Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2022.026331
Article

Tech Science Press

Privacy Preserving Reliable Data Transmission in Cluster Based Vehicular Adhoc Networks

T. Tamilvizhi[1], R. Surendran[2,*], Carlos Andres Tavera Romero[3] and M. Sadish Sendil[4]

[1]Department of Information Technology, Vel Tech Multi Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Chennai, India
[2]Center for Artificial Intelligence and Research (CAIR), Chennai Institute of Technology, Chennai, India
[3]COMBA I+D Research Group of Universidad Santiago de Cali, Santiago de Cali, Colombia
[4]Department of Emerging Technologies, Guru Nanak Institute of Technology, Ibrahipatnam, Telangana, India
*Corresponding Author: R. Surendran. Email: dr.surendran.cse@gmail.com

Received: 22 December 2021; Accepted: 24 January 2022

Abstract: VANETs are a subclass of mobile ad hoc networks (MANETs) that enable efficient data transmission between vehicles and other vehicles, road side units (RSUs), and infrastructure. The purpose of VANET is to enhance security, road traffic management, and traveler services. Due to the nature of real-time issues such as reliability and privacy, messages transmitted via the VANET must be secret and confidential. As a result, this study provides a method for privacy-preserving reliable data transmission in a cluster-based VANET employing Fog Computing (PPRDA-FC). The PPRDA-FC technique suggested here seeks to ensure reliable message transmission by utilising FC and an optimal set of cluster heads (CH). The proposed PPRDA-FC technique utilizes a moth flame optimization with levy flight based clustering (MFO-LFC) process to identify and form clusters from a suitable set of CHs. The CHs are responsible for monitoring each vehicle in their respective clusters. Simultaneously, the CHs provide the most efficient and secure pathways for message transmission. Finally, a deep neural network (DNN) is used as a classification tool to distinguish between attacker-controlled and real-world automobiles. To evaluate the suggested PPRDA-FC technique's increased performance, a series of simulations were run and the results analyzed using a variety of metrics. The acquired experimental findings illustrate the suggested PPRDA-FC technique's superiority to recent state-of-the-art procedures.

Keywords: Clustering; VANET; security; reliability; fog computing; privacy preserving; deep learning

1 Introduction

VANETs are the future of intelligent transportation and automotive technologies. VANET enables vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) data transfer, which improves road safety, sends warning messages, increases comfort, and facilitates the sharing of information (including media), among other benefits. These characteristics are demonstrated by vehicles' ability to exchange security messages with one another and with the framework, enabling drivers to avoid traffic congestion and risks [1]. Vehicles can communicate with one another in a VANET to exchange data on road and traffic conditions. This data transmission is utilised to help reduce traffic accidents and congestion. However, this creates various security issues, as a few vehicles may provide bogus data to other vehicles. As a result, erroneous data must be discovered and treated appropriately. Data communication between automobiles may jeopardise vehicle secrecy [2]. Cisco Systems introduces fog computing (FC) as a revolutionary computing model that extends the life of cloud computing (CC) by doing the majority of time-sensitive data computation and analysis at the network edge [3].

FC is a virtualized architecture that provides end users with computation, storage, and internet services. Fog nodes are put between the end user and the cloud in FC [4,5], as illustrated in Fig. 1. FC is used in lieu of fog nodes when Road Side Units (RSU) are used to estimate road conditions. The gathered data is analysed with RSU to determine the road condition. The fog nodes transmit data between vehicles for the purpose of sensing road conditions. As a result, FC is acknowledged in this study as a consistent storage medium for the vehicle platform's local data. Because the information and event message are the foundations of the vehicular platform, the accuracy and integrity of data, as well as the negative impact of inaccurate information on network efficiency and reliability between vehicles, are difficult difficulties to solve. It is self-evident that the presence of assaults as security threats [6] reduces data accuracy, resulting in decreased network performance. Numerous security threats and vulnerabilities have been identified through physical attacks on network devices and data transmission attacks, including message tampering, message forgery, wormhole attacks, privacy invasion, and reply attacks. Issues such as construction and truck movement on the road could be seen as hazards that could jeopardise the availability, integrity, and dependability of localization services [7]. This object could create a non-line of sight (NLOS) situation, obstructing the driver's visual and data transmission line of sight (LOS). Several resolutions have been proposed in recent years to address the current security issue in vehicle networks, [8]. However, VANET's mobility of network cars is significantly greater, and the number of network entities that comprise malfunctioning nodes, massive impediments, and hostile attackers creates even greater security concerns. Additionally, due to the characteristics of VANET, the network data for each node's specified vehicular platform is imprecise, erroneous, and incomplete. Quality of Service (QoS) is critical for data transfer to be effective. As a result, intelligent clustering algorithms may play a critical role in developing manageable, highly optimised, and scalable vehicular networks capable of distributing network load equally. Clustering in a network refers to the process of joining nodes based on their degree of unlikeness and similarity in order to accomplish specific goals inside the network. Clustering is another acceptable technique that is distinguished from others by a number of regulations and guidelines. A cluster is a collection of nodes. Within the group (cluster), the majority of cluster members or cluster nodes are designated as Cluster Heads (CH). Clustering also fits under all of the NP-hard issue categories and is amenable to solution by metaheuristic optimization techniques.

This paper presents a privacy preserving reliable data transmission using Fog Computing (PPRDA-FC) in cluster based VANET. The proposed PPRDA-FC technique involves moth flame optimization with levy flight based clustering (MFO-LFC) process to select an appropriate set of CHs and construct clusters. The CHs have the accountability to monitor every individual vehicle in their own clusters. In addition, the CHs offer optimal and secure routes to transmit messages. Lastly, deep neural network (DNN) is employed as a classification technique to differentiate among the attacker and real vehicles. The experimental results of the proposed PPRDA-FC technique are validated under different aspects.

