Computers, Materials & Continua
DOI: 10.32604/cmc.2022.032353
Article

Tech Science Press

Blockchain Driven Metaheuristic Route Planning in Secure Vehicular Adhoc Networks

Siwar Ben Haj Hassine[1], Saud S. Alotaibi[2], Hadeel Alsolai[3], Reem Alshahrani[4], Lilia Kechiche[5], Mrim M. Alnfiai[6], Amira Sayed A. Aziz[7] and Manar Ahmed Hamza[8,*]

[1]Department of Computer Science, College of Science & Art at Mahayil, King Khalid University, Saudi Arabia
[2]Department of Information Systems, College of Computing and Information System, Umm Al-Qura University, Saudi Arabia
[3]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh, 11671, Saudi Arabia
[4]Department of Computer Science, College of Computers and Information Technology, Taif University, P.O.Box 11099, Taif, 21944, Saudi Arabia
[5]Department of Sciences and Technology, Taif University, Taif P.O. Box 11099, Taif, 21944, Saudi Arabia
[6]Department of Information Technology, College of Computers and Information Technology, Taif University, Taif P.O. Box 11099, Taif, 21944, Saudi Arabia
[7]Department of Digital Media, Faculty of Computers and Information Technology, Future University in Egypt, New Cairo, 11835, Egypt
[8]Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam bin Abdulaziz University, AlKharj, Saudi Arabia
*Corresponding Author: Manar Ahmed Hamza. Email: ma.hamza@psau.edu.sa
Received: 15 May 2022; Accepted: 17 June 2022

Abstract: Nowadays, vehicular ad hoc networks (VANET) turn out to be a core portion of intelligent transportation systems (ITSs), that mainly focus on achieving continual Internet connectivity amongst vehicles on the road. The VANET was utilized to enhance driving safety and build an ITS in modern cities. Driving safety is a main portion of VANET, the privacy and security of these messages should be protected. In this aspect, this article presents a blockchain with sunflower optimization enabled route planning scheme (BCSFO-RPS) for secure VANET. The presented BCSFO-RPS model focuses on the identification of routes in such a way that vehicular communication is secure. In addition, the BCSFO-RPS model employs SFO algorithm with a fitness function for effectual identification of routes. Besides, the proposed BCSFO-RPS model derives an intrusion detection system (IDS) encompassing two processes namely feature selection and classification. To detect intrusions, correlation based feature selection (CFS) and kernel extreme machine learning (KELM) classifier is applied. The performance of the BCSFO-RPS model is tested using a series of experiments and the results reported the enhancements of the BCSFO-RPS model over other approaches with maximum accuracy of 98.70%.

Keywords: VANET; sunflower optimization; machine learning; blockchain; intrusion detection

1 Introduction

Vehicular Ad-hoc Networks (VANETs) technologies are getting substantial interest from the researchers for the reason that it is the most promising technology for enhancing the Intelligent Transportation System (ITSs) through Vehicle-to-Everything (V2X) transmissions [1]. The application's purpose primarily depends on a vehicle sensor's capability to notice the situations around it intelligently and distribute messages through inter-vehicular transmission to bring important advancements in cities' road traffic. Even though VANET applications drive superior experiences, it delays actual placement and its wide utilization [2] because of various unresolved security menaces. VANETs are revealed to raise risk of being a goal for several forms of attacks because security by design was not a concern [3]. Later the routing protocols and system interfaces have vulnerabilities which obstruct the application readiness. Various researcher scholars made enormous efforts in their work which widely covered several forms of attacks. Several outlines were created and enhanced till now for offering security solutions to assaults in VANETs [4,5].

Owing to the decentralized construction and the dynamic topology of VANETs, the security of users, vehicles, and data is significant, and malignant nodes must be detected [6]. In a VANET, vehicles interchange confidential information, and traffic is altered respectively. The lack of official data results in malignant attacks which may cause severe issues for the drivers [7]. The messages will be approved by employing tracking the vehicles via a network and discovering the particulars which are needed [8–10], but this compromises the user's security. Thus, steadiness must be founded on privacy and authentication of users. Privacy of vehicles and Trust management are difficult issues for VANETs. Intrusion detection (ID) is actually, one of the subjects of widespread research for permitting accessibility of information and other data to only those who are authorized [11,12]. In comparison to co-reactance, acceptance, and prevention, of intrusions, ID is the only methodology able to truly defy probable cyber-attacks. Blockchain (BC) is considered an incorruptible digital record of transaction data [13]. BC performs a dispersed database which saves identical blocks of information over the network (means the system did not have just a single point of failure and, since it is dispersed, it does not control by one single node or entity, or user).

In [14], the authors propose the BC based decentralized trust score structure to participate node for detecting and blacklisting insider attackers from the VANET proactively. It can present a 2-level detection method, whereas, at the primary level, adjacent nodes compute the trust individually. During the secondary level, a consortium BC based model with authorized Road Side Units (RSUs) as validators, aggregate trust score to vehicular node. Afterward, according to the trust score described by the adjacent nodes, the blacklist node tables were dynamically changed. Alkadi et al. [15] examines the outline of cloud structure and categorized potential recent security event dependent upon its occurrence at distinct cloud utilization methods. The Network Intrusion Detection Systems (NIDS) from the cloud, containing kinds of classifiers and general recognition methods are also explained.

Islam et al. [16] present a lightweight vehicular BC structure to distributed method share for enhancing trust, verifiability, and non-repudiation from the distributed vehicular collaboration. It can present a new protocol and effectual 2-step transaction verification process to method sharing application. Choudhary et al. [17] present the machine learning (ML) technique which optimizes BC parameters from the QoS-aware approach. This parameter contains chosen chain length, encrypt block

length, and so on. The ML technique was simulated by Q-Learning and purposes at decreasing the performance result of BC functions on the entire QoS of VANETs.

In [18], the authors established the design of novel BC based Internet of Things (IoT) network structure which leverage Software Defined Network (SDN) and Network Function Virtualization (NFV) to secure IoT transaction. It can be established an IDS from the procedure of Virtualized Network Function (VNF) which enhances both the scalability as well as efficiency of IoT networks. Dhurandher et al. [19] discovers the secure and decentralized method which utilizes the Proof-of-Work (PoW) consensus process and presents a BC based secured routing protocol (named BDRP). During this case, it can be proposal a combined routing protocol which utilizes PoW for routing and illustrates how immutability is executed to the OppNet paradigm. BC promises transparent, distributed, and tamper-resistant ledger and secure models which are offered secure routing solutions for OppNets.

