WEIGHTED COEFFICIENT FIREFLY OPTIMIZATION ALGORITHM AND SUPPORT VECTOR MACHINE FOR TRUST MODEL AND LINK RELIABILITY

Shalini Sharma and Syed Zeeshan Hussain

Department of Computer Science, Jamia Millia Islamia University New Delhi, India

ABSTRACT

Cloud computing is widely used by organizations and individuals due to its flexibility and reliability. The trust model is important for cloud computing to detect malicious users and protect user privacy. The existing research faces the issues of local optima trap and overfitting problems when a training user node is idle for more time. This research proposed Weighted Coefficient Firefly Optimization Algorithm (WC-FOA) with Support Vector Machine (SVM) for the trust model calculation and identifying paths with better Quality of Services (QoS). The weighted coefficient is added to the FOA model to balance the exploration and exploitation in the search of identifying optimal path based on reliability score. The WC-FOA method measures the link reliability in the model and SVM detects the malicious users in the model. The WC-FOA model selects the optimal path for transmission in terms of trust and efficient QoS parameters. The entropy measure and link reliability are provided as input to the SVM model for the detection of attacks in the network. The WCFOA-SVM model has 96% malicious user detection, whereas the Random Forest Hierarchical Ant Colony Optimization (RF-HEACO) has 92 % accuracy.

KEYWORDS

Cloud computing, Entropy Measure, Support Vector Machine, Trust model, Weighted Coefficient Firefly Optimization Algorithm.

1. INTRODUCTION

Trust Management is considered as a new technique to solve network security problems and become a hot research topic in recent years. The trust management techniques have characteristics of multi-dimensional evaluation, flexible application, and deployment, real-time resistance to internal attacks and dynamic [1]. Cloud'sheterogeneitybehaviour is used by malicious users to create trust problems and affect other devices' reliability and service. The trust model is widely required in network security to protect cloud smart services. The Trust management technique identifies untrusted behavior and separates untrusted objects. The existing techniques still have many limitations like continuously changing its trust behaviors and ineffectiveness against a large amount of data [2]. The huge quantity of connected users in the cloud increases the chance of malicious surface on the Internet. The focus of this paper is on the challenges and issues related to trust and security in the context of consumer cloud applications [3]. Traditional security techniques can defend against external threats and lower efficiency in identifying internal attacks due to the malicious inclusion of nodes into the network [4]. The perimeter-based security architecture is applied to solve this problem that divides networks into external networks and internal networks with an Intrusion Prevention System (IPS), Intrusion Detection System (IDS), and firewall as the border [5].

DOI: 10.5121/ijcnc.2022.14508

A huge amount of users in the cloud environment results in higher traffic and flow of data to be slow inside the cloud environment. The higher traffic creates a delay in the network and creates multiple hops for a data to be transferred from one user to another. If in case a malicious user is on the route of data transmission, there is a higher chance of rerouting the data in a misguided path or the loss of data can happen. To avoid these scenario, it is essential for a network to have a reliable path with neighbors for data transmission and effective identification malicious nodes in that path. Malicious node identification in modern network infrastructure are considered severe threats to network security. Traditional network security finds it difficult to distinguish between the malicious node and large legitimate users accessing a targeted network or a resource [6]. Few studies involve in collect and analyzingmalicious node characteristics for these attacks. This research mainly focuses on malicious node detection and to mitigate the attack, which is difficult for legitimate users' traffic patterns and various network services [7, 8]. Networks' crucial issues are reliable data exchange and energy consumption problems. Clouds are a vulnerable target for many security attacks due to the limited resources of sensor nodes. Trust based technique of energy awareness is a powerful tool for the classification of nodes' behavior and provides security solutions in cloud [9, 10].The objectives and contribution of this research are described as follows:

1. SVM is used to classify the malicious users based on the residual energy, bandwidth, entropy, Packet Loss Ratio (PLR) and End to End Delay (EED). After classifying the malicious users, the information about these malicious users are broadcasted to achieve the reliable transmission.
2. The conventional FOA is transformed into WC-FOA by adding the weighted coefficient that helps to enhance the exploration and exploitation capabilities during the secure route discovery. Therefore, the combination SVM based malicious node discovery and WC-FOA based secure routing are used to enhance the link reliability.

The paper is organized as follows: The trust model literature review is given in Section 2, and the WC-FOA-SVM model explanation is given in Section 3. The results of the WC-FOA-SVM model are given in Section 4, and the conclusion of the research paper is given in Section 5.

2. LITERATURE REVIEW

The trust model for the network is important to find the malicious nodes in the network and increases the privacy of the network. Some recent techniques in the trust model and link reliability technique were reviewed in this section.

Guesmi, et al. [11] applied a supervised detection technique for cloud environments using Fast Entropy based on unfair ratings and cloud users' feedback, named Feedback Fast Entropy-based Detection Strategy (FFED). The user's rating was monitored by the provided detection system and fast entropy algorithm was used to detect unfair rating attacks to permit the scale effectively. The unfair rating attacks are considered as events that cause changes in rating computation and help to identify different attacks. These attacks are mitigated and feedback was used to detect changes. The FFED method has lower adaptability and this model has lower efficiency in detecting new attacks.

AbdelAzim, et al. [12] developed a hybrid model that was a combination of entropy and KullbackLeibler (KL)-divergence to consider node trust in routing problems for detecting attacks. The hybrid method is developed to detect denial of service attacks and routing information was considered in the nodes for quick identification and exclusion from the nodes. The developed method allows nodes that have been suspected of participating in an attack if they cease their malicious behavior. The developed method can detect the second attack while another one is ongoing. The developed method of detecting denial of service attacks has higher performance than non-hybrid techniques. This binary class classification technique and lower efficiency in attack classification.