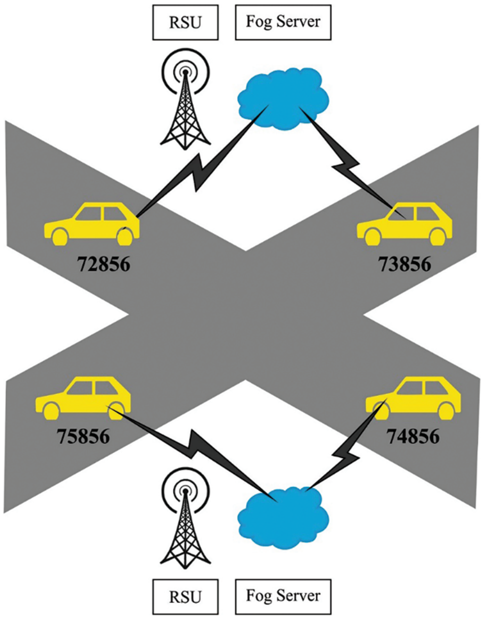

Figure 1: Architecture of fog computing

2 Literature Review

Al-Otaibi et al. [9] proposed new privacy preserving vehicular rogue node detection system by FC. By restricting the exchange of traffic data between vehicles and allowing data transmission solely via RSU, the given system improves computation efficiency, vehicle privacy, and data transmission among vehicles. This system offered an RSU authentication mechanism that would enable the RSU to identify and delete vehicles that produce erroneous traffic data, hence increasing the efficiency and accuracy of VANET. In Erskine et al. [10], FC combines with hybrid optimization method (OA) includes key distribution establishment (KDE), Cuckoo search algorithm (CSA), firefly algorithm (FA), and firefly neural network (NN) to authenticate node and network levels towards entire attacks for reliability in VANET. An FFBPNN named the firefly neural, is utilized as classification for distinguishing among genuine and attacking vehicles. In Soleymani et al. [11], a fuzzy trust module is depending upon plausibility, and experience is presented for securing vehicular networks. This technique employs a series of security checks to ensure the data obtained from licenced vehicles is accurate. Additionally, fog nodes are acknowledged as a means of determining the degree of accuracy with which event locations can be estimated.. Joshi et al. [12] proposed an effective privacy preserved data communication framework that utilizes block chain method in cluster based VANET. This framework is used to achieve location-based services (LBS) and reduce network overhead, while the rainfall optimization method does the clustering procedure (ROA). The ROA-based clustering with block chain-based data transmission approach, dubbed ROA-based clustering with block chain-based data transmission (ROAC-B), clusters the cars first and then transmits data via block chain. Fahad et al. [13] offer a greedy wolf algorithm (GWO)-based VANET clustering strategy that mimics the social behaviour and hunting method of grey wolves in order to construct an effective cluster. Grey wolf nature’s linear reduction factor is applied to earlier convergent states, resulting in an increased number of clusters. Ramalingam et al. [14] introduced dynamic grouping using K-implies, which are well suited for VANETs with changing topology quality. The presented method performs admirably when dealing with a large number of bunches ahead of time and an ambiguous number of groups. The user has the ability to determine the amount of bunches or base groups required using this method. Gupta et al. [15] propose a multi-layer cluster-based key generation technique for securing data transmission within a services-oriented, exceptionally dense VANET. The generated key is used as a secure key for different data transports and authentication. The researchers partitioned the entire VANET into clusters. The character conversion technique would be unique for each cluster. Each cluster would have its own RSU that would distribute the key generated by the database and key generation model in use. The scientists in this investigation successfully balanced the demand on multiple RSUs and authentication centres. Similarly, we present a lightweight and quick approach for key generation that is accurate for the constrained devices in VANET. Hameed et al. [16] suggested a method for dynamic clustering that took into account the direction, position, and speed of vehicles in order to establish a cluster that acts as a pool of computer resources. Additionally, this study proposed a technique for determining a vehicle's departure time from a cluster, which enables forecasting the vehicle's forthcoming position using the dynamic network. Awan et al. [17] describe a trust-based clustering technique that enables clusters to identify a trustworthy CH. The new features included in the presented technique include a trust-based CH selection algorithm that takes into account a node's expertise, knowledge, and reputation. Similarly, a backup head is defined by assessing the trust in the cluster's nodes. The primary benefit of trust in clustering is that it enables the discovery of compromised and malicious nodes.

3 The Proposed PPRDA-FC Technique

The system architecture of the proposed PPRDA-FC technique is given here. Here, the vehicles in the VANET undergo random deployment and initialization process. Then, the MFO-LFC technique is executed to determine the set of CHs using different input parameters. Followed by, FC technique is employed to accomplish secure data transmission by determining the frequently saved vehicular data model depending upon the transmission performance of vehicles. Next, the DNN model is applied to distinguish the vehicle as reliable or not. Finally, the CHs transmit data to the designated vehicles via reliable vehicles that exist in the VANET.

3.1 Design of MFO-LFC Technique

Moths utilize distinct navigational techniques for lateral orientation in night flight. During this technique, the moth flies by preserving a fixed angle of their light comparative to moon. By altering their location vector, moths could fly in 1, 2, 3, and even high dimensions. As the MFO technique is basically a swarm intelligence optimization method, the moth population is given by:

$$M = \begin{bmatrix} m_{1,1} & \cdots & m_{1,d} \\ \vdots & \ddots & \vdots \\ m_{n\prime 1} & \cdots & m_{n\prime d} \end{bmatrix} \tag{1}$$

Whereas n denotes the number of moths and d indicates amount of control parameter to be resolved (dimensional of an optimized problem). For this moth, it can be considered as there is an equivalent record of fitness value vector, denoted by:

$$OM = \begin{bmatrix} OM_1 \\ OM_2 \\ \vdots \\ OM_n \end{bmatrix} \tag{2}$$

In MFO method, every moth should upgrade its individual location only with single flame equivalent to it, for preventing the method falls to the local optimum value that highly improves the global search capability. Thus, the location of the flames and moths in the search space are parameter matrices of a similar dimension. Fig. 2 illustrates the flowchart of MFO technique.

$$F = \begin{bmatrix} f_{1,1} & \cdots & f_{1,d} \\ \vdots & \ddots & \vdots \\ f_{n,1} & \cdots & f_{n,d} \end{bmatrix} \tag{3}$$

