Applied Mathematics and Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/170214

Automated Classification of The Sybil Attack in BlockChain Network Using Multi Neural Memory Network Classifier

D. Nancy Kirupanithi[*], *A. Antonidoss and G. Subathra*

Computer Science and engineering and Hindustan Institute of Technology and Science, Padur, Chennai, India

Received: 22 Nov. 2022, Revised: 22 Dec. 2022, Accepted: 14 Feb. 2023
Published online: 1 Mar. 2023

Abstract: Block chain technology is a distributed form of digital record that does not need any central authority. As all the information available in the block chain are transparent, everyone can see it. Since blockchain technology is almost hack-proof, it has attracted several industries like business, academia, government, and healthcare. Common concerns regarding Blockchain technology's impact on privacy and security are unfounded, and may be attacked in a number of ways. We discovered that the Sybil attack has a significant effect on public/permissionless blockchains because an attacker may undermine the blockchain by generating a large number of pseudonymous identities (i.e. Fake user accounts), making genuine entities a minority. These artificial nodes may mimic real ones and have outsized effect on the network just as they would if theywere real. This might result in a cascade of assaults including denial-of-service and distributed denial-of-service. In this work, we show how a Sybil attack might reduce the throughput of a blockchain test bed. We provide a solution directive in which every node keeps tabs on the actions of the others, looking for the ones that are forwarding the blocks for only one user. Initially by preprocessing the input data from network are normalized. Then by smart contract the transactions are created. By promptly identifying, blacklisting, and notifying other such nodes in the transactions, the Sybil attack's reach may be restricted by using the Multi Neural Memory Network (MNMN) classifier. Then the data can be securely stored in the block chain ledger by using the stream cipher Crypto Fish algorithm. We analyze experimental results of the proposed solution under simulation environment. The evaluation of performance is observed and compared with other traditional method. The proposed model is proved to be an efficient one in its throughput, accuracy and execution time etc.

Keywords: Block chain, Sybil attack, Multi Neural Memory Network(MNMN)classifier, Smart contract, Stream Cipher Crypto Fish, Ledger

1 Introduction

In spite of rapid growth of cloud computing for several centuries, secured data and reliable computation remains to be a challenging one. Hence to solve this issue the blockchain technology was introduced which provides remedy for the lack of scalability and computational complexity along with data integrity. Blockchain technology is comprised of unit that performs work logically in the transaction form that can read or write process and stored in the structure of blocks. This can be accessed from various servers. As third party is not involved in block chain technology, the data are secured with sequential transaction recordings in a transparent manner. The evolution of block chain has modifications with smart contracts to provide the system of security. However, several attacks and vulnerabilities cause financial losses in some cases. For the aspects of security many cryptographic algorithms are validated. Analysis of threats in current system of block chain are discussed in theoretical and practical manner. The model of quantum computing along with present system security was concerned. The technology of block chain makes the cost consumption by digital recording and has lot of advantages like trust ability, accessibility and integrity. Also, utility tokens, equity tokens, currency tokens and asset tokens are available in blockchain. Since Blockchain technology is a peer-to-peer network, it is being employed in many domains like energy systems, cryptocurrencies, healthcare, internet of things-based systems, banking, education and many other systems [1,2,3]. Sybil attack,

[*] Corresponding author e-mail: nancykirupa22@gmail.com

Identity Spoofing and Blackhole are some of the attacks that cause destruction in blockchain implementation. Among this sybil attack causes higher vulnerability, as the attacker misinforms other nodes by observing the identity of users wrongly that are aware from the network nodes. Nodes claim several identities illicitly in the sybil attack. The routing of network, data aggregation, misbehaviour detection and resources allocation have also been intimidated by the sybil attack. In the remote sensor organisation huge damaging assault happens because of sybil attacks accompanied by sinkhole and wormhole. This causes hazardous communication in the hub of organisations and hence the method of password comparison technique is permitted for checking the hub of the companies. Verification of method and Comparison with match position are projected. Identification and prevention of sybil attacks are done by the MAP method. Multicasting and unicasting assaults are handled to ensure the organization's protection [4,5]. Long Short-Term Memory in a densely connected network is utilized in vector based cyclic co-entropy method that can detect the sybil attacks, deceptive jamming and pilot jamming for the security in physical layer. LSTM was integrated with dense network and developed a long short-term memory densely connected network. LSDM was trained with cosine loss for increasing the feature differences in interclass and decreasing the feature variations of intraclass [6]. The method provided the secured scheme with efficient generation of key and authenticity is provided for entities of communication. The characteristics like immutability, openness, fault tolerance, data privacy, traceability and security are exploited in the blockchain technology architecture. As blockchain technology based distributed IoT structure utilizes hash chains for key management security, the trusted third-party management can be performed with key generation [7]. A collaborative model of clustering-characteristics based fusion of data for intrusion detection was proposed in this paper where a mathematical implementation of data fusion was constructed and with the utilization of AI model, data clusters were trained and analyzed in the network of block chain. The irregularity in characteristics of blockchain was observed and weighted coefficients of various nodes were obtained from the multiple rounds within clustering nodes. The behavior of abnormal intrusion was detected by this method accurately [8]. A framework of self-learning-based detection of attack was developed that makes prediction and training of closed loop system based on the false information broadcast of packets in the network communication. By the use of LSTM neural network, the unpredicted malicious behavior was self learnt and self-extracted thereby improves the quality and efficiency of detection in traffic data. This method detects the sybil attack earlier in an accurate manner in the car network [9].

In our work, initially by preprocessing the input data from network are normalized. Then by smart contract the transactions are created. By promptly identifying, blacklisting, and notifying other such nodes in the transactions, the Sybil attack's reach may be restricted by using the Multi Neural Memory Network (MNMN) classifier. Then the data can be securely stored in the block chain ledger by using the stream cipher Crypto Fish algorithm. We analyze experimental results of the proposed solution under simulation environment. The evaluation of performance is observed and compared with other traditional method.

Further organization of this paper is structured as follows: section II is the analysis of various existing methods reviews employed so far. Section III is the detailed explanation of proposed system. The performance analysis of proposed system is estimated, and the outcomes compared are projected in section IV. At last, the conclusion of work is made in section V.

2 Related Work

In this section, several research papers are overviewed for analyzing the blockchain network architecture along with sybil attack classification methods.

[10] provided the model of distributed virtual machine agent which was employed in the technology of mobile agent. A framework of blockchain based integrity protection was built with the help of virtual machine proxy model. A new distributed decentralized computing paradigm called blockchain was applied to cloud computing in this model and mechanism of security was improved. In this paper, the virtual machine agent supports the multitenant to guarantee the verification of data trust. The hash value generated by Merkel hash tree file was aided for monitoring the data change as it uses smart contract on the blockchain. The notification of alert was issued for data tampering and mode of block and response was constructed with scheme of blockchain based cloud data integrity.

[11] proposed the scheme of detecting sybil attack based on the proof of location and work. Time stamped tag was provided for locating anonymous issue in this method. The fake path was identified from the location by proof of work algorithm implementation. Multiple path locations are prevented by using this algorithm. Matching technique are used to identify the paths of sybil attack vehicles. Path overlapping are overviewed in this method. The results of simulation demonstrated shows that this method achieves higher detection rate with less false negative of sybil attacks. It also obtains overhead of computation with acceptable communication in its experiments.