Wu, et al. [13] applied Trustworthiness Assessment with Entropy (TAE) for topological characteristics analysis in IoT networks. The TAE's trustworthiness of qualitative and quantitative were carried out using von Neumann entropy which used to increase the feasibility and robustness of the model. The multi-layer complex network was used to map the model in cloud-fog-edge computing.

Kou, et al. [14] proposed a Simhash-based link prediction technique to improve privacy-preserving. The target user indices were used to determine "probably similar" friends based on Simhash to develop less sensitive users. The developed method effectively protects users' information and trust-distrust values are calculated for each user related to the target user. The Social Balance technique was applied to develop a link of possibility between candidate and target user using trust-distrust values. The real-world Epinions dataset was applied to test the developed model's performance. The developed model has higher performance in terms of overcoming sparsity problems than the existing technique. The Simhash technique only considered user rating data and is highly based on similarity measures.

Sankaran, et al. [15] applied Energy Based Random Repeat Trust Computation (EB-RRTC) for trust nodes encounter with the destination node. The Reliable Fuzzy and Heuristic Concurrent Ant Colony Optimization (RF-HEACO) were applied to improve Quality of Service (QoS). The ACO model was applied to identify candidate deposit routes among a pair of source and destination. The Reliable fitness function, heuristic factors, and QoS metrics are considered for identifying the candidate routes. Each path is measured using the reliability technique and Fuzzy logic with packet loss rate, residual energy and metric link stability for high-reliability path selection. The RF-HEACO QoS routing protocol reduces energy consumption and increases the packet delivery ratio. The ACO model has limitations of local optima trap and overfitting problems in optimization.

Alshammariet al. [16] developed a Trust Model System (TMS) to ensure the security over the cloud storage system. In TMS, the value of interaction trust was computed for malicious attackers to improve the security. The developed TMS was provided the security against the reputation attacks. Further, the developed TMS was provided the enough security, even when the cloud services were processed in dynamic topology. This TMS was failed to consider the reliability of link while performing the data transmission.

Hassan et al. [17] presented the enhanced QoS-based model to estimate the authorization of the cloud provider. The Accumulative/Computed Trust Value (ATV)was computed for each cloud provider for evaluating their own authentication level. Here, the user feedback ratings according to the covariance mathematical approach was used to compute the cloud resource's trustworthiness. Next, the resource power was computed for calculating the trustworthiness of a cloud resource. The elimination of fake users was used to enhance the transaction success rate in cloud environment. If the number of connections were increased, it caused failure in certainjobs in cloud.

Qureshi et al. [18] developed the Software-Defined Network (SDN) based Anomaly Detection System (ADS) for edge computing-based systems in IoT networks. The behavior of device for SDN and edge computing networks were discovered by ADS. An edge device's trust for ensuring the data forwarding was accomplished by developing a trusted authority for edge computing approach. The data delivery of SDN-ADS was less, when the environment has more number of malicious switches.

The related work along with its advantages and limitations is provided in the Table 1.

Table 1. Related work

Author	Approach	Advantages	Limitations
Guesmiet al. [11]	Supervised detection technique and Feedback Fast Entropy-based Detection Strategy (FFED)	An effective detection of unfair rating attacks were done by monitoring the user's rating along with FFED.	The developed FEED has less adaptability while detecting the unknown attacks.
AbdelAzimet al. [12]	Hybrid entropy and KL-divergence model	The Hybrid entropy and KL-divergence method was detected the second attack while the first one is ongoing in network.	This Hybrid entropy and KL-divergence was offered only a binary classification.
Wuet al. [13]	TAE	The TAE method trustworthiness was performed using von Neumann entropy that used to enhance the feasibility.	The TAE was mapped using multi-layer complex network at cloud-fog-edge computing.
Kouet al. [14]	Simhash-based link prediction technique	The Simhash based discovery has enhanced performance in terms of overcoming sparsity issues than the existing method.	The Simhash technique was only considered rating data of user and it was highly depends on the similarity measures.
Sankaran, et al. [15]	EB-RRTC and RF-HEACO	The energy consumption was reduced and packet delivery ratio was increased by using RF-HEACO QoS routing protocol.	The ACO has limitations of local optima trap and overfitting issues in optimization.
Alshammari et al. [16]	TMS	The TMS was provided the enough security, even when the cloud services were processed in dynamic topology	This TMS was failed to consider the reliability of link while performing the data transmission.
Hassan et al. [17]	Enhanced QoS-based model	The elimination of fake users using ATV was used to enhance the transaction success rate.	If the number of connections were increased, it caused failure in certain jobs in cloud.
Qureshi et al. [18]	SDN-ADS	Edge device's trust for providing the data forwarding was accomplished by developing a trusted authority for edge computing approach.	The data delivery of SDN-ADS was less, when the environment has huge number of malicious switches.

The limitations found from the existing research are mentioned as follows: The cloud computing environment possess less adaptability to the unknown attacks from inside malicious users, restricted detection of behaviour between the malicious user and legitimate user is also a challenging issue on cloud and providing security functionalities in addition requires inadequate cost parameters and suffers from local optima trap, overfitting and less data delivery. Hence, an effective secure routing under malicious users is developed using SVM and WC-FOA for achieving the reliable data broadcasting in cloud environment.

