SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379 / https://doi.org/10.14445/23488379/IJEEE-V10I2P114

Volume 10 Issue 2, 143-156, February 2023


*Original Article*

# Optimized Convolutional Neural Network Based Privacy Based Collaborative Intrusion Detection System for Vehicular Ad Hoc Network

M. Azath[1], Vaishali Singh[2]

[1,2]*Department of Computer Science & Engineering, School of Engineering & Technology, Maharishi University of Information Technology, Lucknow, Uttar Pradesh, India*

[1]*Corresponding Author: azathmusthaffacse@gmail.com*

Received: 11 January 2023 Revised: 09 February 2023 Accepted: 19 February 2023 Published: 28 February 2023

***Abstract*** *- The Vehicular Adhoc Network (VANET) secures the communication of vehicles during information generation and transfer. Even though the lack of trust and privacy in this network questions the reliability of information exchange, to overcome this problem, we are designing a blockchain-based VANET framework to establish secure information exchange via blockchain technology and offer improved scalability, confidentiality, and privacy. This study uses an Improved K-Harmonics Mean Clustering (IKHMC) model for cluster formation in VANET. After that, a novel Hybrid Capuchin-based Rat Swarm Optimization (HCRSO) algorithm is used to select the cluster heads, which primarily aims to provide efficient energy utilization, throughput and delay minimization. We use the blockchain as a reliable and highly secure technology, and trust-based collaborative intrusion detection in the VANET model is performed using an optimized (Seagull Optimization) Convolutional Neural Network (CNN). Finally, the three intrusion classes, namely Distributed Daniel of Service (DDoS), Blackmailing and Sybil attacks with non-intrusion class, are classified. The blockchain-based collaborative intrusion detection model solves security issues and motivates (rewarding) vehicles to collaborate, and avoids repetitive detection processes. The experimental results show that the proposed methodology is efficient to be applied in resource-constrained vehicles and also shows bigger improvements in terms of malicious node detection, overhead, end-to-end delay, and energy utilization.*

***Keywords*** *- Blockchain, Security, Convolutional Neural Network, and Ad-hoc, Vector routing protocol.*

## 1. Introduction

The types of Adhoc networks [3] are wireless sensor networks (WSN), Mobile ad-hoc networks (MANET), vehicular ad hoc networks (VANET), and wireless mesh networks (WMN). A group of static or moving automobiles connected to a wireless network is known as a Vehicular Adhoc Network (VANET) [1]. Wireless communication links are connected to each vehicle node. In VANET, every node is denoted as a router and participant of the network connected with intermediate nodes. In a wireless network, the vehicle connects with an Adhoc network from a moving object. An Adhoc network is a Local Area Network that uses multiple devices simultaneously. VANET's main contribution is the development of the MANET [2]. The Intelligent Transportation System (ITS), a traffic system categorized for driver assistance, emergency brake light, and accident notification, is the major source of VANET.

The Adhoc network uses Bluetooth technology to accumulate networks from the past. To share networks and files, an Adhoc network is helpful for accessing the Internet. An access point can transfer messages from the vehicle as a router or node. The automobile can be connected from 100 to 900 meters range. Media access, multicast, and QoS support are the challenges of the Adhoc network. The routers centralize the wireless network [4] through the base station, but the routers are distributed in the Adhoc network. The devices communicate directly from any location to share files. Multiple devices are linked together to communicate with each other without an access point. The roadside equipment is allowed to communicate with vehicles with the help of VANET. An intelligent transportation system is a process associated with mobility nodes. The foundation of VANET is a public utility, traffic monitoring, and mobile communication. The advantages of VANET are limited transmission capacity and power-driven. The recent Adhoc network does not support wireless devices, making it insecure and slower than conventional networks.

Blockchain [5] is a distributed system that stores information through file-sharing nodes in blocks and is denoted as the chain that uses digital currency. A numerical ledger acts as a storage device and accesses the user for transactions. The duplicate is eliminated to record transactions from the network. To view the transactions, the immutable records are shared by the numerical ledger [6]. A smart contract is a set of rules to evaluate and store blockchain to transfer bonds. Transaction of records, cryptographic keys, and file-sharing networks are the combined methods of blockchain. When it is recorded, it cannot be changed. There are four types of blockchain private, public, consortium, and permissioned blockchain. A private blockchain is a peer-to-peer network that shares a ledger to maintain the redundant protocol. Bitcoin uses a public blockchain with less security and numerical power. To maintain the blockchain, many organizations access data for transactions in business. The consortium blockchain shares the data. To enter the network, the permissioned blockchain gives access to obtain the network. It is also secure, clear, and archived immediately, and the data are detectable and tamper-proof.

Several techniques based on intrusion detection systems have been used in the past decades to overcome security vulnerabilities. Generally, the traffic data examination and attack detection were analyzed using several machine learning techniques like support vector machine (SVM), random forest (RF), K-nearest neighbor (KNN), Ensemble learning, etc., with deep learning techniques like convolutional neural network (CNN), Deep neural network (DNN), Long and short term memory (LSTM), Deep belief network (DBN), etc. Even though ML techniques improve trustable detection techniques, there is still no concise review of how ML and DL methods can assist academics and professionals in traversing dissemination safety in VANET. The security problem [7] is solved by blockchain by applying it in the VANET domain. It manages agreements, and the data is processed faster for secure agreements. To predict and analyse data, the information is stored in the blockchain. To evaluate the reliability of blockchain configuration Artificial intelligence to perform classification and features. Machine Learning predicts the correct features. On a smaller scale, it can also operate secure information. The data is shared with the entire network with clarity, security, and tracking ability. The drawbacks are time and energy-consuming, scalable, and complex. The research contribution of this study is summarized as follows:

- The Improved K-harmonics mean clustering (IKHMC) model is used to divide the VANET area into different numbers of clusters. Clustering simplifies routing and bandwidth allocation, resulting in a higher delivery ratio. Based on the traditional K- harmonics mean clustering (KHMC), compute the distances metric to determine the distance between centroids and nodes.
- The main goal of combining the CSA and RSO techniques is to use the best features of both algorithms when selecting cluster heads. In this regard, we used the CSA's estimating velocity and acceleration features and the HCRSO algorithm's location up-gradation feature. The novel Hybrid Capuchin-based Rat Swarm Optimization (HCRSO) algorithm selects the optimal cluster heads.
- The reliable and highly secured blockchain-based privacy preservation model is introduced.
- An optimized CNN model classifies collaborative intrusion detection in VANET. From this, three intrusion classes, namely Distributed Daniel of Service (DDoS), Blackmailing and Sybil attacks, are classified.

The rest of the article is summarized as follows: The related works are discussed in section 2, and section 3 explains the proposed framework of collaborative intrusion detection in VANET. Section 4 discusses the experimental results, concluding the article in section 5.

## 2. Literature Review

In this section, we discussed about the existing work related to blockchain based intrusion detection in VANET. A few of the works are reviewed here.

Ma et al. [8] suggested a decentralized key management mechanism (DB-KMM) to realize the registration. The bivariate polynomial opposes the DoS attacks to determine the key agreement and lightweight authentication. Vehicle-to-Vehicle and Vehicle-to-Infrastructure communication improve the security of the proposed method. This method deters collusion attacks, internal attacks, DoS attacks, and public key tampering attacks to prevent the UC framework. In this method, the efficiency is increased, and the cost is reduced. Thus, the complexity should be improved.

Li et al. [9] described a fine-grained access control scheme for VANET data based on blockchain (FADB) to enhance security. Access, privacy, and security are combined with sharing data to allow the method. The user shares data and identifies the information from the data and identity chains. The smart contracts preserve by the data chain to deter external attacks. The computational pressure is decreased efficiently. However, the retrieval functions are optimized by the revocation functions.