[12] explained the architecture of block chain as the networks consisting of successive blocks which are linked to one another by the former block's preferences. Hence it forms a chain like structure to form a database. Distributed transactions are supported by the formation of digital ledgers. In real world applications, the network of

blockchain faces many risks. In this paper, author aimed to focus on the characteristics, concepts of implementation and distributed transactions of blockchain technology through resources of web. Issues and recent trends of blockchain are also examined in the e-commerce applications.

[13] provided the information about detection of sybil attack in the blockchain network that can create a fake identity was monitored. Simulation series were performed in the environment of implementation for the process of cryptocurrency along with limited computing power and network parameters. It was difficult to extract the blocks in this method. Initially the network nodes are distributed evenly and the output of block distribution was checked. In another test performed, the computing power are allocated randomly to all the network nodes. The simulation results are discussed with statistical analysis and parameter were evaluated finally.

[14] explained about the security level of blockchain network which was said to be proportional directly to the power of hash computing in the blockchain. When the process of mining by miners are increased the attack on block chain by attackers become difficult. Attacks like eclipse attack, DDoS, Sybil attack, parity attack, DAO attack, race attack and Finney attack were tougher to implement, since the power of computation was difficult on the blockchain. Some of the solutions and measures were described for mitigating the risks of the vulnerabilities.

[15] presented a model of Multi-Level Trust Mechanism solution that depends on blockchain for detecting the sybil attack. In this approach, there are three levels: first one was Horizontal Trust Management mechanism to detect the malicious vehicles, that adopts Local Machine Learning algorithm, next one was the Vertical Trust Management mechanism that was utilized to implement verification algorithm. At last, the Distributed Trust Management mechanism that can detect the class in the network. The integration of various components of VANET thus provided an effective scheme for detecting sybil attack.

[16] proposed a framework of blockchain based cyber threat intelligence to expand confidence within content and source data thereby detects and rejects improper data for opposing the sybil attack. As CTI was collected, the process was validated by smart contracts and metainformation of data were stored in the blockchain network. The reliability and validity of CTI were ensured by the proposed system. Also, a system model was proposed to operate and maintain CTI data with the standard of de facto model. the simulation results have proved that the proposed model was effective in terms of cost to attackers and reliability.

[17] offered the mechanism of trust chain that permits data structure of less tamper proof that stores transaction records. The method allows validity, integrity, openness, scalability along with sybil resistance. A novel sybil-resistant algorithm was introduced and termed as NetFlow which is used to resolve agent's trustworthiness. The contribution of NetFlow secures the agents. The results of experiments shows that throughput of TrustChain outperforms the traditional methods of blockchain technology. Also, it was proved that data extracted in the real time are having required information to detect the attackers.

[18] discussed about the approach to detect and compute decentrality in the system of blockchain. Initially, the three layers such as governance layer, storage layer and network layer were identified. Decentrality of these layers were evaluated with the use of different metrics. Entropy, fairness, Kullback-Leibler divergence and Gini coefficient were measured in governance layer whereas in the network layer closeness centrality, betweenness centrality and degree centrality are measured. For defining centrality, distribution index was employed in the storage layer. With the governance of few nodes, the blockchain network tends to act as centralized system.

[19] developed a model to explore the risks of security with the support of security risk management domain. In the blockchain network, Sybil and Double spending have been considered as the security risks. Various illustrations like secured assets, types of threats that were triggered by sybil attack and detection of double-spending threat, threat vulnerabilities and measures to encounter threats were also explained in this paper. Implementation challenges were also recognized and discussed about the permissioned blockchain systems. Outlined the future work of building an ontology-based model of blockchain security.

[20] proposed the scalable and location-based protocol termed as Geographic-PBFT that are used for applications of IoT-blockchain. Data collection and processing are the applications performed by IoT blockchain with IoT devices. Sybil attacks were avoided by exploitation of geographic information by G-PBFT as it uses fixed IoT devices. To minimize the overhead for recording and validating transactions, the loyal, fixed and abled nodes were selected as endorsers. This method attains high efficiency with less traffic intensity. The experiments with proposed and existing model were compared and evaluated extensively show that the network overhead and consensus time were minimized with effective scalability.

[21] presented the work based on block technology for Sybil secured forest fire surveillance. The architecture with three layers namely IoT layer, Fog layer and Cloud layer were encompassed in this work. Also, a framework of secured and sybil protected transmission of data with block chain technology in wildfire was proposed. Further, blockchain consensus algorithm with better energy efficiency had been modelled and implemented. With different QoS metrics the proposed system was evaluated and compared.

[22] described the use of agent-based simulator called parallel and distributed simulation of blockchains which

achieves better scalability. Distributed Ledger technology of blockchain was simulated with the software made of several nodes. Different types of attacks like sybil attack, 51% attack and selfish mining were simulated and the performance analysis shows that the model proposed was accurate with enhanced output detection. The paper mainly focused on the peer-to-peer layer for attack detection. The hash rate, computing power and security aspects were investigated in this model.

3 Proposed Work

In this work, we show how a Sybil attack might reduce the throughput of a blockchain test bed. We provide a solution directive in which every node keeps tabs on the actions of the others, looking for the ones that are forwarding the blocks for only one user. Initially by preprocessing the input data from network are normalized. Then by smart contract the transactions are created. By promptly identifying, blacklisting, and notifying other such nodes in the transactions, the Sybil attack's reach may be restricted by using the Multi Neural Memory Network (MNMN) classifier. Then the data can be securely stored in the block chain ledger by using the stream cipher Crypto Fish algorithm. We analyze experimental results of the proposed solution under simulation environment. The evaluation of performance is observed and compared with other traditional method. The entire flow of the proposed model is as follows:

A. DATA PREPROCESSING:

The data acquisition of network traffic contains raw data of several attributes which are used to find the target variable. In the real time data analysis, input data are gathered from massive traffic records present in internet and are grouped into dataset. From these records of dataset, the attack detection is going to be executed. As the preprocessing of data is a vital technique the categorical information is transformed to binary data by removing the null values, missing values, inappropriate values and data refining. Some of the duplicate values are combined for various attributes and created a dataset which are forwarded to the phases of training and testing.

Initially the datasets are divided into training and testing datasets. In the training datasets, data labelling is performed by identifying the traffic and category of attack present. In the testing phase, normalization is performed to a specific range that is between 0 and 1. This makes the input data to fit effectively. By using the Min-Max normalization function this is done with the equation as follows:

$$y_i(n) = y_i(n) - \frac{Min(y(n))}{Max(y(n)) - Min(y(n))} \tag{1}$$

where Max and Min functions denote the maximum and minimum values correspondingly from the original dataset for every value y_i of the feature n. Since the datasets are partitioned into training and testing datasets the detection accuracy of the model will be best in implementation. By the trained model, the testing is performed in each row on the testing dataset. From this, the records are classified into normal and attack record. Further processing of model is done with this sample records of attack.

B. MULTI NEURAL MEMORY NETWORK (MNMN) CLASSIFIER FOR SYBIL ATTACK CLASSIFICATION:

The sample input given to the Multi Neural Memory Network (MNMN) Classifier identifies the sybil attack existing in the blockchain network. To detect and classify sybil attack accordingly, MNMN classifier was utilized as it exploits the technique of Deep Learning algorithm which has ability to capture data of long-term dependencies. In general, Deep Artificial Neural Networks assumes its input to be independent of one another and only receive inputs of fixed size to generate outputs of fixed size. Since DNN is unable to operate with input of varying length, the adoption of Recurrent Neural Networks is followed to work on varying lengths of input sequences in this proposed system. Hence this combination of DNN with RNN form the Multi Neural Memory Network which can predict the current previous stamp from the information obtained from the previous timestamp. Thus, short-term dependencies between within input and output are extracted. The problem of vanishing gradient is solved by using proposed MNMN as a classifier.

