I. J. Computer Network and Information Security, **2024, 3, 1-15**
Published Online on June 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2024.03.01

Auto-metric Graph Neural Network for Attack Detection on IoT-based Smart Environment and Secure Data Transmission using Advanced Wild Horse Standard Encryption Method

Ranganath Yadawad*
Department of Computer Science and Engineering, SDM College of Engineering and Technology, Dharwad, Karnataka-580002, India
E-mail: ranganathyadawad@gmail.com
ORCID iD: https://orcid.org/0000-0001-9867-2136
*Corresponding author

Umakant P. Kulkarni
Department of Computer Science and Engineering, SDM College of Engineering and Technology, Dharwad, Karnataka-580002, India
E-mail: upkulkarni@yahoo.com
ORCID iD: https://orcid.org/0009-0002-3729-2433

Jafar A. Alzubi
Faculty of Engineering, Al-Balqa Applied University, Salt-19117, Jordan
E-mail: j.zubi@bau.edu.jo
ORCID iD: https://orcid.org/0000-0001-6724-1421

Received: 30 November 2022; Revised: 18 January 2023; Accepted: 15 February 2023; Published: 08 June 2024

Abstract: Smart cities (SCs) are being constructed with the huge placement of the Internet of Things (IoT). Real-time enhancements to life quality based on comfort and efficiency. The key concerns in most SCs that immediately impact network performance are security and privacy. Numerous approaches are proposed for secure data transmission, but the current methods do not provide high accuracy and it provide high computational time. To resolve these problems, an Auto-metric Graph Neural Network for Attack Detection and Secure Data Transmission using Optimized Enhanced Identity-Based Encryption in IoT (AGNN-AWHSE-ST-IoT) is proposed. Primarily, the input data is taken from the NSL-KDD dataset. The input data is gathered with the aid of NSL-KDD is pre-processed using three steps, crisp data conversion, splitting, and normalization. Then the Pre-processed input is fed into the Colour Harmony Algorithm (CHA) based feature selection to select the important features. After feature selection, the preferred features are given to the AGNN classifier. After classifying, the data is given to Enhanced Identity-Based Encryption (EIBE), and it is optimized using Wild Horse Optimizer (WHO) for transmitting the data more safely. The outcomes of the normal data are displayed using the LCD monitor. The AGNN-AWHSE-ST-IoT method is implemented in PYTHON. The AGNN-AWHSE-ST-IoT method attains 8.888%, 13.953%, 19.512% higher accuracy, 2.105%, 6.593%, 8.988% higher cumulative accuracy, 54.285%, 54.285%, 52.941% lower encryption time, 8.2%, 3.3%, 6.9% lower decryption time, 11.627%, 10.344%, 6.666% higher security level and 60.869%, 70% and 64% lower computational time than the existing approaches such as SBAS-ST-IoT, BDN-GWMNN-ST-IoT and DNN-LSTM-ST-IoT respectively.

Index Terms: Attack Detection, Secure Data Transmission, Color Harmony Algorithm, Auto-metric Graph Neural Network, Enhanced Identity-based Encryption, Wild Horse Optimizer.

1. Introduction

A promising technology has arisen called the Internet of Things (IoT). Each IoT product has a distinct character and may be accessed via the network [1]. To improve our social environment and personal and professional lives by

determining the status and placements of the objects and by adding services and intelligence to this expanded internet [2]. It pledges to create a world in which every object around us, commonly referred to as smart objects, is connected to the internet and communicates with one another without the need for human intervention [3]. For elders and people with disabilities, this technology offers the possibility of increasing life quality and independence at an economical cost [4]. The IoT network system uses the relevant security mechanism, including encryption, data backup, user authentication, frameworks, and instrument measures of processed and stored data. [5].

An IoT system is perfectly secure because it has all the required security mechanisms, but the reality is more complicated than that [6]. Cyberattacks on IoT networks study showed that there is still a serious problem with IoT network cyber security [7]. IoT network increment has a large increase in cyberattacks on these systems, particularly distributed denial of service attacks that have severely damaged IoT Application networks [8]. Hackers are drawn to these cyber-attacks, which are simple to implement and can target large-scale websites to be taken down [9]. Furthermore, a DDoS cyberattack negatively affects computer networks and devices and tends to make explicitly clear that registered persons of a system can access data or services [10].