3. PROPOSED METHOD

In this research, the SVM and WC-FOA are used for achieving secure reliable communication over the cloud environment. Specifically, the SVM is used to find the malicious attackers exist in cloud followed by the WC-FOA used to find the optimal path for transmission. The distinct cost metrics used in the WCFOA-SVM are residual energy, bandwidth and entropy. The developed WCFOA-SVM is used to overcome the issues of local optima trap and overfitting. The overview of the WCFOA-SVM model is given in Figure 1.

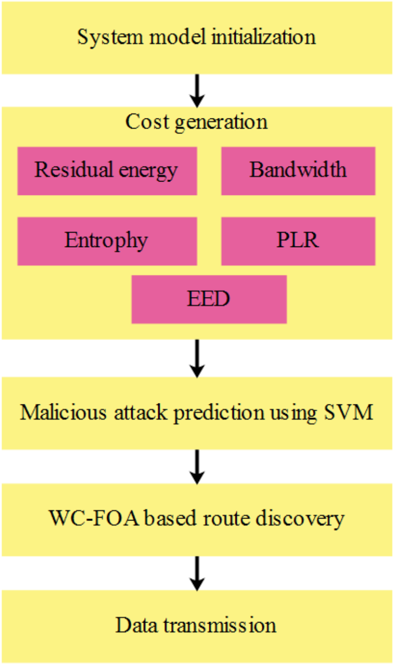
System model initialization
Cost generation
Residual energy
Bandwidth
Entrophy
PLR
EED
Malicious attack prediction using SVM
WC-FOA based route discovery
Data transmission

Figure 1. Block diagram of WCFOA-SVM method

The important process of the WCFOA-SVM method is mentioned as follows:

- The cloud environment is initialized with enough resources i.e., energy and bandwidth during system model initialization. Accordingly, the resources are allocated for each user of cloud.
- For detecting the malicious attackers exist in the cloud, the SVM is trained with unique cost metric. Here, the cost is generated based on residual energy, bandwidth, entropy, PLR and EED.
- Next, the WC-FOA is used to discover the route based on residual energy, bandwidth and entropy. After discovering the route, the data is transmitted from one user to another user in the cloud environment.

The detailed explanation about SVM based malicious user discovery and WC-FOA based route discovery are given as follows:

3.1. Malicious user discovery using SVM

The trustworthy neighboruser discovery is supported among end to end user by using the SVM. After identifying the malicious user, the local routing table of each user is updated in each simulation time. The cost generation and SVM classification is detailed below:

3.1.1. Cost generation

The cost metric used to discover the malicious attacks are residual energy $\left(RE\right)$, bandwidth $\left(BW\right)$, entropy, PLR and EED. The cost metric used during the attack userdiscovery is expressed in equation (1).

$$Cost = RE + BW + Fast\,entropy + PLR + EED \tag{1}$$

The user exist in the cloud environment requires enough energy to transmit the information. Therefore, the user with huge amount of residual energy is preferred in cloud environment. Equation (2) shows the computation of residual energy.The available bandwidth information of the user expressed in equation (3) is used to plan their own or distributed nodes. This used to take the decision about the destination user and data speed. Feedback count is used in supervising the evolution of existing practices used in this step. A threshold k of trust manager is set for the sum of existing feedback counts related to Cloud Service Provider (CSP). During a fixed time period t if this sum is higher than threshold k, the attack detection algorithm is executed by the system based on fast entropy which is expressed in equation (4). The PLR expressed in equation (5) is used to define the loss ratio where the malicious users creates the huge amount of loss during the data transmission. Hence, this used to identify the malicious users in the cloud. Further, the EED shows the amount of time taken to transmit the data to the desired user.

$$RE = Available\,energy - Consumed\,energy \tag{2}$$

$$BW = \left(t_{idle} / t\right) \times Channel\,capacity \tag{3}$$

$$Fast\,entropy = \begin{cases} 1 & if \sum_{i=1}^{n} counter(i) > \lambda \\ 0 & f \sum_{i=1}^{n} counter(i) \le \lambda \end{cases} \tag{4}$$

$$PLR = \frac{Number\,of\,\,lost\,\,packets}{Total\,number\,of\,\,transmitted\,\,packets} \tag{5}$$

Where, t_{idle} is idle time period; t is overall time period; For a fixed time period t, the number of connections (n) attained by CSP is taken as feedbacks count i that is $counter(i)$.The derived cost function is used as the input for SVM to detect the malicious attackers.

3.1.2. Support Vector Machine for attack detection

Vapnik (1995) proposed a Support Vector Machine for solving classification and regression problems [19 – 20]. The SVM is a supervised learning technique for the classification training process in various fields. SVM model can apply for binary and multi-class classification, also suitable for linear and non-linear data classification tasks. SVM model creates a hyper-plane for partitioning the data in high-dimensional space and selects the best hyper-plane based on its capacity to partition the data. The non-linear classifier's margins are estimated using various kernel functions and commonly applied kernel functions are linear, polynomial, radial basis, and sigmoid. The researchers have successfully applied SVM for many applications due to its efficiency in classification, SVM model has been widely used in image processing and pattern recognition models.