Since Multi Neural Memory Network is an improved form of neural network, it utilizes the input at recent timestamp and information from the former timestamps for generating the output. Backpropagated error decay can be sorted out by using MNMN classifier. As the network has many neutron layers, it captures data of long-term dependencies with the aid of recollecting information for longer time. MNMN decides what to be eliminated from the memory and what information to be retained. The classifier uses three gates termed as Input gate, Output gate and Forget gate in order to add, remove information and produce the output.

$$\text{Input Gate} : I_g = \sigma(w_j.[t_{g-1}, x_g] + h_g) \tag{2}$$

$$\text{Intermediate Cell state} : \tilde{S_g} = tanh(w_C.[t_{g-1}, x_g] + h_S) \tag{3}$$

$$\text{Forget gate} : F_g = \sigma(w_F.[t_{g-1}, x_g] + h_F) \tag{4}$$

$$\text{Output Gate} : O_g = \sigma(w_O.[t_{g-1}, x_g] + h_O) \tag{5}$$

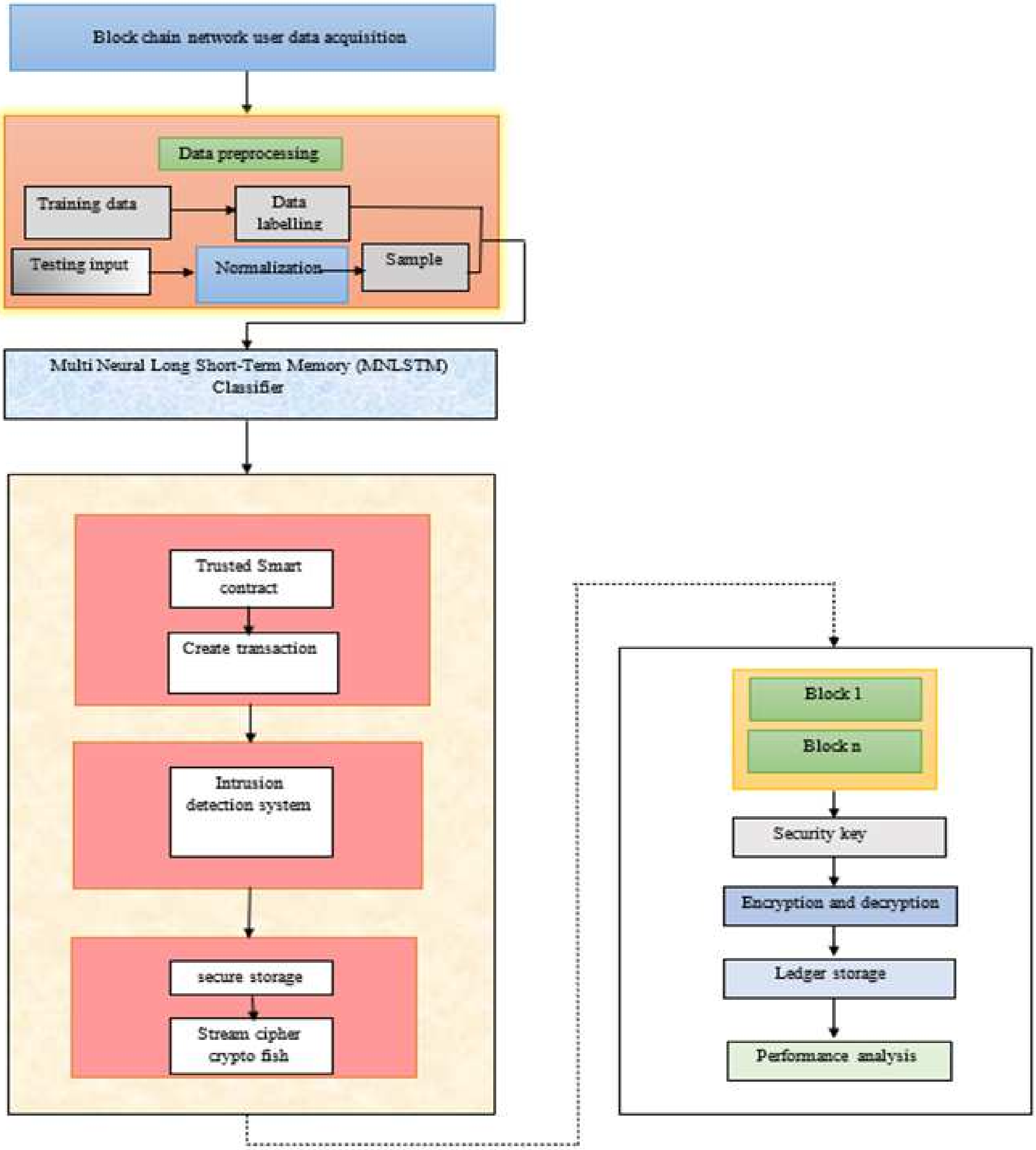

Fig. 1: Schematic Representation of Proposed Model

$$\text{Cell state} : C_g = F_g C_{g-1} + I_g \tilde{S_g} \tag{6}$$

$$\text{Hidden state} : H_g = tanh C_g \times O_g \tag{7}$$

The working progress of three gates along with its different states of MNMN are shown in the above equations (2) to (7) and σ represents the sigmoid activation function, tanh denotes the function of hyperbolic tangent activation, x_g is the input at time g, the weights are denoted as w_O, w_F, w_j, w_C and biases are denoted as h_g, h_S, h_F, h_O. Hence by the architecture of

MNMN, the gating mechanism solves the vanishing gradient problem of neural networks.

ALGORITHM1: MULTI NEURAL MEMORY NETWORK (MNMN) CLASSIFIER

```
Data input: sample t
Output: detected class label for sample t
Do classification on the sample t using MNMN in layer1
Assume the class label detected as$d_i$
If $d_i$ represents the normal class
    $d_i$ is the final predicted class label for sample t
Else if $d_i$ represents attack class
    //perform classification in next layer to identify attack class
    Send sample t to layer 2
Classify sample t using classifier $c_1$
Assume the class label predicted as $d_j$ by $c_1$
Classify sample t using classifier $c_2$
Assume the class label predicted as $d_k$ by $c_2$
// assign O as the set of pretrained dataset
Select $c_3$ as classifier from O so that $c_3$ is trained for
distinguishing classes $d_j$ and $d_k$
Classify sample t by classifier $c_3$
Attack class predicted by $c_3$ is the final sybil attack
of predicted class label for sample t
```

Hence the sybil attack is identified and notified to the other nodes of blockchain network with the support of Multi Neural Memory Network classifier.

C. TRUSTED SMART CONTRACT:

Smart contract is the common trusted central authority agreement between two or more services without involving private parties. It is a computer programs which are executed by the network of distrusting mutual nodes without the help of any trusted nodes. It contains information, process inputs along with outputs. In the blockchain, a new smart contract is hosted by means of invoking the function of constructor and enabled the trusted smart contract function. In general, smart contract includes functions, state variables, events, function modifiers and structures that can execute and regulate the relevant events. It performs actions based on the terms of contract. The final process code of the smart contract will be stored on the blockchain and then the available smart contract function can be invoked by the users through the transactions.