Maskey et al. [10] introduced an Applied Intelligence in blockchain vanet (ALICIA) to select the node from the consensus process. The Miner Node Selection (MNS) detects accidents and validates sending data to the proposed system. The edge nodes are connected with the outer edge

of the connected vehicles. The code nodes connect the edge nodes to determine the metrics and accumulate the reputation model. The proposed method is secure and reliable. Thus, the estimation of the system should be elaborated.

Kudva et al. [11] have developed the Proof of Driving (PoD) technique for an efficient and fair miner node selection process. The number of minor nodes is optimized by planning a real-time service standard score protocol Sc. The consensus nodes ignore the malicious part to execute the performance efficiently. The selected minor nodes are experimentally analyzed to predict feasibility and security. Hence the proposed method is efficient, feasible, and secure. Thus, the miner node should be efficient in various attacks.

Ma et al. [12] have described an attribute-based encryption algorithm to maintain the roadside unit (RSU). The road source unit performs the computation model that utilizes the vehicle to encrypt the data. The storage and computing capabilities are the two roadside unit nodes. The message decrypts the data to the attributes and is examined for traceability and audits. Security and efficiency are achieved from the proposed method. Hence, the immutable characteristics are improved by combining revocations and policy changes.

Buda et al. [13] have stated a distributed clustering approach to determine the edge nodes from record transactions. The quality of the ordinary and edge vehicles is distributed among the velocity of vehicles for edge selection. The sensor information is received and calculated for creating and validating the blocks. The number of transactions is generated to transmit the purely distributed data. By using this approach, communication problems are solved. Thus, the high computation nodes need to be solved.

Horng et al. [14] have suggested that the cipher text-policy attribute-based encryption (CP-ABE) algorithm shares the encryption/decryption data. A set of attributes are determined by the data decrypting the policy itself. The nodes and roadside units are computed by encryption and decryption operations. The data is updated by the user and attribute revocations. Hence the experimental result achieved secure, scalable, and fine-granularity features. Moreover, communication latency is tested in a real-world environment.

Rathee et al. [15] have developed agent-based modeling (ABM) and population-based modeling (PBM) to transmit and record real-time communication. The information is transferred by the communicating device to evaluate the computational models. The social impact theory optimizer (SITO) is examined to calculate the data transmission and receiving rate, preceding and succeeding nodes, and energy consumption. The communications are secure, effective, and comfortable. Thus, the dynamic networking patterns are analyzed by identifying the trusted devices in the network.

Meshcheryakov et al. [16] have performed a practical Byzantine Fault Tolerance (PBFT) consensus algorithm to restore distributed ledger for executing such devices. The Blockchain system is evaluated to explore its performance of the system. The feature of IoT devices determines the data rate and computing power. The data packet, generation period, and block size examine the latency. The network performance is higher, up to 70 nodes. Hence, the network-constrained devices are applied to execute in the network infrastructure.

## 3. Proposed Methodology

In this study, we develop a blockchain-based collaborative intrusion detection model in VANET. The proposed framework consists of four major stages. Figure 1 depicts the overall framework of the proposed model. An improved K- harmonics mean clustering (IKHMC) provides cluster formation. Afterwards, optimal cluster heads are selected using a hybrid Capuchin-based Rat Swarm Optimization (HCRSO) algorithm, and the blockchain-based privacy preservation in VANET is introduced. Finally, an optimized CNN model is used to detect the collaborative intrusion in VANET.

### *3.1. Improved K- Harmonics Mean Clustering (IKHMC)*

The area of VANETs is split into different numbers of clusters using the Improved K-harmonics mean clustering (IKHMC) model. The clustering simplifies the routing and bandwidth allocation, providing a higher delivery ratio. Based on the traditional K- harmonics mean clustering (KHMC), render the distances metric to gauge the relative distance among the centroids and nodes. Where the distance is determined solely by the positions of the centroids and nodes. Characterize position together with the velocity of the vehicle and regards the vehicles' mobility during the cluster formation in VANET [33].

The velocity centered on the vehicle's position is stated via the weighted distance metric. The improved K-harmonics mean clustering (IKHMC) model is the changing of weighted distance metric. Where,$y_j$ and $y_j^{ce}$ are the positions in which the velocity is$VE_{y,j}$ and$VE_{ce}^{j}$. The negative Euclidean distance among the node position is nodes mobility, which is expressed as follows.

$$ED(i,j) = \left(\left\|y_i - y_j\right\| + \left\|y_i^* - y_j^*\right\|\right) \tag{1}$$

$$y_i = \begin{bmatrix} y_i \\ z_i \end{bmatrix} (y_i)^* = \begin{bmatrix} y_i + V_{y,i}FT \\ z_i + V_{z,i}FT \end{bmatrix} \tag{2}$$

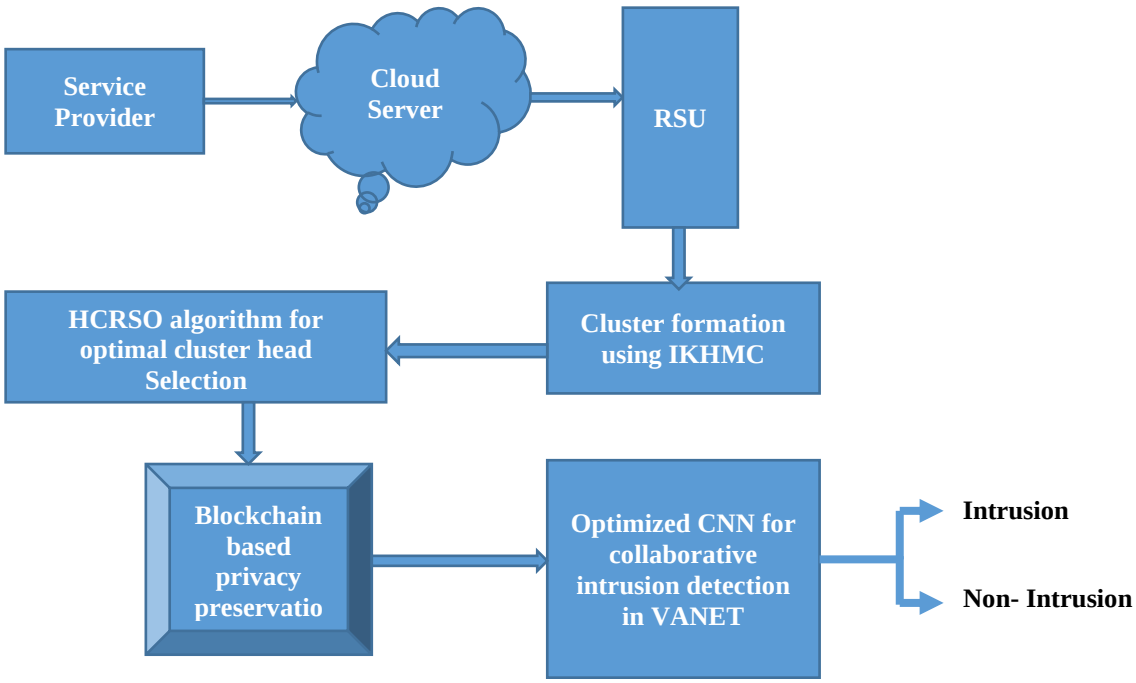


**Fig. 1 Overall diagram of the proposed framework for intrusion detection in VANET**

The predicted next position of node i is implied as $(y_i)^*$, and the transfer function is FT. On the y-direction, the current velocity of the ith node is $V_{y,i}$. On the z-direction, the current velocity of the ith node is $V_{z,i}$. Initialize the self-similarity, and the number of clusters lessened the same values. It is an immovable node, and the value of 0 states the Road Side Unit (RSU) velocity [18]. The following equations signify the clustering objectives.

$$IKHMC_F = \sum_{i=1}^{M} \frac{J}{\sum_{j=1}^{J} \frac{1}{(d_{i,j})^2}} \tag{3}$$

The centroid's position takes the partial derivation $IKHMC_F$ to derive the optimal position of centroids.

