Journal of Theoretical and Applied Information Technology
31st August 2023. Vol.101. No 16

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A NOVEL WOSRCNN-BASED TRUST MODEL WITH SECURE ROUTING AND DATA TRANSMISSION IN WSN USING CLF_AVOA AND ASCII-DSAES

MAHAMMAD MASTAN[1], G. JAI ARUL JOSE[2], LOUAY A. HUSSEIN AL-NUAIMY[3]

[1, 3]Assistant Professor, Department of CS & MIS, Oman College of Management & Technology, Oman
[2]Assistant Professor, Department of Computer Applications, St. John's College of Arts and Science, India
E-mail: [1]mastan.mohammed@omancollege.edu.om, [2]jaiaruljose@gmail.com,
[3]loay.alneimy@omancollege.edu.om

ABSTRACT

Wireless Sensor Networks (WSNs) are networks in which to detect and gather data from the environment, it utilizes various types of Sensor Nodes (SNs) positioned in a specific location. Therefore, for transferring the data accurately as of source to destination, it requires secure Data Transmission (DT). It is prone to error since the data moves in the in-secured channel from one SN to another. Energy-efficient data gathering is also challenging owing to the limited energy resources of each SN. Thus, in this work, to accomplish an optimal trade-off betwixt security and resource utilization, by utilizing Chebyshev Levy Flight African Vulture Optimization Algorithm (CLF_AVOA) and American Standard Code for Information Interchange (ASCII) to Decimal Sorting adapted Advanced Encryption Standard (ASCII-DSAES) algorithms, a novel Weight Optimized Softplus Relu Convolutional Neural Network (WOSRCNN)-centric trust model with Secure Routing (SR) and DT is proposed. To determine the node details, a Node Discovery Message (NDM) is primarily transmitted after the SNs are positioned in the required environment. Then, it extracts the node features. After that, for the detection of trusted nodes, trust scores are calculated utilizing WOSRCNN. Then, by utilizing Euclidean Distance (ED) along with CLF_AVOA, distance and optimal paths are selected for the trusted nodes. With the ASCII-DSAES mechanism, the sensed information is partitioned and encrypted; then, it is transferred to the Base Station (BS) where the partitioned data is combined and stored in the server for further usage. The experimental results displayed that in contrast to the conventional frameworks, the presented model provides high security and throughput with minimum delay.

Keywords: *Wireless Sensor Network (WSN), Optimal path selection, Convolutional Neural Network (CNN), Secure routing, Advanced Encryption Standard (AES), Data partitioning, Trust identification.*

1. INTRODUCTION

In people's daily lives, an important part is occupied by the growth of the Internet of Things (IoT). For routine activities, people utilize numerous devices that are interconnected with each other and also connected to the Internet [1]. In IoTs, WSNs have become a significant part. Also, the main part of the WSN is the SNs [2]. In arising research areas like smart cities, the Internet of vehicles, and body area networks, WSNs have become an important part currently [3]. The wireless frameworks enclosed by densely deployed tiny sensors are named WSNs, which are wielded for sensing environmental changes as well as industries [4]. Node control, event detection, position monitoring, data acquisition, and event identification are performed continuously by the SNs of WSN [5]. The environment information is gathered by these nodes. Then, this information is transmitted to the BS or intermediate gateway directly through wireless links [6]. The BS is the node that slightly differs from the other nodes. Since the BS has strong communication power that follows proper information processing along with collection, higher computational power, and higher energy-related resources, it differs from other nodes [7]. WSNs are application-oriented. In other words, it is designed for particular applications to gratify a predefined set of requirements, which may differ as of application to application [8]. The WSN's architecture is classified as clustered and flat. The SNs communicate directly or by relaying the data via other nodes with the BS in the flat architecture [9]. Instead of a far BS, an SN communicates with a local Cluster Head (CH) in the clustered environment. Generating a transmission schedule, collecting data, and transmitting it to a BS are the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

major duties of a CH [10]. But, the attackers capture the SNs easily; then, act as the malicious node. Also, various sorts of attacks, such as sinkhole, hello flooding stacks, selective forwarding attacks, wormhole attacks, and Sybil attacks are launched [11,12]. Some or all packets are dropped by the malicious nodes. Hence, in such attacks, if the routing protocol is not immune, some significant data cannot reach the sinkhole [13]. Thus, in the positioning of WSNs, it is a significant challenge to secure the network from internal attacks by the malicious node [14]. Figure 1 exhibits the WSN's general representation,

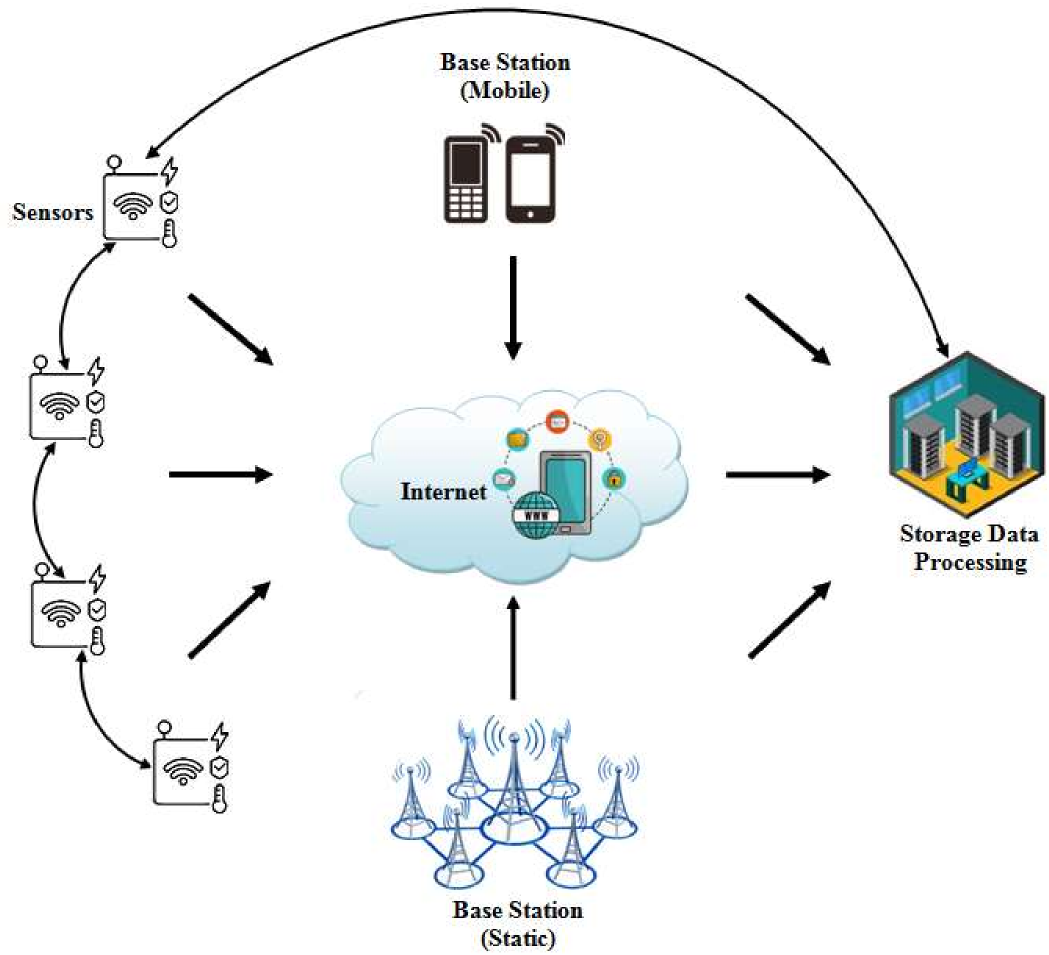


Figure 1: General structure of WSN

For WSNs, numerous SR protocols have been applied. Here, Routing Protocol for Low–Power and Lossy Networks (RPL) grounded routing has become a popular protocol. This can be categorized as Optimizing viable metrics, Optimizing the route discovery process, and Transmission power control [15].There is another protocol, which works on trust along with reputation-centric systems. This provides security to the data transmitted by the node without utilizing cryptosystems [16]. A current algorithm to verify neighbors grounded on their performance is the Trust-based neighbor selection. At the time of DT, this ensures higher reliability together with privacy. Depending upon its actions, the degree of reliability a node acquires is referred to as trust [17]. In addition, to minimize or defend against internal attacks, a trust management system is constructed grounded on the trust model. By captured or compromised nodes, these internal attacks are launched [18]. But, some standard cryptography and authentication methodologies are required by these conventional SR protocols. This also leads to higher processing capability together with routing cost [19]. Moreover, they are computationally intensive as well as traffic-intensive. This is inappropriate for

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

resource-constrained SNs. Therefore, utilizing CLF_AVOA and ASCII-DSAES algorithms, a novel WOSRCNN-based trust model with SR along with DT is proposed in this paper to accomplish an optimal trade-off betwixt security and resource utilization.

The balance part is arranged as: the related works are surveyed in section 2; section 3 explains the proposed methodology; the result and discussion are explicated in section 4; lastly, the paper is winded up with future work in section 5.

