way that every node will agree upon malicious IP address in the block in that way node will allow or discard block, if chain contains all valid IP addresses that chain will be considered,

```
    def verify_and_add_block():

    verify = block_data['IP address']
      added = blockchain.add_block(block, verify)

      if not added:
        return "Block is discarded"

      return "Block is added"

    def consensus_algorithm():
```

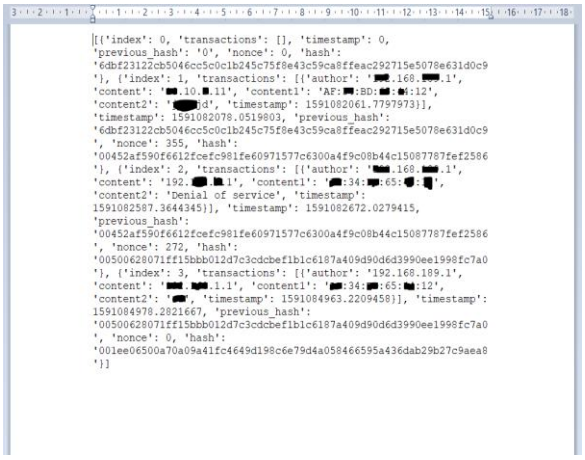
```
    valid_blockchain = None

    for node in nodes:
      response = requests.get('{}chain'.format(node)
      chain = response.(chain)
      if verify > valid and
blockchain.chain_validity(chain)
        valid_blockchain = chain

    if valid_blockchain:
      blockchain = valid_chain
      return True

    return False
```

4.9. ADDING LIST OF IP ADDRESSES, MAC ADDRESSES AND ATTACK SIGNATURE TO FIREWALL

Now this data set in blockchain will content list of malicious IP address, MAC address, Attack type and IP address of reporter node. This data set will be further used in organization firewall to blacklist and filter out these them.

5. RESULT:

By implementing the blockchain mechanism the internet service providers, government agencies and any enterprise dealing in network consisting of IP addresses, MAC addresses and signature of attack , can verify legitimate source and confirm whether source can be trusted or not by sharing secure distributed information about malicious IP addresses and MAC addresses of attacker, detailed information about type and nature of attack for further prevention of attack from same IP addresses and MAC addresses.



```
[{'index': 0, 'transactions': [], 'timestamp': 0,
'previous_hash': '0', 'nonce': 0, 'hash':
'6dbf23122cb5046cc5c0c1b245c75f8e43c59ca8ffeac292715e5078e631d0c9
'}, {'index': 1, 'transactions': [{'author': '[redacted].168.[redacted].1',
'content': '[redacted].10[redacted].11', 'content1': 'AF:[redacted]:8D:[redacted]:12',
'content2': '[redacted]d', 'timestamp': 1591082061.7797973}],
'timestamp': 1591082078.0519803, 'previous_hash':
'6dbf23122cb5046cc5c0c1b245c75f8e43c59ca8ffeac292715e5078e631d0c9
', 'nonce': 355, 'hash':
'00452af590f6612fcefc981fe60971577c6300a4f9c08b44c15087787fef2586
'}, {'index': 2, 'transactions': [{'author': '[redacted].168.[redacted].1',
'content': '192.[redacted].1', 'content1': '[redacted]:34:[redacted]:65:[redacted]',
'content2': 'Denial of service', 'timestamp':
1591082587.3644345}], 'timestamp': 1591082672.0279415,
'previous_hash':
'00452af590f6612fcefc981fe60971577c6300a4f9c08b44c15087787fef2586
', 'nonce': 272, 'hash':
'00500628071ff15bbb012d7c3cdcbef1b1c6187a409d90d6d3990ee1998fc7a0
'}, {'index': 3, 'transactions': [{'author': '192.168.109.1',
'content': '[redacted].[redacted].1.1', 'content1': '[redacted]:34:[redacted]:65:[redacted]:12',
'content2': '[redacted]', 'timestamp': 1591084963.2209458}], 'timestamp':
1591084978.2821667, 'previous_hash':
'00500628071ff15bbb012d7c3cdcbef1b1c6187a409d90d6d3990ee1998fc7a0
', 'nonce': 0, 'hash':
'001ee06500a70a09a41fc4649d198c6e79d4a058466595a436dab29b27c9aea8
'}]
```

Fig: 2 Generated File consisting Blockchain data

Above figure represents resultant file generated by this system which consists of reported IP addresses, MAC addresses and signature of attack that will be shared among all nodes of organisation. This Content will be used by Administrator for filtering traffic from malicious sources.

6. FUTURE WORK

This system can be implemented on large network of organisation which can have any number of nodes. For Effective management and performance, we can build this system with web application framework and deploy this system to the cloud. Alternatively, we can use cross platform application and create locally hosted web server and deploy it in network with domain, this way we can built system where multiple nodes can participate.

7. CONCLUSION:

Blockchain is decentralized, distributed and a public ledger in a digital form that is used to record processes, transactions across many systems so the data cannot be altered without the changing other connected blocks. This mechanism helps the nodes and the network to verify and audit the processes and data individually and in cheap manner. By implementing Blockchain technology this system can be used by the internet service providers, government agencies and any enterprise dealing in network consisting of IP addresses and MAC addresses to be safe from banned IP addresses, MAC addresses and signature of attack , can verify legitimate source and confirm whether source can be trusted or not by sharing secure distributed information about malicious IP addresses and MAC addresses of attacker, detailed information about type and nature of attack for further prevention of attack from same IP addresses and MAC addresses..

REFERENCES:

[1] Eric Piscini, Gys Hyman, and Wendy Henry, “Blockchain: Trust economy,” Tech Trends 2017, Deloitte University Press, February 7, 2017.

[2] Ouaddah A, Abou Elkalam A, Ait Ouahman A. FairAccess: a new Blockchain-based access control framework for the Internet of Things. Security and Communication Networks. Wiley Online Library; 2016;9: 5943–5964. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.1748.

[3] China Academy of Information and Communication Technology Trusted Blockchain Initiatives December , 2018.

[4] D. Puthal, N. Malik, S. Mohanty, E. Kougianos, and C. Yang, “The Blockchain as A Decentralized Security Framework”, IEEE Consumer Electronics Magazine, Vol. 7, No. 2, pp. 18--21, 2018.

[5] A Next Generation Smart Contract & Decentralized Application Platform, https://www.weusecoins.com/assets/pdf/library/Ethereum_white_papera_next_generation_smart_contract_and_decentralized_application_platformvitalik-buterin.pdf, Accessed 15th December 2017.

[6] "Blockchains: The great chain of being sure about things". The Economist. 31 October 2015. Archived from the original on 3 July 2016. Retrieved 18 June 2016.

[7]] "Move over Bitcoin, the blockchain is only just getting started". Wired. Archived from the original on 8 November 2016. Retrieved 9 November 2016.