International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7955
***Article Received**: 12 May 2023 **Revised**: 02 July 2023 **Accepted**: 29 July 2023*

Detecting Sybil Attack in Blockchain and Preventing through Universal Unique Identifier in Health Care Sector for privacy preservation

Nidhi Raghav[1], Anoop Kumar Bhola[2]
[1]Research scholar, Department of CSE, Banasthali Vidyapith,Rajasthan,India
raghav.nidhi@gmail.com
[2] Assistant Professor, Department of CSE, Banasthali Vidyapith,Rajasthan,India
anupbhola@banasthali.in

Abstract— Health care data requires data secrecy, confidentiality, and distribution through public networks. Blockchain is the latest and most secure framework through which health care data can be transferred on the public network. Blockchain has gained attention in recent year's due to its decentralized, distributed, and immutable ledger framework. However, Blockchain is also susceptible to many attacks in the permission less network, one such attack is known as Sybil attack, where several malicious nodes are created by the single node and gain multiple undue advantages over the network. In this research work, the Blockchain network is created using the smart contract method which gets hampered due to Sybil attack. Thus, a novel method is proposed to prevent Sybil attack in the network for privacy preservation. Universal Unique Identifier code is used for identification and prevention of the Sybil attack in the self-created networks. Results depict that proposed method correctly identifies the chances of attack and the prevention from the attack. The approach has been evaluated on performance metrics namely, true positive rate and accuracy which were attained as 87.5 % and 91% respectively, in the small network. This demonstrates that the proposed work attains improved results as compared to other latest available methods.

Keywords- Health care data, Block chaining, Sybil Attack, Privacy Prevention, UU Code

I. INTRODUCTION

The global health care system has deteriorated since the Pandemic, with a lack of beds, huge waiting lists for patients, and enormous costs. This state of the global healthcare system is challenging for healthcare practitioners and patients. As per the study of Deloitte's 2022, Global healthcare industry is at the breaking point. Therefore, to prevent global healthcare system from complete failure, blockchain technology emerged as a boon to healthcare industry. Blockchain technology is a decentralized and distributed ledger system that records transactions in a safe and transparent manner. The system is made up of a network of computers that share a database, and each new transaction is validated and added to the ledger by a network of participants known as nodes. The integrity of the system is ensured by the fact that once a transaction is put to the blockchain, it cannot be changed. The technology was originally developed to support the use of digital currencies like Bitcoin, but it has since found applications in other fields such as supply chain management, voting systems, and identity verification. Blockchain technology enables secure and transparent record-keeping and eliminates the need for intermediaries in transactions, reducing the cost and time required for settlements. A block in a blockchain is a collection of data that is stored in a specific format, containing a set of transactions and other important information. The block includes a header and a body. The header contains metadata about the block, such as a timestamp, a unique identification number called a hash, and a reference to the previous block in the chain, creating a linked list of blocks. The hash is a cryptographic function that takes the block data as input and produces a fixed-size output that uniquely identifies the block. This makes it difficult to modify or tamper with the data in the block, as any changes to the data would result in a different hash. The body of the block contains the actual data, which in the case of a cryptocurrency blockchain, includes information about transactions, such as the sender, the receiver, and the amount of currency transferred. Once a block is created and added to the chain, it is considered immutable and cannot be modified without changing the hashes of all subsequent blocks. This makes blockchain a secure and reliable way to store and verify data. Complete working of Block chaining is explained in forthcoming section.

Blockchain technology is profoundly underused in the global healthcare industry. It can be used to establish a competent, translucent, secure, and adequate way of communication of data and information among various users in the healthcare industry. Also, it utilizes tokenization and smart contracts which reduces the process of pre-authorization in the healthcare sector. Some companies such as IBM, SAP and Nebula are employing

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7955
***Article Received**: 12 May 2023 **Revised**: 02 July 2023 **Accepted**: 29 July 2023*

blockchain for some of the primely focused tasks such as credential verification, monitoring costs, payment, organs, and transplants and storing of medical records among medical practitioners.

Thus, due to decentralized consensus, cryptographic functions, and immutable ledger, it is less vulnerable to security attacks. Still, it is susceptible to attacks as reviewed in literature [2]. Some authors demonstrated how Blockchain is susceptible to data tampered risk and how an authentication-based mechanism is developed to overcome the drawbacks of single factor authentication [3].

With the exchange of such crucial and personal information over the network, it can be leaked to any other user who pretends to be a genuine user. One such type of attack is called Sybil Attack, which can impair the information of healthcare system. It is a severe attack in which an attacker node dispatches several messages with numerous fake identities. The attacker which is spoofing the identity of other nodes is called Sybil Attacker and spoofed nodes whose identities have been stolen are called Sybil Nodes. Some possibilities of Sybil attack are delusion of a traffic jam or accident that forces data to take another route or insert erroneous knowledge through forged nodes [4-7]. Sybil attacks can further lead to several attacks such as mining pool attack, DOS attacks and others [8-10].