2. LITERATURE SURVEY

M. Hema Kumar *et.al* [20] suggested a trust-aware localized routing along with a class-centered dynamic encryption system. To reach the destination, the route was discovered initially by the methodology; then, the data packet was transmitted. After that, it measured the Trusted Data Forwarding Support (TDFS)'s value. Then, for route selection, it selected only the route with a specific neighbor. The data being transmitted into several classes were maintained and classified by the model. Then, for different classes, the technique wielded various signatures along with encryption systems. Before transmission, the data had been encrypted with a class-specific structure together with a key. A block chain in which every single block comprises the encrypted data's part and was denoted by a hash along with a pointer to the next block was produced. For generating original data as of the encrypted key, the same had been reversed. High-performance data security was introduced by the model; also, the overall network performance was enhanced. But, the network was increased overhead and the throughput performance was affected.

S. Sujanthi and S. Nithya Kalyani [21] established a Secure Deep Learning (SecDL) mechanism for dynamic cluster-centric WSN-IoT networks. Within the Bi-Hex network, dynamic clusters were formed; also, Quality Prediction Phenomenon (QP2) selected the CHs. In every single cluster, data aggregation was enabled; then, with a Two-way Data Elimination along with a reduction model, it was handled. To attain high-level security for data aggregation, the One Time-PRESENT (OT-PRESENT) cryptography model was introduced. In order to ensure high-level QoS, through the optimal route, the cipher text was then transmitted to the mobile sink. A Crossover-centric Fitted Deep Neural Network (Co-FitDNN) was established to select the route optimally. The outcomes exhibited enhanced performance when analogized to the prevailing frameworks. However, high availability was not ensured by the cryptography's use, which was the basic aspect of information security.

Deebak B D and Fadi Al-Turjman [22] presented an SR along with a monitoring protocol with multi-variant tuples utilizing Two-Fish (TF) symmetric key algorithm for determining and averting the adversaries in the global sensor network. Grounded on the Authentication and Encryption Model (ATE), this model was designed. The sensor guard nodes were chosen by utilizing the Eligibility Weight Function (EWF); then, with the complex symmetric key model's help, it was hidden. Through inheriting the properties of Multipath Optimized Link State Routing (OLSR) as well as Ad hoc On-Demand Multipath Distance Vector (AOMDV) protocols, a secure hybrid routing protocol was selected to be constructed. The outcomes displayed that when analogized to the previous techniques, the presented model had a higher percentage of monitoring nodes. However, this model did not execute the real-time implementation of hybrid routing along with the monitoring framework. This resulted in lowered information secrecy.

M. Selvi *et.al* [23] proffered an SR approach named an energy-aware trust-centric SR system in which the trust score estimation was wielded for identifying the malicious users efficiently in WSN along with Spatio-temporal constraints were utilized with a decision tree system to select the best route. The experimental outcomes showed that regarding energy efficiency, packet delivery ratio, along with security, the projected trust-centered routing approach attained superior performance to the prevailing frameworks. However, the methodology did not perform detection of malicious nodes. This affected the routing performance.

Azam Beheshtiasl and Ali Ghafari [24] developed a secure, trustable, together with energy-efficient routing methodology for WSNs. For attaining the routes' trust values, the scheme wielded Fuzzy logic. After that, via considering trust along with security, the technique selected the shortest route as of the source to the destination. The Multidimensional Scaling-Map (MDS-MAP) optimal routing system was wielded here; then, the trust model was measured via fuzzy logic. After

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

that, with Trust and Centrality Degree Based Access Control (TC-BAC) together with Trust-Aware Routing Framework (TARF) protocols, it was analogized. The outcomes proved that regarding consumption of energy, average end-to-end delay, along with average packet delivery rate, the presented technique outperformed the TC-BAC as well as TARF methodologies. But, this scheme concentrated on primary encryption along with an identity acknowledgment framework, which is not suitable for WSNs.

Shahana Gajala Qureshi and Shishir Kumar Shandilya [25] proffered the shortest secure path routing grounded on trust via Hybridized Crow Whale Optimization (H-CWO) along with QoS-centric bipartite Coverage Routing (QOS-CR) to evaluate the scheme's performance. In the network area, the nodes were positioned randomly. Firstly, via H-CWO, a trust metric formation was employed; also, it selected the authenticated nodes. After that, to perform clustering, the CH was selected through the SR protocol. For determining the shortest path routing, neighborhood hop prediction was performed; then, through QOS-CR, the data was transferred securely. Therefore, the presented H-CWO as well as QOS-CR displayed higher energy, higher throughput, maximum alive nodes, along with minimum delay. This ensured safe DT as of the source node to the destination node. Here, for energy-efficient transmission, the cluster grounded routing protocol utilized to employ huge data was not executed.

3. PROPOSED TRUST-BASED SECURITY FRAMEWORK IN WSN

In the past epochs, the WSN's usage has increased hugely owing to its wide range of applications. The SNs are installed in various zones depending on their requirements; then, the detected information will be transmitted to the BS. WSN becomes an insecure environment owing to the number of vulnerable attacks that are performed on numerous nodes by attackers. Few attacks are executed at the routing level. In this study, by utilizing CLF_AVOA and ASCII-DSAES mechanisms, a novel WOSRCNN-centric trust model with SR along with DT is presented to solve these problems. (1) NDM transmission, (2) Trust score estimation, (3) Feature extraction, (4) Classification, (5) Distance computation, (6) Optimal path selection, (7) Data partitioning, and (8) Encryption are the phases that come under this security system. Figure 2 exhibits the block diagram of the presented trust-centric security technique in WSN.

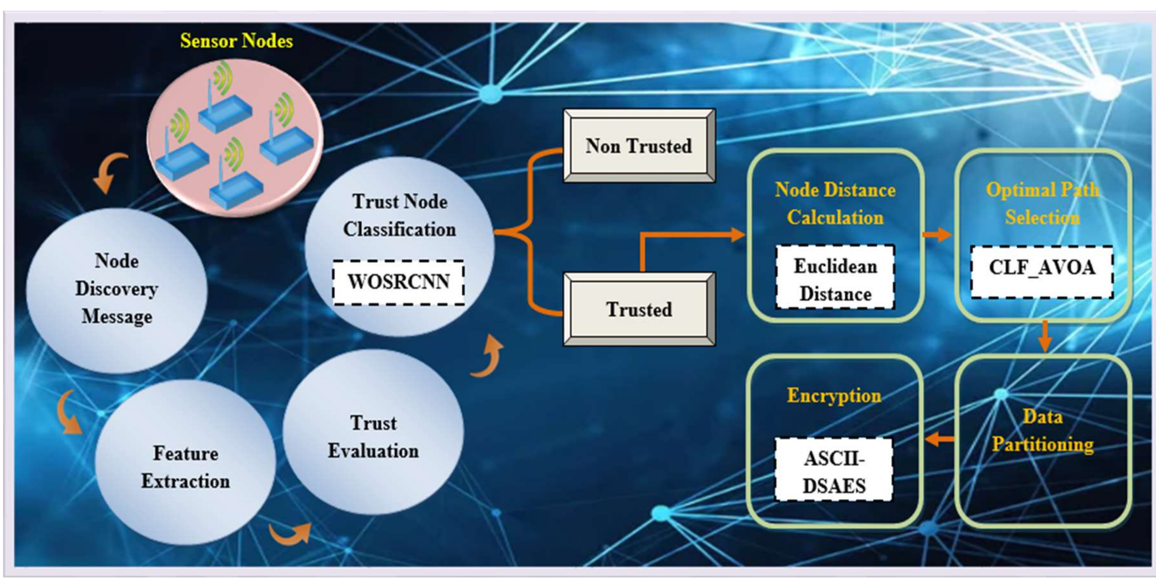


Figure 2: Proposed Trust-based security framework in WSN

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.1 NDM Transmission

The process of transmitting data securely through trusted nodes along with optimal paths has begun by organizing the number of SNs randomly in the observing area. Meanwhile, NDM is sent betwixt nodes in each time slot to detect the secure route for the transmission of sensitive data. Node ID(N_{ID}), Energy(E), and Neighbor node ID$\left(N_{N_{ID}}\right)$ are comprised by the NDM request (NDM). These are formulated as,

$$NDM = \left(Source, NDM\ request, N_{ID}, E, N_{N_{ID}}\right) \quad (1)$$

This NDMrequest is disseminated betwixt each SN in the network. Therefore, each node replies with its energy, node ID, number of successful transmissions, type of node, number of re-transmissions, and location for the incoming request. All the necessary information is extracted from the reply message on receiving the reply. Then, it will be stored in the node table for further processing.

3.2 Feature Extraction

The SN features like Energy consumption, mobility, communication time, number of transmitting packets, number of receiving packets, node ID, etc., are extracted after the NDM request-response. These are required for the classification of malicious nodes from normal nodes. Some of the features are described below,

- ***Energy consumption:*** The amount of energy expended by the networks to execute DT, reception, and aggregation is termed energy consumption.
- ***Mobility:*** After initialization, the ability of SNs to change their location is referred to the mobility.
- ***Communication time:*** It is proffered as the amount of time taken by the SNs for DT and reception.

Hence, the$N$- number of extracted SN features $\left(\hbar^{(i)}\right)$ is specified as,

$$\hbar^{(i)} = \left\{\hbar^{(1)}, \hbar^{(2)}, \dots\dots, \hbar^{(N)}\right\} ;\ i = 1,2,\dots,N \quad (2)$$

3.3 Trust Evaluation

Here, for secure DT in the WSNs, to identify the malicious along with trusted nodes, the trust scores are computed. The relationship betwixt adjacent SNs in the WSN to monitor the level of subjective likelihood is described as trust. To provide a secure service, trust is calculated grounded on the trust degree that one node gets as of another node. A necessary parameter to elect the secure nodes so as to improve the network communication securely is named the trust factor. Centered on the following conditions, the trust score is computed.