Trusted Smart Contracts integrated with blockchain features provides authentication, access control and authorization. Also, the integrity of the data, data security and integrity preservation are also maintained. The trusted smart contract sustains with function secrets, utilize cryptography and prevent data revealing on the blockchain. Distributed storage, immutable characteristics and enforcement mechanisms are adopted by the trusted smart contract

(i) Create transaction:

In the block chain network, transaction can be a confidential information or financial data based on the type of application. Using the trusted smart contract, transaction address is created in the block chain network. The transaction is created with the fields namely transaction type, user, identity, public key, user name, time stamps and signatures. They are explained in detail as follows,

1.Transaction type: The variable termed as transaction type is used in the blockchain through which the actual transaction takes place. This occurs between the authorized user who has signed with the private key of individual user. The transaction type is registered in the block and cannot be forged or modified after the completion process of authentication.

2.User and Identity: In this smart grid system, user represents any entity and an identity describes a unique representation of the user.

3.Public key: Public key is generated in the blockchain that works as an address string and it acts as the role of an account. Additionally, the public key uploaded in the blockchain and it is open to all.

4.User Name: As the length of public key is too long, a human readable user name is provided for user access. The model allows user to choose a unique user name and links this name to their public key. The users can get other users public key along with relevant information by means of usernames.

5.Timestamp: In our model, timestamp is utilized to authenticate every transaction record and displays the authenticity of the transaction records like that of authorization of the transaction contracts. In the transaction sequence the timestamp delivers the natural time record as the part of blockmetadata.

6.Signature: Another important entity is signature, as it is essential to ensure that the transaction contents are not forged by signing. Since the transactions are public, anybody can retrieve all the details even though they were not added to the list of blockchain.

The transaction data to be secured is further encrypted and authenticated for future transaction to uphold data security. In our method private key authentication is allowed to sign the hashed data of individual and produced a digital signature to authenticate. The other nodes in blockchain network uses the public key for authentication of data transaction.

(ii) Intrusion Detection system by Deep learning models:

In the cloud network, RNNs are applied for intrusion detection (IDS) for identifying vulnerabilities. As it uses its internal memory for sequence of data within loops, it is considered to be a prevalent deep neural network. Temporal sequence must be tackled relevantly in the IDS system. When depending on the spatial domain, the temporal patterns would enhance the anomaly or outlier detection, which does not take time into an account. The sequence of input is tackled in a series of period steps and memory associated is updated.

Let us assume that the series of input vectors as $i(t)$ and the sequence of output vectors as o(t) that are produced in the time step of $t \in [1,t_s]$ for particular time interval t_s. When the process starts with one vector of the input sequence, with the internal state vector is represented as $v_0(t) = i(t), \forall t \in [1,t_s]$ and $v_j(0) = i(t), \forall j \in [1,N]$. Using the cost function, the parameters of RNN are evaluated with affine transformation, output of previous vectors and linear transformation. Hence the calculation is shown below as:

$$W_j(t) = A_j v_{j-1}(t) + B_j v_j(t-1) + p_j \tag{8}$$

$$v_j(t) = \sigma_j(W_j(t)) \tag{9}$$

where $v_j(t)$, $W_j(t) \in T^{nj}$ and $m(t) = v_j(t)$, and A_j is the weight matrix from input to the hidden layer, B_j is the weight matrix between two subsequent hidden states $(v_j(t-1)$ and $v_j(t))$, p_j is the bias vector of the hidden layer and σ_j is the activation function to generate the hidden state. The output of network can be hence structured as:

$$o(t) = \sigma_j(H_j v_j(t) + p_y) \tag{10}$$

In equation (10), H_j is the weight matrix from the hidden layer to the output layer, p_y is the bias vector of the output layer and σ_j is the activation function output layer. By means of back propagation method the parameters are trained and updated in an iterative manner. The hidden layer will produce the value $o(t)$ and the final output $o(t_s)$ is the predicted attacks of network in each time step t.

(iii) Crypto Fish method based on Stream ciphers:

After intrusion detection the data stored securely are further process by stream cipher based Crypto Fish method. The stream cipher encrypts each character of text data bit by bit or byte by byte. It uses an encryption method that differs with time. As it has higher efficiency based on resources and speed, stream cipher is considered to be main source of cryptographic algorithms for securing data. In this paper, a stream cipher-based algorithm named crypto fish is used to encrypt the data obtained. By the principle of shrinking to the stream cipher, algorithm depending on Fibonacci generator is used for implementation.

Let us consider Gand H to be two pseudo random generators. Both of the generators produce sequence of elements. By the method of mapping, the elements of generators are either acceptable or discardable. For the word length of 32 bit, the processor chosen is P_a = 32 and P_b = 32. The fastest software additive generator called Fibonacci generator is utilized for both the G and H

It is defined that

$$g_i = g_{i-55} + g_{i-24} \; mod 2^{32} \tag{11}$$

$$h_i = h_{i-52} + h_{i-19} \; mod 2^{32} \tag{12}$$

where carry is included in equations (11) and (12). The unsigned numbers are the interpretation of binary vectors. The initial values of generators are assigned as $g_{-55}, g_{-54}, \ldots, g_{-1}$ and $h_{-52}, h_{-51}, \ldots, h_{-1}$. The least sequence significant bits are generated by the Fibonacci shrinking generator from which the trinomial feedback is generated.

By mapping 32-bit vector to its least significant bit is obtained. The resulting structure is linear. Hence the attackers may try to identify it, the linear structure could be hidden.

Hence the sequences are divided into $n_0, n_1, \ldots$ and $m_0, m_1, \ldots$ up to pairs (n_{2i}, n_{2i+1}) and (m_{2i}, m_{2i+1}) and the two 32-bit output words p_{2i}, and p_{2i+1} were derived by this. Its defined that

$$a_{2i} = n_{2i} \oplus (m_{2i} \wedge m_{2i+1}) \tag{13}$$

$$b_{2i} = m_{2i+1} \wedge (a_{2i} \oplus n_{2i+1}) \tag{14}$$

$$p_{2i} = a_{2i} \oplus b_{2i} \tag{15}$$

$$p_{2i+1} = n_{2i+1} \oplus b_{2i} \tag{16}$$

where $\oplus$ represents the bitwise logical exclusive OR and $\wedge$ represents bitwise logical AND. Equations (14) to (16) achieve an exchange of bits in a_{2i} and n_{2i+1} which are 1 in m_{2i+1}. The value of least significant bits m_{2i} and m_{2i+1} are 1 as we have selected function b. hence it is possible to build the least significant bits of n_{2i} and n_{2i+1} from p_{2i}, and p_{2i+1} and vice versa the least significant bits of p_{2i}, and p_{2i+1} follows n_{2i} and n_{2i+1}. This infers the output words of crypto fish are the bits of the shrinking generator which achieves the trinomial feedback. This type of sequence encryption generally simulates the one time one key system. Therefore, random keys are easy to create, synchronize and manage. The plain text sequence and bitwise key sequence are operated with exclusive OR function to obtain the cipher text. The selected plaintext and key are independent to each other.