The SVM model used in this study is based on Radial Basis Function (RBF) with the proposed model. Two numeric vectors are used in Squared Euclidean distance of kernel function is applied and for optimal partition of input data, input data is mapped to high-dimensional space. The kernel RBF model is effective to partition a set of shared complex boundaries. This study uses the multi-class classification problem for attack classification. A two-class problem is divided from a multi-class problem. This study uses Radial Basis Function (RBF), as given in equation (6).

$$K(x,y)=e^{-\gamma\|x-y\|^2},\gamma>0 \tag{6}$$

For training samples $(x_i,y_i),i=1,2,..n$, where maximum number of samples is given as $i,y_i\in\{1,-1\}\,and\,x_iR_n$ where the positive class is 1 and the negative class is -1, and the subspace of labels corresponding to x_i is represented as R_n. The solution to the following problem is provided when using the SVM model, which shown in equation (7).

$$\min_{w,b,\xi}\tfrac{1}{2}w^Tw+C\textstyle\sum_{i=1}^{n}\xi \tag{7}$$

Subject to $y_i(wTw\phi(x_i)+b)\geq 1-\xi_i$

Where, b is the bias term of the SVM. The training vector x_i transforms ϕ to higher dimensional space. A hyper-plane of SVM has a maximum margin to partition various classes of data.

The SVM model has the benefits of having minimal parameter requirement and the disadvantage is that the requirements of a Gaussian function in the training set for each instance cause performance degradation and increases training time on a large dataset in classification case. Soft margin is used if the model fails to find a hyper-plane. The positive slack variables in soft margin use $\xi_i,i=1,2,..N$ in the constraints, as in equations (8 - 10).

$$\left(w.x_i-b\right)\geq +1-\xi_i\ \ for\,y_i=+1 \tag{8}$$

$$(w.x_i-b)\geq -1+\xi_i\ \ for\,y_i=-1 \tag{9}$$

$$\xi\geq 0 \tag{10}$$

Where ξ_i must exceed unity if an error occurs. Then, an upper bound is $\Sigma_i\,\xi_i$ for training error. The Lagrange is given in equation (11).

$$Lp=\frac{1}{2}\left\|w^2\right\|+C\textstyle\sum_{i=1}^{n}\xi_i-\Sigma_i\,\alpha_i\left\{y_i(x_i.w-b)-1+\xi_i\right\}-\Sigma_i\,\mu_i\xi_i \tag{11}$$

Where Lagrange multipliers are denoted as μ_i and this is used to provide ξ_i positive value.Therefore, the SVM provides the information about the malicious attackers and this information is broadcasted over the network. Accordingly, the ID of malicious attackers is removed from the neighbouring user routing table. Further, the route from one user to another user is generated by using the WC-FOA.

3.2. Link Reliability using Weighted Coefficient Firefly Optimization Algorithm (WC-FOA)

The WC-FOA is developed for discovering the route between one user to another user according to the fitness values of residual energy, bandwidth, and EED. Xin-She developed the optimization technique of the Firefly algorithm at the University of Cambridge[21–23]. The conventional FOA is changed into WC-FOA by considering the weighted coefficient during the position update which used to improve the position update according to the best solution.Firefly characteristics related to its activities of locomotion are mimicked in this firefly algorithm. Firefly algorithm is considered to be an effective technique to find a solution to various engineering problems due to its high exploration capacity, flashlight capability, and brightness. The bionics principle is used by the firefly algorithm and the best optimal value is selected based on the most effective firefly algorithm for non-linear and complex design. The light capability of flash is used by each firefly based on the arbitrary solution to attract the adjacent firefly.

3.2.1. Purpose of flashing light

1. Commonly, every firefly is unisexual and attracts a partner for mating.
2. The attraction capability is based on its brightness and light capability is used by fireflies to attract prey for survival.
3. Light flashing is used by fireflies to protect against their other enemies.

3.2.2. Light Intensity variation and Attraction Capability

The initialization considered in the WC-FOA is the possible routes from the transmitter user to the destination user. These possible routes are given as input to the WC-FOA followed by the iterative process of position update takes place to find the optimal route. In the firefly algorithm, the attraction capability and variation of light intensity play a significant role. Light intensity is used to determine the fitness value of the algorithm. The firefly algorithm can handle highly non-linear and several multi-optimization problems. The firefly with low or high intensity attracts neighbouring fireflies with low or high intensity. Consider D_{XY} is the distance between two fireflies such as X and Y. The light intensity reduces concerning distance from the source and media absorb light. Equation (12) provides the intensity of the light as per the law of square inverse.

$$I(D) = \frac{I_s}{D_{XY}^2} \tag{12}$$

The source intensity is denoted as I_S. The light intensity expression L_I varies related to distance D_{XY}, as in equation (13).

$$L_I = I_0 e^{-\beta D_{XY}} \tag{13}$$

The fixed light of absorption coefficient is denoted as β. The initial light intensity is denoted as I_0.

Strong attractive capacity is present in each firefly and this has strong firefly behavior attraction over neighboring firefly groups. Two firefly distances namely X and Y are used to vary the attractive capability. Fireflies' attractive capability is directly proportional to the light intensity of neighboring fireflies. The attractive function expression is given in equation (14).

$$\alpha = \alpha_0 e^{-\beta D_{XY}^2} \tag{14}$$

The attractive capability at distance $D_{XY} = 0$ is denoted as α_0 in equation (15). The calculation of characteristic length for a fixed light is given in equation (15).

$$\Psi = \beta - \frac{1}{M} \rightarrow 1, M \rightarrow \infty \tag{15}$$

Two different fireflies X and Y Cartesian distances are represented as P_X and P_Y, respectively. The two fireflies' Cartesian distance formula is given in equation (16).The Cartesian distance among two points in Euclidean space is the length of a line segment among the two points.

$$D_{X,Y} = \left\| P_X - P_Y \right\| = \sqrt{\sum_{R=1}^{\alpha} (P_X^R - P_Y^R)^2} \tag{16}$$

Attraction movement from one fly to another fly is X and Y as in equation (17). The firefly movement determination related to attraction capability is given in equation (17).

$$P_X^{R+1} = P_X^R + \alpha_0 e^{-\beta D_{XY}^2} (P_Y - P_X) + J\eta \tag{17}$$

Where an attractive term is denoted as $\alpha_0 e^{-\beta D_{XY}^2} (P_Y - P_X)$ and random variable is in term $J\eta$ in range of [0, 1].