- The node that sends its acknowledgment genuinely to the neighbor nodes after receiving the message packets is regarded as 1st group of trusted nodes.
- During transmission, whenever any SN drops one or more message packets, it will be considered as 2nd group of trusted nodes.
- During DT, when there is no congestion, if a node drops packets more often, then it will become 3rd group node. Further, it will not be wielded for transmission and discarded from the group.

The nodes are chosen for DT and reception grounded on these trust groups. For the 1st group of trusted nodes, the trust score is computed utilizing the equation given below,

$$\Re_1{}^{(j)} = \frac{\alpha_1 * \beta + \alpha_2 T_S + \alpha_3 S_S}{\alpha_{mean}} \quad (3)$$

Here, the sum of weights $(\alpha_1, \alpha_2, \alpha 3)$ for different trust scores is signified as $\alpha_{mean} = \alpha_1 + \alpha_2 + \alpha_3$,$\Re_1{}^{(j)}$ stands for 1st trust score for j^{th} node, the temp score and spatial score of SNs is denoted as T_S, S_S, the parameter (β) is evaluated as,

$$\beta = \frac{Ne_{num}}{P_R} * 100 \quad (4)$$

Where, the number of transmitted acknowledgments to the neighboring node is specified as Ne_{num}, and the number of packets received from the neighborhood nodes is denoted as P_R. After that, the 2nd group of trust nodes $\left(\Re_2{}^{(j)}\right)$ grounded on packet drop is expressed as,

$$\Re_2{}^{(j)} = 100 - \left(\frac{N_{DP}}{T_{NDP}} * 100\right) + f(t_1, t_2) \quad (5)$$

Here, the number of dropped packets while the transmission is indicated as N_{DP}, the total number of dropped packets in the network is indicated as T_{NDP}, and t_1, t_2 models the temporal constraint time boundaries for lower and upper bounds

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

correspondingly. Lastly, the total trust score $\left(\Re^{(j)}\right)$ for $j^{th}$the node is represented as,

$$\Re^{(j)} = \frac{\Re_1{}^{(j)} + \Re_2{}^{(j)}}{2} \tag{6}$$

Similarly, for all the SNs in the wireless sensor network, the trust score is calculated. Then, to sort the trusted and non-trusted SNs, the extracted features $\left(\hbar^{(i)}\right)$ and trust scores $\left(\Re^{(j)}\right)$ are given to the proposed WOSRCNN classifier. The combined features and trust scores are indicated by $\left(\xi_{(k)}\right)$,

$$\xi_{(k)} = \left(\xi_{(1)}, \xi_{(2)}, \dots \dots, \xi_{(n)}\right) \tag{7}$$

Here, the number of extracted features and trust scores is signified as$n$.

3.4 Trust Node Classification with WOSRCNN

CNN is a sort of DL architecture. Here, for SNs' classification, the output of each layer is given as the input of the succeeding layer. The number of training parameters is lowered and the computational efficiency of the complex networks is improved owing to the local perception along with the weight-sharing characteristics of CNN. A pooling layer, fully connected layer, input layer, activation layer, and convolutional layer are comprised by the CNN. By applying a vector of weights and biases, the output is computed by every neuron in the CNN. But, grounded on the loss function, these weight values need to be adjusted in every single iteration to get an enhanced classification outcome. Moreover, the Rectified linear unit (Relu) activation function, which is utilized in the traditional CNN, suffers from the problem of unbounded and the gradients at the negative inputs are zero. This means during back propagation, the weight values are not updated. Thus, by utilizing the Kaiming variance system along with the replacement of the Relu activation function with Softplus Relu (SR), the weight values are optimized. Therefore, the modified CNN is renamed WOSRCNN. Figure 3 represents the general CNN architecture.

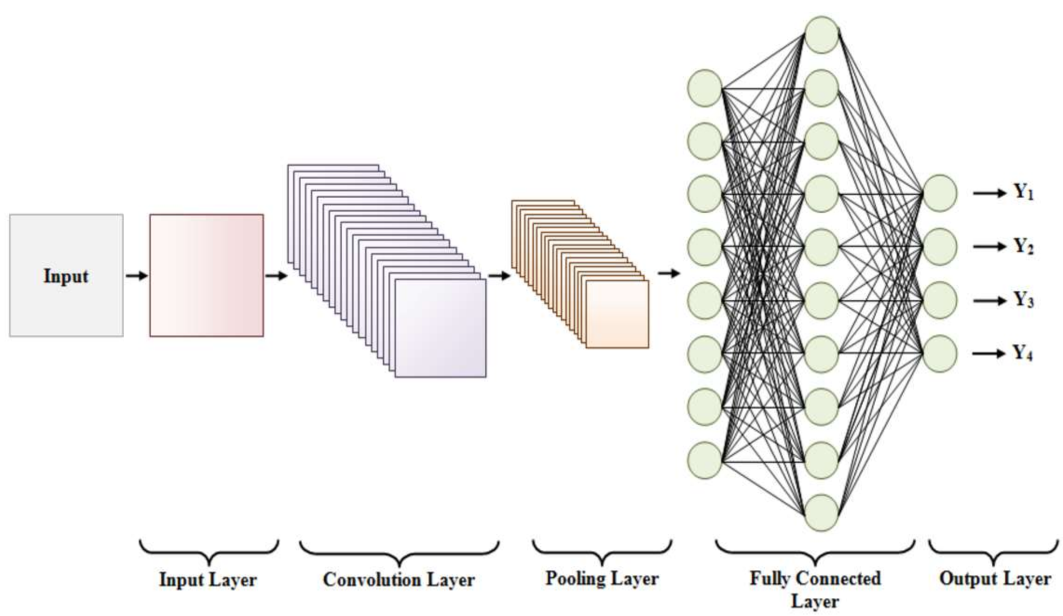


Figure 3: General architecture of CNN

The classification steps utilizing WOSRCNN are detailed below,

Input layer: Here, it receives the input and multiplied it by the weight and bias values of each neuron and produces the outcome. In this layer, the extracted node features and trust scores $\left(\xi_{(k)}\right)$ are given as input and the resultant outcome of the input layer (I_m) with $M(m = 1,2, \dots \dots, M)$ neurons can be expressed as,

$$I_m = \xi_{(k)} * WIm_{Im} \tag{8}$$

Where, the input layer optimized weight and biases are differentiated by W_{Im} and ℓ_{Im}.

Convolutional layer: Numerous maps of neurons that are defined as maps of features or filters are consisted in this layer. In size, it is quite identical to the input data's dimensionality. It contains a series of 5*5 filters with a fixed size that is utilized to perform convolution on the input. The convolution operation in the convolution layer (C_m) can be expressed as,

$$C_m = \left(\xi_{(k)} \oplus W_{Cm}\right) \tag{9}$$

Here, the updated weight value connecting the input with the convolutional layer is denoted as W_{Cm}.

Pooling layer: This layer, which lowers the number of output neurons in the convolutional layer and combines the adjacent elements in the convolution output, is applied after the convolution. The output of the pooling operation (P_m) is mentioned as,

$$P_m = SR(W_{Pm} C_m + \ell_{Pm}) \tag{10}$$

Where, the activation function is specified as $SR(\circ)$, and the pooling layer optimized weight and bias values are exhibited as W_{pm}, ℓ_{pm}.

Activation Function: For applying a non-linear function to the previous layer's output, the SR activation function utilized in the proposed WOSRCNN is responsible. This can be formulated as,

$$SR\left(\xi_{(k)}\right) = \begin{cases} ln\left(1 + e^{\xi_{(k)}}\right) - ln(2) & \xi_{(k)} < 0 \\ max\left(0,\ \xi_{(k)}\right) & otherwise \end{cases} \tag{11}$$

Fully connected layer: The learned feature vectors are flattened into one vector after the pooling layer; then, this vector is wielded as the input of the fully connected layers. It is wielded for understanding patterns that are produced by the prior layers. To all activations in the previous layer, neurons here have full connections. Hence, the network's final result is,

$$O_m = SR(W_{Om} P_m + \ell_{Om}) \tag{12}$$

Here, the network's final output is signified as O_m, and the fully connected layer optimized weight and bias values are represented as W_{Om}, ℓ_{Om}.

Error Calculation: Here, the mean square error (E) betwixt the estimated output (O_{est}) and the obtained output (O_m) is calculated by utilizing the equation given below,

$$E = \frac{\sum_{k=1}^{N} O_{est}(k) - O_m(k)}{2} \tag{13}$$

Thus, the trusted SNs from the non-trusted nodes are categorized correctly by the classifier; then, for the trusted nodes to carry out DT, the optimal paths are selected. The trusted SNs classified are signified by $\left(\vartheta_j (j = 1,2, \dots \dots, J)\right)$. The weight optimization in each layer of the neural network is represented by,

$$var(W) = \frac{2}{M} \tag{14}$$

Where, the number of incoming neurons in the WOSRCNN network is denoted as M, and $var(W)$ signifies the weight optimization parameter.

3.5 Node Distance Calculation

To identify the shortest distance betwixt the source and destination, the distance betwixt every single node is computed after categorizing the trusted SNs. Grounded on the ED, the distance betwixt trusted SNs is computed. The Euclidean distance $(E_D(j,l))$ is computed utilizingthe equation given below,

$$E_D(j,l) = \left(\sum_{j=1}^{J} \left(\vartheta_j - \vartheta_l\right)^2\right)^{1/2} \tag{15}$$

Here, ϑ_j and ϑ_l signifies the j^{th} and l^{th} SNs correspondingly. Then, for efficient communication, the optimal paths are selected centered on this distance.