D. BLOCKCHAIN NETWORK:

A unique and innovative technology for sharing and transferring confidential data between untrusted nodes in the network is termed as block chain technology. As it consists of non-erasable information records or blocks in its distributed database, they are managed by set of nodes and not by an individual centralized authority. In blockchain, one block is linked to its preceding block with the aid of previous hash value of the block. Every block in the network holds a copy of ledger in it. When the attacker wants to hack the security of the blockchain, it will be more difficult for him/her as mathematical problem of each node has to be solved and it involves more computational power and expensive at the same time. Hash function for encryption and digital signature for authentication are the two security functions involved in security of blockchain. Hence, blockchain technology has an unbreakable security.

Data integrity through Encryption and Decryption:

In general, on the consensus mechanism sybil attacks waste the computational resources of the nodes by controlling most of the nodes in the network of blockchain. An attacker intends to broadcast the newly invented block to the whole network. Also, in sybil attack, they continue to mine for valid new block. On the network, sybil attacks refer to weakening of malicious node or destroying the mechanism of redundant backup or controlling multiple nodes. Due to this attack multiple data backup on the sybil nodes would be compromised or corrupted. In the designed protocol in network side, each entity could have only one public key an identity and hence it could have only one secret key in association with the public key. To ensure integrity of the system, each message is signed in by the secret key. The system verifies the public key embedded to the Username and so the attacker cannot use false public key. This prevents the sybil attack in the block chain.

Finally, after the process of cryptography in the blockchain network, both the digital signature and transaction data are broadcasted. The transactions are validated by the process of decryption of digital signature as it utilizes sender's public key for authentication. Next, comparison of decrypted digital signature and hashed transaction data is performed for integrity. This collects the valid transactions in the block. In the network, to produce the valid block for the selected miners, a block with valid transactions is broadcasted. To validate the block, the miners use consensus protocol. Next to validation, the miners broadcast a valid block, which is then added to the blockchain network. The ledger of every node is then updated and this is transparent or visible to everyone publicly. Identical copies of records are hold by all the nodes in the blockchain network with transaction update and hence it is resistible to the attacks and leakage of information.

4 Performance Analysis

In this section, performance analysis of proposed model is evaluated and is compared with the existing techniques to prove the efficiency of the proposed technique.

Evaluation metrics of classifiers:

Accuracy =

$$\frac{Truenegative + Truepositive}{Truepositive + Truenegative + Falsepositive + Falsenegative} \quad (17)$$

Recall represents the number of sybil nodes of a network that were detected among the nodes that belongs to the network. If network A comprises of p nodes, out of which only q nodes are detected accurately and it is termed as recall that is calculated as

$$\text{Recall} = \frac{q}{p} \quad (18)$$

Precision represents the number of nodes that belong to the network out of all the nodes that were identified as belonging to the network. If p_{nA} denotes the number of nodes that were identified as network of A nodes, out of these only q_{nA} nodes belong to network A, then the formula for precision is represented as follows:

$$\text{Precision} = \frac{q_{nA}}{p_{nA}} \quad (19)$$

F1-score denotes to the harmonic mean value of Recall and Precision. As it is a metric for evaluation, it offers equal weightage to both Precision and Recall scores. Hence F1-score is calculated by the formula,

$$\text{F1-Score} = \frac{2}{\frac{1}{Recall} + \frac{1}{Precision}} \quad (20)$$

Attack detection rate is calculated based on the number of correctly identified attacks.

From the table 1, it is observed that evaluation metrics like accuracy, attack detection ratio, recall, precision and F1-score are evaluated for proposed Multi Neural Memory Network and existing classifiers. The

Table 1: Performance Analysis of Various Classifier in Attack Detection [23]

Classifiers	Accuracy	Attack Detection Rate	Recall	Precision	F1-score
DNN	0.57	0.61	0.59	0.65	0.62
CNN	0.77	0.64	0.76	0.75	0.73
XGB	0.43	0.58	0.53	0.55	0.53
RF	0.42	0.76	0.68	0.69	0.65
LIO-IDS	0.87	0.85	0.82	0.85	0.82
Proposed MNMN	0.97	0.91	0.93	0.94	0.95

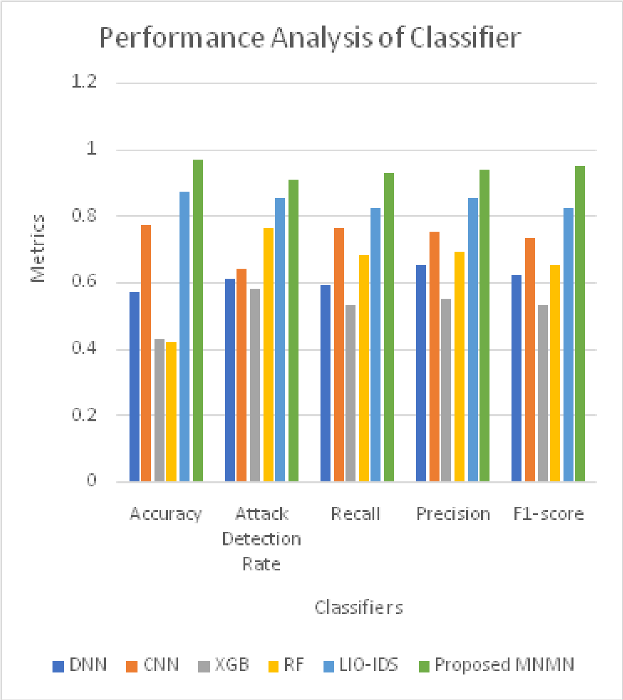

Fig. 2: Analysis of Various Classifier in Attack Detection [23]

comparison shows that the proposed MNMN classifier outperforms in its accuracy, attack detection ratio, recall, precision and f1-score.

In the figure 2, various classifiers and proposed classifier are compared for its accuracy, attack detection ratio, recall, precision and F1-score. It is analyzed that proposed MNMN classifier has achieved accuracy, attack detection ratio, recall, precision and F1-score greater than other classifiers.

Additionally, True Positive Rate (TPR) and False Positive Rate (FPR) are calculated. FPR is referred as incorrectly detected malicious node and TPR is same as recall.

Table 2: Performance Comparison of Classifiers based on TPR and FPR [23]

Classifiers	TPR	FPR
DNN	0.1	0.7
CNN	0.04	0.65
XGB	0.1	0.45
RF	0.12	0.4
LIO-IDS	0.2	0.8
Proposed MNMN	0.1	0.9

It is observed from the table 2, that TPR and FPR values are higher in proposed MNMN classifier than other existing techniques.

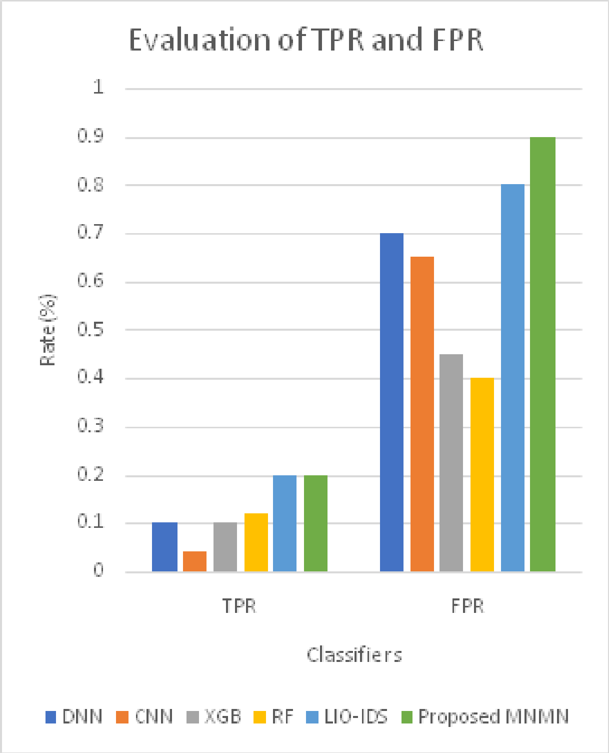

Fig. 3: Analysis of Classifiers based on TPR and FPR [23]

The figure 3 represents the analysis of proposed MNMN and existing classifiers. It shows that the proposed model is effective than other existing classifiers.