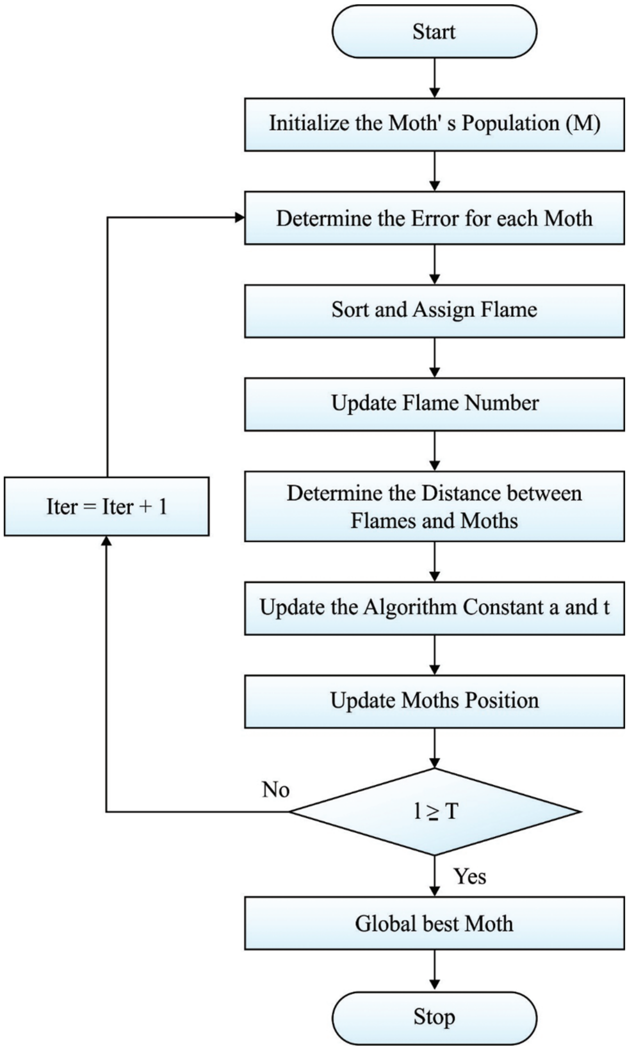
Start
Initialize the Moth' s Population (M)
Determine the Error for each Moth
Sort and Assign Flame
Update Flame Number
Determine the Distance between Flames and Moths
Update the Algorithm Constant a and t
Update Moths Position
l ≥ T
No
Yes
Iter = Iter + 1
Global best Moth
Stop

Figure 2: Flowchart of MFO

In order to these flames, it can be considered as there occurs an equivalent column of fitness value vector is denoted by:

$$OF = \begin{bmatrix} OF_1 \\ OF_2 \\ \vdots \\ OF_n \end{bmatrix} \tag{4}$$

In this iteration procedure, the upgrade approach of the parameter in the 2 matrices is distinct. Moths are generally searching individual that moves with the search space, and the flame is the optimum location that the iteratively enhanced moths could attain up to now. By this technique, it can detect global optimum solutions [18]. To perform numerical modeling for the flight performance of moth to flame, the upgrading technique to place of all the moth's comparative to a flame is stated as follows:

$$M_i = S(M_{i'}F_j) \tag{5}$$

whereas *Mi* denotes ith moth, *Fj* indicates *j*th flame and *S* denotes the helical function. The helical function of moth flight path is given by:

$$S(M_j,\ F_j) = D_j \cdot e^{bt} \cdot cos(2\Pi t) + F_j \tag{6}$$

$$t = \ \ (a-1) * \ \gamma and + 1 \tag{7}$$

$$a = -1 + Iteration * \left(- \frac{1}{T_{\max}} \right) \tag{8}$$

whereas *Dj* denotes linear distance among the i^{th} moth and j^{th} flame, *b* indicates logarithmic helix shape constants determined, and path coefficient *t* denotes arbitrary amount in $[-1,\ 1]$. The magnitude of *t* is denoted in Eq. (7), where a is denoted in Eq. (8), and magnitude reduces linearly from -1 to -2. The formation of Dj is given by:

$$D_j = |F_j - M_j| \tag{9}$$

Eq. (9) pretends the path of moth's spiral flight. To this formula, it is viewed that the following place of moth's regeneration is defined using flame it surroundings from modern time.

To enhance the global exploration capability of the original moth flame optimization technique, including the LF technique to the global exploration flight path of moth could efficiently develop the search space of moth and enhance global search capability of the moth. An arbitrary walk is a scientific module which contains a sequence of trajectories, every arbitrary is utilized for representing irregular pattern of modification. LF is a usual arbitrary walk technique that denotes a class of non-Gaussian stochastic processes and is interrelated to the Lévy stable distribution. LF is considered by several smaller steps however sometimes larger steps, thus movable entity don't frequently search the similar place, altering the system behavior. The integration of the MFO technique and LF approach could extend the search range of the method, increases the variety of population, and facilitate the technique for jumping out of the local optimal. In global upgrade of the moth technique, the LF method is included for expanding the search possibility of the method, makes it complex for falling to local optimization. The enhanced Eq. (10) is:

$$S(M_j,\ F_j) = D_j \cdot e^{bt} \cdot \ \ \cos(2\Pi t) + L(d) \cdot F_j \tag{10}$$

Now, *t* represents present iteration amount, M_j denotes ith moth, F_j indicates jth flame, and D_j denotes distance among the i^{th} moth and j^{th} flame. If the moth spiral flight upgrades its location, the count of LF technique could develop the search range of moth and avoid it from falls to local optimization. The Eq. of LF is given by:

$$Levy(x) = 0.01 \frac{r_1 \delta}{|r_2|^{\frac{1}{\phi}}} \tag{11}$$

where r_1 and r_2 indicates arbitrary amounts amongst zero and one, mϕ denotes constant 1.5, and δ Eq. (12) given by:

$$\delta = \left(\frac{\tau(1+\phi)\ \sin\left(\frac{n\phi}{2}\right)}{\tau\left(\frac{1+\phi}{2}\right)\phi 2^{\left(\frac{\phi-1}{2}\right)}} \right)^{\frac{1}{\phi}} \tag{12}$$

whereas $\tau(x+1) = x!$;200 step sizes were drawn for forming a succeeding fifty steps of LF.

The proposed MBO-LFC technique derives a weighted function using different parameters to elect CHs, as given in Eq. (13)

$$W_j = \alpha.NN_j + \beta.R + \delta.\theta + \gamma.S - \eta.DT_j \tag{13}$$

NV_j denotes the number of neighboring vehicles, R indicates the communication range, θ represents direction, S is speed and DT_j is the trust degree of the vehicle v and is determined using the vehicle v. α, β, δ, γ and η are weighted constant values in the interval of [0,1] The vehicles with lower weights in the neighboring list can be chosen as CHs. It is considered that the CHs are the highly trustable and effective vehicles in the VANET. When many vehicles hold identical weighted values, the vehicle which has lower distance from its neighbors can be chosen as CH, and therefore, the cluster lifetime can be raised [19].