3.6 Optimal Path Selection by CLF_AVOA

A newly developed nature-inspired meta heuristic optimization is named the African Vulture Optimization Algorithm (AVOA). It is grounded on the scavenging behaviour along with living habits of African vultures. Vultures are the '2' groups of hunting birds. These birds are native to Asia, America, Africa, along with Europe. In a natural environment, for searching for food, vultures can be physically classified into '2' groups. To find food and eat, each group has a different inability. These birds escape from the hungry trap due to each vulture's tendency to search for food for hours and eat. But, there is no assurance that the final population will comprise accurate estimations for the global optimum at the exploration phase's end while solving the complex optimization problems. In the optimal local location, this leads to premature convergence. Therefore, the Chebyshev Chaotic Map (CCM) is utilized to surge the performance in resolving complex problems. To avert premature convergence and to obtain the best optimal solution, this map initializes the population in the primary step. Moreover, to boost the convergence speed of the AVOA algorithm, the Levy flight step size is adjusted adaptively. The proposed optimization mechanism is named CLF_AVOA owing to the adoption of the CCM along with Levy flight step size. The CLF_AVOA-based optimal path selection's step-by-step procedure is given below,

Step 1: Here, $\omega_{(i)} = \omega_{(1)}, \omega_{(2)}, \dots \dots, \omega_{(H)}$ represents the number of trusted SNs, which becomes the initial population of African vultures, where $(i = 1,2, \dots \dots, H)$indicates the number of weight values in every single layer of the network (number of vultures in the population). Then, utilizing the Chebyshev chaotic mapping function, the H vultures are initialized and positioned in the$d$ $-$dimensional search space. A chaotic map, which displays some kind of chaotic behavior over time (t), is a mathematical function. It is characterized as,

$$\omega_{(i)}{}^{t+1} = f\left(\omega_{(i)}{}^{t}\right) \tag{16}$$

The chaotic variable $\omega_{(i)}{}^{t+1}$ at time $(t+1)$ depends on the variable $\omega_{(i)}{}^{t}$ at time(t) in the chaotic system. Therefore, the Chebyshev chaotic function wielded to initialize and position the initial vulture population is described as,

$$\omega_{(i)}{}^{t+1} = cos\left(\frac{\chi}{cos\left(\omega_{(i)}{}^{t}\right)}\right) \tag{17}$$

Step 2: Here, to divide the population into two groups, the fitness value is computed. Then, the best solution is considered the best first vulture; also, the second solution becomes the second-best vulture. A population is formed by others, which moves or substitutes one of the two best vultures in every single performance. The fitness is evaluated grounded on the node degree, shortest distance, high trust score, centrality factor, and high residual energy to obtain the optimized weights. The fitness calculation $\left(F_{(i)}\right)$ is denoted by,

$$F_{(i)} = max\left(E_D(j,l)\right) + closeness(\partial) + max(node\ \ deg\,r\,ee) \tag{18}$$

Where, ∂ is the centrality factor, which is the closeness of nodes to their neighbors. The weakest along with the hungriest vultures are represented by the lower fitness. This corresponds to the worst vultures at present. Conversely, the strongest along with the most abundant vulture is represented by the higher fitness that corresponds to the best vulture at present. Here, all the vultures migrate towards the best vultures; also, move away from the worst ones.

Step 3: The vulture population is grouped according to the fitness measure after fitness calculation. In the first group, the vulture that belongs to the best solution is positioned. Similarly, in the second group, the vulture that belongs to the second-best solution is positioned. In the third group, other vultures are positioned. As the first along with second-best vultures have guiding effects, the movement of vultures in the current iteration is formulated as,

$$\boldsymbol{\delta}_{(i)} = \begin{cases} \boldsymbol{F}_{(i1)}{}^{*} & \boldsymbol{for}\ \boldsymbol{P}_{(i)} = \boldsymbol{\varepsilon_1} \\ \boldsymbol{F}_{(i2)}{}^{*} & \boldsymbol{for}\ \boldsymbol{P}_{(i)} = \boldsymbol{\varepsilon_2} \end{cases} \tag{19}$$

Where, $F_{(i)}{}^{*}, F_{(i)}{}^{*}$ stands for the 1st and 2nd best vultures respectively. In the range of (0, 1), $\varepsilon_1, \varepsilon_2$ is the random number. By utilizing the Roulette wheel to select each of the best solutions, the probability of choosing the best solution is increased.

$$P_{(i)} = \frac{F_{(i)}}{\sum_i F_{(i)}} \tag{20}$$

Step 4: The vultures cannot travel long distances when they are partially hungry owing to their lacking physical strength. It has adequate strength to find food when they are not very hungry. Thus, hungry vultures will become aggressive. Therefore, instead of searching for food by themselves, they will remain nearby the vultures with food. Accordingly, the exploration stage along with the exploitation stage of vultures can be made. The degree of hunger is wielded as a sign of vultures' transition as of the exploration to the exploitation stage. The hunger degree $\left(\varphi_{(i)}\right)$ can be estimated as,

$$\varphi_{(i)} = (2 * \varepsilon + 1) * \gamma * \left(1 - \frac{t}{t_{max}}()\right) \tag{21}$$

Where, γ is a random number betwixt -1 and 1, the maximum iteration number is described as t_{max}, and η can be calculated as,

$$\eta = \iota \times sin_{(i)}\left(\frac{\pi}{2} * \frac{t}{t_{max}}()\, cos\left(\left(\frac{\pi}{2} * \frac{t}{t_{max}}()\right)()\right)\right) \quad (22)$$

Here, ι stands for the random number in the interval [-2, 2].

Step 5: The exploration behavior of vultures can be modeled based on the levy flight distribution. The levy flight $(l(f))$ is mentioned as,

$$l(f) = \frac{mean}{|var\,iance|^{1/\psi}} \quad (23)$$

In equation (23), ψ is a fixed parameter. Therefore, the exploration stage becomes,

$$\omega_{(i)}{}^{t+1} = \begin{cases} \delta_{(i)} - d_{(i)}{}^{t} * \varphi_{(i)} & l(f) \geq \tau_1 \\ \delta_{(i)} - \varphi_{(i)} + \tau_2 \cdot (upper - lower) \cdot \tau_3 + lower \end{cases} \quad (24)$$

Here, τ_1, τ_2, τ_3 are the random numbers, which are uniformly distributed in the range [0, 1], $lower, upper$ states the lower and upper bounds respectively, and the distance betwixt the vulture and the current optimal vulture is expressed as $d_{(i)}{}^{t}$, which is measured as,

$$d_{(i)}{}^{t} = \left|\zeta * \delta_{(i)} - \omega_{(i)}{}^{t}\right| \quad (25)$$

Step 6: Here, food competition and rotating flight stages are developed to balance the exploration along with exploitation ability. The vulture is energetic and full if $\delta_{(i)}$ is betwixt 0.5 and 1 during the food competition phase. Then, the strong vultures share their food while the weak vultures attack the stronger ones for food. Hence, the vulture's position is denoted as,

$$\omega_{(i)}{}^{t+1} = d_{(i)}{}^{t} + \left(\varphi_{(i)} + \tau_4\right) - h_{(i)}{}^{t} \quad (26)$$

$$h_{(i)}{}^{t} = \delta_{(i)} - \omega_{(i)}{}^{t} \quad (27)$$

When the vulture will not undergo food competition, the rotating flight stage takes place. At this juncture, the vulture experiences spiral movement, and the position is updated as,

$$\omega_{(i)}{}^{t+1} = \varphi_{(i)} - \left(A_{(i1)} + A_{(i2)}\right) \quad (28)$$

$$A_{(i1)} = \varphi_{(i)} * \left(\frac{\tau_5 * \omega_{(i)}{}^{t}}{2\pi}\right) * cos\left(\omega_{(i)}{}^{t}\right) \quad (29)$$

$$A_{(i1)} = \varphi_{(i)} * \left(\frac{\tau_6 * \omega_{(i)}{}^{t}}{2\pi}\right) * sin\left(\omega_{(i)}{}^{t}\right) \quad (30)$$

Likewise, all vultures have enough food and are full when $\delta_{(i)}$ becomes less than 0.5. Yet, the best vultures become hungry; then, they attack for food. Therefore, with aggregation along with attack behavior, the exploitation takes place. The set of optimal solutions is attained finally. These are the optimal weight values. Figure 4 reveals the proposed CLF_AVOA optimal path selection methodology's pseudo code.