The current method for detecting security threats does not reliably identify attacks. Some solutions must be proposed to address these problems to overcome them. The existing security-based attack detection method does not provide sufficient accuracy for prediction and classification, which inspired to do this research work.

The key contribution of this paperwork is summarized below,

- In this paperwork, the AGNN-AWHSE-ST-IoT Method is proposed.
- Primarily, the input data is taken from the NSL-KDD dataset.
- The input data of the NSL-KDD dataset is pre-processed. The pre-processing stage includes three stages. The splitting, crisp data conversion and normalization are performed in this process.
- The CHA is used to choose the significant features of the pre-processed data.
- After feature selection, the chosen features are fed into the Auto-metric Graph Neural Network (AGNN) classifier, it divides the selected features as as the attack and non-attack (Normal data).
- After guessing the outcomes, with the support of EIBE, they are sent to the user.
- To transmit the data safely, the EIBE is optimized with the help of Wild Horse Optimizer (WHO).
- After transmitting the data securely, the results of the normal data are showed using LCD monitor.
- The AGNN-AWHSE-ST-IoT method is implemented in PYTHON, and the efficiency of the suggested method is projected with the support of numerous evaluating metrics like accuracy, Cumulative accuracy, Computational time, Decryption Time (DT), Encryption Time (ET), and Security Level.
- The outperforms of the proposed AGNN-AWHSE-ST-IoT are likened to three existing approaches such as SBAS-ST-IoT [11], BDN-GWMNN-ST-IoT [12] and DNN-LSTM-ST-IoT [13] respectively.

The remaining manuscript is arranged as follows: Part 2 defines the Literature survey. Part 3 describes the AGNN-AWHSE-ST-IoT methodology. Part 4 explains the results and discussion. Part 5 concludes this manuscript.

2. Literature Survey

Several lessons were formerly recommended in the literature related to secure data transmission in IoT-based Smart environments. Among these, a few recent studies are expressed below,

In 2022 Manikandan VM [11] has presented a Secure-Biometric Authentication System (SBAS) for smart buildings that use adjustable data disguising through encryption for a safe procedure to convey face, body photos and fingerprints. Face and fingerprint recognition are the various modes of biometric authentication that are most widely used. Reversible Data Hiding (RDH) proposed a safe procedure for conveying face and body photos and fingerprints. An innovative methodology uses crushed fingerprint facts as a covert message secretly inserted into the face duplicate using a revocable data walloping technique. The cloud service provides the encrypted image attained for RDH through encryption for further processing. But its accuracy rate is low.

In 2021 Peneti S et al. [12] has proposed a BDN-GWMNN to maintain the security of the smart environment. Today's intelligent environment is made possible by following group networks like the IoT and 6G. The built applications are accessible by any user, making it difficult to maintain safety, secrecy, and discretion. To succeed the security of the smart environment, this study introduces Grey Wolf Optimized Modular Neural Networks (BDN-GWMNN), or blockchain-defined networks. Formerly, in IoT permitted keen submissions, the enhanced neural network is used to uphold potential and computative source consumption. But the computational time is high.

In 2022 Al Razib M [13] has proposed Cyber Threats Detection in Smart Environments with the help of SDN Framework for secure data transmission. The IoT is a rapidly advancing communicating technique that has a spectacular impact on transforming traditional network communication methods. IoT applications cover our standard of living, and IoT's connection with other technologies further widens this range of applications. When it comes to common and infrequently recurring cyber intimidations in IoT communications, DNNLSTM is accomplished offending them off. But this method provides a high error rate.

In 2021 Selvaraj R et al. [14] has presented Wide-Mouth Frog Protocol (WMFP) for protected data transmission. The IoT, which comprises numerous networked smart gadgets, has a significant impact on the creation of successful

communication. IoT device communication began using several communicating protocols, such as ZigBee and WiFi. Smart devices are vulnerable to intermediate assaults during the communication process, resulting in several communication flaws. This protocol streamlines communication while enhancing the overall integrity protocol for Internet of Things devices. The WMFP helps to lessen replay and overhearing attacks by verifying the user's identity. But the accuracy rate is low.