This article presents a blockchain with sunflower optimization enabled route planning scheme (BCSFO-RPS) for secure VANET. The presented BCSFO-RPS model employs SFO algorithm with a fitness function for effectual identification of routes. Besides, the proposed BCSFO-RPS model derives an intrusion detection system (IDS) encompassing two processes namely feature selection and classification. To detect intrusions, correlation based feature selection (CFS) and kernel extreme machine learning (KELM) classifier is applied. The performance of the BCSFO-RPS model is tested using a series of experiments and the results reported the enhancements of the BCSFO-RPS model over other approaches.

2 The Proposed Model

In this article, a new BCSFO-RPS model has been introduced for the identification of routes in such a way that vehicular communication is security. In addition, the BCSFO-RPS model employs SFO algorithm with a fitness function for the effectual identification of routes. Besides, the proposed BCSFO-RPS model derives the IDS encompasses two processes namely feature selection and classification. Fig. 1 illustrates the overall process of proposed method in VANET.

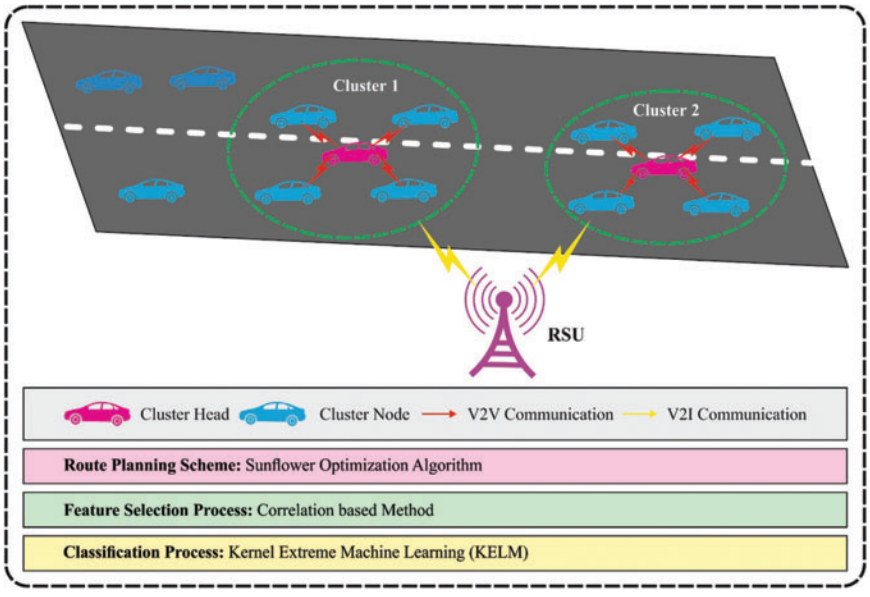

Figure 1: Overall process in proposed method

2.1 Overview of SFO Algorithm

Yang [20] projected a novel approach according to flower pollination method of the flowering plants assuming the biological procedure of reproductions. During this approach, the researcher assumes the peculiar nature of sunflowers by defining an optimal direction of sun. The pollination was considered to take arbitrary with minimal distance amongst the flower i and flower i + 1. At present, all the flower patches continually discharge millions of pollen gametes. However, to easiness, it assumed that all the sunflowers only generate 1 pollen gamete and separately reproduce. Otherwise, a further distance of plants in sun, smaller the quantity of heat obtained by it, so the same approach is subsequent under this research is proceeds massive step for obtaining adjacent global optimal (sun). Afterward, the quantity of heat Q reached by all the plants is demonstrated as:

$$Q_i = \frac{P}{4\pi r_i^2}, \tag{1}$$

Whereas P implies the source of power and r_i signifies the distance amongst existing plants and optimum i. The sunflower direction to sun is provided as:

$$\vec{s_i} = \frac{X^* - X_i}{||X^* - X_i||}, i = 1,\ 2,\ \ldots,\ n_p. \tag{2}$$

The sunflower in the direction s is measured as:

$$d_i = \lambda \times P_i\left(||X_i + X_{i-1}||\right) \times ||X_i + X_{i-1}||, \tag{3}$$

Whereas λ signifies the constant value which defines the "inertial" displacement of plants, $P_i\left(||X_i + X_{i-1}||\right)$ denotes the pollination probability, i.e., the sunflower i pollinates with their nearby neighbor $i-1$ generating a novel individual from the random place which varies dependent on all the distances amongst the flowers [21]. In detail, an individual nearby the sun proceeds lesser step from the local refinement searching but more distant individuals are commonly moving. It is also important for limiting the maximal steps offered to all the individuals, for avoiding skip areas inclined that global minimal candidates. At this point, it can be represented as:

$$d_{\max} = \frac{||X_{\max} - X_{\min}||}{2 \times N_{\text{pop}}}, \tag{4}$$

In which $X_{\max}$ and $X_{\min}$ denotes the lower as well as upper bound values, and $\mathrm{N_{pop}}$ implies the count of plants in the entire population. The novel plantation was provided as:

$$\vec{X}_{t+1} = \vec{X}_i + d_i \times \vec{s_i}. \tag{5}$$

2.2 Route Planning Process

In this study, the BCSFO-RPS model employs SFO algorithm with a fitness function for effectual identification of routes. For defining a best set of directions, the SFO derived a function provided in the following:

$$f\ (x) = \left\{ i,\ for\ which \left| \left(\frac{i}{k} - X_{i_f j} \right) \right| is\ minimum,\ \forall_i 1 \le i \le k \right. \tag{6}$$

The objective is to define a best set of directions in CHs to BS exploiting a fitness function (FF) encompassing 2 variables such as distance and energy. At first, the RE of next-hop vehicle is described and the vehicle with maximum energy is provided as relay vehicle. Hence, the vehicle with better RE

is provided as next-hop vehicle. The primary sub-objective $f1$ is shown below:

$$f1 = E_{CH} \tag{7}$$

Likewise, Euclidean distance is executed for defining the distance in cluster head (CH) to base station (BS). The reduction of energy dissipation is dependent mostly on the communication distance. Consequently, the vehicle with minimum distance is considered a relay vehicle. Therefore, the following sub-objective using distance is $f2$ shown in the following:

$$f2 = \frac{1}{\sum_{i=1}^{\mathrm{m}} dis\,(CH_i, NH) + dis\,(NH, BS)} \tag{8}$$

The abovementioned sub-objective is studied as to FF as providing where the α_1 and α_2 indicates the weight allotted for each sub-objective.

$$Fitness = \alpha_1\,(f1) + \alpha_2\,(f2)\,,\ where \sum_{i=1}^{2} \alpha_i = 1 \alpha_i \varepsilon (0, 1); \tag{9}$$

2.3 Intrusion Detection and Classification

To detect intrusions, a two stage process is carried out namely CFS and KELM classification. CFS measured the goodness of element subset by assuming the redundancy amongst the elements and individual prediction abilities of elements. The CFS chooses subsets that are extremely connected to target class however the lower inter-correlation. The worth of elements subset S with r elements is demonstrated in Eq. (10) in which C estimates the similarity of 2 elements, such as correlation (not essentially $Pearson^1 sr$ and $n^1 s\,p$).