Pseudo code of Proposed CLF_AVOA

Input: Number of trusted sensor nodes $\omega_{(i)}$

Output: Optimal paths (ω^{*})

Begin

Generate initial population of African vultures $\omega_{(i)}$

Initialize H vultures in the d – dimensional search space

Compute $\omega_{(i)}^{i+1} = \cos\left(\frac{\chi}{\cos(\omega_{(i)}^{i})}\right)$

While $(t < t_{max})$

Calculate fitness value and sort out $F_{(i_1)}{}^{*}, F_{(i_2)}{}^{*}$

For each $1 \leq i \leq H$

Estimate the movement of vultures $\delta_{(i)}$

Calculate the probability $P_{(i)} = \frac{F_{(i)}}{\sum_i F_{(i)}}$

Evaluate hunger degree $(\varphi_{(i)})$

Perform levy flight $(l(f))$ computation

If $l(f) \geq \tau_1$

Update the position of vultures $(\omega_{(i)}{}^{i+1})$

Else

Renew the position with $\delta_{(i)} - \varphi_{(i)} + \tau_2 .(upper - lower). \tau_3 + lower$

End if

Perform distance $d(i)i = \left|\xi * \delta_{(i)} - \omega_{(i)}{}^{i}\right|$

If $0.5 \leq \delta_{(i)} \leq 1$

Bring up-to-date the position of vultures $(\omega_{(i)}{}^{i+1})$

Accomplish spiral movement $\omega_{(i)}{}^{i+1} = \varphi_{(i)} - (A_{(i1)} + A_{(i2)})$

Else

Implement aggregation and attack behavior

End if

End For

Recognize the optimal solution (ω^{*})

End While

End

Figure 4: Pseudo code of the proposed CLF_AVOA

3.7 Data Partitioning

The sensor data is divided into various parts of fixed size, encrypted, and then transfers into the BS through different routes after optimal paths are identified. All the partitioned data are amalgamated into a single message and are stored for the further process when the packet receives the BS. To secure the data from intruders, data splitting is executed.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Because all the packets of the message had to be tracked if an intruder needs to access the data. One has to take care of the whole network to track that. This is more complicated. Thus, after partitioning, such encryption of data enhances the security of DT. Let Xbe the input message that is sensed by the SNs, it is further separated into G-number of individual data$\left(X_g\right)$,

$$X_g = [x_1, x_2, \dots \dots, x_G] \quad (31)$$

3.8 Data Encryption via ASCII-DSAES

Here, by utilizing ASCII-DSAES, the detached data in equation (30) is encrypted to send them through various optimal paths. Advanced Encryption Standard (AES), which utilizes a single key for the encryption along with the decryption process, is a symmetric key iterative block cipher-centric encryption approach. The number of encryption together with decryption rounds to be performed is decided by the key length. This may be 10, 12, and 14 rounds for various input bits. SubBytes, ShiftRow, MixColumn, and AddRound key are the four transformations comprised by each round. However, the limitation of this model is that it may be susceptible to fault occurrence with complex computational steps. In this paper, to solve these issues and add more security, a modified form of AES with ASCII to the decimal conversion of input is performed at first with the replacement of the MixColumn step with a sorting operation. This replacement along with conversion lowers the complexity and adds more security than general AES. Thus, the proposed encryption system is named ASCII-DSAES. The steps are explained below,

ASCII conversion: The input message $\left(X_g\right)$ is converted into ASCII form. The broadly utilized character encoding format for text data is ASCII. The conversion of $\left(X_g\right)$ into $\hat{X}_g$is,

$$\hat{X}_g \to \prod\nolimits_{0-128} X_g \quad (32)$$

Decimal conversion: After the conversion of partitioned input into ASCII form, for adding more security to the input, it is converted into a decimal number. It is expressed as,

$$Y_g \to \prod\nolimits_{0to255} D\left(\hat{X}_g\right) \quad (33)$$

Where, Y_g is the decimal form of $\hat{X}_g$.

SubBytes: It is the only non-linear along with invertible byte transformation. Through the substitution box (S-box)'s row and column, it replaces the input data block's every single byte. The S-Box has distinct mathematical properties. This ensures changes in individual state bits propagate across the cipher text rapidly, which provides confusion. During decryption, to undo the SubBytes transformation's effect, the inverse substitution table is wielded. This can be stated as,

$$\boldsymbol{Y_g}^* \leftrightarrow \boldsymbol{Y_g} \ \& \ \boldsymbol{L_{uptab}} \quad (34)$$

Where, $Y_g{}^*$ describes the replaced bit with the data from the look-up table $\left(L_{uptab}\right)$.

ShiftRows: By utilizing a certain offset, this manipulates the state's rows to shift the bytes in every single row. This is the cycling shifting of each row. Here, the first row is left with no change. Then, with one-byte, two-byte, along with three-byte circular shifts, the other rows are shifted. The same process is executed during decryption. Here, the first row remains unchanged. Whereas grounded on the same offset utilized during encryption to shift them to the left, the other rows are shifted to the right.

Sorting: Sorting is performed in ascending order after shifting each row. The process of arranging data in an orderly sequence is named sorting.

AddRound key: In ASCII-DSAES, this is the last step. The round key bytes are XORed. It has every single byte resulting from the prior phase to provide confusion. This operation is expressed as,

$$C_{ph} = \Psi_g \oplus \wp \quad (35)$$

In the above equation, the encrypted cipher text is signified asC_{ph}, the sorted data is indicated asψ_g, and the round key is denoted as$\wp$. This operation is executed grounded on creating the relationship betwixt key and cipher text, which is from the previous step. On the key, which is denoted by users, the AddRound Key output exactly depends. Till the final round, these steps are continued. Figure 5 displays the structure of the ASCII-DSAES encryption algorithm.

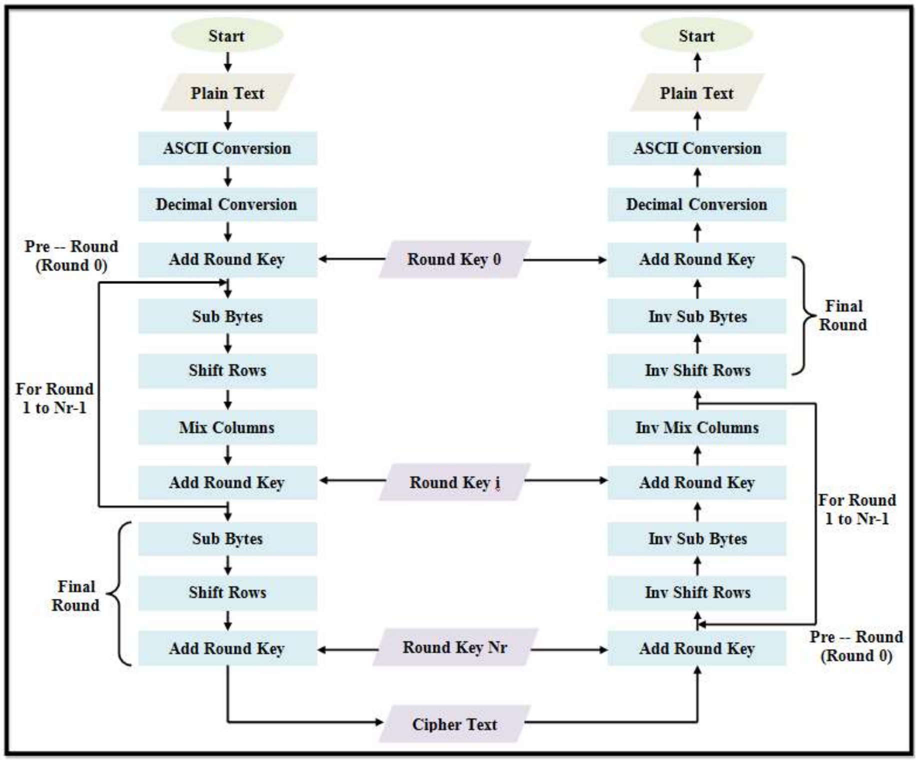


Figure 5: Structure of ASCII-DSAES

4. RESULTS AND DISCUSSION

By analogizing the attained results of the presented technique with the prevailing frameworks, the proposed trust-centric SR mechanism's performance is verified in this part. For optimal path selection, malicious node classification, and data encryption, the superiority measurement is made.

4.1 Performance Assessment of Proposed WOSRCNN

Regarding False Positive Rate (FPR), precision, f-measure, specificity, Negative Predictive Value (NPV), accuracy, recall, and sensitivity, the results are evaluated by analogizing the presented WOSRCNN classifier for trusted node classification with prevailing classifiers like Feed Forward Neural Network (FFNN), Recurrent Neural Network (RNN), Long-Short Term Memory (LSTM), and CNN. Figure 6 illustrates the graphical estimation of accuracy, precision, along with recall.

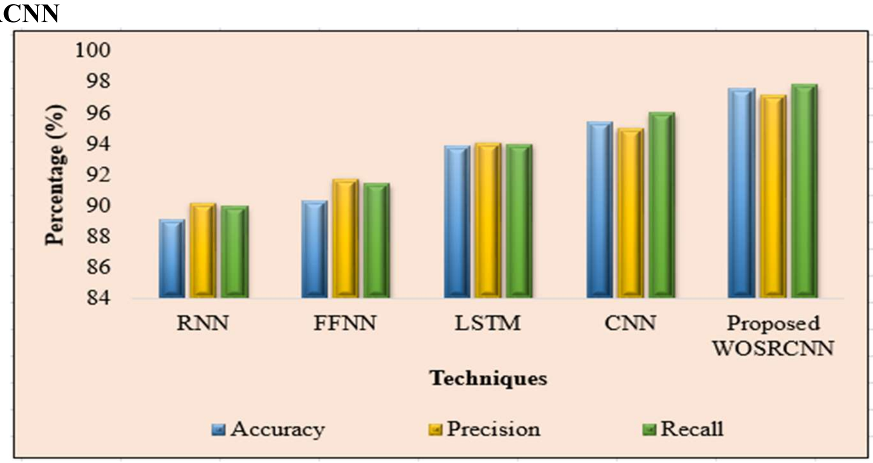


Figure 6: Graphical comparison of proposed WOSRCNN with existing classifiers

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

From Figure 6, the presented WOSRCNN achieves accuracy (97.56%), precision (97.14%), and recall (97.84%). Whereas, the accuracy, precision, and recall attained by the prevailing CNN are 95.42%, 95.02%, and 96.01% correspondingly. In contrast to the previous CNN, the WOSRCNN achieves higher percentages. This is due to the optimized weights along with SR activations. Conversely, the conventional LSTM, FFNN, and RNN achieve lower accuracy, precision, and recall than CNN as well as WOSRCNN. Therefore, it is clear that when compared to the baseline classifiers, the WOSRCNN classifies the trusted nodes from the non-trusted nodes accurately. Table 1 depicts the superiority measurement grounded on f-measure, sensitivity, along with specificity.