The total trust computation makes use of trust degree (TD) among vehicles and TD among vehicles with RSU for evaluating the nature of the vehicle j. Every vehicle i derives a total trust value for every adjacent vehicle j in its transmission radius with or without RSU. The total trust computation can be defined as $T(i, j)$. The vehicles get the past trust values and in-segment trust value of every vehicle in the identical part in a periodical way enabling the vehicles to get clear view about their direct and indirect neighborhood for the prevention of intrusions or abnormalities. The trust update procedure takes place if the vehicles in the RSU range are determined by Eq. (14):

$$T(i,\ j) = \alpha[AVG[T^d_{new}(i,\ j),\ \ SRSU\ (j)]] + \beta[AVG[T^r(i,\ j),\ HRSU(j)]] \tag{14}$$

If the vehicles exist exterior to the transmission radius of the RSU, they can compute one another depending upon the direct as well as indirect TD and past report of the RSU. Therefore, the TD of the vehicle j can be determined using Eq. (15):

$$T(i,\ j) = \left(1 - \frac{t_1}{t_2}\right)[\alpha.T^d_{new}(i,\ j) + \beta.T^r(i,\ j)] + \left(\frac{t_1}{t_2}\right)[HRSU\ \ (j)\ \ ] \tag{15}$$

t_1/t_2 denotes importance factor, t_1 represents the report reception time and t_2 indicates the present current time. Besides, α and β are weighting factors, $\alpha + \beta = 1$ and $\alpha > \beta$. The estimation of TD is an important factor used to choose the CH. In case of every vehicle, a total TD can be determined depending upon the trust degree of the available vehicles in the neighborhood list allocated to it:

$$DT_j = \frac{\sum_{i \in NL_j} T(i,\ j)}{NV_j} \tag{16}$$

NL_j is the neighboring list of the vehicle j and W_j is node degree of the vehicle j.

3.2 Fog Computing Based Secure Framework

In the proposed model, the 2 DSRC technology instances are utilized to transmit data. Firstly, data transmission between the vehicles (V2V data transmission). Secondly, the fog server (FS) creates a link to the RSU and distributes inter-vehicle details to every vehicle in the VANET. The details include congestion, intrusions, vehicle condition, road condition, etc. This model uses additional preventive actions for the detection and mitigation of every kind of attack like a denial-of-service (DoS) attack. The VANET structure with integrated fog server (VSIF) model comprises the RSU link. The FS gathers intruders or collided vehicles or other abnormal attack details, which attain data related to every kind of DoS and server name indication (SNI) attacks. The VSIF model uses inter-vehicle communication links depending upon the following.

RSU: The RSU represents the gateway, which is placed to establish connection to the FS. It includes a set of networking devices and it uses dedicated short-range communication (DSRC) DSRC inter-vehicle data transmission depending upon Institute of Electrical and Electronics Engineers (IEEE) 802.11.

RSU to FS: VANET uses $V2V$ and $V2RSU$ data transmission for the propagation of safety or non-safety details. The RSU transmits data with one another and it acts as the backbone of the FS.

FS-to-FS: They are detected at distinct places. They get interacted with one another. As a result, the set of VANET resources which are identified can be effectively handled. Besides, the cloud is logically linked to the FS and has the nature of data aggregation.

FS to Cloud: The FS makes use of FC for addressing location awareness related to cloud. Therefore, cloud denotes a major portal of data that unnecessitated location awareness to process data. The cloud handles the FS in different places. The FS has the ability of aggregating data that comes from other FS.

Owing to the open chartists of VANET and its related vulnerable issues, the RSU and FS make use of authentication schemes to ensure real time packet delivery. The proposed model involves authentication in two stages namely fog level (FL) and RSU level (RSU-L). The RSU-L considers the vehicle's displacement and jitter from VANET, while the FL employs the Lagrange Polynomial for detection of untrustworthy nodes [20].

The FL maintains a global key for the whole network; therefore, every individual vehicle can be recognized by global key itself. The distribution of global keys to the vehicles is not secure and thus a shared system is followed in which every vehicle owns a shared value. If a vehicle requests data from the server straightaway or via RSU, the FS requests 3 shares from any vehicles in the network or selects two vehicles arbitrary [21]. A set of 3 total shares are treated encompassing the demanding vehicle. The FS makes use of the Lagrange polynomial for computing the following. The Lagrange polynomial $S(X)$ comprising the degree $\leq (n-1)$ necessitates n vehicles with coordinate points $(x_1, y_1 = f(x_1))$, $(x_2, y_2 = f(x_2))$, $\ldots(x_n, y_n = f(x_n))$ as represented below:

$$S(X) = \sum_{k=0}^{n} P_k(X) \tag{17}$$

where P_k can be defined as

$$P_k(X) = y_k \frac{x - X_1}{X_{j-\times 1}} \quad where \;\; 1 \geq 1, \; 1 \leq n \;\; and \;\; 1! = k \tag{18}$$

For $n = 3$ vehicles,

$$S(X) = \frac{(\times - X_2)(\times - X_{3)}}{(X_{1-x_2})(x1 - x)} y_1 + \frac{(\times - X_1)(\times - X_3)}{(X_{2-x_1})(X_2 - x_3)} y_2 + \frac{(\times - X_1)(\times - X_{2)}}{(x - x)(x - x)} y_3 \tag{19}$$

$$S(X_1) = \frac{x_2 \, * \, \mathrm{x}_3}{(x - x2)(x - x3)} y_1 \;\; for \;\; 1st \;\; vehicle \tag{20}$$

$$S(X_2) = \frac{x_1 \, * \, \mathrm{x}_3}{(x - x_1)(x - x_3)} y_2 \;\; for \;\; 2nd \;\; vehicle \tag{21}$$

$$S(X_3) = \frac{x_1 * x_2}{(\times - x_2)(\times - X_{3)}} y_3 \ \ for \ \ 3rd \ \ vehicle \tag{22}$$

The key produced through the combination of separate polynomials can be defined by

$$G_k = \sum_{k=0}^{n} S(k) \tag{23}$$

When G_k matches the network key, then the vehicle can send data to the FS. Secondly, RSU-level security can also be employed to make the network highly secure.