$$Worth\ \ (S_t) = \frac{\sum_{f_i \epsilon S_t} \mathrm{C}\,(f_i, class)}{\sqrt{\sum_{f_i \epsilon S_t} \sum_{f_j \epsilon S_t - \{f_i\}} C\left(f_{\mathrm{i}}, f_j\right)}} \tag{10}$$

Once the features are chosen, the intrusions are classified by the use of KELM model. The extreme learning machine (ELM) can be determined by a single hidden layer feedforward neural network (SLFN). It is apparent that a hidden state is assumed as nonlinear because of the presence of nonlinear activation function [22]. It is encompassed 3 layers such as output, input, and hidden layers. Let x be a trained instance and $f\,(x)$ be the outcome of neural network (NN). Next, single layer feed forward network (SLFN) using k hidden node is represented as follows:

$$f_{ELM}\,(x) = B^T \cdot G(w,\ b, x), \tag{11}$$

Whereas $G\,(w,\ b, x)$ indicates the hidden state, w represents the input weight matrixes, b illustrates a bias weight, and $B = [\beta_1 \beta_2 \ldots \beta_m]$ characterizes the weight amongst hidden and output layers. For ELM using n trained samples, k hidden neurons, m output neurons, and d input neurons are produced by

$$t_j = B^T \cdot g\left(\langle w_j, x_i\rangle + b_j\right), i = 1, 2,\ \ldots n, \tag{12}$$

In Eq. (12), t_i represents the m-dimension target output vector for $i, j\text{-}th$ trained samples x_i, the d-dimension w_j indicates $j\text{-}th$ weight vector from the inputted to $j{-}th$ hidden neurons, and b_j indicates the bias of $j{-}th$ hidden neurons. Here, $\langle w_j, x_i\rangle$ indicates the inner product of w_j and x_i. Thus, sigmoid

operation g can be simplified by activation function, therefore the outcome of $j-th$ hidden neurons as

$$g\left(\left\langle w_j, x_i\right\rangle + b_j\right) = 1/\left(1 + \exp\left(-\frac{w_j^T x_i + b_j}{2e^2}\right)\right), \tag{13}$$

Now, exp $(\cdot)$ denotes the exponential arithmetical values, and ϵ^2 illustrates the steepness parameter. It is expressed in the following

$$HB = T, \tag{14}$$

Here, $T \in R^{n\times m}$ is meant to be target output, $B \in R^{k\times m}.H = \begin{bmatrix} h(x_1) \\ \vdots \\ h(x_n) \end{bmatrix}$ means the hidden-neuron output matrix of ELM using (n, k), is applied by:

$$H = g(W.X + b) = \begin{bmatrix} g(\langle w_1, x_n\rangle + b_1) & \cdots & g(\langle w_1, x_n\rangle + b_1) \\ \vdots & \ldots & \vdots \\ g(\langle w_1, x_n\rangle + b_1) & \cdots & g(\langle w_1, x_n\rangle + b_1) \end{bmatrix}_{n\times k} \tag{15}$$

Then, B is defined with a low norm least-squares solution:

$$B = H^{\dagger}T = H^T\left(\frac{I}{C} + HH^T\right)^{-1}T, \tag{16}$$

In which C represents a regularization variable and the ELM technique is formulated by,

$$f_{ELM}(x) = h(x)\,H^T\left(\frac{I}{C} + HH^T\right)^{-1}T, \tag{17}$$

ELM is improvised by KELM with kernel trick.

$$\Omega = HH^T, \tag{18}$$

Whereas

$$\Omega_{i,j} = k(x_j, x_j), \tag{19}$$

Now x_i and x_j displays i-th and j-th trained instance. Afterward, interchange HH^T using Ω, the inference of KELM is shown below

$$f_{KELM}(x) = h(x)\,H^T\left(\frac{I}{C} + \Omega\right)^{-1}T, \tag{20}$$

In Eq. (20), $f_{KELM}(x)$ represents the outcome of KELM method and $h(x)\,H^T = \begin{bmatrix} k(x'x1) \\ k(x, x_n) \end{bmatrix}$. Unlike ELM, the substantial feature of KELM is a hidden node count attained and no arbitrary feature mapping is applied. Furthermore, the processing time is alleviated in comparison to ELM. Fig. 2 depicts the framework of ELM.

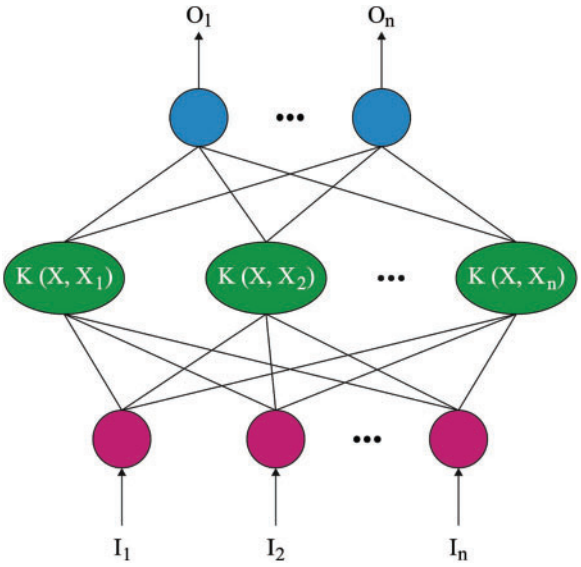

Figure 2: Structure of ELM

2.4 Blockchain Assisted Vehicular Communication

A blockchain is a group of blocks where all the blocks consist of: the timestamp, the current block, information about the transactions (bitcoin, Ethereum), and hash values of the preceding blocks. Also, a blockchain is determined by a shared automated ledger viz. employed for storing the details of the transaction. Consider that vehicle interacts with others via vehicle-to everything (V2X) and V2V transmission, also that vehicle is connected to the Internet effectually. It should be assumed that each vehicle is indispensable namely global positioning system (GPS), on-board unit (OBU), and sensors. Additionally, the amount of legitimate road side unit (RSU) is greater when compared to susceptible RSU. Consider that important event message is dispersed within the region of interest. The message number is very important for guarantying the events and the messages are acknowledged as accurate. A novel category of blockchain is required, as standard blockchain could not be employed for the objective. A conventional blockchain employed is cryptocurrency, where the user requires a blockchain that handles secure event messages with no crypto coins. Consequently, it applies security event messages [23–27].