Table 1: Comparative analysis of proposed WOSRCNN using f-measure, sensitivity, and specificity

Techniques/ Performance metrics	F-measure (%)	Sensitivity (%)	Specificity (%)
RNN	88.88	88.76	89.09
FFNN	91.37	90.72	92.85
LSTM	94.46	93.96	93.74
CNN	95.83	96.19	95.91
Proposed WOSRCNN	96.98	97.05	97.28

The proposed and prevailing classification mechanisms' specificity, sensitivity, along with f-measure is demonstrated in table 1. The accuracy measure of the classifier, which results from the weighted mean of precision and recall metrics is termed F-measure. Sensitivity along with specificity describe the accuracy of classification, which reports the presence or absence of malicious nodes in WSN. Therefore, the superior performance of the classification system is depicted by the higher percentage of these metrics. Accordingly, the WOSRCNN attains the F-measure, sensitivity, and specificity of 96.98%, 97.05%, and 97.28% respectively, which is higher compared to the previous RNN, FFNN, LSTM, and CNN that attain the F-measure, sensitivity, and specificity of RNN (88.88%, 88.79%, and 89.09%), FFNN (91.37%, 90.72%, and 92.85%), LSTM (94.46%, 93.96%, and 93.74%), and CNN (95.83%, 96.19%, and 95.91%). Therefore, the proposed classifier out performs the conventional techniques. The presented classifier's performance evaluation grounded on FPR and NPV is shown further.

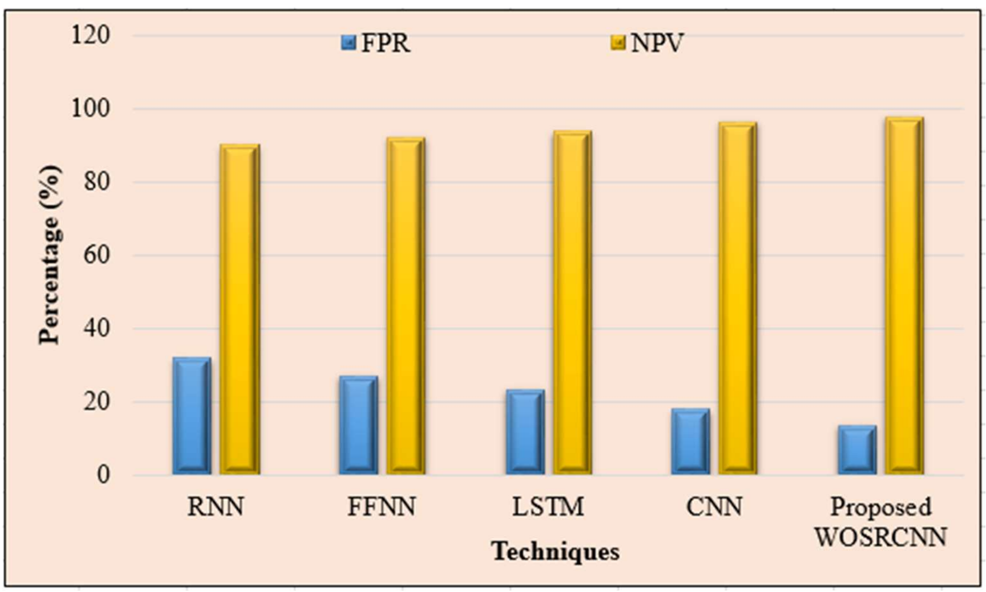


Figure 7: FPR and NPV analysis

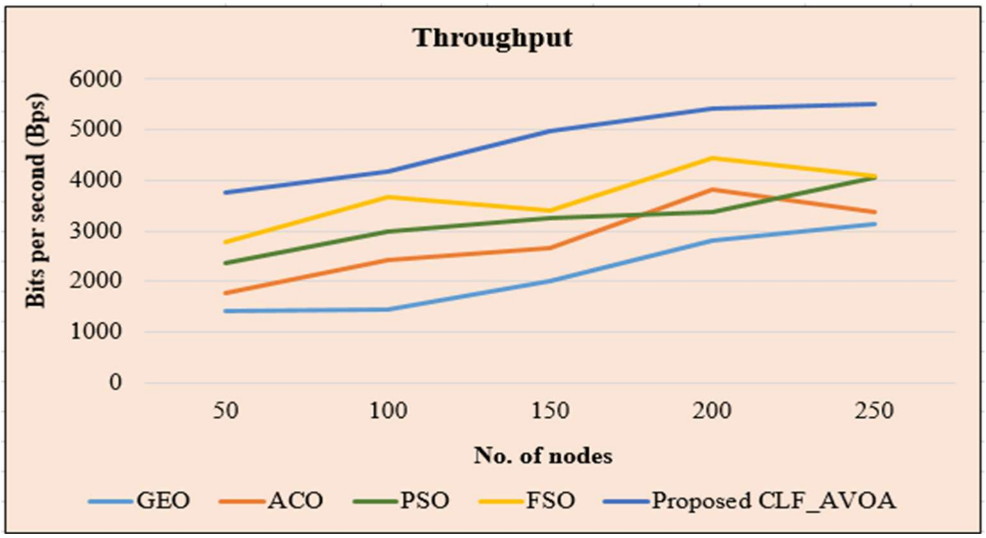
To reveal the proposed classifier's effectiveness, the FPR and NPV of the proposed and prevailing classification algorithms are shown in Figure 7. The WOSRCNN attains a higher NPV (97.84%) with a lower FPR (13.42%). The classification of the trusted node as trusted is determined by the NPV. The higher NPV displays that the presented classifier classifies the trusted nodes efficiently. On the other hand, the percentage of falsely detecting the trusted nodes as non-trusted ones is denoted by FPR. The lower rate of FPR indicates that the proposed classifier proficiently

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

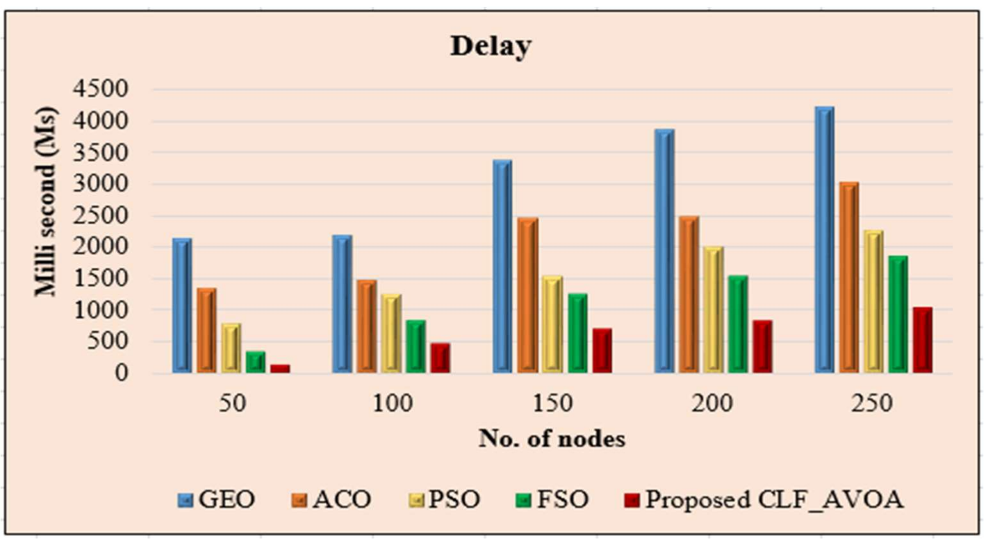
classifies the trusted nodes with less false detection. However, the prevailing techniques have higher FPR and lower NPV analogized to the proposed mechanism. Thus, it displays that the presented methodology outperforms the conventional models. From the overall analysis, it shows that the proposed classifier classifies the trusted and non-trusted nodes more apparently than any other conventional methodologies.