3.3 DNN Based Reliable Vehicle Detection

At the final stage, the DNN based classification process gets executed to determine the vehicle as genuine or attacker. The DNN model is appropriate for learning discriminate and active variables. A large number of unlabeled data of DNN has been employed [22]. The effort to categorize the information is considered to be significant problem since it generates issues in pattern learning. For managing these difficulties, via sparse auto-encoders (AE) an improved DNN is projected. Fig. 3 demonstrates the structure of DNN model.

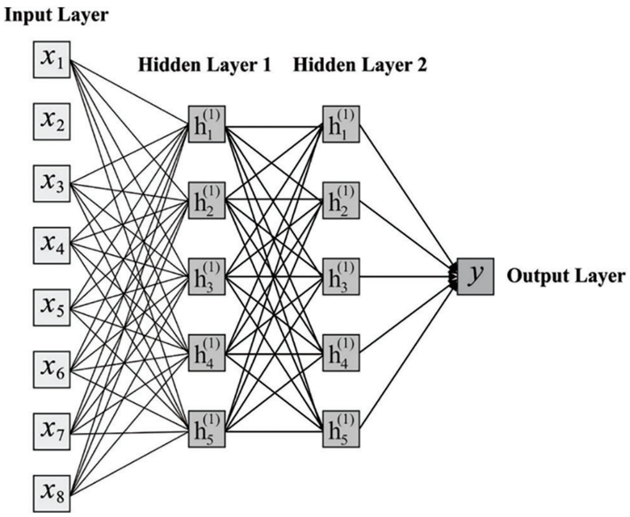

Figure 3: Structure of DNN

To learn the feature module depending upon existing method, an AE is adaptive that are combined with denoising method. In addition to the NN classifier, this learned feature is assumed as input. The entire procedure of existing module is defined in output. In earlier stage of DNN training, it considered the average activation function value nearer to zero due to neuron redundancy [23,24]. It performs penalty for maximal activation function. It is executed by various forms of significant average activation function value. The representation of penalty is given by Eq. (24).

$$P_{penalty} = \sum_{n=1}^{s_2} \rho // \rho_n \tag{24}$$

where, s_2 indicates the whole amount of secret layer neurons, KL (.) indicates Kullback Leibler divergence (KL divergence) and is given by:

$$KL(\rho//\rho_n) = \rho_{\log} \frac{\rho}{\rho_n} + (1-\rho)\ \ \log\ \ \frac{1-\rho}{1-\rho_n} \tag{25}$$

$KL(\rho//\rho_n) = 0$ for $\rho_n = p$ denotes improved divergence, usually considered by adaptive constant. It is accomplished by performing the cost function as,

$$C_{adaptive}(w,\ b) = C(w,\ b) + \beta \sum_{n=1}^{s2} KL(\rho//\rho_n) \tag{26}$$

β denotes penalty weight performed with KL divergence method.

4 Performance Validation

The performance validation of the proposed model takes place using different aspects. Fig. 4 illustrates the performance of the proposed PPRDA-FC technique in terms of number of clusters (NOC) under varying number of vehicles in VANET. From the figure, it is shown that the proposed PPRDA-FC technique accomplishes better performance with a lower NOC under all vehicle count. Besides, it is noted that the NOC gets decreased with a reduction in transmission distance indicating fewer number of clusters with maximum transmission distance. It is also noted that the comprehensive learning particle swarm optimization (CLPSO) algorithm exhibited ineffective outcomes with the maximum NOC [25,26]. Though the multiple objective particle swarm optimization (MOPSO), grey wolf optimization based clustering in vehicular ad-hoc networks (GWOCNET), and ROAC-B techniques have offered moderate NOC, they have failed to outperform the proposed PPRDA-FC technique.