$$\frac{\partial F}{\partial y_j^{cen}} = J \sum_{j=1}^{M} \frac{4\left(y_i - y_j^{cen}\right) + \left(V_{y,i} - V_j^{cen}\right)}{d_{i,j^3}\left(\sum_{j=1}^{J} \frac{1}{d_{i,j^2}}\right)} \tag{4}$$

The jth centroid $y_j^{cen}$ with optimal position is obtained and set $\frac{\partial F}{\partial y_j^{cen}} = 0$.

$$y_j^{cen} = \frac{\sum_{j=1}^{M} \frac{y_j + V_{y,j}}{d_{i,j^3}\left(\sum_{j=1}^{J} \frac{1}{d_{i,j^2}}\right)^2}}{\sum_{j=1}^{M} \frac{1}{d_{i,j^3}\left(\sum_{j=1}^{J} \frac{1}{d_{i,j^2}}\right)^2}} \tag{5}$$

### *3.2. Cluster Head Selection*

This section used a novel Hybrid Capuchin-based Rat Swarm Optimization (HCRSO) algorithm to select cluster heads. The cluster head is present in every cluster, and the HCRSO algorithms select the clusters. Regularly update the cluster heads on the VANET if the new service enters the network. Synchronize the cluster head in which the latest service description is encompassed via cluster head. The below section selects the optimal cluster heads together with the cluster formation using the HCRSO model is given as follows:

#### *3.2.1. Capuchin Search Algorithm*

This algorithm relies on the characteristic features of the Capuchin monkey and has utilized food-searching strategies. Numerically, the global and local strategies are explained as delineated below. The movement of the Capuchins from one tree to another is similar to projectile motion, and hence the motion can be formulated as,

$$a = a_0 + v_0 t + \frac{1}{2} r t^2 \tag{5}$$

Here, a is the distance from the source tree to the destination tree, like the source node to the targeted node [19]. The initial location of the node is $a_0$. The acceleration of the vehicle is denoted as r under the time instance t. the velocity of the vehicle is indicated as $v$ and can be determined with the help of the first law of motion as expressed below,

$$v = v_0 + rt \tag{6}$$

According to the capuchin monkey, the initial velocity components of the vehicles are given as a and b and can be expressed as,

$$v_{0a} = v_0 \, cos(\phi_0) \tag{7}$$

$$v_{0b} = v_0 \, sin(\phi_0) \tag{8}$$

The initial velocities of the vehicles in the a and b directions are represented as $v_{0a}$ and $v_{0b}$correspondingly. The angle concerning the a-direction is given as $\phi_0$. The next step is to estimate the horizontal velocity of the vehicle obtained from equations 2 to 4.

$$v_a = v_{0a} + r_a t$$

$$= v_0 \, cos(\phi_0) \tag{9}$$

The acceleration of the vehicle in the horizontal direction $r_a$is set as 0. Then the distance can be evaluated as,

$$a = a_0 + v_0 \, cos(\phi_0) t \tag{10}$$

*3.2.2. Rat Swarm Optimizer*

This relies on the fighting and chasing behaviors of the rat in search of food. It is numerically expressed, as shown below.

*Chasing the Prey*

The chasing behavior of the Rat is based on the agonistic nature and searching for the prey after knowing the location of the prey [20]. The location of the search agents is updated with respect to the best search agent or vehicle. The location up-gradation of the vehicle is expressed as shown below,

$$\vec{D} = X . \vec{D_i}(a) + F . (\vec{D_o}(a) - \vec{D_i}(a)) \tag{11}$$

The location of the vehicle is indicated as $\vec{D_i}(a)$, and the best optimal vehicle node is represented as $\vec{D_o}(a)$. The parameters X and F are estimated as shown below,

$$X = P - a \times \left(\frac{P}{Max_{iter}}\right) \tag{12}$$

Here, $a = 0,1,2,\ldots\ldots, Max_{iter}$

$$F = 2 . ran() \tag{13}$$

The P and F are random integers with the values lying in the range s of 1 to 5 and 0 to 2 correspondingly. During iterations, the parameters X and F are used for the exploration and exploitation stage.

*Fighting with prey*

The fighting process of rats for the prey is used for the location up-gradation of vehicles while conducting the cluster head selection. It can be numerically expressed as,

$$\vec{D_i}(a+1) = \left|\vec{D_o}(a) - \vec{D}\right| \tag{14}$$

$\vec{D_i}(a+1)$ shows the updated location of the vehicle. Moreover, it is selected as the best vehicle node and arranged with the other nodes with respect to it. Besides, it can also be used to find the optimal vehicle node from n-dimensional search space.

*3.2.3. HCRSO Algorithm for Cluster Head Selection*

The main aim of hybridizing both the CSA and RSO algorithms is to take the important features from both algorithms while performing the cluster head selection. With respect to this, we have taken the estimating velocity and acceleration features from the CSA and the location up-gradation feature from the HCRSO algorithm.

CSA:

- Initialization
- Movement of the vehicles
- Velocity and acceleration of the vehicle nodes

RSO:

- Location updated using the known features
- Updating the location of the nodes after estimating the optimal solution

Based on the HCRSO algorithm, the optimal cluster heads are selected by minimizing the delay and energy consumption as well as increasing the throughputs. The schematic structure in figure 2 delineates the Hybrid CRSO algorithm used for the optimal cluster head selection.

***3.3. Blockchain-Based Privacy Preservation in VANET***

The security of the VANET faces two issues while transferring data from one vehicle to another. The task manager in the VANET has no required data sensed by the vehicles before sharing. Hence there is a chance to upload modified data into the VANET system. to surmount these problems; we used the blockchain-based privacy preservation technique, which effectively perpetuates the security throughout the system [21]. Blockchain is a point-to-point network system in which each vehicle node includes the replication of the global machine method. It can also circumvent the risks of downtime and attack at a single point with the distributed data sharing and storage capacity.

Moreover, the open ledger in the blockchain can be used to ensure the integrity and authenticity of the original global approach [22]. The vehicles in the VANET system upload precise information based on the incentive and punishment mechanism. This averts the uploading of fake information. Each transaction's characteristics can be easily traceable. The overlay of blockchain-based security in the VANET system is illustrated in figure 3.

The forwarded information in the roadside units contains parameters such as the sender’s identity, model accuracy,

and data signature. The privacy-preserving of our proposed blockchain-based approach is evaluated by the metrics such as the evaluation of offset of the trusted computing of RSUs, and the incentive mechanism for multiple RSUs.

### *3.4. Collaborative intrusion detection in VANET*

The collaboration aspect is primarily in charge of providing assistance to a node in calculating the trust values of some other node through transmitting out normal queries or obstacles. The collaborative intrusion can assist an experimented node in providing feedback in response to requests or questions. This study detects collaborative intrusion in VANET using seagull optimization-based CNN or optimized CNN model, which is explained in the following section.

#### *3.4.1. Convolutional Neural Network*

The multi-layer structure with a neural network is present in the convolutional neural network (CNN). In the previous layer, the weighted sum of the elements activates and obtains each neuron's outputs [23].

#### *3.4.2. Input layer*

The statistical characteristics information is obtained via the network data traffic attributes. On the jth feature plane is the kth neuron in the Con1layer.

$$Con_{jk}^{O} = H\left(\sum_{j=1}^{FI} W_t^{IN} \times h\_Original_T^{IN}\right) \quad (15)$$

The Tth convolution kernel weight is $W_t^{IN}$, and the filter length is$FI$. Based on the input layer, the characteristics plane feature plane position related to the convolutional kernel weight is$h_Original_T^{IN}$. Where, $H_j(\cdot)as(j = 1,2,3)$ is the ReLU, tanh and sigmoid activation functions, which are explained as follows:

$$H_1(y) = Re\,L\,U(y) = max(0, y) \quad (16)$$

$$H_2(y) = tanh(y) = (exp^{y} - exp^{-y}) \Big/ (exp^{y} + exp^{-y}) \quad (17)$$

$$H_3(y) = sig(y) = \frac{1}{(1+exp^{-y})} \quad (18)$$

An advanced and deeper feature of the original data is obtained through the convolutional layer and flattened the feature plane. The training set provides higher precision, as well as the validation set provides lower precision results and overfitting issues in the process of training the network. The network generalization ability is improved. Train the samples of each batch and different neuron nodes working in every training cycle.