In this work, a novel methodology is proposed to prevent such Sybil attacks in Blockchain network. In the proposed work, the behavior of every node will be monitored by every participating node to check whether the forwarding blocks are coming from the same user or different users over a certain interval of time. If the blocks are being forwarded by the same user, it can be malicious node which leads to the possibility of Sybil attack. Such nodes are kept in a suspected list and every other node in the network is notified with this suspected list. The Sybil attack decreases the throughput of the system and harms the resources which is demonstrated in forthcoming sections.

II. RELATED WORK

2.1 Privacy Preservation in Healthcare System Using Blockchain

As per the literature, blockchain is widely used in healthcare sector which includes storing, protecting, and sharing medical information and medical data application. It's also applied in forecast analysis and discover all possible influences, goals and potentials that are related to healthcare sector.

Health data is at most important for humans, now a days Blockchain technology is used to provide security, protection, sharing and storing the health care data. Many applications were used in past for health care for sharing and storing health care data of patients, hospital data. Lab specific data and used for forecasting the data applying various machine learning algorithms. Blockchain provides the security to data and not easily hampered by the hackers. Blockchain provides more security to Health care data as compared to the past methods.

In this work, a novel Gateway was proposed for Healthcare Data based on secure multifactor computing. The proposed architecture control and share data easily and securely. It also ensures that medical and health data is processed by untrusted third parties without hampering privacy of patients [11]. To construct secure platform for storing and analysing medical data, Enigma encryption platform was proposed based on blockchain [12]. Another framework was proposed to address the challenges associated with access control of sensitive data stored in cloud. The framework was based on immutability and built-in-autonomy properties of blockchain [13]. In another work, an interinstitutional medical health prediction model was constructed to share patient's data [14]. The author proposed a platform for privacy preservation of medical data in which data is encrypted and stored in federation blockchain and to access the data, the user must request the decryption key from the data owner [15].

2.2. Related work on Sybil Attack

Sybil attack is the most serious attack in blockchain technology which abused peer to peer network by constructing illegitimate nodes/users. The work done to prevent Sybil attack in various fields has been reviewed in this section.

J. Yun and M. Kim proposed a method SybilEye, which disseminates the role of observer to the users. The approach was an effective approach for privacy preservation against sybil attack. To evaluate the performance of the proposed approach, wi-fi connection-based model was established for mobile crowdsensing system. The model was evaluated using the most crucial factor i.e., detection-rate. It also minimizes the overhead occurring through traditional sybil attack detection techniques [22]. S. Frieba et.al. proposed a novel approach named SybilHedge for decentralized validation of virtual-identities registration requests. The approach was based on trust relations between various users in social network. It does not reveal the relationships of a user to other participants [23]. Two other algorithms namely, SybilGuard [24] and SybilLimit [25] are proposed against Sybil attack. N. Tram et.al. proposed another approach against Sybil attacks without random walks [26]. X. Vine. imparts a decentralized hash table and permanently stored random walk using trails, which blocks the access by sybil nodes [27]. Based on trustworthy transaction in a digital network, A. Almogren et.al. proposed a mechanism named Fuzzy-based trust management which works in the emerging field of Internet of Medical Things (IoMT) to prevent against Sybil Attacks. It is developed for users of eHealth system which

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7955
***Article Received**: 12 May 2023 **Revised**: 02 July 2023 **Accepted**: 29 July 2023*

collects genuine and reliable information from neighbouring nodes and trust value is evaluated using fuzzy logic. The approach was evaluated through various performance measures and attain better results as compared to state-of-the-art approaches [28]. Newsome et.al. proposed a registration-based method based on identity registration to prevent sybil attack [29]. Another method was proposed by Yu., et.al. based on the physical position of each node in a network [30]. Further Xu et.al. proposed another method to prevent sybil attack based on clustering of network. In this, two separate clusters of honest nodes and sybil nodes are formed in a network connected through attack edges [31]. Despite of several types of sybil attacks and difficulty in their prevention, still preventive measures exist. Numan et.al. categorized preventive measures intro three categories: i) Trusted centralized and decentralized certification based on cryptographic primitives ii) resource testing which includes network coordinates and IP addresses iii) social network techniques such as SybilGuard, Vote Aggregation and others [38]. Some other methods have been proposed by other authors [32-37] but none of the work focussed on the UUID of the system that is being proposed in this work.