At this point, the event is local, and event message is restricted to vehicles that establish within a certain geographical region. During the conventional blockchain, the recently produced block is commonly transmitted. However, the VANET message doesn't cross the limit of a certain position, meanwhile, the accident and traffic details of a position are unidentified to vehicles that establish in other locations. Consequently, a novel blockchain architecture is needed. From the individual blockchain, each miner mines fresh block based on the event message and forwarded each recently produced block to the local blockchain networks. Next, vehicles could inquiry about their protection levels, if necessary, by using the blockchain. When the generation is accomplished, the novel block is transmission, and vehicle in the network upgrades and validates the blockchains.

3 Experimental Validation

This section offers a comprehensive simulation analysis of the BCSFO-RPS model with recent models.

Tab. 1 and Fig. 3 report a detailed examination of the BCSFO-RPS model with existing models in terms of number of clusters (NOC). Fig. 3a shows the NOC inspection of the BCSFO-RPS model with recent models under 30 nodes (vehicles) and diverse transmission ranges (TR). The results implied that the BCSFO-RPS model has attained minimal NOC over other models. For instance, with TR of 10, the BCSFO-RPS model has offered reduced NOC of 22 whereas the grey wolf with cluster scheme (GWCS), multi-objective particle swarm optimization (MOPSO), comprehensive learning particle swarm optimization (CLPSO), and rainfall optimization algorithm (ROA) models have provided increased NOC of 35, 34, 31, and 28 respectively. At the same time, with TR of 60, the BCSFO-RPS method has provided decreased NOC of 3 wherein the GWCS, MOPSO, CLPSO, and ROA techniques have granted increased NOC of 15, 14, 13, and 8 correspondingly.

Table 1: Result analysis of BCSFO-RPS technique with distinct nodes under interms of NOC

Transmission range	Grey wolf cluster scheme	Multi objective PSO	Comprehensive-LPSO	Rainfall opt. algorithm	BCSFO-RPS
Nodes = 30					
10	35	34	31	28	25
15	33	33	30	28	22
20	30	29	29	27	21
25	26	25	25	20	28
30	24	24	23	19	17
35	23	22	22	19	15
40	22	20	20	18	15
45	20	20	16	18	6
50	18	18	16	16	5
55	17	15	13	12	5
60	15	14	13	8	3
Nodes = 40					
10	32	34	35	31	26
15	31	29	34	30	27
20	29	25	31	25	21
25	27	25	25	22	17
30	26	24	25	20	16
35	22	21	21	19	16
40	22	19	21	17	14
45	18	17	19	15	10
50	17	16	16	14	8
55	14	16	13	11	8
60	12	15	9	8	3
Nodes = 50					
10	35	34	33	31	27

(Continued)

Table 1: Continued

Transmission range	Grey wolf cluster scheme	Multi objective PSO	Comprehensive-LPSO	Rainfall opt. algorithm	BCSFO-RPS
15	34	30	29	28	26
20	31	28	27	26	22
25	29	27	26	24	19
30	29	25	24	24	19
35	26	24	23	22	17
40	22	20	19	21	12
45	21	19	18	15	11
50	19	17	15	14	9
55	18	16	12	11	6
60	16	15	9	5	4
Nodes = 60					
10	35	35	32	34	31
15	32	34	29	31	26
20	31	28	28	25	21
25	27	23	26	24	17
30	23	22	26	22	16
35	23	20	25	22	16
40	20	19	23	16	12
45	20	17	17	15	11
50	16	14	13	13	10
55	16	13	12	10	9
60	14	12	11	5	3

Fig. 3b displays the NOC examination of the BCSFO-RPS methods with recent models under 40 nodes (vehicles) and diverse TR. The outcomes implied that the BCSFO-RPS methodology has recached minimum NOC than other models. For example, with TR of 10, the BCSFO-RPS model has rendered reduced NOC of 26 wherein the GWCS, MOPSO, CLPSO, and ROA techniques have offered increased NOC of 32, 34, 35, and 31 respectively. Meanwhile, with TR of 60, the BCSFO-RPS method has granted minimized NOC of 3 whereas the GWCS, MOPSO, CLPSO, and ROA models have offered increased NOC of 12, 15, 9, and 8 correspondingly.

Fig. 3c displays the NOC review of the BCSFO-RPS method with recent models under 50 nodes (vehicles) and diverse TR. The outcomes implied that the BCSFO-RPS model has gained minimum NOC than other models. For example, with TR of 10, the BCSFO-RPS method has rendered reduced NOC of 27 whereas the GWCS, MOPSO, CLPSO, and ROA techniques have offered increased NOC of 35, 34, 33, and 31 correspondingly. Meanwhile, with TR of 60, the BCSFO-RPS model has provided decreased NOC of 4 wherein the GWCS, MOPSO, CLPSO, and ROA algorithms have offered increased NOC of 16, 15, 9, and 5 correspondingly. Fig. 3d depicts the NOC scrutiny of the BCSFO-RPS method with recent models under 60 nodes (vehicles) and diverse TR. The results implied that the BCSFO-RPS methodology has gained the least NOC over other models. For example, with TR of 10, the BCSFO-RPS algorithm has rendered minimized NOC of 31 wherein the GWCS, MOPSO, CLPSO, and ROA models have offered increased NOC of 35, 35, 32, and 24 correspondingly.

Meanwhile, with TR of 60, the BCSFO-RPS methodology has granted reduced NOC of 3 whereas the GWCS, MOPSO, CLPSO, and ROA algorithms have offered increased NOC of 14, 12, 11, and 5 correspondingly.