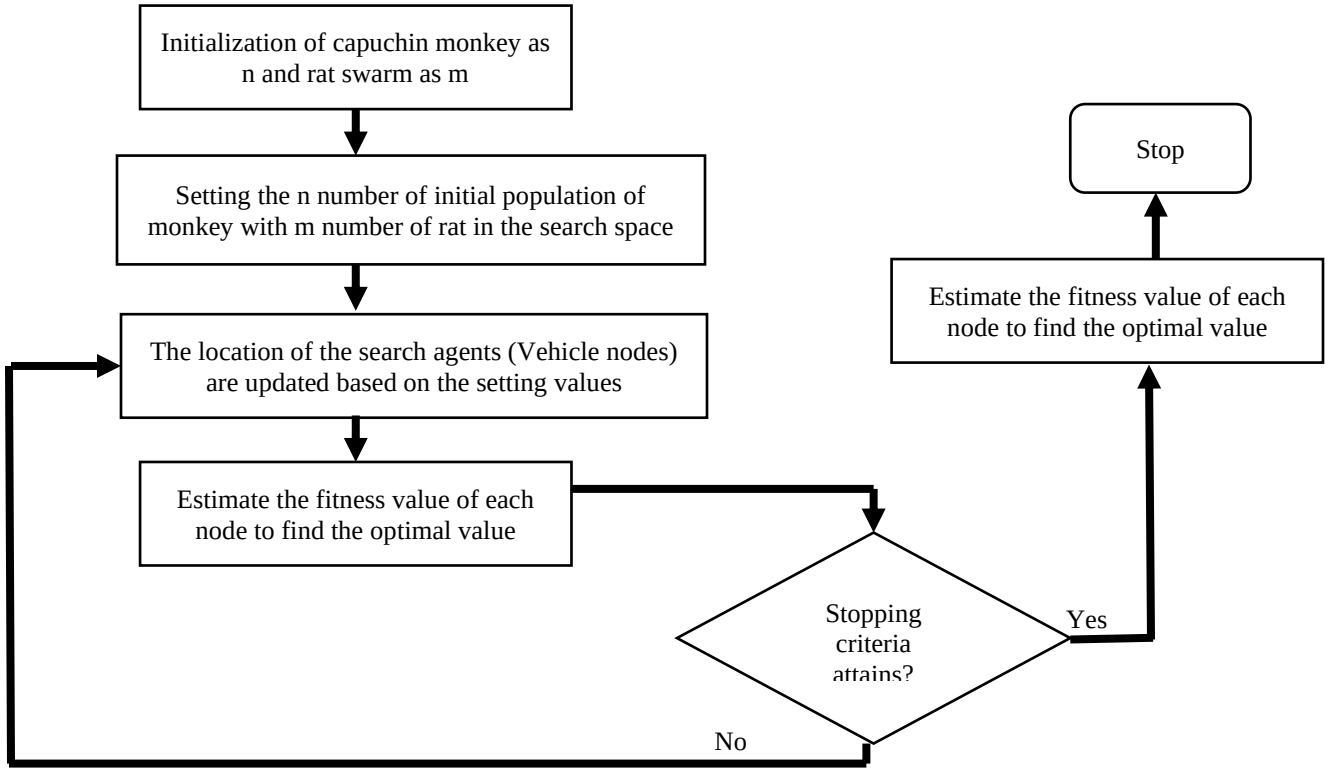


**Fig. 2 Systematic Flow diagram of proposed hybrid CRA algorithm for the cluster head selection**

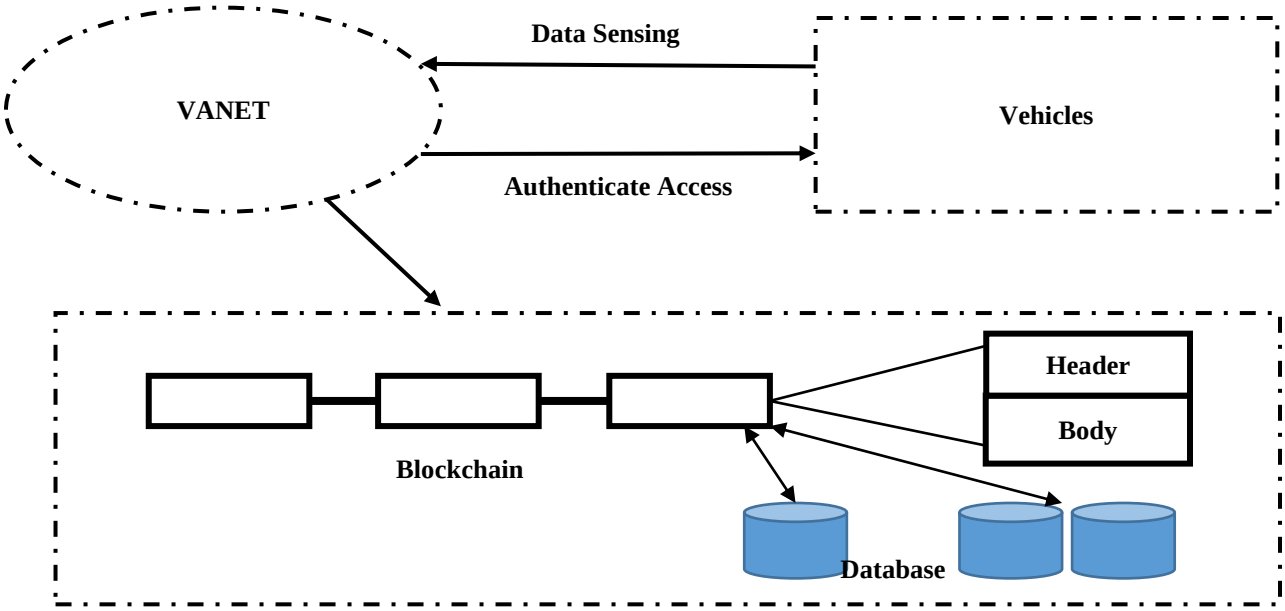


**Fig. 3 Blockchain privacy preservation in our proposed VANET system**

*3.4.3. Fully Connected Layers*

The shole connection layer sets the number of activation mode neurons. In the fully connected layer, the below equation expresses the nth neurons$FLC_n^{Out}$.

$$FLC_n^{Out} = H(\sum_{m=1}^{cw} \times cw_m + a_n) \quad (19)$$

After the flattening and dropout, the number of neurons is denoted as $cw_m$ , and the connection weight is$cw$. The offset of the nth neuron is $a_n$.

*3.4.4. Output Layers*

An output layer transfers the output value of the last fully connected layers. The expression of softmax classifies various kinds of VANET attacks.

$$SM(z)_j = exp^{z_j} \quad / \sum_{j=1}^{AT} exp^{z_j} \quad (20)$$

Various kinds of attack detection are represented $AT$, and the output value is$y_j$.

$$CEL(q,r) = -\sum_y APD(y)\, log \;\; EPD(y) \quad (21)$$

The distance between the estimated probability distribution$EPD(y)$ and the actual probability distribution $APD(y)$ are measured using the cross-entropy loss function as$CEL(q,r)$.

*3.4.5. Seagull Optimization (SO) Algorithm*

The Laridae is the scientific name of a seagull. The omnivorous are seagull that eats earthworms, fishes, amphibians, reptiles and insects. The behavior of the seagull inspires the seagull optimization (SO) algorithm. The mathematical modeling of the SO algorithm is delineated in this section.