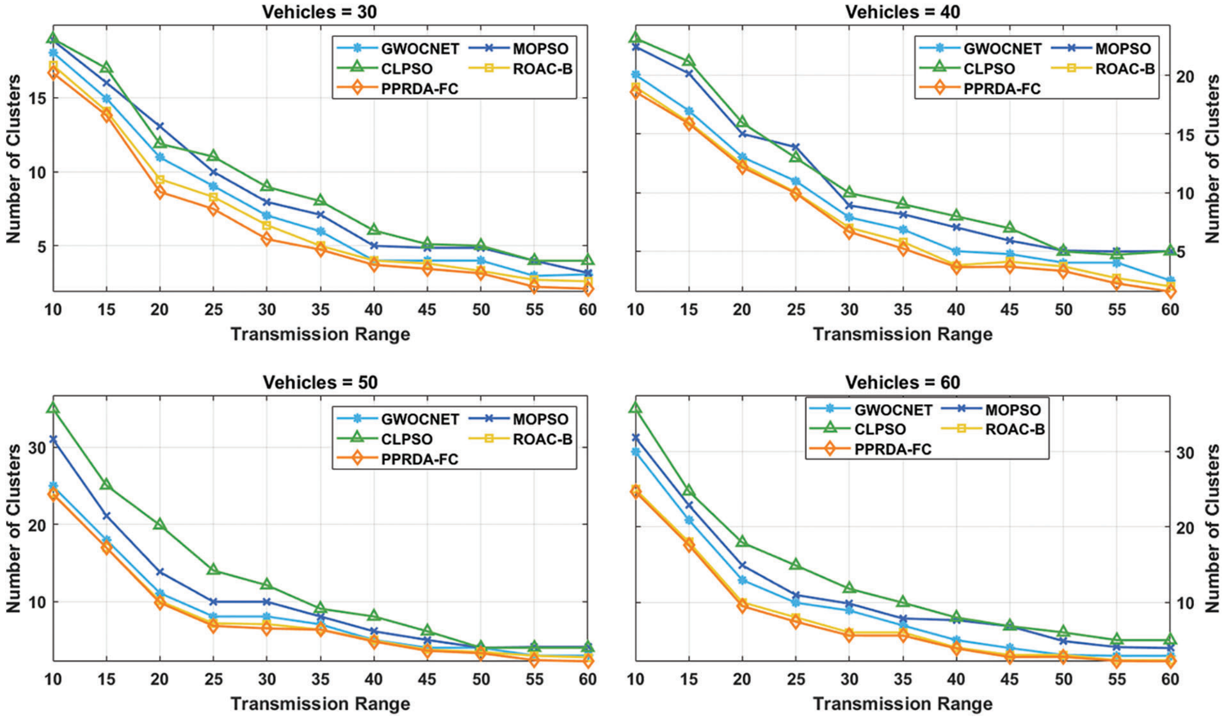

Figure 4: Number of clusters analysis of PPRDA-FC model

A brief end to end (ETE) delay analysis of the PPRDA-FC technique with other methods takes place in Fig. 5. The figure portrayed that the proposed PPRDA-FC technique shows its supremacy by accomplishing the least ETE delay under distinct number of vehicles. At the same time, the hybrid method for a privacy-preserving authentication approach (HEPPA) and lightweight authentication and key agreement protocol (LAKAP) techniques have showcased poor outcomes with the maximum ETE delay [27]. Concurrently, the authentication scheme smart card (ASC) and ROAC-B techniques have demonstrated moderately closer ETE delay, the PPRDA-FC technique has gained better performance with the minimal ETE delay.

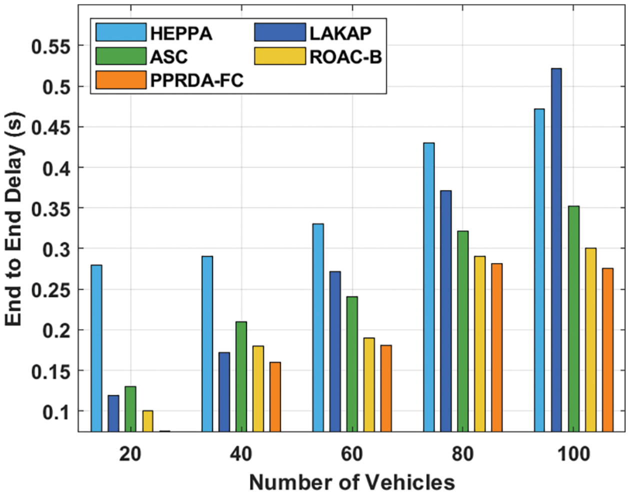

Figure 5: ETE delay analysis of PPRDA-FC model

A brief preliminary design review (PDR) analysis of the PPRDA-FC model with other methods takes place in Fig. 6. The figure depicted that the presented PPRDA-FC method illustrates their supremacy by accomplishing a maximum PDR under different numbers of vehicles. Likewise, the ASC and LAKAP approaches have illustrated worst result with the lowest PDR. Simultaneously, the HEEPA and ROAC-B techniques have demonstrated moderately closer PDR, the PPRDA-FC technique has gained better performance with the higher PDR. An analysis of throughput offered by the PPRDA-FC technique under different passive infrared sensor (PIR) is made in Tab. 1 and Fig. 7. The results depicted that the proposed PPRDA-FC technique has outperformed all the other methods by offering a higher throughput under all PIR levels. For instance, with the PIR of 0.001, the PPRDA-FC technique has obtained a higher throughput of 1744.47 whereas the Cuckoo, Firefly, Firefly Neural, and Secure Intelligent Vehicular Network Using Fog Computing (SIVNFC) techniques have achieved a lower throughput of 1304.90, 1413.68, 1359.29, and 1631.25 respectively. Followed by, with the PIR of 0.006, the PPRDA-FC algorithm has attained a superior throughput of 2847.48 whereas the Cuckoo, Firefly, Firefly Neural, and SIVNFC methodologies have obtained a lower throughput of 2338.34, 2501.52, 2719.08, and 2719.08 respectively. Moreover, with the PIR of 0.010, the PPRDA-FC technique has obtained a higher throughput of 3784.54 whereas the Cuckoo, Firefly, Firefly Neural, and SIVNFC techniques have achieved a lower throughput of 3371.78, 3371.78, 3589.35, and 3698.13 respectively. Furthermore, with the PIR of 0.014, the PPRDA-FC technique has obtained a higher throughput of 4763.87 whereas the Cuckoo, Firefly, Firefly Neural, and SIVNFC approaches have achieved a lower throughput of 3752.52, 3915.70, 4078.87, and 4514.01 respectively. At last, with the PIR of 0.020, the PPRDA-FC technique has obtained a maximum throughput of 8355.89 whereas the Cuckoo, Firefly, Firefly Neural, and SIVNFC methods have attained a minimum throughput of 7559.93, 7451.15, 7940.68, and 8158.24 correspondingly.

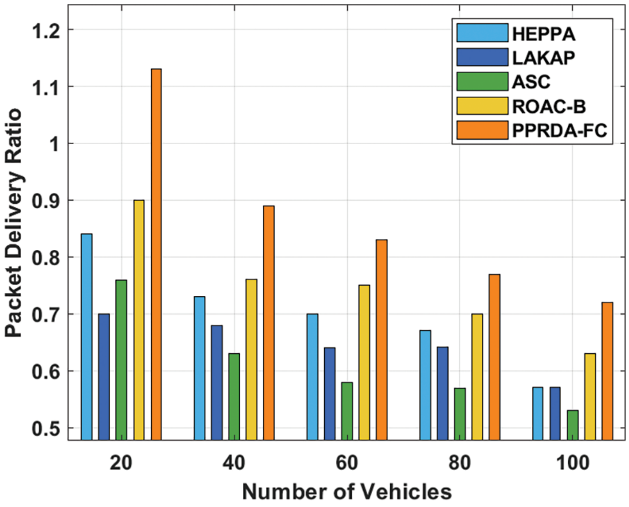

Figure 6: PDR analysis of PPRDA-FC model

Table 1: Result analysis of existing with proposed method in terms of throughput *vs.* packet injection rate (PIR)

	Throughput				
PIR	Cuckoo	Firefly	Firefly neural	SIVNFC	PPRDA-FC
0.001	1304.90	1413.68	1359.29	1631.25	1744.47
0.002	1196.12	1359.29	1576.86	1576.86	1632.92
0.006	2338.34	2501.52	2719.08	2719.08	2847.48
0.008	3263.00	3480.56	3698.13	4078.87	4163.91
0.010	3371.78	3371.78	3589.35	3698.13	3784.54
0.012	3534.96	4024.48	4078.87	4296.44	4361.49
0.014	3752.52	3915.70	4078.87	4514.01	4763.87
0.018	5329.88	5329.88	5928.19	6363.32	6538.90
0.020	7559.93	7451.15	7940.68	8158.24	8355.89