4.2 Superiority measurement of Optimal path selection method

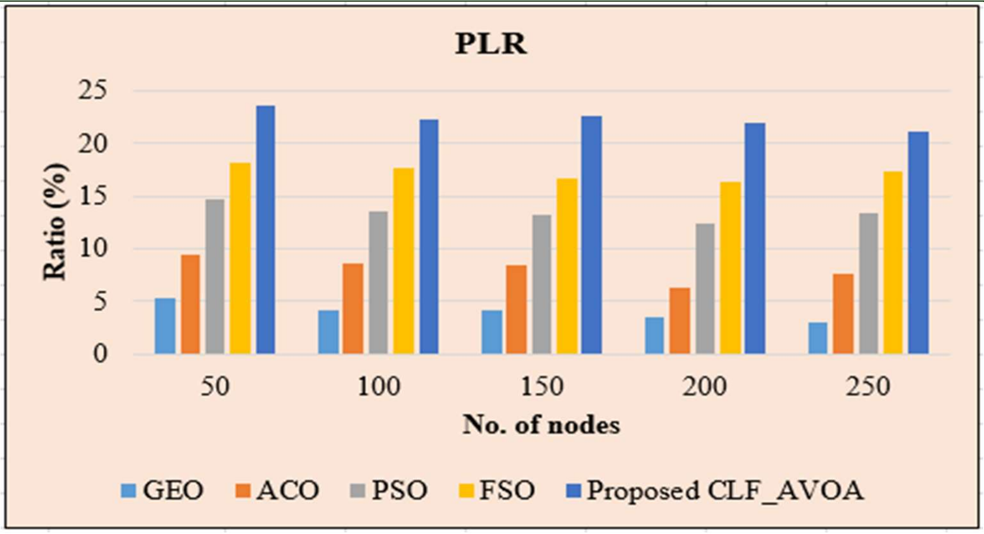
Here, the approach wielded for selecting the optimal trusted paths for efficient DT in the presented model is analogized with baseline optimization approaches viz., Golden Eagle Optimizer (GEO), Particle Swarm Optimization (PSO), AVOA, along with Ant Colony Optimization (ACO). Regarding the Packet Loss Ratio (PLR), delay, network lifetime, throughput, and energy consumption, the comparative evaluation takes place. The assessments are explained as follows,



(a)



(b)



(c)

Figure 8: performance measurement based on (a) throughput, (b) delay, and (c) PLR

The proposed and existing techniques' throughput, delay, and PLR are displayed in figure 8. Grounded on the number of SNs in the range of 50 – 250, the assessment is made. The amount of data processed in a given time is calculated by the throughput. This is analyzed in figure 8 (a). Regarding Bits per second (Bps), it is computed. Better performance is shown by the higher throughput. For 50 nodes, the throughput rate attained by the proposed CLF_AVOA is 3747 Bps. The throughput increases when the number of nodes increases, that is, 5509Bps for 250 nodes. Whereas, the prevailing GEO has a throughput of 1411bps for 50 nodes, which is lower. The delay in DT of the proposed and conventional frameworks is shown in figure 8 (b). The lower delay shows better performance. From the figure, the CLF_AVOA has a lower delay of 159ms for 50 nodes and reaches a maximum of 1043ms for 250 nodes. This shows that the DT is done efficiently. Conversely, for 50 nodes, the existing FSO has 364ms and for 250 nodes, it reaches 1843ms. Therefore, in contrast to the presented algorithm, the previous approach has a higher delay. The PLR, which defines the number of data loss that occurs during DT, is displayed in figure 8 (c). The CLF_AVOA obtains a lower PLR of 23.5433% - 21.1147%. This is shown in the graph. PLR decreases when the number of nodes increases. When analogized with the proposed technique, the prevailing FSO, PSO, ACO, and GEO has higher PLR. From the overall evaluation, it is clear that the presented model transfers data efficiently through the optimal path with high throughput, low delay, and low PLR.

Table 2: Result comparison in terms of (a) energy consumption and (b) network lifetime

(a)

Techniques	Energy consumption (J)				
	50	100	150	200	250
GEO	4932	5733	6862	7914	8947
ACO	3753	4792	5837	6696	8143
PSO	2646	3736	4812	5699	6523
FSO	2113	3095	4112	5162	6105
Proposed CLF_AVOA	1672	2334	3316	4287	5212

(b)

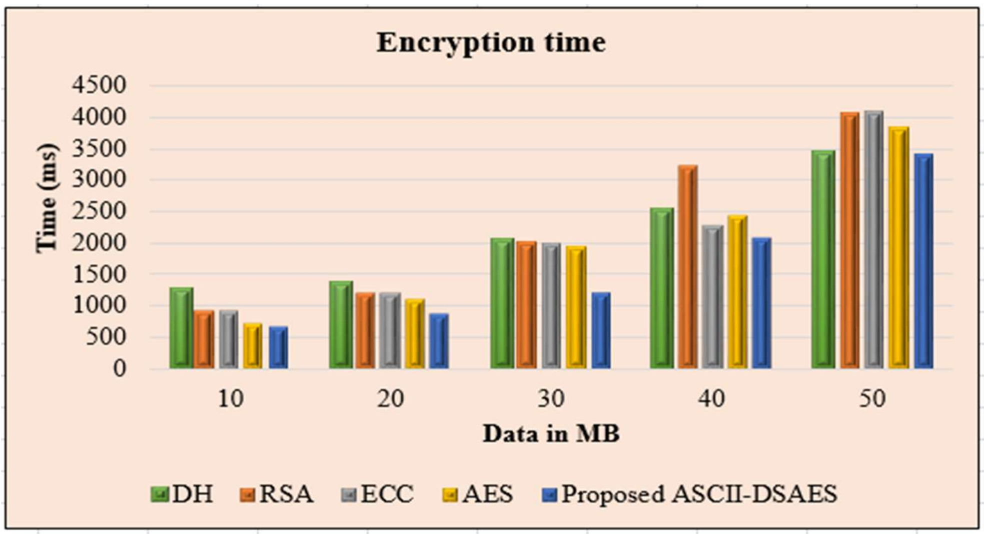
Techniques	Network lifetime (ms)				
	50	100	150	200	250
GEO	1587	2774	4157	6517	8236
ACO	2235	3657	5847	7463	8547
PSO	2754	4278	6433	8477	11014
FSO	3477	5124	7633	9665	12127
Proposed CLF_AVOA	3686	5847	8245	11025	144634

The comparative analysis of network (a) energy consumption and (b) lifetime is demonstrated in table 2.For a minimum of 50 nodes and a maximum of 250 nodes, the energy consumption of the presented technique is 1672J to 5212J, which is lower when compared to the prevailing FSO that has the energy consumption of 2113J to 6105J and other conventional techniques. In table 2 (b), as the optimal path is utilized in the proposed mechanism, the network lifetime is larger than other methodologies for a varying number of nodes. Due to the proposed optimal routing path selection, the technique attains lower energy consumption together with a higher network lifetime. This is energy-efficient, shortest, and secure for DT betwixt SNs. Therefore, it shows that the presented technique balances the throughput, energy consumption, along with network lifetime efficiently in contrast to the other models.

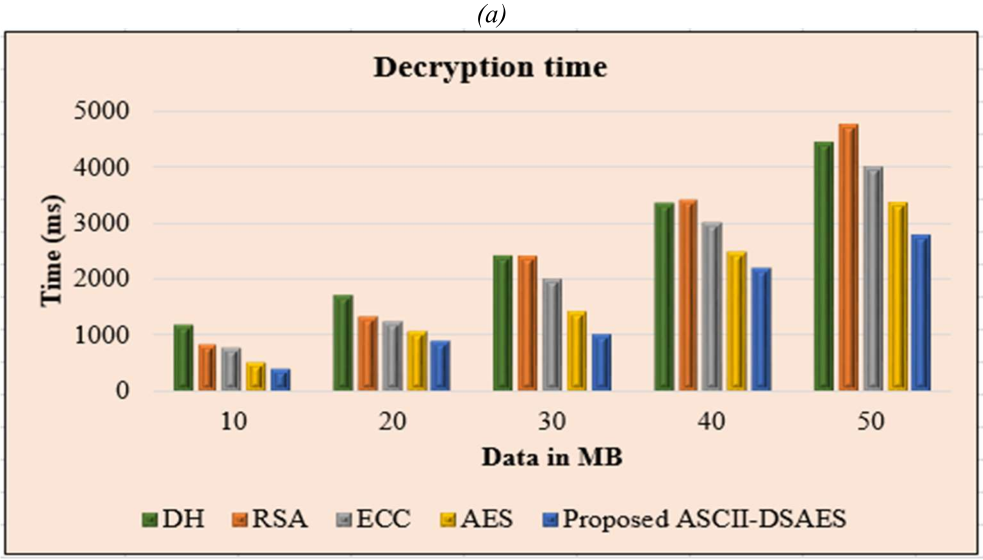
4.3 Performance analysis of proposed ASCII-DSAES

With conventional techniques like Diffie-Helmann (DH), AES, Rivest-Shamir-Adleman (RSA), and Elliptic Curve Cryptography (ECC) grounded on Encryption Time (ET), decryption time, along with security level, the performance of the presented ASCII-DSAES approach wielded for data encryption is evaluated in this subsection. Figure 9 explicates the ET together with decryption time assessments.

The proposed and prevailing algorithms' ET along with decryption time is depicted in figures 9 (a) and (b). From the graphs, the encryption along with decryption time taken by the proposed methodology is much lesser. Regarding the data size in Mega Bytes (MB), the time varies. The ASCII-DSAES takes 3408ms to encrypt the message and 2766ms to decrypt the information when the data size is 50MB. Conversely, to encrypt and decrypt the data, the conventional AES, ECC, RSA, along with DH mechanisms take more time. Therefore, it proves that the presented scheme is more secure and faster than previous techniques.