To improve Firefly algorithm performance, the weight coefficient (w) is applied and the change firefly random follows the object into the best individual. The modified position update is described using state i as shown in equation (18).

$$x^{i,iter+1} = w(t) \times x^{i,iter} + D_i \times f^{\,i,iter} \times \left(gbest - x^{i,iter} \right) \tag{18}$$

Where, D_i is the distance from the firefly to the light source;the current iteration of the optimal solution is denoted as $gbest$ and adaptively changes $w(t)$ related to equation (19).

$$w(t) = w_{\max} * \exp(-t^2 / (2 \times \left(\frac{iter_{\max}}{40} \right)^2)) \tag{19}$$

Where w maximum initial value is denoted as $w_{\max}$ which is equal to 0.01. If w value is higher in an early stage, it benefits exploration and if it was smaller in a later stage, it benefits exploitation.Therefore, the developed WC-FOA used to discover the optimal secure route which used to enhance the robustness against the malicious user. The elimination of malicious user helps to improve the PDR of the cloud environment.

4. RESULTS

The WCFOA-SVM technique is applied in cloud computing and evaluated various metrics such as attack detection accuracy, energy consumption, Packet delivery ratio, and Throughput. The simulation parameters of WCFOA-SVM are given in the following Table 2.

Table 2. Simulation parameters

Parameter	**Value**
Number of users (Nodes)	50-500
Network area	$1000m \times 1000m$
Propagation model	Propagation/TwoRayGround
Mac type	Mac/802_11
Channel type	Channel/WirelessChannel
Phy type	Phy/WirelessPhy
Packet size	20 bits

The WCFOA-SVM method is compared with the existing technique to evaluate the efficiency of the model.

Metrics: The metrics such as Accuracy, Packet Delivery Ratio and Throughput were measured from the proposed model and mathematically expressed in equations (20-22).

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \times 100 \tag{20}$$

$$Packet\,Delivery\,Ratio = \frac{\sum Number\,of\;\;packet\,receive}{\sum Number\,of\;\;packet\,send} \tag{21}$$

$$Throughput = \frac{D_p \times P_s}{total\,duration\,of\;\,simulation} \tag{22}$$

Where D_p is the number of packets delivered, P_s is the size of a packet, TP is True Positive, TN is True Negative, FP is False Positive, and FN is False Negative.

Parameter Settings: The number of iterations for the WCFOA method is set as 50 and the population size is set as 50. The MATLAB tool is used to simulate and evaluate the WCFOA-SVM model.

Table 3. Attack detection accuracy of WCFOA-SVM

Number of Nodes	**FFED [11]**	**TAE [13]**	**Simhash [14]**	**RF-HEACO [15]**	**WCFOA-SVM**
0	0	0	0	0	0
50	70	70	85	85	90
100	71	71	85	86	90
150	73	71	87	86	90
200	75	72	88	87	91
250	75	73	88	87	93
300	75	77	88	87	94
350	75	80	88	88	96
400	76	81	88	90	96
450	78	81	90	91	96
500	79	83	90	92	96

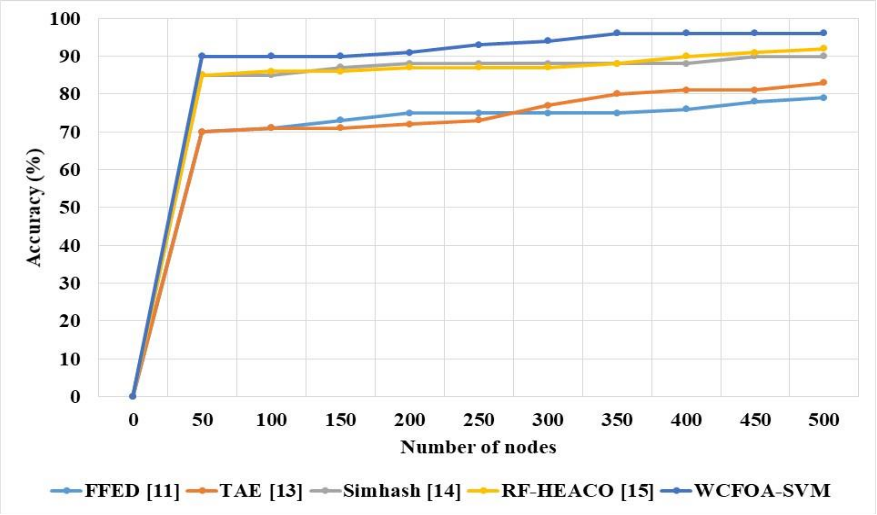

Figure 1. Detection Accuracy of WCFOA-SVM for various nodes

The WCFOA-SVM technique is tested for various nodes in terms of detection accuracy, as in Table 3and Figure 2. The WCFOA technique applies the weighted coefficient technique to balance the exploration and exploitation. The WCFOA technique helps to find reliable links for transmission and increases the attack detection performance. The WCFOA model finds the optimal path for transmission and the SVM model can handle high dimensional data. The WCFOA method has higher efficiency in attack detection than existing methods. The RF-HEACO [15] method has a local optima trap and overfitting problem in attack detection. The Simhash [14] focuses on similar based measures for attack classification in the model. The WCFOA-SVM model has 96 % accuracy in attack detection and RF-HEACO method has 92 % accuracy for 500 nodes.