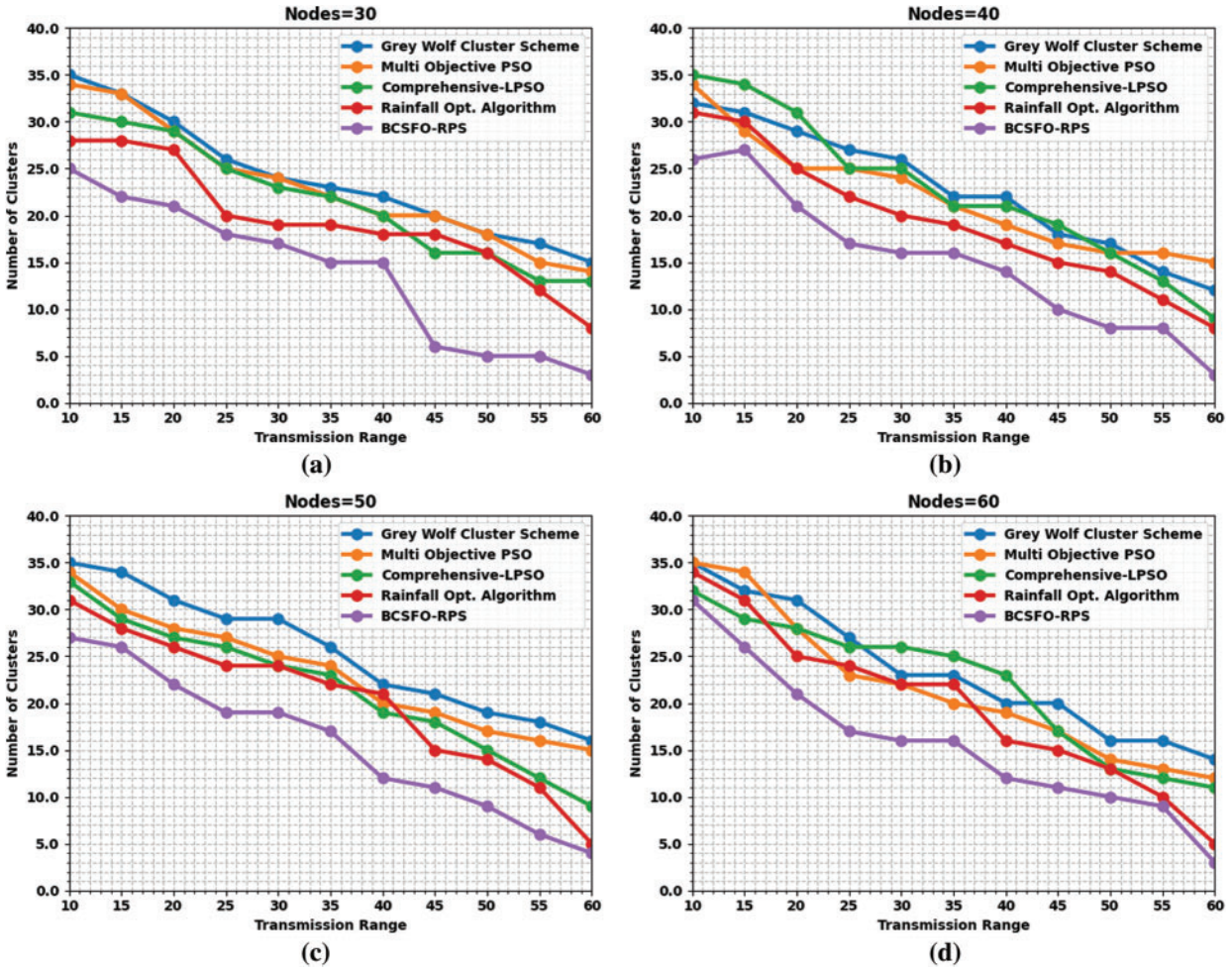

Figure 3: NOC analysis of BCSFO-RPS technique (a) 30 nodes, (b) 40 nodes, (c) 50 nodes, and (d) 60 nodes

A detailed end to end delay (ETED) examination of the BCSFO-RPS model with other models takes place in Tab. 2 and Fig. 4. The experimental values inferred that the BCSFO-RPS model has resulted in minimal values of ETED. For instance, with 20 nodes, the BCSFO-RPS model has offered lower ETED of 0.122 s whereas the GWCS, MOPSO, CLPSO, and ROA models have reached increased ETED of 0.291, 0.221, 0.166, and 0.142 s respectively. Along with that, with 100 nodes, the BCSFO-RPS algorithm has provided lower ETED of 0.271 s whereas the GWCS, MOPSO, CLPSO, and ROA methods have reached increased ETED of 0.475, 0.430, 0.383, and 0.317 s correspondingly.

Table 2: ETED analysis of BCSFO-RPS technique with various counts of nodes

End to end delay (sec)					
No. of nodes	Grey wolf cluster scheme	Multi objective PSO	Comprehensive-LPSO	Rainfall opt. algorithm	BCSFO-RPS
20	0.291	0.221	0.166	0.142	0.122
40	0.301	0.258	0.221	0.189	0.148
60	0.341	0.310	0.275	0.235	0.170
80	0.437	0.393	0.339	0.284	0.223
100	0.475	0.430	0.383	0.317	0.271

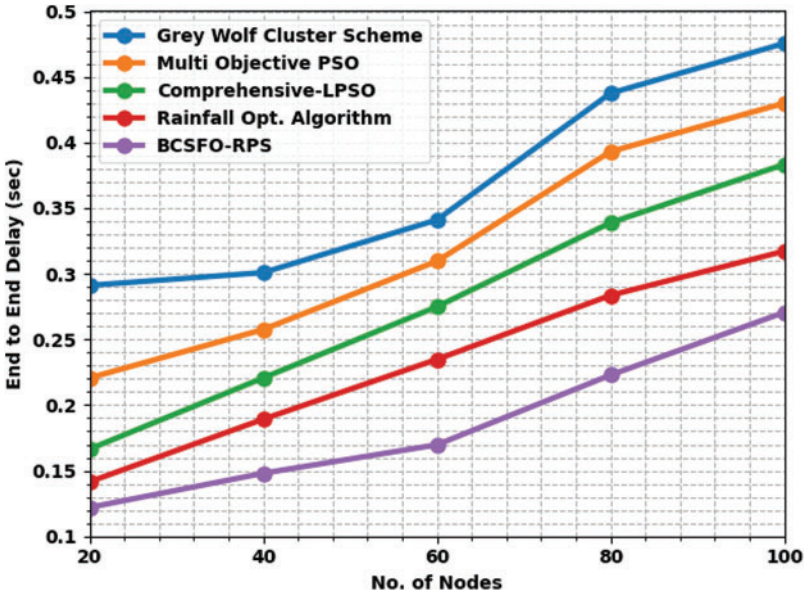

Figure 4: ETED analysis of BCSFO-RPS algorithm with various counts of nodes

A comprehensive ETED inspection of the BCSFO-RPS model with other models is carried out in Tab. 3 and Fig. 5. The simulation results demonstrated that the BCSFO-RPS model has accomplished maximum packet delivery ratio (PDR) values. For instance, with 20 nodes, the BCSFO-RPS model has reached improved PDR of 0.965 whereas the GWCS, MOPSO, CLPSO, and ROA models have obtained decreased PDR of 0.663, 0.694, 0.732, and 0.788 respectively. Besides, with 100 nodes, the BCSFO-RPS methodology has reached improved PDR of 0.706 whereas the GWCS, MOPSO, CLPSO, and ROA techniques have gained decreased PDR of 0.558, 0.585, 0.625, and 0.651 correspondingly.