Table I Various Proposed Methods with Its Advantages and Disadvantages

Authors	Methods	Advantages	Disadvantages
1. Yue, X *et al.* [11]	Healthcare Data Gateway architecture	Patients' data can be owned, controlled, and share securely.	Its arduous to attain Privacy-aware data access policies.
2. Chen, Y *et al.* [16]	Framework for Storage and service	Provides a possible solution to share the data ensuring it's privacy.	Does not address numerous medical and health institutions.
3. Al Omar *et al.*[15]	Patient healthcare data storing system	Encrypts and secure healthcare data at low cost.	Does not address the issue of key distribution techniques.
4. Hussein, A.F *et al.* [17]	Blockchain-based data sharing	Robust and efficient system to ensure dependable data privacy.	Increased processing time
5. Daghera, G.G *et al.* [18]	Ancile -Blockchain-based framework	Cost and storage effective.	legislative standards are not met.
6. Zhang, A. and Lin, X [19]	BSPP	Time and cost effective	Unable to achieve security goals.
7. Tian, H *et al.* [20]	Sibling Intractable Function Families	Ensures data privacy and integrity.	Cost of communication increases
8. Zhu, L *et al.* [21]	Controllable Blockchain data management (CBDM) model	Terminates vicious activities	Does not fit into actual environment

III. MOTIVATION

A Sybil attack is a type of attack in which an attacker creates multiple fake identities, called Sybils, to gain control or influence over a network. In the context of blockchain, a Sybil attack can be used to manipulate the consensus mechanism, which is the process by which nodes in the network agree on the state of the blockchain. There are several reasons for motivation to study Sybil attacks in blockchain. One reason is that blockchain technology is being used in an increasing number of applications, including finance, supply chain management, and voting systems. As these applications become more widespread and critical, it is important to understand the potential vulnerabilities of blockchain technology and to develop ways to mitigate these vulnerabilities. Sybil attacks can be especially damaging to blockchain networks because they can undermine the decentralization and trust that are key features of blockchain technology. Researchers are motivated to study Sybil attacks to develop new strategies for detecting and preventing these attacks, or to develop new consensus mechanisms that are more resilient to Sybil attacks. Additionally, studying Sybil attacks in blockchain can lead to a better understanding of network security and cryptography in general, which can have broader implications for cybersecurity research and development.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7955
***Article Received**: 12 May 2023 **Revised**: 02 July 2023 **Accepted**: 29 July 2023*

IV. SCOPE OF RESEARCH

As per review of literature, very few researchers have worked on detection of Sybil attack in Blockchain on healthcare systems. The work done in literature suffers from a drawback of high computational complexity which is not advisable to use in active Blockchain system. A researcher P. winter et.al. addresses that to analyse and detect Sybil attack manual verification is required which is time-consuming and not an efficient process [38]. Therefore, to increase the efficiency and throughput of a system, Swathi P. et.al. proposed a solution to attain improved accuracy and detection of suspicious nodes in a sybil attack using physical address [8]. Thus, in this work, the author has focussed on attaining improved accuracy and low error rate based on another method. It is used to trick the user about the state of transaction. Therefore, in this work, Sybil attack is focused and proposed a prevention method which can detect the Sybil attack in a network.

V. RESEARCH METHODOLOGY

In this part authors have briefly explained the Blockchain and the working of Sybil Attacks in a network. However, in the forthcoming sections explained the prevention method for Sybil Attack in networks.

5.1 *BlockChain*

A blockchain is a decentralized and distributed digital ledger that is maintained by a network of computers, or nodes, that work together to validate and record transactions. A Merkle tree is a data structure used in blockchain technology to efficiently verify the integrity and consistency of large sets of data. In a blockchain, Merkle trees are used to organize transactions into blocks, which are then added to the blockchain in a sequentialorder. The process of forming a blockchain with Merkle trees and blocks involves several steps, including:

1. Transaction creation: A transaction is created when a user wants to send cryptocurrency to another user. The transaction includes information such as the sender's public key, the receiver's public key, and the amount of cryptocurrency being sent.

2. Merkle tree creation: Once a set of transactions has been created, they are organized into a Merkle tree. A Merkle tree is a binary tree where each leaf node represents a transaction, and each non-leaf node represents a hash of its children's nodes. The top node of the tree, known as the Merkle root, represents the hash of all the transactions in the tree.

3. Block creation: Once the Merkle tree is created, it is combined with other information such as a timestamp and a nonce to create a block. The block also includes a reference to the previous block in the chain, creating a linked list of blocks.

4. Block validation: Each node in the network then validates the block to ensure that it meets the rules of the blockchain protocol. This includes verifying the proof-of-work or other consensus mechanism used to confirm the validity of the block.

5. Block addition: Once the block is validated, it is added to the blockchain and broadcast to the rest of the network.

6. Consensus maintenance: The nodes in the network continue to work together to maintain consensus on the state of the blockchain. Any attempted changes to the blockchain are only accepted if they are verified and validated by many of the nodes in the network.

By using Merkle trees to organize transactions into blocks, blockchains can efficiently verify the integrity and consistency of large sets of data, making them more secure and reliable. Additionally, the use of blocks and Merkle trees allows blockchains to be easily scaled to handle large amounts of data and traffic. This process repeats for every new transaction that is added to the blockchain, creating an immutable and secure record of all transactions in the network.