In 2021, Duraisamy et al. [15] has presented the Attack Detection on IoT Based Smart Cities using IDS Based Using IRSA Encryption. Because of the security flaws in IoT systems, SE applications are subject to security risks. An improved system is constructed on an intrusion detection system (IDS) to recognize attacks on IoT Smart Cities (SM). There are "2" steps in this method. They are being evaluated while they practise. Pre-processing, feature selection (FS), and classification are the first three techniques used to train the IDS. The IoT sensor data are then evaluated using the training techniques. The output of the test includes "2" models. Attacked and unattacked data are the two groups. Any data that hasn't been attacked can be delivered to the user safely using the Improved Rivest Shamir Adleman method.

In 2021, Reddy et al. [16] has presented the DNN based anomaly recognition in IoT for the applications of upcoming smart cities. Machine learning algorithms are less likely to look at performance than deep learning models. The analysis of deep learning neural network designs led to increased compute performance with respect to categorical attacks. This article's major themes include a thorough examination of investigation performance and assessments of the deep learning neural network architecture for the representation of seven categorised assaults found in the traffic trace data set from the Distributed Smart Space Orchestration System.

In 2020 Rahman et al. [17] has presented the Scalable machine learning-based intrusion detection system for IoT-enabled smart cities. In order to get over the drawback of centralised IDS for devices with limited resources, this research suggests two distributed and semi-distributed approaches that combine efficient feature extraction and selection with potential fog-edge coordinated analytics. Create distinct concurrent machine learning models that are matched to a partitioned assault dataset to divide the computational work. In the semi-distributed environment, side-by-side feature selections are made using parallel models that operate on the edge. The following stage involves a single, multi-layer, fog-side perceptron classification.

Table 1. Comparison of related works

Author	Method	Advantage	Disadvantage
Manikandan VM	SBAS bases IDS	Best classifiers are selected	Low accuracy
Peneti S et al.	BDN-GWMNN	the enhanced neural network is used to uphold potential	High computational time
Al Razib M	LSTM based IDS	Provides better accuracy	high error rate
Selvaraj R et al.	WMFP based IDS	The WMFP helps to lessen replay and overhearing attacks by verifying the user's identity	Low accuracy
Duraisamy et al.	MANFIS based IDS	Achieves highest security level	Need to compare with more classifiers
Reddy et al.	Deep learning-based IDS	Achieved good accuracy	Need to compare with more deep learning models
Rahman et al.	Machine learning (ML) based IDS	The utilization of ML methods takes the form of feature extraction.	The availability of current datasets is the primary limitation of this investigation.

Problem Formulation

Several limitations are addressed from the above-discussed methods, such as inaccurate detection results, overfitting issues and very high computational time [11-14]. Due to these issues, the detection accuracy was lowered. For secure data transmission and to overcome these issues this research work is motivated.

3. Proposed AGNN-AWHSE-ST-IOT Method

In this paperwork, AGNN-AWHSE-ST-IoT is proposed for secure data transmission. The block diagram of the AGNN-AWHSE-ST-IoT technique is given in Fig. 1. The complete discussion about Auto-Metric Graph Neural Network for Attack Detection and Secure Data Transmission using Advanced Wild Horse Standard Encryption Method is as follows.

3.1. Data Acquisition

Initially, input data is drawn from NSL-KDD. Hence, the NSL-KDD dataset is the newest form of the KDD'99 database. Then the input data is given for preprocessing [18,19].

3.2. Pre-processing

Initially, the input data is pre-processed. The pre-processing phase comprises three phases: splitting, crisp data conversion and normalization. Following a full clarification of these levels, the input data is first delivered for crisp data conversion, marked as an important transmission control protocol. Converting crisp data occurs when other data are commonly expressed as numbers. After conversion, crisp data is categorized into attack categories. Normal data is

normalized with the help of the Min-Max method after being split. Usually, normalization is used to scale data between 0 and 1 that is expressed in (1) as follows,

$$Ex_{oc} = \left\{ \left[\left[\frac{v - v_{\min}}{v_{\max} - v_{\min}} \right] \times [1-0] \right] + 0 \right\} \tag{1}$$

From (1), Ex_{oc} specifies normalized outcome, input data is represented by $v, v_{\min}$ denotes the minimum value of data, $v, v_{\max}$ indicates the maximal value of data. After preprocessing, the data is given for CHA-based feature selection.