Table 3: PDR analysis of BCSFO-RPS algorithm with various counts of nodes

Packet delivery ratio					
No. of nodes	Grey wolf cluster scheme	Multi objective PSO	Comprehensive-LPSO	Rainfall opt. algorithm	BCSFO-RPS
20	0.663	0.694	0.732	0.788	0.965
40	0.637	0.685	0.719	0.779	0.897
60	0.581	0.609	0.671	0.740	0.810
80	0.559	0.575	0.626	0.672	0.742
100	0.558	0.585	0.625	0.651	0.706

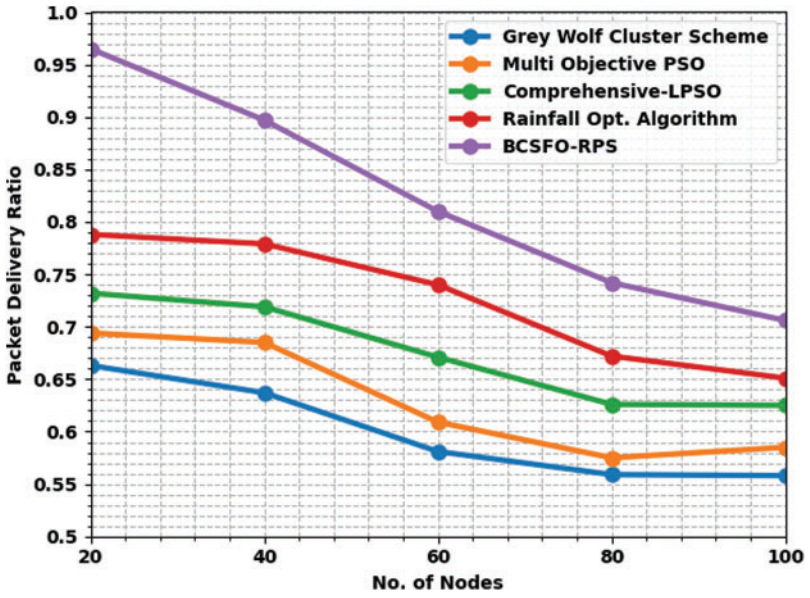

Figure 5: PDR analysis of BCSFO-RPS algorithm with various counts of nodes

Next, the intrusion detection results are examined on NSL-KDD 2015 dataset comprising 67343 samples under normal class and 58630 samples in anomaly class. Fig. 6 demonstrates a set of confusion matrices offered by the BCSFO-RPS model. On entire dataset, the BCSFO-RPS model has provided 66650 samples into normal and 57661 samples into anomaly class. Along with that, on 30% of TS data, the BCSFO-RPS method has offered 19778 samples into normal and 17521 samples into anomaly class.

Tab. 4 and Fig. 7 exemplify comprehensive classification outcomes of the BCSFO-RPS model on test data. On entire dataset, the BCSFO-RPS model has offered average $accu_y$, $prec_n$, $reca_l$, F_{score}, and kappa of 98.68%, 98.69%, 98.66%, 98.67%, and 97.35% respectively. Also, on 70% of TR data, the BCSFO-RPS methodology has provided average $accu_y$, $prec_n$, $reca_l$, F_{score}, and kappa of 98.67%, 98.68%, 98.65%, 98.67%, and 97.33% correspondingly. Besides, on 30% of TS data, the BCSFO-RPS techniques have provided average $accu_y$, $prec_n$, $reca_l$, F_{score}, and kappa of 98.70%, 98.71%, 98.68%, 98.69%, and 97.38% correspondingly.

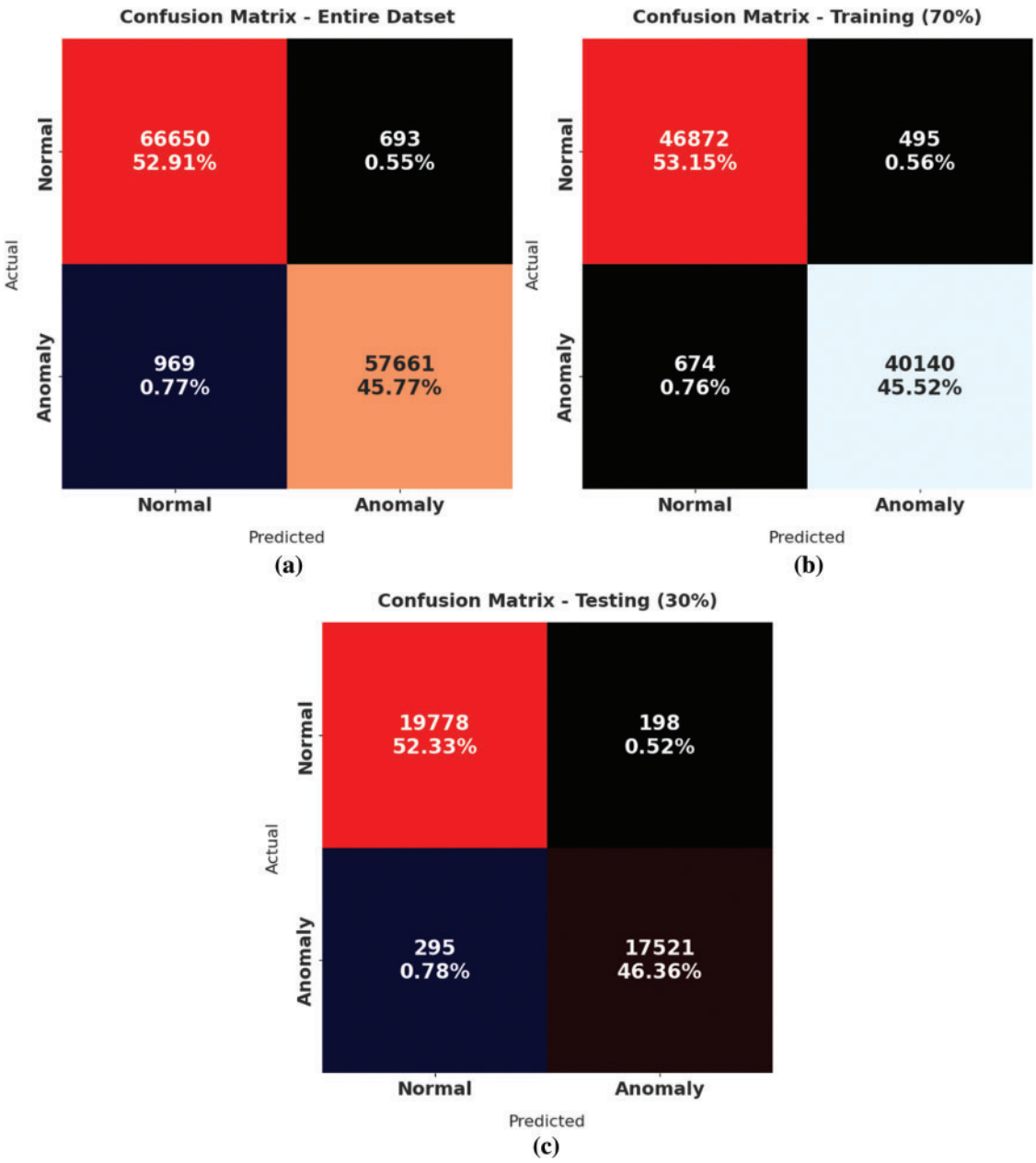

Figure 6: Confusion matrices of BCSFO-RPS technique (a) entire dataset, (b) 70% of TR data, and (c) 30% of TS data

At last, a comparative accuracy examination is made with recent models in Fig. 8. The figure pointed out that the VGG-19 and ResNet models have shown least outcomes. At the same time, the DBN, cuckoo optimization, and CNN-ResNet 101 models have obtained moderately closer accuracy values. Though the behaviour-BIDS model has exhibited reasonable accuracy of 98.43%, the BCSFO-RPS model has shown maximum accuracy of 98.70%.