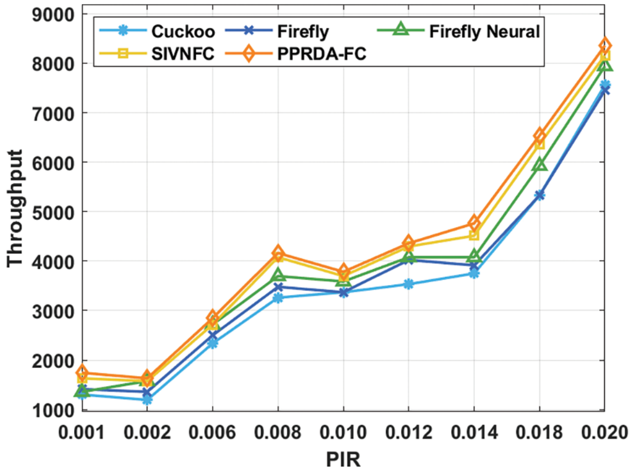

Figure 7: Throughput analysis of PPRDA-FC model

Tab. 2 and Fig. 8 perform a comparative study of the PPRDA-FC technique with other techniques in terms of jitter under distinct levels of PIR. From the resultant values, it is assumed that the PPRDA-FC technique has gained improved outcomes with minimal jitter values. For instance, with the PIR of 0.001, the least jitter of 70.470 has been offered by the PPRDA-FC technique whereas the Cuckoo, Firefly, Firefly Neural, and SIVNFC techniques have reached a maximum jitter of 72.105, 69.782, 79.073, and 88.364 correspondingly. Besides, with the PIR of 0.006, the least jitter of 75.570 has been offered by the PPRDA-FC technique whereas the Cuckoo, Firefly, Firefly Neural, and SIVNFC techniques have reached a maximal jitter of 79.073, 99.977, 102.300, and 111.591 respectively. In addition, with the PIR of 0.010, the least jitter of 84.380 has been offered by the PPRDA-FC technique whereas the Cuckoo, Firefly, Firefly Neural, and SIVNFC techniques have reached a maximal jitter of 86.041, 90.686, 109.268, and 132.495 correspondingly. Simultaneously, with the PIR of 0.014, the least jitter of 93.890 has been offered by the PPRDA-FC technique whereas the Cuckoo, Firefly, Firefly Neural, and SIVNFC approaches have reached a maximum jitter of 95.332, 102.300, 109.268, and 123.204 correspondingly. Finally, with the PIR of 0.020, a minimum jitter of 82.570 has been offered by the PPRDA-FC technique whereas the Cuckoo, Firefly, Firefly Neural, and SIVNFC methods have reached a superior jitter of 86.041, 97.654, 109.268, and 118.559 correspondingly.

Table 2: Result analysis of existing with proposed method in terms of jitter *vs.* packet injection rate

	JITTER (ms)				
PIR	SIVNFC	Firefly neural	Cuckoo	Firefly	PPRDA-FC
0.001	72.105	69.782	79.073	88.364	70.470
0.002	67.459	76.750	79.073	95.332	65.430
0.006	79.073	99.977	102.300	111.591	75.570
0.008	83.718	93.009	111.591	127.849	81.460
0.010	86.041	90.686	109.268	132.495	84.380
0.012	86.041	95.332	102.300	111.591	83.580
0.014	95.332	102.300	109.268	123.204	93.890
0.018	88.364	90.686	95.332	106.945	86.500
0.020	86.041	97.654	109.268	118.559	82.570

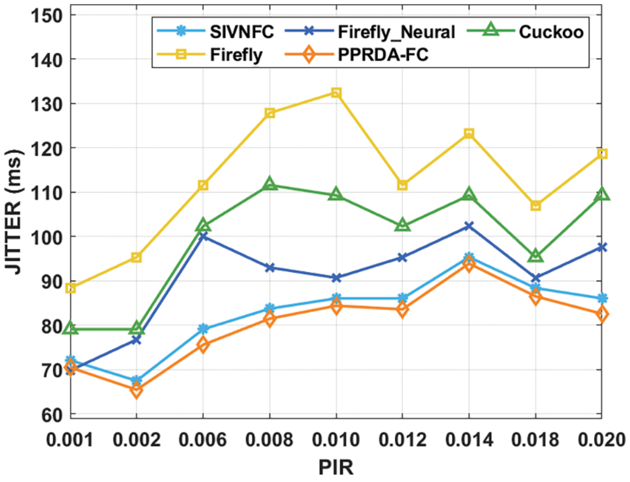

Figure 8: JITTER analysis of PPRDA-FC model

From the above mentioned tables and figures, it is ensured that the proposed PPRDA-FC technique has demonstrated superior performance over the other existing methods. It can also be employed as an effective tool for achieving reliable data transmission using FC in VANET.

5 Conclusion

The purpose of this article was to offer an effective PPRDA-FC technique for achieving reliable data transfer in a VANET using FC. The PPRDA-FC technique suggested here seeks to ensure reliable message delivery by utilising FC and an optimal selection of CH. After deploying and initializing the cars in VANET, the MFO-LFC approach is used to find the set of CHs using various input parameters. Additionally, the FC technique is used to ensure secure data transmission by detecting the most commonly saved vehicular information procedure based on the vehicle's communication behaviour. Additionally, the DNN model is used to determine whether a vehicle is reliable or not. Finally, the CHs communicate data to the chosen cars via the VANET's dependable vehicles. The suggested PPRDA-FC technique's experimental results are validated in a variety of ways. The resulting results revealed that the suggested model outperformed recent state-of-the-art approaches. In the future, the suggested PPRDA-FC model can be expanded to the development of low-weight cryptographic algorithms for enhancing VANET security.

Acknowledgement: The authors would like to thank Vel Tech Multi Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Chennai Institute of Technology and Guru Nanak Institute of Technology for providing us with various resources and unconditional support for carrying out this study

Funding Statement: This research has been funded by Dirección General de Investigaciones of Universidad Santiago de Cali under call No. 01-2021.

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

References

[1] K. Zaidi, M. Milojevic, V. Rakocevic and M. Rajarajan, "Data-centric rogue node detection in VANETs," in *Proc. IEEE 13th Int. Conf. on Trust, Security and Privacy in Computing and Communications*, Beijing, China, IEEE, pp. 398–405, 2014.