*3.4.6. Exploration or Migration*

The seagull's group moves from one position to another are simulated during the migration. Three conditions include collision avoidance, motion to the optimal nearer direction, and closer remaining to the optimal search agent [34]. To calculate the new search agent, employ an additional variable, AV, to avoid collision among the neighbors.

$$\overrightarrow{SC} = AV \times \overrightarrow{PS}\,(y) \quad (22)$$

The y-search agent position and current search agent position are $\overrightarrow{SC}$and$\overrightarrow{PS}$. The current iteration is y. The frequency variable is controlled using the factor$CF$.

$$AV = CF - (y \times (CF/Itr_{max}\,())()_{max}) \quad (23)$$

The search agent moves in the best neighbor's direction after avoiding the collision among the neighbors. The search agent position $\overrightarrow{S}_p$and the best search agent$\overrightarrow{B}_P$ are represented as$\overrightarrow{SM}$. The randomization behavior is$K$. The random number falls into the interval [0, 1].

$$\overrightarrow{SM} = K \times \left(\overrightarrow{B}_P\,(y) - \overrightarrow{S}_p\,(y)\right) \quad (24)$$

$$K = 2 \times AV^2 \times random \quad (25)$$

Based on the best search agent, the position is updated. The distance among both search agents and optimal best fit is$S\vec{D}$.

$$S\vec{D} = \left|\vec{SC} + \vec{SM}\right| \quad (26)$$

*3.4.7. Exploitation or Attacking*

The below equation updates the position of the search agent. The best solution is stored by using$S\vec{p}(y)$ , and the other search agent position is updated. Algorithm 1 explains the pseudocode of the seagull optimization algorithm.

$$S\vec{p}(y) = \left(\vec{SD} \times y` \times z` \times x`\right) + \vec{B_P}(y) \quad (27)$$

*3.4.8. Optimized CNN model for Collaborative Intrusion Detection in VANET*

Generally, the CNN architecture has several advantages, such as better detection and classification results, provides faster implementation and easy understanding. However, it met a few shortcomings in case of higher computational complexity, improper hyperparameter tuning, lower detection results, etc. To solve these issues, we apply the seagull optimization (SO) algorithm to optimize the hyperparameters involved in the CNN structure, thereby providing better detection and classification accuracy for VANET attack detection. Because the SO algorithm consists of better searchability and convergence speed to solve the optimization issues. Hence, we combined used optimized CNN or seagull optimization-based CNN model to detect collaborative intrusion detection is VANET [25-30]. Initially, the seagull position comprises every layer of CNN parameters and initializes the position parameters.

Figure 4 expresses the collaborative intrusion detection model in VANET using optimized CNN.

The CNN structure related to every seagull's position and continuous iteration determines the optimal network structure parameter. In order to determine various kinds of attacks, consider the actual requirements and requirements to predict the effect of optimal prediction. The predicted and real value difference is evaluated via the loss function. Encode the actual labels in the CNN model, and the softmax layer obtains every class (intrusion and non-intrusion) prediction probability. In the initial training cycle, the SO algorithm provides less cross entropy loss function, which is set as the fitness function. Determine the minimum loss function value depending upon the variable structure parameters of every layer via the SO algorithm. The cross-entropy loss function is calculated by obtaining each seagull fitness value in the current iteration. AN average fitness value is calculated and stores the minimum fitness value of every seagull. The migration or exploration step of the seagull is initialized to optimize the CNN parameters. The optimal solution or optimal intrusion detection results are obtained whether the SO algorithm meets the maximum number of iterations or otherwise repeats the entire process. Finally, we have to classify the collaborative intrusion and non-intrusion classes in VANET. From this, the three intrusion classes in VANET are also classified. Distributed Daniel of Service (DDoS), Blackmailing and Sybil attacks.

**Algorithm 1:**Pseudocode of the seagull optimization algorithm

**Input:** Population of seagull$\vec{S}_p$

Initialization of $AV$and $K$parameters with the maximum number of iterations

set$CF \leftarrow 2$

**While** (y< maximum iteration) **do**

$$\vec{B}_P \leftarrow fitnesscalculation\left(\vec{S}_p(y)\right)$$

$$random \leftarrow random(0,1)$$

$$x \leftarrow random(0,2\pi)$$

Calculate the distance the distance$S\vec{D} = \left|\vec{SC} + \vec{SM}\right|$

$$S = y` \times z` \times x`$$

$$S\vec{p}(y) \leftarrow \left(\left(\vec{SD} \times S\right) + \vec{B_P}\right)$$

$$y \leftarrow y + 1$$

**End While**

Return $S\vec{p}(y)$

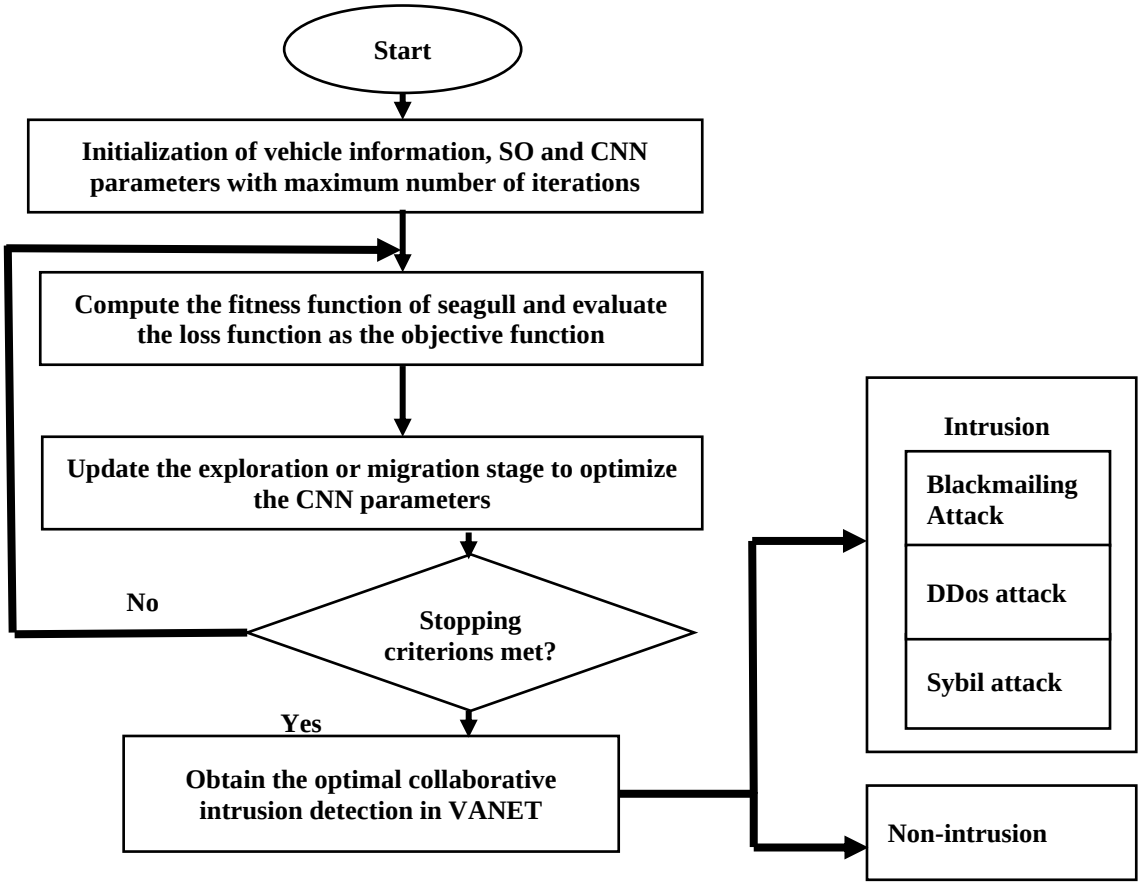


**Fig. 4 Flowchart of optimized CNN model for collaborative intrusion detection model in VANET**

## 4. Results and Discussion

The proposed model's effectiveness is evaluated, and the comparative results are listed in this section, which is analyzed through various performance metrics with respect to the state-of-art techniques. The dataset is taken from https://www.kaggle.com/bigquery/ethereum-blockchain, and the recoverable sampling scheme is used [31,32]. The simulation is performed using NS-2 software. Table 1 expresses the parameters used for the simulation.