Table 4. Energy consumption of WCFOA-SVM

Number of Nodes	FFED [11]	TAE [13]	Simhash [14]	RF-HEACO [15]	WCFOA-SVM
0	0	0	0	0	0
50	60	51	40	36	21
100	60	56	40	37	21
150	60	57	41	37	22
200	61	57	42	39	23
250	61	57	43	39	23
300	65	58	43	41	24
350	66	59	43	42	25
400	67	61	44	43	25
450	69	65	53	44	27
500	69	65	55	45	27

The energy consumption of the WCFOA-SVM model is measured for various nodes and compared with existing techniques, as given in Table 4and Figure 3. The weighted coefficient in the Firefly algorithm helps to balance exploration and exploitation. This helps to reduce energy consumption in exploration or exploitation. The WCFOA method also finds link reliability and this helps to provide optimal transmission. The WCFOA-SVM method has less energy consumption than existing methods. The WCFOA-SVM model has 27 J energy consumption and the RF-HEACO method has 45 J energy consumption for 500 nodes.

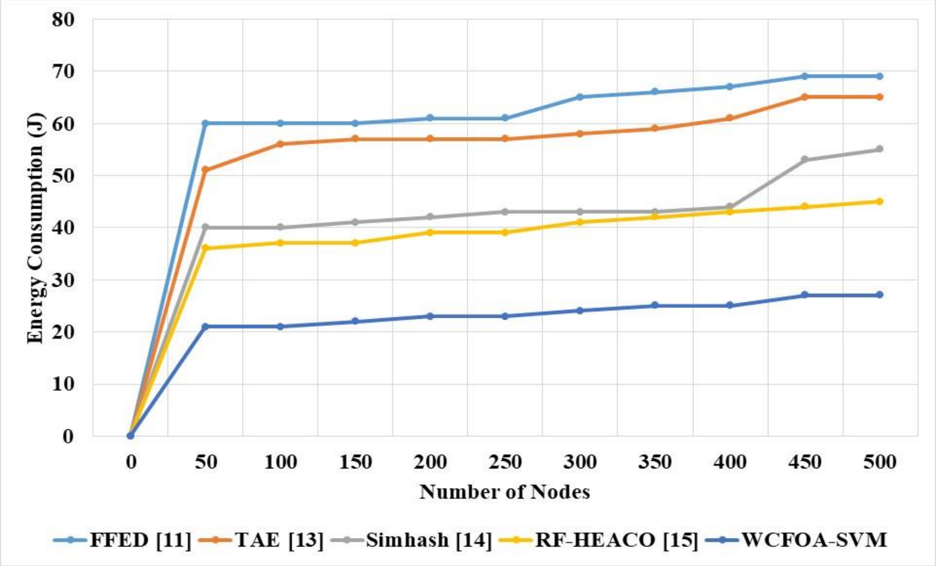

Figure 2. WCFOA-SVM energy consumption for various nodes

Table 5. Packet Delivery ratio of WCFOA-SVM

Number of Nodes	**FFED [11]**	**TAE [13]**	**Simhash [14]**	**RF-HEACO [15]**	**WCFOA-SVM**
0	0	0	0	0	0
50	80	74	79	85	91
100	71	76	83	87	96
150	71	76	79	89	94
200	70	78	75	90	92
250	80	70	76	80	95
300	77	74	85	85	93
350	80	78	77	80	95
400	72	72	82	81	94
450	79	72	75	82	94
500	73	74	85	83	96

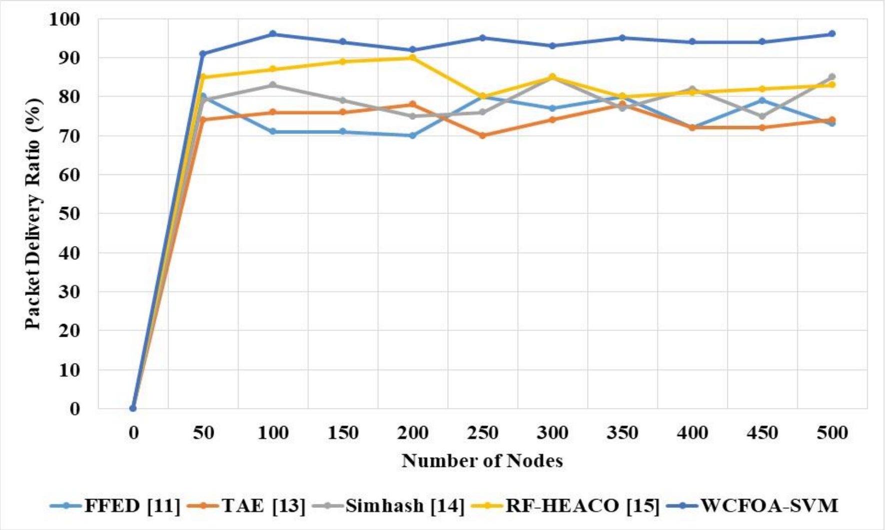

Figure 3. WCFOA-SVM Packet delivery ratio for various nodes

The WCFOA-SVM model packet delivery ratio is measured and compared with existing techniques in trust model, as in Table 5and Figure 4. The WCFOA-SVM model uses a weighted coefficient to balance exploration and exploitation in the search process. Balancing the exploration and exploitation helps to effectively detect the attack and reduce the packet loss. The WCFOA-SVM model has a higher packet delivery ratio than existing methods in cloud computing. The existing methods have a limitation of local optima trap and overfitting problems in the model. The WCFOA-SVM model has 96 % packet delivery ratio and RF-HEACO method has 83 % for 500 nodes.