Table 4: Result analysis of BCSFO-RPS technique with various measures and datasets

Class names	Accuracy	Precision	Recall	F-score	Kappa score
Entire dataset					
Normal	98.68	98.57	98.97	98.77	-
Anomaly	98.68	98.81	98.35	98.58	-
Average	98.68	98.69	98.66	98.67	97.35
Training (70%)					
Normal	98.67	98.58	98.95	98.77	-
Anomaly	98.67	98.78	98.35	98.56	-
Average	98.67	98.68	98.65	98.67	97.33
Testing (30%)					
Normal	98.70	98.53	99.01	98.77	-
Anomaly	98.70	98.88	98.34	98.61	-
Average	98.70	98.71	98.68	98.69	97.38

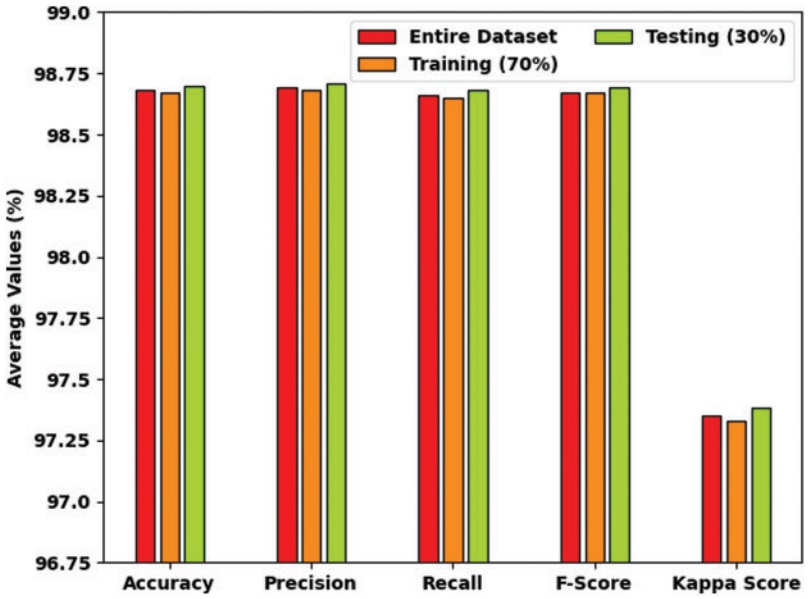

Figure 7: Result analysis of BCSFO-RPS technique with various measures

Therefore, the BCSFO-RPS model has appeared as an effectual tool for accomplishing improving network performance.

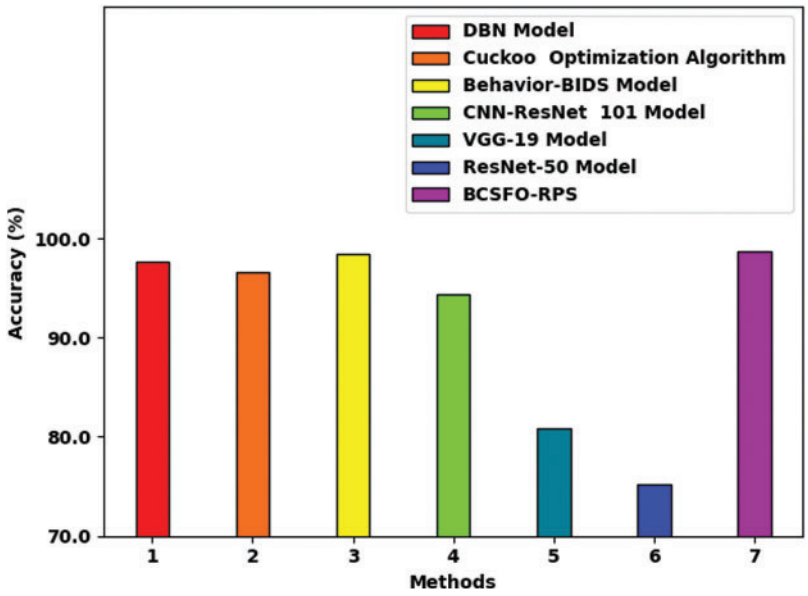

Figure 8: $Accu_y$ analysis of BCSFO-RPS technique with existing approaches

4 Conclusion

In this article, a new BCSFO-RPS model has been introduced for the identification of routes in such a way that vehicular communication is security. In addition, the BCSFO-RPS model employs SFO algorithm with a fitness function for effectual identification of routes. Besides, the proposed BCSFO-RPS model derives the IDS encompasses two processes namely feature selection and classification. To detect intrusions, a two stage process is carried out namely CFS and KELM classification. The performance of the BCSFO-RPS model is tested using a series of experiments and the results reported the enhancements of the BCSFO-RPS model over other approaches with maximum accuracy of 98.70%. Thus, the BCSFO-RPS model can be utilized for security accomplishment in VANET. In the future, lightweight cryptographic algorithms can be employed to improve secrecy and privacy.

Funding Statement: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through Large Groups Project under Grant Number (25/43). Taif University Researchers Supporting Project Number (TURSP-2020/346), Taif University, Taif, Saudi Arabia. Princess Nourah bint Abdulrahman University Researchers Supporting Project Number (PNURSP2022R303), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by Grant Code: (22UQU4210118DSR17).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. More, R. Sonkamble, U. Naik, S. Phansalkar, P. More *et al.,* "Secured communication in vehicular adhoc networks (vanets) using blockchain," *IOP Conference Series: Materials Science and Engineering*, vol. 1022, no. 1, pp. 012067, 2021.

[2] J. Wang, Y. Liu, S. Niu and H. Song, "Lightweight blockchain assisted secure routing of swarm UAS networking," *Computer Communications*, vol. 165, pp. 131–140, 2021.

[3] A. M. Krishna and A. K. Tyagi, "Intrusion detection in intelligent transportation system and its applications using blockchain technology," in *2020 Int. Conf. on Emerging Trends in Information Technology and Engineering (ic-ETITE)*, Vellore, India, pp. 1–8, 2020.