**Table 1. Parameter setting for simulation**

| Parameters | Ranges |
|---|---|
| **Number of Population Size** | 50 |
| **Maximum number of iterations** | 100 |
| **Number of nodes** | 100 |
| **Transmission range** | 280 m |
| **Speed Movement** | 4 m/sec |
| **Range of Simulation** | 1.5 km*1.5 km |

### *4.1. Performance Metrics*

The performance metrics such as accuracy, delay, energy consumption, throughput, detection rate, encryption and decryption time validate the effectiveness of the proposed framework.

$$Accuracy = \frac{T^{-ve}+T^{+ve}}{T^{+ve}+T^{-ve}+F^{+ve}+F^{-ve}} \quad (27)$$

Over a time period, the total number of attacks are detected using the detection rate. Accurate classification of intrusion and non-intrusion classes is detected.

$$Detectionrate = \frac{T^{+ve}}{T^{+ve}+F^{-ve}} \quad (28)$$

From the above equations, the true positive and negative classes are expressed as $T^{+ve}$and$T^{-ve}$. Further, $F^{+ve}$and

$F^{-ve}$are the false positive and negative classes.

Delay: The amount of time it takes for a packet to travel from source to destination across a network.

Throughput: The total number of data units a scheme can handle in a predetermined period of time is called throughput.

Energy consumption: From the source to the destination, the total energy consumed by the packet is referred to as energy consumption.

### *4.2. Performance Analysis*

Figure 5 illustrates the detection accuracy rate of our proposed and other existing approaches, such as DB-KMM, FADB, CP-ABE, and PBFT. Since our proposed approach utilizes collaborative CNN-based intrusion detection, the efficacy is the very high irrespective number of VANET nodes used. From the graphical representation, the accuracy of the proposed approach is equal to 94.2%, whereas DB-KMM achieves the least detection accuracy of about 89% when the VANET node is equal to 100. The state-of-art work PBFT exhibits a detection accuracy of 91.9%, CP-ABE achieves 90.12%, and FADB achieves 89.75%, and are lower than our proposed approach. Hence our proposed approach can be used for intrusion detection in VANET with higher nodes.

Figure 6 depicts the performance of several nodes Vs energy consumption. There are 20 to 100 nodes selected with varying energy consumptions obtained. The state-of-art techniques, namely DB-KMM, FADB, CP-ABE, and PBFT and the proposed method to validate the energy consumption performance with respect to the number of nodes. Here, we have selected 20, 40, 60, 80 and 100 nodes with state-of-the-art methods. The proposed method demonstrated lesser energy consumption outputs than all these existing techniques.

Figure 7 illustrates the performance analysis with respect to the delay in passing the information from one VANET node to another. Here we have considered 100 nodes, and the delay increases with the number of nodes in the VANET system. Our proposed approach utilizes a hybrid approach for cluster head selection and Blockchain-based collaborative CNN-based intrusion detection. Hence, the delay has been decreased when compared to other approaches. The delay of the proposed approach when the number of nodes is equal to 100 is just 10 sec whereas; the DB-KMM approach has a higher delay of equal to 20.65sec. Meanwhile, the approaches PBFT, CP-ABE, and FADB have a delay of 18.4sec, 16.4sec, and 13.9sec, respectively.

Figure 8 summarizes the performance of the number of nodes versus the throughput. The state-of-the-art techniques DB-KMM, FADB, CP-ABE, and PBFT, as well as the proposed method, are used to validate the throughput performance with respect to the number of nodes. We chose 20, 40, 60, 80, and 100 nodes, thereby evaluating throughput performance. The proposed method produced lower energy consumption outputs compared to all of these existing techniques, namely DB-KMM, FADB, CP-ABE, and PBFT, respectively. The intrusion detection ratio with respect to the number of nodes is illustrated in figure 9. The proposed approach detects the intrusion more effectively from the implementation result than the other approaches. When the node is equal to 100, our proposed approach detects the intrusion with a ratio of 94.23%. Meanwhile, the DB-KMM achieves a detection ratio of 86.98% and the least. Besides, the PBFT, CP-ABE, and FADB achieve a detection ratio of 91. 67%, 89.26%, and 87.20% respectively.

Table 2 shows the security level analysis of different approaches in percentage. Our proposed approach utilizes blockchain-based privacy preservation and intrusion detection CNN; based SGO approach is used. It enhances the security level in the VANET system irrespective of the VANE nodes in the system. Hence the security level of our proposed approach is 97%. The state-of-art work methods DB-KMM, PBFT, CP-ABE, and FADB achieve security of about 89%, 93%, 92%, and 94%, respectively, lower than the proposed approach.

**Table 2. Performance Analysis in terms of Security Level**

| Methods | Security Level |
|---|---|
| **DB-KMM** | 89% |
| **PBFT** | 93% |
| **CP-ABE** | 92% |
| **FADB** | 94% |
| **Proposed** | 97% |

## 5. Conclusion and Future work

This article presented the seagull optimization-based CNN or optimized CNN model for the detection of collaborative intrusion detection. From this, we have classified the non-intrusion class with three intrusion attacks, such as blackmailing, Sybil, and DDoS attacks, respectively. The implementation platform of NS-2 provides the simulation results. The proposed method outperformed superior results in terms of throughput, accuracy, attack detection ratio, and security level. When compared to the previous methods like DB-KMM, PBFT, CP-ABE, and FADB, the proposed method offers minimum delay and energy consumption results during cluster head selection. When the number of nodes is equal to 100, the proposed approach has a delay of just 10 seconds, but the DB-KMM approach has a delay of 20.65 seconds.

Meanwhile, the delays for the approaches PBFT, CP-ABE, and FADB are 18.4sec, 16.4sec, and 13.9sec, respectively. Our proposed approach detects the intrusion with a ratio of 94.23 % when the node is equal to 100. The proposed method demonstrated 97% security level and 94.2% accuracy results. This method met a few limitations, such as computational complexity and cost and failed to discuss the latency. In the future, we will use any novel optimization technique with a deep learning model-based blockchain system for intrusion detection in VANET. Moreover, we will use more parameters like distance, bandwidth, and coverage.

## Acknowledgements

The researchers would like to thank the University Vice Chancellor.