Table 6. Throughput of WCFOA-SVM

Number of Nodes	FFED [11]	TAE [13]	Simhash [14]	RF-HEACO [15]	WCFOA-SVM
0	0	0	0	0	0
50	1	1	5	7	14
100	2	1	7	10	15
150	3	1	7	11	17
200	3	4	7	11	19
250	4	6	7	11	20
300	4	7	9	12	22
350	5	8	9	13	27
400	6	8	11	15	29
450	8	10	14	15	35
500	8	11	15	17	35

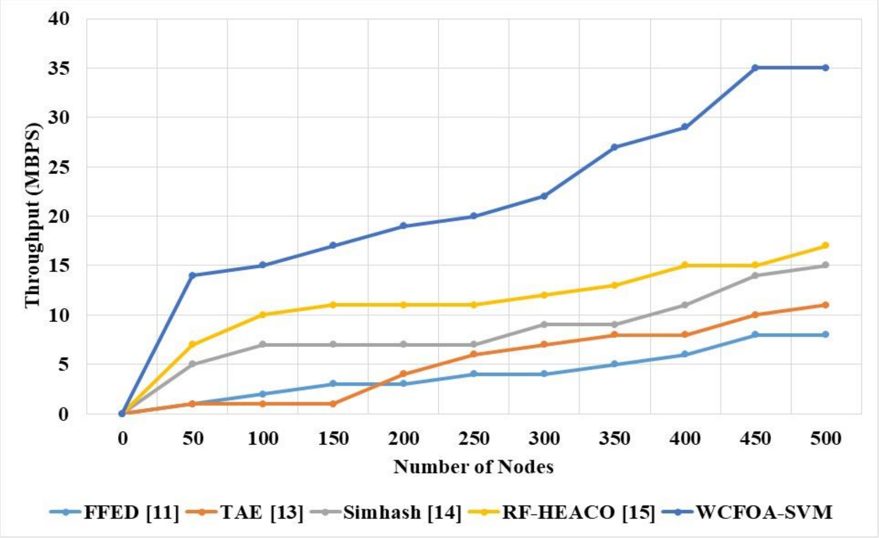

Figure 4. WCFOA-SVM Throughput for various nodes

The WCFOA-SVM throughput is measured for various nodes and compared with existing techniques, as in Table 6and Figure 5. The WCFOA-SVM model balances exploration and exploitation using a weighted coefficient. The balancing of exploration and exploitation helps to increase the transmission capacity of the model. The WCFOA-SVM model has higher throughput than the existing technique. The RF-HEACO model has a limitation of local optima trap and overfitting problem. The WCFOA-SVM model has 35 MBPS throughput and RF-HEACO model has 17 MBPS throughput.

The SVM based malicious attack detection with unique cost metrics is used to overcome the issue of overfitting. The incorporation of weighted coefficient in WC-FOA is used to enhance the exploration and exploitation capabilities that used to overcome the issue of local optima trap. The attacks classified by the SVM is avoided while discovering the route using WC-FOA that used to enhance the packet delivery of the network.

5. CONCLUSION

The existing researches on the trust model for the cloud have the limitations of local optima trap and overfitting problem. The WCFOA-SVM model is proposed to increase the performance of the trust model in attack detection and efficiency. The WCFOA model is applied for link reliability measures and path selection. The SVM model is applied for attack detection using entropy measure and link reliability. The RF-HEACO model has the limitation of local optima trap and overfitting problem. The Simhash technique mainly focuses on similarity measures for attack detection. The WCFOA method has higher efficiency than existing methods in terms of attack detection, energy consumption, packet delivery ratio, and throughput. The WCFOA-SVM model has 27 J energy consumption and the RF-HEACO model has 45 J energy consumption.The developed WCFOA-SVM is identified only the malicious users, so further it is required to be developed for identifying the network traffic-related attacks. The future work of this method involves applying multi-class classification for attack classification using the deep learning technique.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] Rahman, M.A., Asyhari, A.T., Leong, L.S., Satrya, G.B., Tao, M.H. &Zolkipli, M.F. (2020). Scalable machine learning-based intrusion detection system for IoT-enabled smart cities. *Sustainable Cities and Society*, Vol. 61, pp. 102324.

[2] Ali, M.H., Al Mohammed, B.A.D., Ismail, A. &Zolkipli, M.F. (2018). A new intrusion detection system based on fast learning network and particle swarm optimization. *IEEE Access*, 6, pp.20255-20261.

[3] Manzoor, I. and Kumar, N. (2017). A feature reduced intrusion detection system using ANN classifier. *Expert Systems with Applications*, Vol. 88, pp. 249-257.

[4] Haider, W., Hu, J., Slay, J., Turnbull, B.P. and Xie, Y. (2017). Generating realistic intrusion detection system dataset based on fuzzy qualitative modeling. *Journal of Network and Computer Applications*, 87, pp.185-192.

[5] Jeyanthi, D.V. and Indrani, B. (2022). An Efficient Intrusion Detection System with Custom Features Using Fpa-Gradient Boost Machine Learning Algorithm.*International Journal of Computer Networks & Communications (IJCNC)*, Vol.14, No.1, pp. 99-115.