[4] S. Rajasoundaran, S. V. N. S. Kumar, M. Selvi, S. Ganapathy, R. Rakesh *et al.,* "Machine learning based volatile block chain construction for secure routing in decentralized military sensor networks," *Wireless Networks*, vol. 27, no. 7, pp. 4513–4534, 2021.

[5] M. Benguenane, A. Korichi and N. Azzaoui, "Geographical routing protocols in vanets: Performance and security analysis," in *2nd Int. Conf. on Industry 4.0 and Artificial Intelligence (ICIAI 2021)*, Sousse, Tunisia, pp. 158–163, 2022.

[6] G. Rathee, A. Sharma, R. Iqbal, M. Aloqaily, N. Jaglan *et al.,* "A blockchain framework for securing connected and autonomous vehicles," *Sensors*, vol. 19, no. 14, pp. 3165, 2019.

[7] A. Hakiri and B. Dezfouli, "Towards a blockchain-sdn architecture for secure and trustworthy 5 g massive iot networks," in *Proc. of the 2021 ACM Int. Workshop on Software Defined Networks & Network Function Virtualization Security*, Virtual Event USA, pp. 11–18, 2021.

[8] M. A. Ferrag and L. Maglaras, "DeliveryCoin: An ids and blockchain-based delivery framework for drone-delivered services," *Computers*, vol. 8, no. 3, pp. 58, 2019.

[9] A. Al-Qarafi, F. Alrowais, S. Alotaibi, N. Nemri, F. N. Al-Wesabi *et al.,* "Optimal machine learning based privacy preserving blockchain assisted internet of things with smart cities environment," *Applied Sciences*, vol. 12, 2022. https://doi.org/10.3390/app12125893.

[10] M. A. Hamza, S. B. Haj Hassine, I. Abunadi, F. N. Al-Wesabi, H. Alsolai *et al.,* "Feature selection with optimal stacked sparse autoencoder for data mining," *Computers, Materials & Continua*, vol. 72, no. 2, pp. 2581–2596, 2022.

[11] I. Abunadi, M. M. Althobaiti, F. N. Al-Wesabi, A. M. Hilal, M. Medani *et al.,* "Federated learning with blockchain assisted image classification for clustered UAV networks," *Computers, Materials & Continua*, vol. 72, no. 1, pp. 1195–1212, 2022.

[12] R. Iqbal, T. A. Butt, M. Afzaal and K. Salah, "Trust management in social internet of vehicles: Factors, challenges, blockchain, and fog solutions," *International Journal of Distributed Sensor Networks*, vol. 15, no. 1, pp. 155014771982582, 2019.

[13] M. U. Hassan, M. H. Rehmani and J. Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions," *Future Generation Computer Systems*, vol. 97, pp. 512–529, 2019.

[14] S. Kudva, S. Badsha, S. Sengupta, H. La, I. Khalil *et al.,* "A scalable blockchain based trust management in VANET routing protocol," *Journal of Parallel and Distributed Computing*, vol. 152, pp. 144–156, 2021.

[15] O. Alkadi, N. Moustafa and B. Turnbull, "A review of intrusion detection and blockchain applications in the cloud: Approaches, challenges and solutions," *IEEE Access*, vol. 8, pp. 104893–104917, 2020.

[16] S. Islam, S. Badsha and S. Sengupta, "A light-weight blockchain architecture for v2v knowledge sharing at vehicular edges," in *2020 IEEE Int. Smart Cities Conf. (ISC2)*, Piscataway, NJ, USA, pp. 1–8, 2020.

[17] S. Choudhary and S. Dorle, "A quality of service-aware high-security architecture design for software-defined network powered vehicular ad-hoc networks using machine learning-based blockchain routing," *Concurrency and Computation: Practice and Experience*, 2022. https://doi.org/10.1002/cpe.6993.

[18] A. Hakiri, B. Sellami, S. B. Yahia and P. Berthou, "A blockchain architecture for sdn-enabled tamper-resistant iot networks," in *2020 Global Information Infrastructure and Networking Symp. (GIIS)*, Tunis, Tunisia, pp. 1–4, 2020.

[19] S. K. Dhurandher, J. Singh, P. Nicopolitidis, R. Kumar and G. Gupta, "A blockchain-based secure routing protocol for opportunistic networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 4, pp. 2191–2203, 2022.

[20] X. S. Yang, "Flower pollination algorithm for global optimization," in *Int. Conf. on Unconventional Computing and Natural Computation UCNC 2012: Unconventional Computation and Natural Computation*, Lecture Notes in Computer Science Book Series, Springer, Berlin, Heidelberg, vol. 7445, pp. 240–249, 2012.

[21] I. V. Pustokhina, D. A. Pustokhin, R. H. Aswathy, T. Jayasankar, C. Jeyalakshmi *et al.,* "Dynamic customer churn prediction strategy for business intelligence using text analytics with evolutionary optimization algorithms," *Information Processing & Management*, vol. 58, no. 6, pp. 102706, 2021.

[22] J. Xia, H. Zhang, R. Li, Z. Wang, Z. Cai *et al.,* "Adaptive barebones salp swarm algorithm with quasi-oppositional learning for medical diagnosis systems: A comprehensive analysis," *Journal of Bionic Engineering*, vol. 19, no. 1, pp. 240–256, 2022.

[23] O. A. Alzubi, J. A. Alzubi, K. Shankar and D. Gupta, "Blockchain and artificial intelligence enabled privacy-preserving medical data transmission in internet of things," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 12, pp. e4360, 2021.

[24] G. N. Nguyen, N. H. L. Viet, M. Elhoseny, K. Shankar, B. B. Gupta *et al.,* "Secure blockchain enabled cyber-physical systems in healthcare using deep belief network with ResNet model," *Journal of Parallel and Distributed Computing*, vol. 153, pp. 150–160, 2021.

[25] G. N. Nguyen, N. H. L. Viet, A. F. S. Devaraj, R. Gobi and K. Shankar, "Blockchain enabled energy efficient red deer algorithm based clustering protocol for pervasive wireless sensor networks," *Sustainable Computing: Informatics and Systems*, vol. 28, pp. 1–10, 2020.

[26] G. P. Joshi, E. Perumal, K. Shankar, U. Tariq, T. Ahmad *et al.,* "Toward blockchain-enabled privacy-preserving data transmission in cluster-based vehicular networks," *Electronics*, vol. 9, no. 9, pp. 1–15, 2020.

[27] B. L. Nguyen, E. L. Lydia, M. Elhoseny, I. V. Pustokhina, D. A. Pustokhin *et al.,* "Privacy preserving blockchain technique to achieve secure and reliable sharing of iot data," *Computers, Materials & Continua*, vol. 65, no. 1, pp. 87–107, 2020.