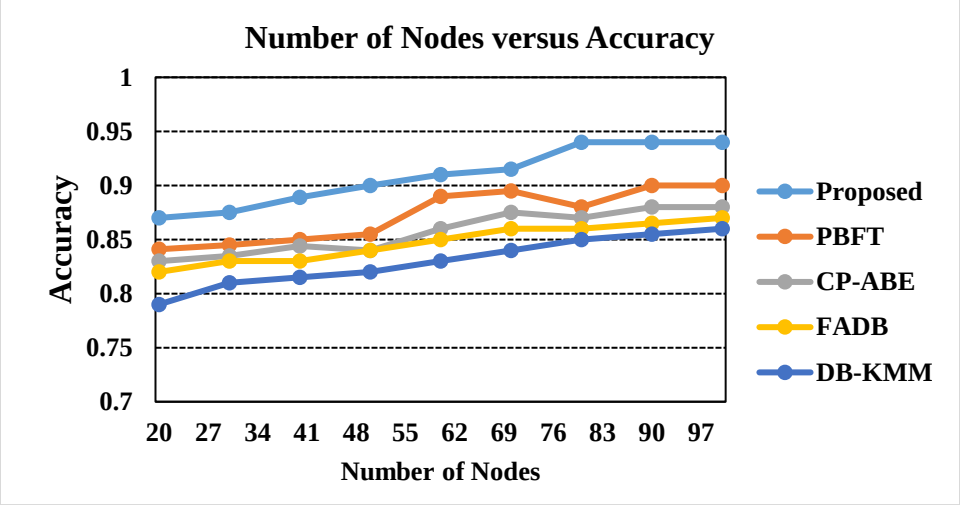


**Fig. 5 Performance analysis in terms of detection accuracy with respect to the number of nodes**

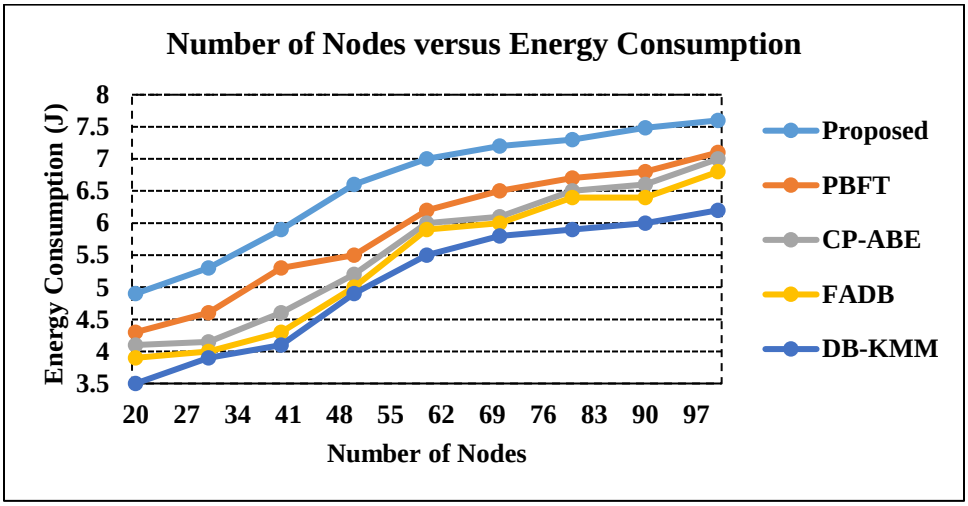


**Fig. 6 Performance of number of nodes Vs energy consumption (J)**

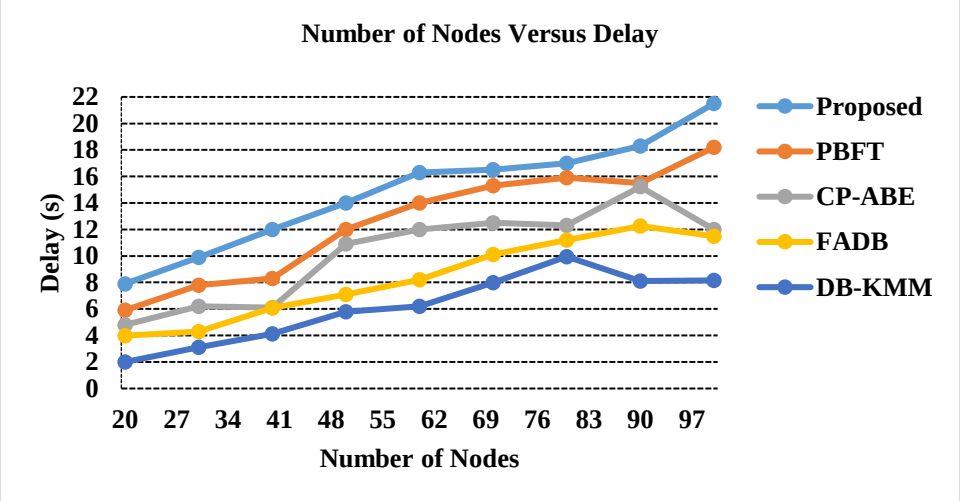


**Fig. 7 Performance analysis in terms of delay with respect to the number of VANET nodes**

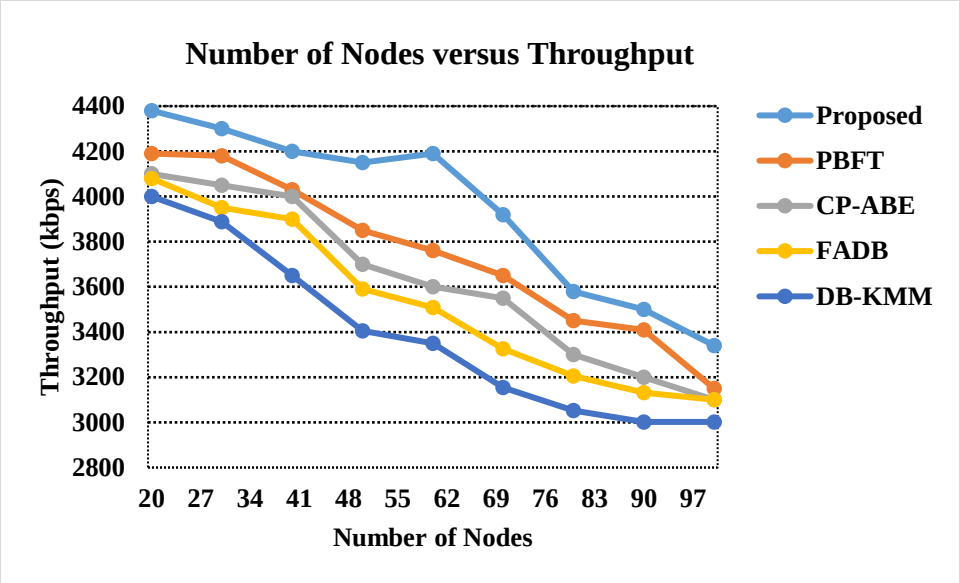


**Fig. 8 Performance of number of nodes Vs throughput**

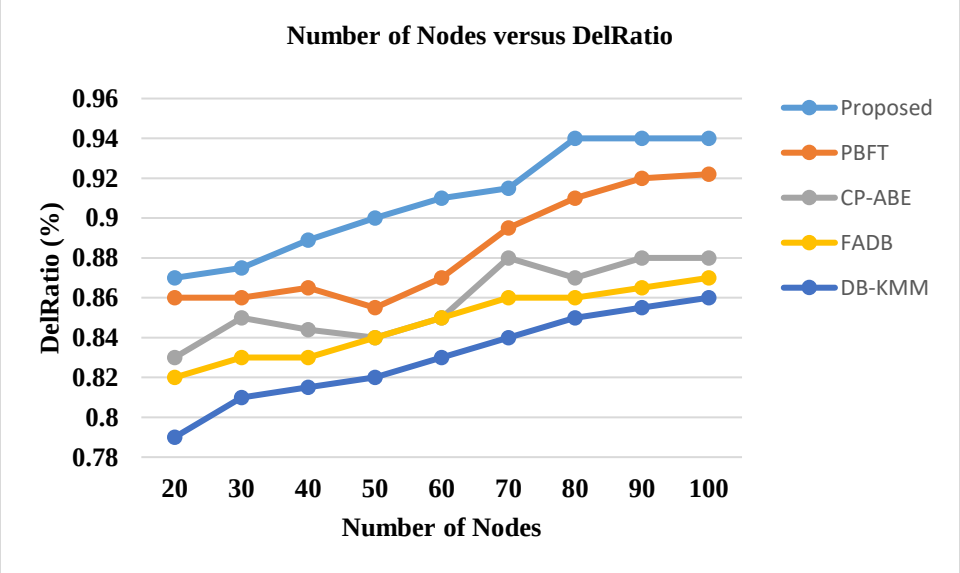


**Fig. 9 Performance analysis in terms of detection ratio with respect to the number of nodes**

## References

[1] Mustafa Maad Hamdi et al., "A Review of Applications, Characteristics and Challenges in Vehicular Ad Hoc Networks (VANETs)," *International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, pp. 1-7, 2020. [CrossRef]