The proposed MNMN model can enhance the performance of the intrusion detection system better than other existing models. As it is a multi-neural memory classifier, it has better adaptability and computation. Also, memory requests are reduced significantly. MNMN can better distinguish the attack types and further classifies the sybil attacks abnormality. Identifying attack behaviors and preservation of privacy are the perfect benchmarks of the proposed MNMN classifier. The model of two-fold privacy with blockchain and smart contracts achieves the flawless protection by validating transaction of data and feature extraction from the source data for training and testing of intrusion detection model. initially in the privacy-based block chain data integrity is validated and then the records are verified with the hash values. Next the data is encrypted by validating abnormal behavior identification. False Alarm rate obtained is lower in the proposed MNMN classifier than the other models like RF, NB, SVM, BiLSTM and MLO. This proves that the proposed scheme achieves best rate of sybil attack detection compared with other existing models.

Table 3: Evaluation of False Alarm rate for Classifiers [24]

Classifiers	False Alarm Rate (%)
BiLSTM	1.5
SVM	3
RF	2.7
NB	3.1
MLO	2
MNMN	0.8

The above table 3, shows the false alarm ratio of proposed MNMN and other existing models. The comparison shows that for the proposed MNMN classifier the false alarm rate is lesser than others and this outstates the efficiency of proposed scheme is better.

In figure 4, graph is plotted for the false alarm rate comparison for different classifiers. The analysis of it shows that the proposed MNMN has obtained lesser false alarm rate and hence it is validated to be an efficient classifier.

Throughput Analysis in Stream Cipher based Crypto Fish:

Achieving high throughput in a data encryption and decryption is a challenging process. The performance of an algorithm will be higher when its throughput is high as they are directly proportional to each other. Throughput is computed by calculating the average amount of data that is encrypted or decrypted in byte per unit. The formula for throughput is hence represented as:

$$\text{Throughput} = \frac{No.of\ bytes\ that\ are\ encrypted\ or\ decrypted}{Time\ Taken} \qquad (21)$$

The proposed Crypto Fish, RC4, Salsa20, Rabbit and SCKHA are the stream cipher methods that are characterized by its efficiency. The data files of different sizes as 100KB, 500 KB and 1MB are used to evaluate the throughput. By the dynamic key selection process, the proposed Crypto Fish method is performed.

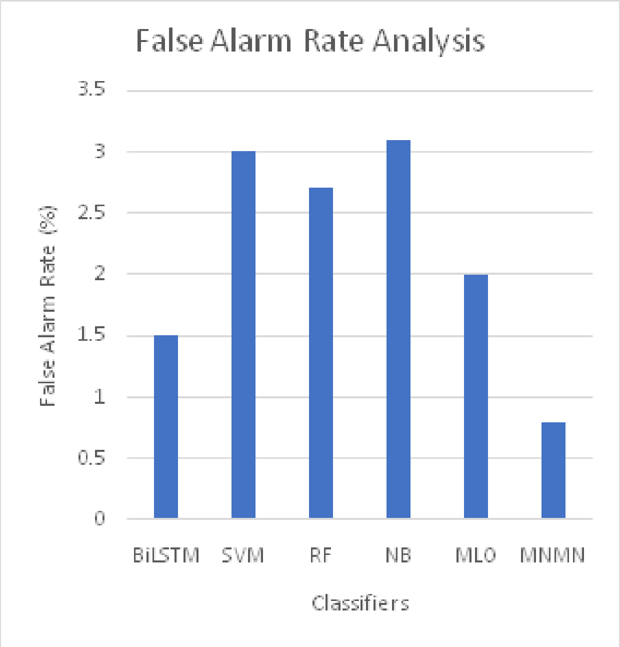

Fig. 4: Analysis of classifiers based on False Alarm Rate

Table 4: Throughput comparison of Stream Cipher Techniques [25]

Technique	Throughput of 100KB	Throughput of 500KB	Throughput of 1MB
RC4	36.93	25.06	9.66
Rabbit	13.37	8.49	3.21
Salsa20	7.21	4.01	1.56
SCKHA	38.90	24.45	9.55
Proposed Crypto Fish	40.67	31.45	13.76

The comparison of throughput for proposed Crypto Fish and existing techniques are evaluated and depicted in the table 4. It is observed from the it that the proposed model has increased throughput than other existing techniques.

In the figure 5, a graph is plotted to analyze the performance throughput of various stream cipher techniques for different size of files. It is demonstrated that the throughput is higher in proposed Crypto Fish of sizes 100KB, 500KB and 1MB than other existing techniques. Hence the proposed model outperforms other models in its performance.

Speed Analysis in Stream Cipher based Crypto Fish:

Amount of time needed for encryption and decryption of data is evaluated to find the efficiency of the proposed model. The analysis of speed is performed in the files of

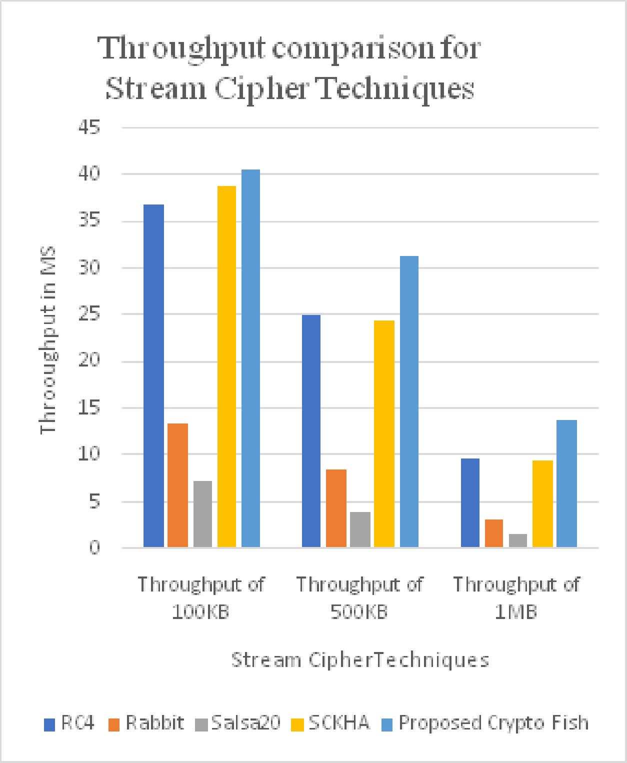

Fig. 5: Analysis of Throughput comparison for various Stream Cipher Techniques

varied sizes as 100KB, 500KB and 1 MB. For the proposed Crypto Fish and existing models, the analysis is carried out and compared. The proposed Crypto Fish algorithm takes lesser time than other existing models. This means that Crypto Fish is faster than other existing algorithms for different ranges of file sizes.