[2] E. Zeinab, S. Karthikeyan, S. Daisy Flora, S. Jose Plathottam and R. Prakash, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, pp. 100214–100226, 2020.

[3] S. Khan, S. Parkinson and Y. Qin, "Fog computing security: A review of current applications and security solutions," *Journal of Cloud Computing*, vol. 6, no. 1, pp. 1–22, 2017.

[4] Y. W. Law, M. Palaniswami, G. Kounga and A. Lo, "WAKE: Key management scheme for wide-area measurement systems in smart grid," *IEEE Communications Magazine*, vol. 51, no. 1, pp. 34–41, 2013.

[5] F. Bonomi, R. Milito, J. Zhu and S. Addepalli, "Fog computing and its role in the internet of things," in *Proc. First Edition of the MCC Workshop on Mobile Cloud Computing*, Helsinki Finland, pp. 13–16, 2012.

[6] J. M. De Fuentes, A. I. González-Tablas and A. Ribagorda, "Overview of security issues in vehicular ad-hoc networks," in *Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts*, Hershey, Pennsylvania, USA: IGI global, pp. 894–911, 2011.

[7] T. Sudeep, V. Jayneel, T. Sudhanshu, K. Neeraj and S. O. Mohammad, "A systematic review on security issues in vehicular ad hoc network," *Security and Privacy*, vol. 1, no. 5, pp. 1–26, 2018.

[8] R. G. Engoulou, M. Bellaiche, S. Pierre and A. Quintero, "VANET security surveys," *Computer Communications*, vol. 44, pp. 1–13, 2014.

[9] B. Al-Otaibi, N. Al-Nabhan and Y. Tian, “Privacy-preserving vehicular rogue node detection scheme for FC,” *Sensors*, vol. 19, no. 4, pp. 965, 1–18, 2019.

[10] S. K. Erskine and K. M. Elleithy, “Secure intelligent vehicular network using FC,” *Electronics*, vol. 8, no. 4, pp. 455–472, 2019.

[11] S. A. Soleymani, A. H. Abdullah, M. Zareei, M. H. Anisi, C. Vargas-Rosales *et al.,* “A secure trust model based on fuzzy logic in vehicular ad hoc networks with FC,” *IEEE Access*, vol. 5, pp. 15619–15629, 2017.

[12] 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. 1358–1376, 2020.

[13] M. Fahad, F. Aadil, S. Khan, P. A. Shah, K. Muhammad *et al.,* “Grey wolf optimization based clustering algorithm for vehicular ad-hoc networks,” *Computers & Electrical Engineering*, vol. 70, pp. 853–870, 2018.

[14] M. Ramalingam and R. Thangarajan, “Mutated k-means algorithm for dynamic clustering to perform effective and intelligent broadcasting in medical surveillance using selective reliable broadcast protocol in VANET,” *Computer Data Transmissions*, vol. 150, pp. 563–568, 2020.

[15] D. N. Gupta and R. Kumar, “Distributed key generation for secure data transmissions between different actors in service oriented highly dense VANET,” *Cloud and IoT-Based Vehicular Ad Hoc Networks*, vol. 11, pp. 221–232, 2021.

[16] A. R. Hameed, S. ul Islam, I. Ahmad and K. Munir, “Energy-and performance-aware load-balancing in vehicular FC,” *Sustainable Computing: Informatics and Systems*, vol. 30, pp. 100454–100462, 2021.

[17] K. A. Awan, I. U. Din, A. Almogren, M. Guizani and S. Khan, “StabTrust—A stable and centralized trust-based clustering mechanism for IoT enabled vehicular ad-hoc networks,” *IEEE Access*, vol. 8, pp. 21159–21177, 2020.

[18] Y. Li, X. Zhu and J. Liu, “An improved moth-flame optimization algorithm for engineering problems,” *Symmetry*, vol. 12, no. 8, pp. 1234, 2020.

[19] F. Mirsadeghi, M. K. Rafsanjani and B. B. Gupta, “A trust infrastructure based authentication method for clustered vehicular ad hoc networks,” *Peer-to-Peer Networking and Applications*, vol. 14, pp. 1–17, 2020.

[20] J. Liu, J. Li, L. Zhang, F. Dai, Y. Zhang *et al.,* “Secure intelligent traffic light control using fog computing,” *Future Generation Computer Systems*, vol. 8, pp. 817–824, 2018.

[21] M. Sookhak, F. R. Yu and H. Tang, “Secure data sharing for vehicular ad-hoc networks using cloud computing,” in *Adhoc Networks*, Cham: Springer, pp. 306–315, 2017.

[22] R. Surendran, O. I. Khalaf and C. A. T. Romero, “Deep learning based intelligent industrial fault diagnosis model,” *Computers, Materials & Continua*, vol. 70, no. 3, pp. 6323–6338, 2022.

[23] R. Surendran, R. Karthika and B. Jayalakshmi, “Implementation of dynamic scanner to protect the documents from ransomware using machine learning algorithms,” in *2021 Int. Conf. on Computing, Electronics & Communications Engineering (iCCECE)*, Southend, United Kingdom, pp. 65–70, 2021.

[24] J. Goutham Kumar, S. Gowri, R. Surendran, J. S. Vimali, J. Jabez *et al.,* “Identification of cyber threats and parsing of data,” in *5th Int. Conf. on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India, pp. 556–564, 2021.

[25] S. Rajendran, O. I. Khalaf, Y. Alotaibi and S. Alghamdi, “Mapreduce-based big data classification model using feature subset selection and hyperparameter tuned deep belief network,” *Scientific Reports*, vol. 11, no. 24138, pp. 1–18, 2021.

[26] M. Rajalakshmi, V. Saravanan, V. Arunprasad, C. A. T. Romero, O. I. Khalaf *et al.,* “Machine learning for modeling and control of industrial clarifier process,” *Intelligent Automation & Soft Computing*, vol. 32, no. 1, pp. 339–359, 2022.

[27] R. V. Raghupathy, O. Ibrahim Khalaf, C. A. T. Romero, S. Sengan and D. K. Sharma, “Interactive middleware services for heterogeneous systems,” *Computer Systems Science & Engineering*, vol. 41, no. 3, pp. 1241–1253, 2022.