The structure of the entire block chain and various attributes of the block are presented in Figure1. Table II presents various block elements and their descriptions.

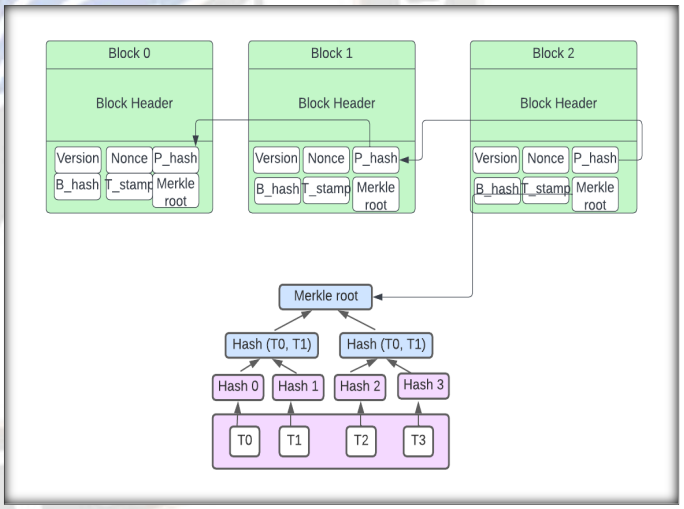

Figure1 Block Structure in Blockchain Technology

Table II
Different Block elements and their Description

Block Element	Description
B_Hash	Distinct cryptographic hash
P_Hash	Distinct cryptographic hash of previous block
Version	Represents Version
Nonce	An arbitrary counter
T_stamp	Indicates the time of creation of a block
Merkle Tree	cryptographic hash of Merkle tree
T0-T3	All transactions stored

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7955
***Article Received**: 12 May 2023 **Revised**: 02 July 2023 **Accepted**: 29 July 2023*

In decentralized network, this structure of data makes it an irreversible timeline of data. Blockchain network can be further classified into two types; based on permission protocols such as permission-less and permission based. In permission-based networks only the verified user can join the network, it is less susceptible to the security challenges, however in permission-less network (Ethereum and Bitcoin) any new block can join the networks and do the transactions based on the consensus protocols. Major security threats are present on these networks as anyone can enter the network and do the verifications and earn the coins. Sybil attack is also one of such attacks present in permission less network.

5.2 Sybil Attack

Sybil attack is a network attack against peer-to-peer network that do not trust a central party for verification of node identity. In this, several fake identities are created by an attacker to attain large influence over the network. As blockchain is a peer-to-peer network, therefore, it is exposed against a threat of sybil attack. After gaining substantial influence over the network, an attacker triggers several threats to damage the reputation of a system. The various threats that are triggered by an attacker in Sybil attack are explained. i) Break consensus protocol attack is mostly found in shared-based Blockchain systems. In these systems, transactions are executed in parallel to achieve maximum throughput and network scalability and are susceptible to break consensus protocol attack in which the shared-based consensus process is disrupted. Another type of threat on shared-based blockchain is ii) Generate fake transaction attack. In this sybil nodes are used fake transactions are created to corrupt the transactions. iii) Another type of data structure in Blockchain is Trust-Chain which is made to create reputation based distributed trust. It consists of one transaction per block consists of two incoming and two outgoing pointers. Tampering node reputation attack is detected if this rule is violated. iv) another type of sybil attack is Node partitioning attack, in which an honest node is seized by an attack and a network is splitted into two or more groups. v) In blockchain, information of each node is kept with their neighbouring nodes in the form of routing table which consists of NodeId, network communication IP address and port. Insertion of any sybil node in routing table is referred to as Routing table Insertion attack. vi) other types of attacks are sybil-based linking attack which are related to Pseudo-anonymous blockchain system and Sybil based DDOS attack which disturb the functioning of Blockchain systems. A network having the Sybil node is shown in Figure 2. Algorithm 1 presents how sybil attack is performed.