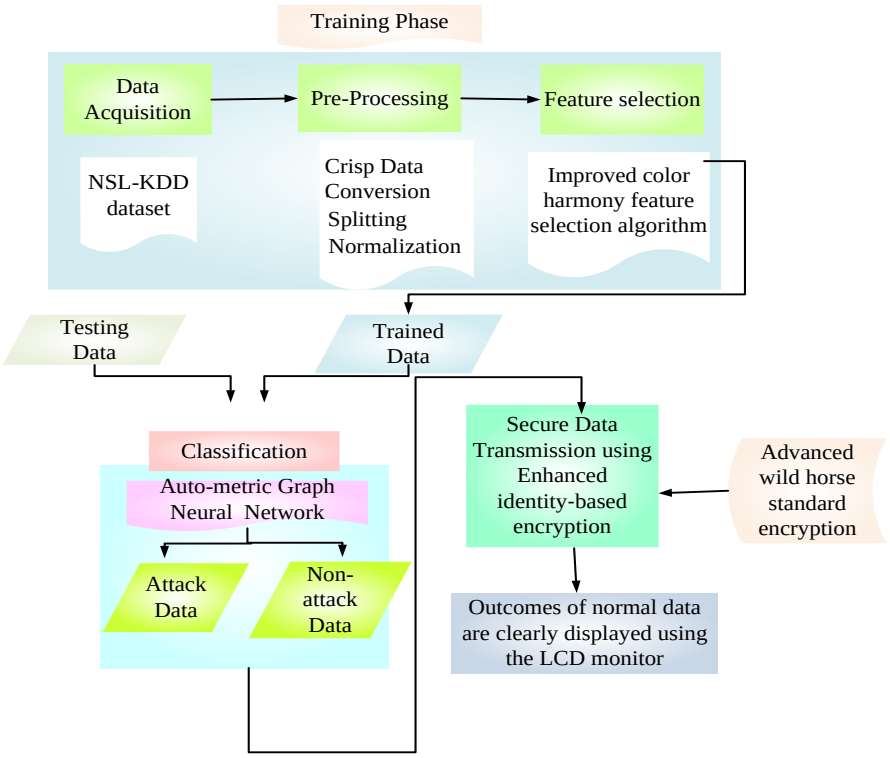

Fig.1. Block diagram of proposed AGNN-AWHSE-ST-IoT method

3.3. Feature Selection based on Color Harmony Algorithm (CHA)

The pre-processed information is then given to CHA for feature selection. Utilizing the feature selection procedure is adopted to diminish overfitting, accelerate training, and enhance detection accuracy. Additionally, making the best feature choice reduces the time needed to learn new features for arrangement. The CHA employs the useful reduced feature sets from the interruption datasets. The suggested CHA also grips nonlinear programming, continuous optimization, and single-objective optimization difficulties. Additionally, it is used to resolve optimization issues, including both restricted and unrestricted. The stepwise procedure of CHA for feature selection is detailed below.

Step 1: Initialization

Prepare the parameters of the CHA algorithm. The colours are spread at random crosswise the exploration area. The primary populace is created in a technique that populace variety is superior than or identical to the primary variety verge rate D_{th}, (2) shows the initial population generation.

$$x^0 = I^L(i) + rand.\left(I^L(i) - I^L(i)\right); \begin{matrix} a = 1,2,.....T_V \\ b = 1,2,.....T_c \end{matrix} \tag{2}$$

where $x^0(a,b)$, $I^L(i)$ and $I^U(i)$ are the primary worth for the b_{th} color, Low and high bounds of the a_{th} constraint; $rand$ is a consistently spread quantity in the intermission [0,1]; T_V and T_C resemble to the entire amount of colors and variables respectively.

Step 2: Random generation

The primary populace is generated based on the count of colors and its dimension of the problem through endless

random generation in search space.

Step 3: Fitness function (FF)

In this, the FF of the CHA is utilized for selecting the features of the dataset.

This feature is being evaluated to excite the objective function and increase feature selection performance. The fitness function is calculated with the support of (3).

$$Fitness\ \ function = \{optimal\ \ feature\ \ \ selection\} \tag{3}$$

Step 4: Concentration phase

Based on the harmonic templates, several harmonic colors are chosen in this phase, and the various contributions of each Color's qualities are then merged to create new colors. After rotation of all the stencils rendering to the situation of an explicit agent, the choice of the vocal colors from the ashen areas is completed, and then Nw_{cm} are the novel colors that formed for individual template using following (4)-(5),

$$Z^{'}(x,y) = c_1.X(A_{num}, j) + c_2.X(B_{num}, j); \begin{matrix} x = 1,2,.....Nw_{cm} \\ y = 1,2,.....N_V \end{matrix} \tag{4}$$