In table 5, comparison of various stream cipher techniques is performed along with proposed Crypto Fish method. The analysis of process time is done for different file sizes like 100KB, 500KB and 1MB. The comparison shows that proposed model takes lesser time for process than existing algorithms and proves its efficiency.

Table 5: Process time comparison of Stream Cipher Techniques [25]

Techniques	Time taken for 100KB	Time taken for 500KB	Time taken for 1MB
Rabbit	19.74	129.97	148.88
Salsa20	33.6	241.44	283.88
SCKHA	11.16	87.38	60.83
Proposed Crypto Fish	7.43	63.56	48.32

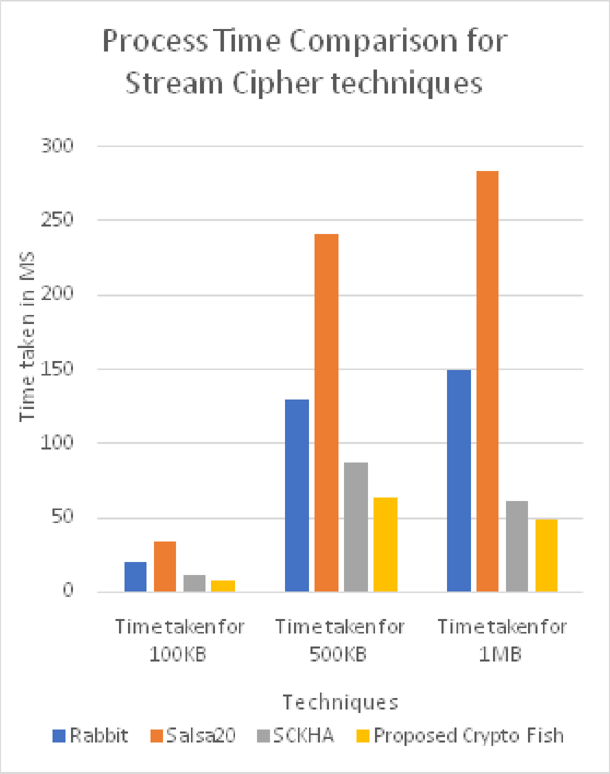

Fig. 6: Analysis of Process time comparison for various Stream Cipher Techniques

In the figure 6, analysis of Process time comparison for various Stream Cipher Techniques is done for different file sizes like 100KB, 500KB and 1MB. The comparison shows that proposed Crypto Fish model takes lesser time for process than existing algorithms and proves its efficiency.

Table 6: Comparison of Speed for Stream Cipher techniques [25]

Hashing Function	MD5	SHA1	SHA256	Crypto Fish
Encryption Time	2.6	1.68	1.5	1
Decryption time	0.77	0.75	0.74	0.59
Execution time	3.37	2.75	2.24	1.97

It is viewed from the table 6 that encryption time, decryption and execution time of various dynamic keys are compared. The proposed Crypto Fish algorithm takes lesser amount of time for execution when compared to other existing techniques and hence illustrated to be an efficient method.

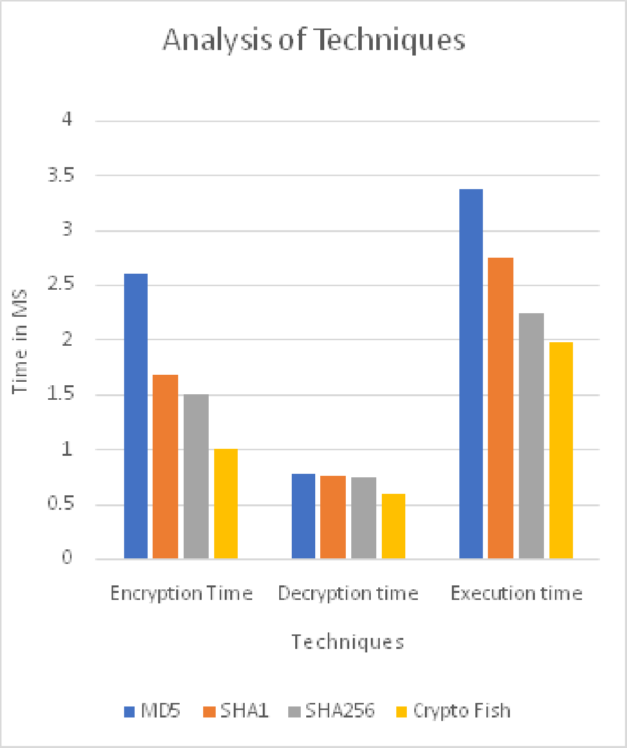

Fig. 7: Analysis of Speed for Stream Cipher techniques

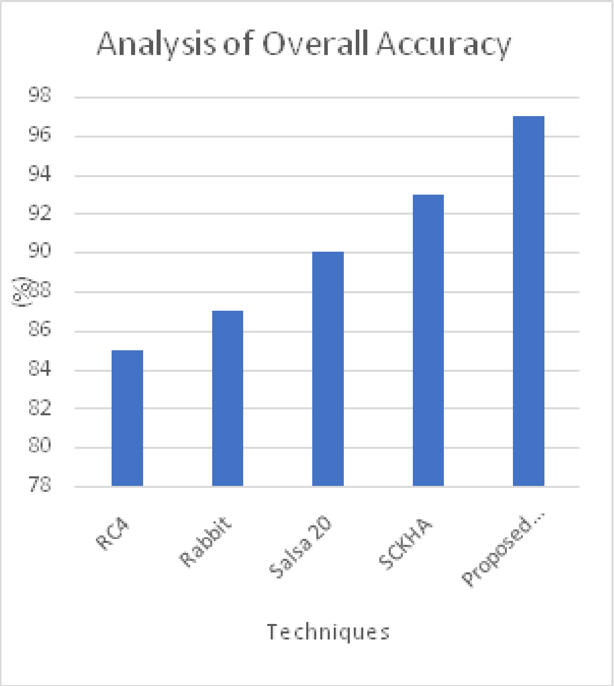

Fig. 8: Analysis of Overall performance

In figure 7, various stream cipher techniques are compared for its speed and analysed. It shows that the proposed Crypto Fish is effective than other existing techniques as it takes lesser time for execution.

Table 7: Comparison of Overall Accuracy [25]

Techniques	Overall Accuracy (%)
RC4	85
Rabbit	87
Salsa 20	90
SCKHA	93
Proposed Crypto Fish	97

In table 7, overall accuracy of proposed and existing techniques is compared. The table shows that the proposed Stream Cipher Crypto Fish method has higher overall accuracy compared to other existing models.

The overall performance accuracy of the existing and proposed Crypto Fish method is compared and plotted in the figure 8 which depicts that the proposed model achieves higher accuracy than other existing techniques.

5 Conclusion

Sybil attack might reduce the throughput of a blockchain test bed. In this paper, we have proposed a model for detecting sybil attacks in the block chain network. We also provide a solution directive in which every node keeps tabs on the actions of the others, looking for the ones that are forwarding the blocks for only one user. Initially by preprocessing the input data from network are normalized. Then by smart contract the transactions are created. By promptly identifying, blacklisting, and notifying other such nodes in the transactions, the Sybil attack's reach may be restricted by using the Multi Neural Memory Network (MNMN) classifier. Then the data can be securely stored in the block chain ledger by using the stream cipher Crypto Fish algorithm. We analyze experimental results of the proposed solution under simulation environment. The evaluation of performance is observed and compared with other traditional method. Various metrics like attack detection rate, recall, precision, f1-score, accuracy, TPR, FPR are compared for both proposed MNMN classifiers and other existing techniques which illustrates that the proposed classifier model achieves higher efficiency than others. Also, throughput, accuracy and speed analysis were performed for proposed Stream Cipher Crypto Fish and other traditional techniques which shows that proposed model outperforms other model efficiently.