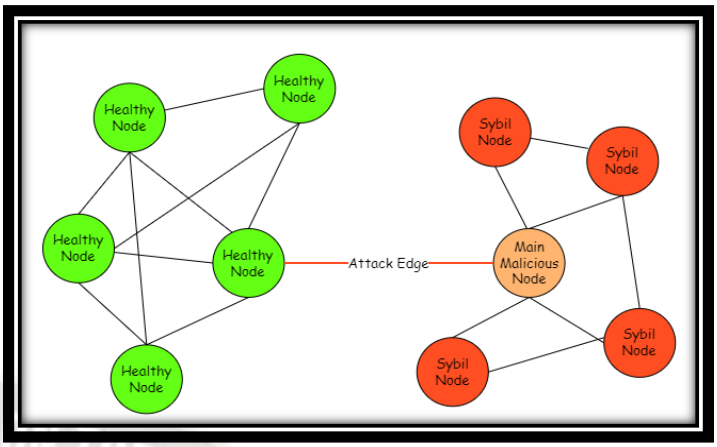

Figure 2 Sybil Attack in Networks

Algorithm1

$C <- Correct\ nodes$

$F <- Fictious\ nodes$

$A <- Attacker\ nodes$

while (true) do

A creates F

F connects with C

A attains Influence on system $<- I$

If (I == True), then

A attacks the system

End

5.3 Proposed Solution & Implementation

The prime objective of the proposed work is to detect and prevent the permissionless blockchain from sybil attack and in turn improving the performance of the system. In blockchain, each block has a unique address known as block Hash address which is a unique address for every user, also it does not reveal user's identity. This is also called as Wallet address. To generate this address, an identity of a user is fed to the wallet which generates a pseudo-random number. This number has 0x80 as its initial number and a hash function SHA256 is applied. A private key of a wallet is generated by combining the first four bytes of the output of a hash function when added at the end of initial pseudo-random number. The resultant private key is converted into a public key based on elliptic curve cryptography. Then, this generated public key is hashed using two algorithms namely, SHA 256 and output is again hashed using algorithm RIPEMD-160. The output of this hash function is converted into a binary address which is the unique block address of the user. This is also called as Miner's address, as it is the address of the miner who creates the block for

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7955
***Article Received**: 12 May 2023 **Revised**: 02 July 2023 **Accepted**: 29 July 2023*

broadcasting. To demonstrate the implementation first, nodes/ blocks are created, and then different blocks are joined in a network. Four blocks are created in Blockchain. It shows the Name of the block, timestamp, previous hash, block hash and the amount that is transferred to the other node/ block as represented in Figure. 3.

Figure 3: Transactions in Blockchain Showing Four Nodes

5.4 Proposed algorithm

$$Input: Number\ of\ Blocks, NB$$

$$Notations:\ D_P: Docker\ platform, E_N: Etherum\ network,$$
$$B: Block, IP_A: Internet\ protocol\ Address,$$
$$SN: Suspected\ Node, SL: Suspected\ List,$$
$$MT: Monitoring\ Table, UUID: Universal\ Unique\ Identifier$$
$$P2P: Peer\ to\ Peer\ protocol, BN: Blockchain\ Network,$$
$$MN: Malicious\ node,$$
$$\tau: threshold\ value$$

// Creating blockchain network using Etherum

1. $D_P \leftarrow NB$
2. $B \leftarrow E_N\ (D_P)$
3. $BN \leftarrow P2P\ (B)$
4. $If\ (IP_A \equiv \exists B\ ),$
5. $then\ p(MN) is\ more, Hence, Sybil\ attack\ is\ possible$

// Detection of Sybil Attack

6. $MT \leftarrow Miner'address\ (B) \cup \#B\ \cup \#blocks_{transmitted}\ \cup UUID$
7. $If\ (\#blocks_{transmitted}\ \geq\ \tau)$
8. $then, SN \leftarrow UUID\ (B)$
9. $SL\ \leftarrow SN_1\ \cup SN_2\ \cup \ldots\ldots\ldots\ldots \cup SN_i$
10. $Broadcast_{network} \leftarrow SL$
11. $If\ UUID\ (B_{transmitted}) \epsilon\ SL$
12. $then\ B(UUID) is\ a\ Sybil\ Node$

To diagnose the Sybil attack in the block chaining technology, first created the block-chain network. The authors have created private multi-node Ethereum network where different nodes are connected to each other via P2P protocol. The Ethereum application is built using an open source Ethereum platform. The application uses Geth as the ethereum client, meteror as the main development framework, solidity for smart contact and truffle for testing. To scale the network easily without the deployment of these frameworks on each node, the author has used docker to spawn multiple nodes as shown in Figure 4.

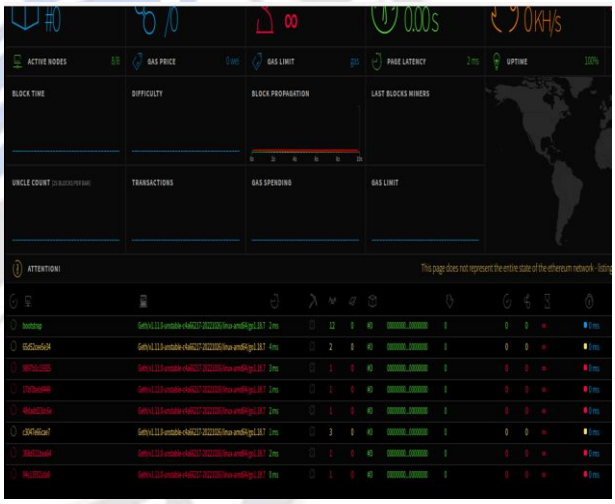

Figure 4 Block-Networks created using Docker

Geth provides a JavaScript interactive runtime environment and console which can be connected using the commands mentioned below as blocks are created as depicted in fig. 5.