[6] Lv, L., Wang, W., Zhang, Z. and Liu, X. (2020). A novel intrusion detection system based on an optimal hybrid kernel extreme learning machine. *Knowledge-based systems*, Vol. 195, pp. 105648.

[7] Almiani, M., AbuGhazleh, A., Al-Rahayfeh, A., Atiewi, S. and Razaque, A. (2020). Deep recurrent neural network for IoT intrusion detection system. *Simulation Modelling Practice and Theory*, Vol. 101, pp. 102031.

[8] Alazzam, H., Sharieh, A., &Sabri, K.E. (2020). A feature selection algorithm for intrusion detection system based on pigeon inspired optimizer. *Expert systems with applications*, Vol. 148, pp. 113249.

[9] Le,H. D., Luong, N. T. and Nguyen, T. V. (2022). AODVMO: A Security Routing Protocol Using One-Time Password Authentication Mechanism Based On Mobile Agent.*International Journal of Computer Networks & Communications (IJCNC)*, Vol.14, No.3, pp. 17-35.

[10] Eskandari, M., Janjua, Z.H., Vecchio, M. and Antonelli, F.(2020). Passban IDS: an intelligent anomaly-based intrusion detection system for IoT edge devices. *IEEE Internet of Things Journal*, 7(8), pp.6882-6897.

[11] Guesmi, H., Kalghoum, A., Ghazel, C. &Saidane, L.A.(2021). FFED: a novel strategy based on fast entropy to detect attacks against trust computing in cloud. *Cluster Computing*, Vol. 24, No. 3, pp.1945-1954.

[12] AbdelAzim, N.M., Fahmy, S.F., Sobh, M.A. &Eldin, A.M.B.(2021). A hybrid entropy-based DoS attacks detection system for software defined networks (SDN): A proposed trust mechanism. *Egyptian Informatics Journal*, Vol. 22, No. 1, pp.85-90.

[13] Wu X., Wang, J., Wang, P., Bian, Z., Huang, T., Guo, Y. & Fujita, H. (2021). Trustworthiness assessment for industrial IoT as multilayer networks with von Neumann entropy. *Applied Soft Computing*, Vol. 106, pp.107342.

[14] Kou, H., Liu, H., Duan, Y., Gong, W., Xu, Y., Xu, X. & Qi, L., (2021). Building trust/distrust relationships on signed social service network through privacy-aware link prediction process. *Applied Soft Computing*, 100, p.106942.

[15] Sakthidasan, K., Gao, X.Z., Devabalaji, K.R. &Roopa, Y.M., (2021). Energy based random repeat trust computation approach and Reliable Fuzzy and Heuristic Ant Colony mechanism for improving QoS in WSN. *Energy Reports*, 7, pp.7967-7976.

[16] Alshammari, S.T., Albeshri, A. and Alsubhi, K., 2021. Building a trust model system to avoid cloud services reputation attacks. Egyptian Informatics Journal, 22(4), pp.493-503.

[17] Hassan, H., El-Desouky, A.I., Ibrahim, A., El-Kenawy, E.S.M. and Arnous, R., 2020. Enhanced QoS-based model for trust assessment in cloud computing environment. IEEE Access, 8, pp.43752-43763.

[18] Qureshi, K.N., Jeon, G. and Piccialli, F., 2021. Anomaly detection and trust authority in artificial intelligence and cloud computing. Computer Networks, 184, p.107647.

[19] Zhou, J., Huang, S., Wang, M. &Qiu, Y. (2021). Performance evaluation of hybrid GA–SVM and GWO–SVM models to predict earthquake-induced liquefaction potential of soil: a multi-dataset investigation. *Engineering with Computers*, pp.1-19.

[20] Dong, S., (2021). Multi class SVM algorithm with active learning for network traffic classification. *Expert Systems with Applications*, Vol. 176, pp.114885.

[21] Hassan, B.A. (2021). CSCF: a chaotic sine cosine firefly algorithm for practical application problems. *Neural Computing and Applications*, Vol. 33, No. 12, pp. 7011-7030.

[22] Altabeeb, A.M., Mohsen, A.M., Abualigah, L. &Ghallab, A. (2021). Solving capacitated vehicle routing problem using cooperative firefly algorithm. *Applied Soft Computing*, Vol. 108, pp. 107403.

[23] Ewees, A.A., Abualigah, L., Yousri, D., Algamal, Z.Y., Al-qaness, M.A., Ibrahim, R.A. &AbdElaziz, M., (2021). Improved Slime Mould Algorithm based on Firefly Algorithm for feature selection: A case study on QSAR model. *Engineering with Computers*, pp. 1-15.

AUTHORS

Shalini Sharma pursuing Ph.D. in computer Science from Jamia Millia Islamia University, New Delhi, India. She acquired Master of Technology in Information Technology from Guru Gobind Singh University, Delhi in 2011.She worked as Assistant Professor in Sharda University during 2011- 2015.She has served IT organization Infogain India, IRIS Software & Accenture 2015 onwards.

Syed Zeeshan Hussain acquired Ph.D. from Jamia Millia Islamia, New Delhi, India, and Master of Computer Applications (MCA) from IGNOU, New Delhi respectively. He is currently working as Associate Professor in department of Computer Science Jamia Millia Islamia, New Delhi, India. His research interests include Computer Networks, Network Security, Web Technology and Applications, Object-Oriented Computing, Scripting Languages.