(a)



(b)

Figure 9: (a) Encryption and (b) decryption time analysis

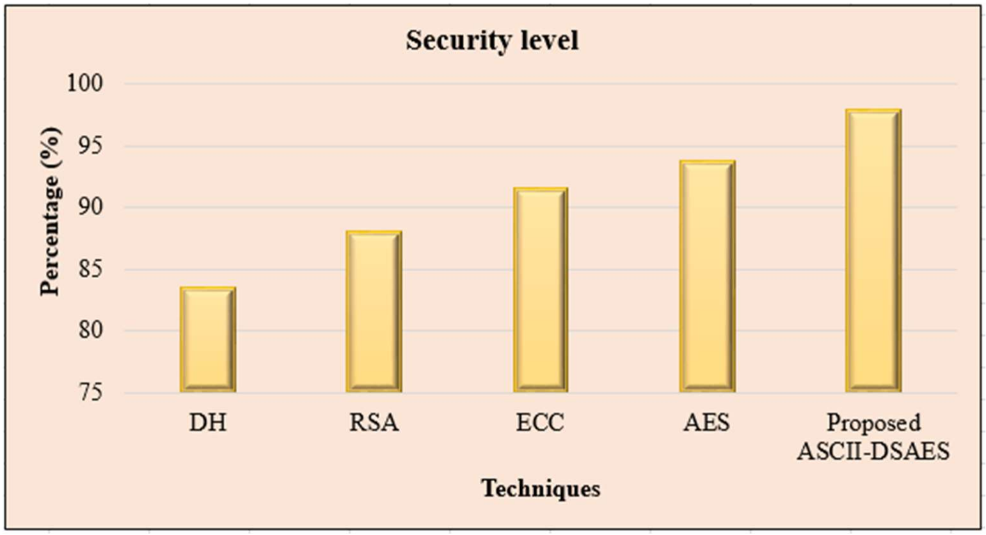


Figure 10: Security level of proposed and existing systems

Figure 10 compares the presented and conventional models' security levels. The higher security level defines that the proposed system is highly secure for DT. The security percentage achieved by the proposed ASCII-DSAES is 97.84%. Whereas, the security level for the previous AES, ECC, RSA, and DH is 93.65%, 91.45%, 87.93%, and 83.45% correspondingly, which are lower compared to the ASCII-DSAES. Hence, it is clear that the proposed framework is more secure and faster than other systems.

5. CONCLUSION

A novel WOSRCNN-centric trust model with SR along with DT protocol utilizing CLF_AVOA and ASCII-DSAES algorithms is proposed in this paper. Here, to categorize the SNs, WOSRCNN is wielded. Also, for transmitting the data securely, CLF_AVOA is utilized to identify the optimal paths. In addition, to prevent the data from any attacks, ASCII-DSAES is utilized. The outcomes display that the proposed mechanism attains the detection accuracy of 97.56%, precision of 97.14%, and recall of 97.84%. The presented technique also obtains a higher throughput (3747Bps), lesser energy consumption (1672J) with a longer network lifetime (3686ms) for 50 nodes. To withstand various attacks, the security level achieved by the proposed scheme is 97.84% with less ET (701ms) and decryption time (411ms) for 10MB of data. Therefore, the presented model is found to be strong and efficient for the estimation of trusted nodes and secure DT. By adopting more advanced systems with energy-efficient DT along with user and device authentication, this work will be improved in the future.

REFERENCES

[1] Syeda M Muzammal, Raja Kumar Murugesan and Jhanjhi N. Z, "A comprehensive review on secure routing in internet of things mitigation methods and trust based approaches", IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4186-4210, 2020.
[2] Xinying Yu, Fengyin Li, Tao Li, Nan Wu, Hua Wang and Huiyu Zhou, "Trust based secure directed diffusion routing protocol in WSN", Journal of Ambient Intelligence and Humanized Computing, vol. 13, no. 3, pp. 1405-1417, 2020.
[3] Manisha Rathee, Sushil Kumar, Amir H Gandomi, Kumar Dilip, Balamurugan Balusamy and Rizwan Patan, "Ant colony optimization based quality of service aware energy balancing secure routing algorithm for wireless sensor networks", IEEE Transactions on Engineering Management, vol. 68, no. 1, pp. 170-182, 2019.
[4] Smys S, "Energy aware security routing protocol for WSN in big data applications", Journal of IoT in Social Media Analytics and Cloud, vol. 1, no. 1, pp. 38-55, 2019.
[5] Junyao He and Feng Xu, "Research on trust based secure routing in wireless sensor networks", Journal of Physics Conference Series, vol. 1486, no. 2, pp. 1-9, 2019.

[6] Robbi Rahim, Murugan S, Priya S, Magesh S and Manikandan R, "Taylor based grey wolf optimization algorithm for energy aware secure routing protocol", International Journal of Computer Networks and Applications, vol. 7, no. 4, pp. 93-102, 2020.

[7] Surinder Singh and Hardeep Singh Saini, "Learning based security technique for selective forwarding attack in clustered WSN", Wireless Personal Communications, vol. 118, no. 3, pp. 789-814, 2021.

[8] Tayyab Khan, Karan Singh, Mohd Hilmi Hasan, Khaleel Ahmad, Thippa Reddy G, Senthilkumar Mohan and Ali Ahmadian, "ETERS a comprehensive energy aware trust based efficient routing scheme for adversarial WSNs", Future Generation Computer Systems, vol. 125, no. 6, pp. 921-943, 2021.

[9] Umashankar Ghugar, Jayaram Pradhan, Sourav Kumar Bhoi and Rashmi Ranjan Sahoo, "LB-IDS securing wireless sensor network using protocol layer trust based intrusion detection system", Journal of Computer Networks and Communications, 2019, https://doi.org/10.1155/2019/2054298.

[10] Kubra Kalkan, "SUTSEC SDN utilized trust based secure clustering in IoT", Computer Networks, vol. 178, no. 5, pp. 1-31, 2020.

[11] Pradeep Sadashiv Khot and Udaykumar Naik, "Particle water wave optimization for secure routing in wireless sensor network using cluster head selection", Wireless Personal Communications, vol. 119, no. 2, pp. 2405-2429, 2021.

[12] Liu Yang, Yinzhi Lu, Sheng Liu, Tan Guo and Zhifang Liang, "A dynamic behavior monitoring game based trust evaluation scheme for clustering in wireless sensor networks", IEEE Access, vol. 6, pp. 71404-71412, 2017.

[13] Qiong Shi, Li Qin, Yinghua Ding, Boli Xie, Jiajie Zheng and Lipeng Song, "Information aware secure routing in wireless sensor networks", Sensors, vol. 20, no. 1, pp. 1-21, 2020.

[14] Raja Waseem Anwar, Anazida Zainal, Fatma Outay, Ansar Yasar and Saleem Iqbal, "BTEM belief based trust evaluation mechanism for wireless sensor networks", Future Generation Computer Systems, vol. 96, no. 1, pp. 605-616, 2019.

[15] Chuan Xu, Zhengying Xiong, Guofeng Zhao and Shui Yu, "An energy efficient region source routing protocol for lifetime maximization in WSN", IEEE Access, vol. 7, pp. 135277-135289, 2019.

[16] Deep Kumar Bangotra, Yashwant Singh, Arvind Selwal, Nagesh Kumar and Pradeep Kumar Singh, "A trust based secure intelligent opportunistic routing protocol for wireless sensor networks", Wireless Personal Communications, 2021, https://doi.org/10.1007/s11277-021-08564-3.

[17] Osama Al Farraj, Ahmad Al Zubi and Amr Tolba, "Trust based neighbor selection using activation function for secure routing in wireless sensor networks", Journal of Ambient Intelligence and Humanized Computing, 2018, https://link.springer.com/article/10.1007/s12652-018-0885-1.

[18] Weidong Fang, Wuxiong Zhang, Wei Chen, Tao Pan, Yepeng Ni and Yinxuan Yang, "Trust based attack and defense in wireless sensor networks a survey", Wireless Communications and Mobile Computing, 2020, https://doi.org/10.1155/2020/2643546.

[19] Khalid Haseeb, Naveed Islam, Ahmad Almogren, Ikram Ud Din, Hisham N Almajed and Nadra Guizani, "Secret sharing based energy aware and multi-hop routing protocol for IoT based WSNs", IEEE Access, vol. 7, pp. 79980-79988, 2017.

[20] Hema Kumar M, Mohanraj V, Suresh Y, Senthilkumar J and Nagalalli G, "Trust aware localized routing and class based dynamic block chain encryption scheme for improved security in WSN", Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 4, pp. 5287-5295, 2020.

[21] Sujanthi S and Nithya Kalyani S, "SecDL QoS aware secure deep learning approach for dynamic cluster based routing in WSN assisted IoT", Wireless Personal Communications, vol. 114, no. 3-4, pp. 2135-2169, 2020.

[22] Deebak B. D and Fadi Al-Turjman, "A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks", Ad Hoc Networks, vol. 97, pp. 1-36, 2019.

[23] Selvi M, Thangaramya K, Sannasi Ganapathy, Kulothungan K, Khannah Nehemiah H and Kannan A, "An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks", Wireless Personal Communications, vol. 105, no. 1, pp.1475-1490, 2019.

[24] Azam Beheshtiasl and Ali Ghaffari, "Secure and trustaware routing scheme in wireless sensor networks", Wireless Personal Communications, vol. 107, no. 3-4, pp. 1799-1814, 2019.
[25] Shahana Gajala Qureshi and Shishir Kumar Shandilya, "Novel hybridized crow whale optimization and QoS based bipartite coverage routing for secure data transmission in wireless sensor networks", Journal of Intelligent & Fuzzy Systems, vol. 41, no. 1, pp. 2085-2099, 2021.