#// docker exec -it bootstrap geth -datadir=~/.ethereum/devchain attach

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7955
***Article Received**: 12 May 2023 **Revised**: 02 July 2023 **Accepted**: 29 July 2023*

Fig 5. Blocks Creation Code

As specified in previous section each node maintains a routing table in blockchain which contains block number, miners address that uniquely identify the node. But in case of Sybil attack the many malicious node are also participated in the network with same id which is not visible to any of the users and the attacker gain the network coins and hampered the network. In the above created network where 8 nodes are generated 5 are malicious nodes. In this network Sybil attack can happen. To detect sybil attack, the monitoring table is used to monitor the count of each node. In sybil attack, the receiver's node accepts large number of blocks from attackers address as compared to genuine user address. It is because sybil nodes forward only fake nodes and drop genuine blocks. It leads to innocent forwarding of fake nodes even by the genuine nodes in the whole blockchain. Thus, fake nodes propagates faster than the genuine blocks which can be monitored by higher number of counts for sybil nodes. This effect will be observed by every node for a certain period by tracking the monitoring table as presented in Table III.

To prevent the Sybil Attack in the network authors used the UU code and the count of nodes. The UU code or UUID is the Universal Unique Identifier which is a 128-bit number that is used to uniquely identify the system. It consists of 32-bit alphanumeric characters and consists of 4 hyphens. It is different from the physical or MAC address of the system. It can be retrieved with the following command on windows system,

// wmic path win32_computersystemproduct get uuid

For illustration, UUID

93EAA0F6-32AA-D8B0-3F44-C01850160ED4

The block number and miners address are received from header of the block, Further, count indicates the number of times a node has sent various blocks for a particular UUID.

Table III Blocks with UU code and its Count

UUID	Miner's address in the block	Block number	Count
93EAA0F6-32AA-D8B0-3F44-C01850160ED4	1ECp2Rt6mbBkR8pG7DLmNq84HTYcAo69JK	#156789, #167453, #146739	3

If the count at the node N, reaches the threshold value T, then the UUID of node N is kept in the suspected list which represents that UUID is suspected as a Sybil node as presented in Table 4. This suspected list is spread among all nodes in the blockchain.

Table IV Suspected Node and its UUID

S.No.	Suspected UUID	No. of suspected nodes
1.	93EAA0F6-32AA-D8B0-3F44-C01850160ED4	7
2.	83EBB0H68-14VV-E7F0-2D55-P181189JK5	6

In this blockchain, if any block is received at a node, the miner's address in the block and the corresponding UUID is checked from suspected UUID list to check whether the block can be forward to other nodes. If the UUID with higher nodes count is found in the suspected UUID list, then it is considered that block is coming from the sybil nodes and the block coming from that node is dropped. Using the UU Code authors restrict the nodes identities that are found malicious.

VI RESULTS

To check the validity of the proposed method, authors have created the different genuine nodes and the suspected nodes on the networks are created as demonstrated in Table V.

Table V
Showing different Nodes and Network Creation

S.No.	No of Genuine Node	No of Suspected Node	Total Nodes
1	8	5	13
2	10	3	13
3	15	9	24
4	17	10	27
5	12	6	18
6	5	2	7
7	20	12	32
8	18	11	29

True Positive Rate (Tpr) is defined as the correctly identify the Sybil node present in the actual nodes. In the table actual nodes are the suspected nodes in the network. Using the proposed method

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7955
***Article Received**: 12 May 2023 **Revised**: 02 July 2023 **Accepted**: 29 July 2023*

True positive Rate= (Identify the Sybil Node Correctly) / (Total Sybil Node in network) (1)

False Negative Rate (FnR) is defined as Sybil node considered as genuine node in a network using the proposed method.

False negative Rate= (Identify the Sybil Node) / (Total Genuine Node in network) (2)

True Negative rate (Tnr) is defined as identifying the genuine node by the proposed method from the actual genuine nodes in the networks.

True Negative Rate= (Identify the Genuine Node Correctly)/ (Total Genuine Node in network) (3)

Accuracy is defined as, number of correctly identifying the genuine node and suspected node from the total nodes.

Accuracy= (Identify the Genuine Node and Sybil node Correctly) / (Total Node in network) (4)

The Final Results are shown in Table VI and Figure 6. For a clear presentation, a few instances of Table V are selected.