References

[1] M. A. Shahriar, F. H. Bappy, A. F. Hossain, D.D.Saikat, M.S. Ferdous, M.J.M. Chowdhury and M.Z.A. Bhuiyan, *Modelling attacks in blockchain systems using petri nets*, In 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, 1069-1078, (2020).

[2] R.Prasad and V. Rohokale, Cyber security: the lifeline of information and communication technology, *Cham, Switzerland: Springer International Publishing*, (2020).

[3] R. S. Bhadoria, A. Nimbalkar, and N. Saxena, On the role of blockchain technology in the Internet of Things, *In Advanced applications of blockchain technology, Springer, Singapore*, 129-140, (2020).

[4] A. S. Koleshwar, S. S. Sherekar, V. M. Thakare, and A. Kanhe, Analytical Classification of Sybil Attack Detection Techniques, *In Intelligent Data Communication Technologies and Internet of Things Springer, Singapore*, 89-98 (2021).

[5] B. BaraniSundaram, T. Kedir, M. K. Mishra, S. H. Yesuf, S. M. Tiwari, and P. Karthika, Security analysis for Sybil attack in sensor network using compare and match-position verification method, *In Mobile Computing and Sustainable Informatics, Springer, Singapore*, 55-64, (2022).

[6] S. Huang, C. Lin, W. Xu, Y. Gao, Z. Feng, and F. Zhu, Identification of active attacks in internet of things: joint model-and data-driven automatic modulation classification approach, *IEEE Internet of Things Journal*, **8**(3), 2051-2065, (2020).

[7] S. S.Panda, D. Jena, B. K. Mohanta, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, Authentication and key management in distributed iot using blockchain technology, *IEEE Internet of Things Journal*, **8**(16), 12947-12954, (2021).

[8] W. Liang, L. Xiao, K. Zhang, M. Tang, D. He, and K. C. Li, Data fusion approach for collaborative anomaly intrusion detection in blockchain-based systems, *IEEE Internet of Things Journal*, (2021).

[9] Y. Y. Zhang, J. Shang, X. Chen, and K. Liang, A self-learning detection method of Sybil attack based on LSTM for electric vehicles, *Energies*, **13**(6), 1382, (2020).

[10] P. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, Blockchain data-based cloud data integrity protection mechanism, *Future Generation Computer Systems*, 102, 902-911, (2020).

[11] M. Baza, M. Nabil, M. M. N. Mahmoud, Bewermeier, K. Fidan, W. Alasmary, and M. Abdallah, Detecting sybil attacks using proofs of work and location in vanets, *IEEE Transactions on Dependable and Secure Computing*, **19**(1), 39-53 (2020).

[12] R. P. Sarode, M. Poudel, S. Shrestha, and S. Bhalla, Blockchain for committing peer-to-peer transactions using distributed ledger technologies, *Int. J. Comput. Sci. Eng.*, **24**(3), 215-227, (2021).

[13] M. Kedziora, P. Kozlowski, and P. Jozwiak, Security of Blockchain Distributed Ledger Consensus Mechanism in Context of the Sybil Attack. In International Conference on Industrial, *Engineering and Other Applications of Applied Intelligent Systems*, 407-418, (2020).

[14] S. Aggarwal and N. Kumar, Attacks on blockchain, *In Advances in Computers*, **121**, 399-410, (2021).

[15] A. Haddaji, S. Ayed, and L. C. Fourati, *Blockchain-based Multi-Levels Trust Mechanism Against Sybil Attacks for Vehicular Networks*, In 2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE), 155-163, (2020).

[16] S. Gong, and C. Lee, Blocis: blockchain-based cyber threat intelligence sharing framework for sybil-resistance, *Electronics*, **9**(3), 521, (2020).

[17] P. Otte, M. de Vos and J. Pouwelse, TrustChain: A Sybil-resistant scalable blockchain, *Future Generation Computer Systems*, **107**, 770-780, (2020).

[18] S. P. G ochhayat, S. Shetty, R. Mukkamala, P. Foytik, G. A. Kamhoua, and L. Njilla, Measuring decentrality in blockchain based systems, *IEEE Access*, **8**, 178372-178390, (2020).

[19] M. Iqbal, and R. Matulevicius, Exploring sybil and double-spending risks in blockchain systems, *IEEE Access*, **9**, 76153-76177, (2021).

[20] L. Lao, X. Dai, B. Xiao, and S. Guo, *G-PBFT: a location-based and scalable consensus protocol for IOT-Blockchain applications*, In 2020 IEEE International Parallel and Distributed Processing Symposium (IPDPS), 664-673, (2020).

[21] S. Datta, S. Kumar, D. Sinha, and A. K. Das, BSSFFS: Blockchain-based sybil-secured smart forest fire surveillance, *Journal of Ambient Intelligence and Humanized Computing*, **13**(5), 2479-2510, (2022).

[22] L. Serena, G. D'Angelo, and S. Ferretti, Security analysis of distributed ledgers and blockchains through agent-based simulation, *Simulation Modelling Practice and Theory*, **114**, 102413, (2022).

[23] N. Gupta, V. Jindal, and P. Bedi, LIO-IDS: handling class imbalance using LSTM and improved one-vs-one technique in intrusion detection system, *Computer Networks*, 192, 108076, (2021).

[24] O. Alkadi, N. Moustafa, B. Turnbull, and K. K. R. Choo, A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks, *IEEE Internet of Things Journal*, **8**(12), 9463-9472, (2020).

[25] S. Souror, N. El-Fishawy and M. Badawy, Security Analysis for SCKHA Algorithm: Stream Cipher Algorithm Based on Key Hashing Technique, *Chinese Journal of Electronics*, 1-16, (2022).

D. Nancy Kirupanithi completed her B.E. in Computer Science Engineering in Kings Engineering College, M. Tech in Software Engineering in Hindustan Institute of Technology and science and pursuing doctoral research in the domain of Blockchain Technology in the Department of Computer Science and Engineering in Hindustan Institute of Technology and Science, Deemed to be University with Graded Autonomous Status, Chennai, India. She published four articles in the IEEE indexed conferences, two papers published in referred International Indexed journals, including filed two Patents and also a member in ACM.

A. Antonidoss B.E., M.E., Ph.D currently working as Associate Professor in Hindustan Institute of Technology and Science, Chennai. He has published 26 research works with 43 citations and 686 reads. His area of interest Cloud Computing, database, Big data analytics, Network analysis, Machine Learning and Block chain.

G. Subathra completed her B.E in Computer Science Engineering in Bhajarang Engineering college , M.E in Software Engineering in Saveetha Engineering College and pursuing doctoral research in the domain of Block chain Technology in the Department of Computer Science and Engineering in Hindustan Institute of Technology and Science, Deemed to be University with Graded Autonomous Status, Chennai, India. She published two articles in the Indexed conferences, four papers in refereed International Indexed journals, including SCI to her credit, filed two Patents also a member in ACM.