[2] Zheng Chen et al., "An Adaptive on-Demand Multipath Routing Protocol with QoS Support for High-Speed MANET," *IEEE Access*, vol. 8, pp. 44760-44773, 2020. [CrossRef]

[3] Ahmed Muhi Shantaf, Sefer Kurnaz, and Alaa Hamid Mohammed et al., "Performance Evaluation of Three Mobile Ad-Hoc Network Routing Protocols in Different Environments," *International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, pp. 1-6, 2020. [CrossRef]

[4] R. Santhana Krishnan et al., "Modified Zone Based Intrusion Detection System for Security Enhancement in Mobile Ad Hoc Networks," *Wireless Networks*, vol. 26, no. 2, pp.1275-1289, 2020. [CrossRef]

[5] Chao Lin et al., "BCPPA: A Blockchain-Based Conditional Privacy-Preserving Authentication Protocol for Vehicular Ad Hoc Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 12, pp.7408-7420, 2020. [CrossRef]

[6] Sarah Iqbal et al., "Blockchain-Based Reputation Management for Task Offloading in Micro-Level Vehicular Fog Network," *IEEE Access*, vol. 8, pp. 52968-52980, 2020. [CrossRef]

[7] Bin Cao et al., "A Many-Objective Optimization Model of Industrial Internet of Things Based on Private Blockchain," *IEEE Network*, vol. 34, no. 5, pp.78-83. 2020. [CrossRef]

[8] Zhuo Ma et al., "An Efficient Decentralized Key Management Mechanism for VANET with Blockchain," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp.5836-5849, 2020. [CrossRef]

[9] Hui Li et al., "FADB: A Fine-Grained Access Control Scheme for VANET Data Based on Blockchain," *IEEE Access*, vol. 8, pp. 85190-85203, 2020. [CrossRef]

[10] Shirshak Raja Maskey et al., "ALICIA: Applied Intelligence in Blockchain Based VANET: Accident Validation as a Case Study," *Information Processing & Management*, vol. 58, no. 3, pp.102508, 2021. [CrossRef]

[11] Sowmya Kudva et al., "Towards Secure and Practical Consensus for Blockchain Based VANET," *Information Sciences*, vol. 545, pp. 170-187, 2021. [CrossRef]

[12] Jianfeng Ma et al., "Attribute-Based Secure Announcement Sharing Among Vehicles Using Blockchain," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp.10873-10883, 2021. [CrossRef]

[13] Su Buda et al., "Empowering Blockchain in Vehicular Environments with Decentralized Edges," *IEEE Access*, vol. 8, pp. 202032-202041, 2020. [CrossRef]

[14] Shi-Jinn Horng, Cheng-Chung Lu, and Wanlei Zhou, "An Identity-Based and Revocable Data-Sharing Scheme in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp.15933-15946, 2020. [CrossRef]

[15] Geetanjali Rathee et al., "Trusted Computation Using ABM and PBM decision models for ITS," *IEEE Access*, vol. 8, pp. 195788-195798, 2020. [CrossRef]

[16] Yaroslav Meshcheryakov et al., "On Performance of PBFT Blockchain Consensus Algorithm for IoT-Applications with Constrained Devices," *IEEE Access*, vol. 9, pp. 80559-80570, 2021. [CrossRef]

[17] Hasan Thabit Rashid, and Israa Hadi Ali, "Traffic Violations Detection Review based on Intelligent Surveillance Systems," *International Journal of Computer and Organization Trends*, vol. 11, no. 4, pp. 1-9, 2021. [CrossRef]

[18] Nitha C. Velayudhan, A. Anitha, and Mukesh Madanan, "Sybil Attack Detection and Secure Data Transmission in VANET Using CMEHA-DNN and MD5-ECC," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, pp. 1297–1309, 2023. [CrossRef]

[19] Malik Braik, Alaa Sheta, and Heba Al-Hiary, "A Novel Meta-Heuristic Search Algorithm for Solving Optimization Problems: Capuchin Search Algorithm," *Neural Computing and Applications*, vol. 33, no. 7, pp.2515-2547. [CrossRef]

[20] Gaurav Dhiman et al., "A Novel Algorithm for Global Optimization: Rat Swarm Optimizer," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 8, pp.8457-8482. [CrossRef]

[21] Xia Feng, and Jin Tang, "Obfuscated RSUs Vector Based Signature Scheme for Detecting Conspiracy Sybil Attack in Vanets," *Mobile Information Systems*, 2017. [CrossRef]

[22] Zhaojun Lu et al., "A Blockchain-Based Privacy-Preserving Authentication Scheme for Vanets," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 12, pp.2792-2801, 2019. [CrossRef]

[23] R Vinayakumar, K P Soman, and Prabaharan Poornachandran "Applying Convolutional Neural Network for Network Intrusion Detection," *International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 1222-1228, 2017. [CrossRef]

[24] Kulkarni Sagar S., and Kahate Sandip A., "Review of a Semantic Approach to Host-Based Intrusion Detection Systems Using Contiguous and Dis-Contiguous System Call Patterns," *SSRG International Journal of Computer Science and Engineering* , Vol. 2, No. 6, pp. 9-12, 2015. [CrossRef]

[25] Xiu Kan et al., "A Novel IoT Network Intrusion Detection Approach Based on Adaptive Particle Swarm Optimization Convolutional Neural Network," *Information Sciences*, vol. 568, no. 5, pp.147-162, 2021. [CrossRef]

[26] S.Navya Sai, and K.Kishoreraju, "Improved Privacy Preserving Decision Tree Approach for Network Intrusion Detection," International Journal of Computer & Organization Trends, vol. 6, no. 1, pp. 55-60, 2016. [CrossRef]

[27] Basant Subba, Santosh Biswas, and Sushanta Karmakar, "A Game Theory Based Multi Layered Intrusion Detection Framework for VANET," *Future Generation Computer Systems*, vol. 82, pp. 12-28, 2018. [CrossRef]

[28] Sunil M. Sangve, Reena Bhati, and Vidhya N. Gavali, "Intrusion Detection System for Detecting Rogue Nodes in Vehicular Ad-Hoc Network," *International Conference on Data Management, Analytics and Innovation (ICDMAI)*, pp. 127-131, 2017. [CrossRef]

[29] Shivam Kumar Chauhan, Abhishek Sharma, and Avinash Kaur, "Animal Intrusion Detection and Prevention System," *International Journal of Computer and Organization Trends*, vol. 11, no. 2, pp. 25-28, 2021. [CrossRef]

[30] Hind Bangui, and Barbora Buhnova, "Recent Advances in Machine-Learning Driven Intrusion Detection in Transportation: Survey, " *Procedia Computer Science*, vol. 184, pp. 877-886, 2021. [CrossRef]

[31] Wenjuan Li et al., “Challenge-Based Collaborative Intrusion Detection in Software-Defined Networking: An Evaluation,” *Digital Communications and Networks*, vol. 7, no. 2, pp. 257-263, 2021. [CrossRef]

[32] Mohammad Dawood Momand, Vikas Thada, and Utpal Shrivastava, "Intrusion Detection System in IoT Network," *SSRG International Journal of Computer Science and Engineering* , vol. 7, no. 4, pp. 11-15, 2020. [CrossRef]

[33] Meysam Azizian, Soumaya Cherkaoui, and Abdelhakim Senhaji Hafid, “DCEV: A Distributed Cluster Formation for VANET Based on End-to-End Realtive Mobility,” *International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 287-291, 2016. [CrossRef]

[34] Gaurav Dhiman, and Vijaya Kumar, “Seagull Optimization Algorithm: Theory and Its Applications for Large-Scale Industrial Engineering Problems,” *Knowledge-Based Systems*, vol. 165, pp.169-196, 2019. [CrossRef]