Table VI Results Based on Proposed Method

S.no	Tpr	Fnr	TnR	Accuracy
1	0.80	0.25	1	0.9
2	0.67	0.10	0.90	0.78
3	0.78	0.40	1.00	0.89
4	0.90	0.29	0.94	0.92

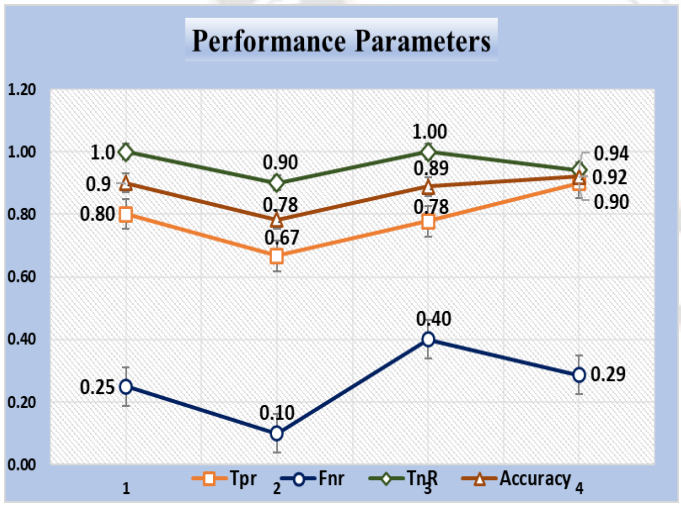

Figure 6 Results based on proposed method

VII DISCUSSION

One of Sybil prevention technique ensures that a single identity cannot control the Blockchain network. Similarly, a new method is proposed to control the identity creation in the network. Universal Unique Identifier is used to validate the identity of the node. It creates the validation check on each newly created node. Suspected nodes can easily be identified in the Blockchain network. The proposed methodology is validated on small networks, however, can be applied on social media and big networks. Single node validation is a highly effective way of verifying identities without requiring users to share their real-world identities. Results also confirm that it can easily & accurately identify the malicious and actual nodes in network.

VIII CONCLUSION

Sybil attack is an attack where single node creates many fake identities and hamper the network. In the permission less network any user can act as a malicious node if it gains 51% consensus in a Block chain network. In a small network, Sybil attacks are more frequent and gain undue advantages in the network. In the proposed work, UUID code is used for identity identification and prevention from the Sybil attack. The proposed method is illustrated on health care data that can be secured on the small networks. The results depict that the proposed methodology is better than the previous state-of-the-art approaches.

ACKNOWLEDGMENT

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

[1] I. Mubashar, and R. Matulevičius. "Exploring sybil and double-spending risks in blockchain systems." IEEE Access 9, 2021, pp.76153-76177.

[2] M. Iqbal and R. Matulevicius, ‘‘Comparison of blockchain-based solutions to mitigate data tampering security risk,’’ in Business Process Management: Blockchain and Central and Eastern Europe Forum. Cham, Switzerland: Springer, 2019, pp. 13–28.

[3] M. Iqbal and R. Matulevicius, ‘‘Blockchain-based application security risks: A systematic literature review,’’ in Proc. Adv. Inf. Syst. Eng. Workshops, 2019, pp. 176–188.

[4] J. R. Douceur. “The Sybil attack”, In Proceedings of the International Workshop on Peer to Peer Systems, 2002, pp. 251–260.

[5] J. Newsome, E. Shi, D. Song, and A. Perrig, “The Sybil attack in sensor networks: Analysis and defences", In Proceedings of International Symposium on Information Processing in Sensor Networks,2004, pp. 259–268.

[6] F. Anjam, P. Mouchtaris, “Security For Wireless Ad Hoc Networks”, Proc. Intersience Publishing, IEEE, 2007.

[7] M. Rahbari and M. A. J. Jamali. "Efficient detection of Sybil attack based on cryptography in VANET.", 2011.

[8] P. Swathi, C. Modi, and D. Patel. "Preventing sybil attack in blockchain using distributed behavior monitoring of miners." In 2019 10th International Conference on Computing, Communication and Networking Technologies,2019, pp. 1-6.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7955
***Article Received**: 12 May 2023 **Revised**: 02 July 2023 **Accepted**: 29 July 2023*

[9] M. Conti, S. K. E, C. Lal, and S. Ruj, "A Survey on Security and Privacy Issues of Bitcoin," in IEEE Communications Surveys & Tutorials, 2018. DOI: 10.1109/COMST.2018.2842460

[10] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," Financial Cryptography, 2014, pp. 1-18.

[11] Xiao Yue, H. W. "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control". Journal of medical systems, 2016, 218.

[12] Allison Ackerman Shrier, A. C.-t. "Blockchain and Health IT: Algorithms, Privacy, and Data,", 2017.

[13] Qi Xia, E. B. "BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments. Information, 2017.

[14] Kevin Peterson, R. D. "A Blockchain-Based Approach to Health Information Exchange Networks", 2016.

[15] Abdullah Al Omar, M. S. "MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data". International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, 2017, pp. 534-543.

[16] Yi Chen, S. D. "Blockchain-Based Medical Records Secure Storage and Medical Service Framework". Journal of Medical Systems, 5, 2018.

[17] Ahmed Faeq Hussein, A. N.-G. "A Medical Records Managing and Securing Blockchain Based System Supported by a Genetic Algorithm and Discrete Wavelet Transform". Cognitive Systems Research, 2018, pp. 1-11.

[18] Gaby G. Daghera, J. M. Ancile, "Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology", Sustainable Cities and Society, 2018, pp. 283-297.

[19] Zhang, A. and Lin, X., "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," Journal of medical systems, vol.42, no.8, 2018, pp.140.

[20] Tian, H., He, J. and Ding, Y., "Medical Data Management on Blockchain with Privacy," Journal of medical systems, vol.43, no.2, pp.26, 2019.

[21] Zhu, L., Wu, Y., Gai, K. and Choo, K.K.R., "Controllable and trustworthy blockchain-based cloud data management," Future Generation Computer Systems, vol.91, pp.527-535, 2019.

[22] J. Yun, and Mihui Kim. "SybilEye: Observer-Assisted Privacy-Preserving Sybil Attack Detection on Mobile Crowdsensing." Information 11, no. 4, 2020, pp. 198.

[23] S. Friebe, M. Florian, and I. Baumgart. "Decentralized and sybil-resistant pseudonym registration using social graphs." In 2016 14th Annual Conference on Privacy, Security and Trust (PST), pp. 121-128, 2016.

[24] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybilguard: Defending against sybil attacks via social networks," SIGCOMM Comput. Commun. Rev., vol. 36, no. 4, pp. 267–278, Aug. 2006.

[25] H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, "Sybillimit: A nearoptimal social network defense against sybil attacks," in Proceedings of the 2008 IEEE Symposium on Security and Privacy, ser. SP '08. Washington, DC, USA: IEEE Computer Society, 2008, pp. 3–17.

[26] N. Tran, J. Li, L. Subramanian, and S. S. Chow, "Optimal sybil-resilient node admission control," in the 30th IEEE International Conference on Computer Communications, 4 2011.

[27] P. Mittal, M. Caesar, and N. Borisov, "X-vine: Secure and pseudonymous routing in dhts using social networks," in 19th Annual Network and Distributed System Security Symposium, NDSS 2012, San Diego, California, USA, February 5-8, 2012.

[28] A. Almogren, I. Mohiuddin, I. Ud Din, H. Almajed, and N. Guizani. "Ftm-iomt: Fuzzy-based trust management for preventing sybil attacks in internet of medical things." IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4485-4497, 2020.

[29] J. Newsome, E. Shi, D. Song and A. Perrig, "The sybil attack in sensor networks: Analysis and defenses," Proc. Int. Symp. Information Processing in Sensor Networks (IPSN), 2004, pp. 259- 268.

[30] C. Yu , S. Gupta and A. Agrawal, "Location based Technique to prevent Sybil attack in wireless sensor networks," International Journal of Reliable Information and Assurance, vol. 5, no. 1, 2017, pp. 1-8.

[31] L. Xu, S. Chainan, H. Takizawa and H. Kobayashi, "Resisting Sybil Attack By Social Network and Network Clustering," 10th IEEE/IPSJ International Symposium on Applications and the Internet, Seoul, 2010, pp. 15-21.

[32] B. Triki, S. Rekhis, M. Chammem and N. Boudriga, "A privacy preserving solution for the protection against sybil attacks in vehicular ad hoc networks," 6th Joint IFIP Wireless and Mobile Networking Conference (WMNC), Dubai, 2013, pp. 1-8.

[33] G. Bissias, A. Pinar, O. Brian, N. Levine and M. Liberatore, "SybilResistant Mixing for Bitcoin," Workshop of privacy in the electronic society, 2014, pp. 149-158.

[34] S. J. Samuel and B. Dhivya, "An efficient technique to detect and prevent Sybil attacks in social network applications," 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, 2015, pp. 1-3.

[35] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll and E. W. Felten, "Mixcoin: Anonymity for bitcoin with accountable mixes," in 18th International Conference, FC 2014. Springer Berlin Heidelberg, 2014, pp. 486–504.

[36] L. Valenta and B. Rowan, "Blindcoin: Blinded, accountable mixes for bitcoin," in Financial Cryptography Workshops, 2015, pp. 112-126.

[37] E. Heilman, L. Alshenibr, F. Baldimtsi, A. Scafuro and S. Goldberg, "Tumblebit: An untrusted bitcoin-compatible anonymous payment hub," NDSS Symposium, 2017, pp. 1-36. http://eprint.iacr.org/2016/575.

[38] M. Numan, F. Subhan, W. Z. Khan, S. Hakak, S. Haider, G. T. Reddy, A. Jolfaei, and M. Alazab, ''A systematic review on clone node detection in static wireless sensor networks,'' IEEE Access, vol. 8, pp. 65450–65461, 2020.

[39] P. Winter, R. Ensafi, K. Loesing, and N. Feamster, "Identifying and characterizing Sybils in the Tor network," 25th USENIX Security Symposium, 2016, pp. 1169-1185.