And

$$c_2 = 1 - c_1 \tag{5}$$

where, Z' is the grouping set c_1 and c_2 are the random-numbers in (0,1); Nw_{cm} is the whole number of groupings. $X(A_{num}, j)$ and $X(B_{num}, j)$ are components of num_{th} combination. A_{num} and B_{num} specify the sector statistics of each module. To govern investigation and clarification, the power of agent (PA), specifies sum of an agent should be seemed as a module in the mixture set Z'. Equations (6)-(9) show sum of periods an agent would be looked as a constituent in the grouping.

$$PA = \min\left(Nw_{cm}, floor\left(\frac{Iter_{cp}}{Step} \right) \right) \tag{6}$$

$$\text{where, } step = \frac{Nw_{cm} + 1}{Nw_{cm} + N_i} \tag{7}$$

$$\text{And; } N_i = \min\left(Nw_{cm}, floor\left(\frac{Iter_{dp}}{ND_{th} / Nw_{cm}} \right) \right) \tag{8}$$

$$ND_{th} = floor\left(\frac{\log\left(\frac{D_{th_f}}{D_{th_i}} \right)}{\log(damp)} \right) \tag{9}$$

The ND_{th}, $Iter_{dp}$ and $Iter_{cp}$ characterizes the four parameters of Nw_{cm}. ND_{th} is the quantity of time that D_{th_i} is increased by a continual saving issue, moist, to be identical to the last variety worth D_{th_f}, where D_{th_i} is experimentally set at $0.5max(Z'', Z')$.

Step 5: Dispersion phase

This phase is used for exploration of the search space. Equation (10) is used for exploration of search space.

$$S_X^{new}(i,j) = r_{cm} S_{CM}(i,j) + (1 - r_{cm}) S_X(i,j); \begin{matrix} i = 1,2,.....N_V \\ j = 1,2,.....N_S \end{matrix} \tag{10}$$

where S_{CM} and $S_X(j)$ are the nominated colors from X; N_s and CM is the sum of the swapped colors; r_{cm} is a weight parameter that consistently circulated in the range of $(r_{cm0}, 1)$ respectively. The weight parameter r_{cm} has a good

effect in improving the convergence behaviour in Color Harmony Algorithm for selecting the optimal features.

Step 6: Termination

Once the ideal resolution has been found from the first resolution, stop the process. If the perfect answer is not found, iteratively repeat steps 5 through 3 until the halting requirements $i = i + 1$ is satisfied. The best characteristics are chosen by CHA, and these features automatically speed up classification, cutting down on computation time. After the future selection the data is given to AGNN for classification process [20].

3.4. Classification of Data using AGNN

The selected features are given to AGNN for categorization, this technique categorizes the data as attacked and non-attacked. Employing this AGNN classifier allows for the classification of the chosen characteristics though reducing computational time, enhancing speed and accuracy by providing the AGNN classifier with the feature-extracted data for classification in relation to the training and testing phases. A fresh graph can be directly classified using the AGNN model using unknown label nodes. The remaining of this segment is ordered as follows:

- *Initialization of Graph Structure*

Samples nominated casually aids as the input X . It comprises m identified models per group. It is given in (11).

$$X = \{\{(W_1, K_1), ..., (W_{n-1}, K_{n-1})\}, \{\overline{W}\}; Z_i \in \{1, K\}\} \tag{11}$$

where W is the model, K is the label, Z is the sum of groups, and $n = Z_m + 1$. x is used to prepare the graph $G = \{N, J, Y\}$, where N characterizes the information set, J is the edge likelihood matrix, Y is the weight matrix. The primary structures of N_i is calculated using following (12),

$$N_i = [A_i, B_i, C_i, D_i,] \tag{12}$$

where, A_i is single hot encrypting of label, B_i signifies the hazard issues, C_i perceptive score for nodes, D_i characterizes the features of nodes, for bulges with unidentified labels A is a nil vector.

- *Construction of an AGNN*

Afterward finding an original graph, the input is given to the AGNN layer. It comprises two phases:

The procedure of computing the likelihood restraint with the hazard influences $p1, p2, ..., pn$ is calculated using following (13)-(14),

$$e_{r,s}^d = \begin{Bmatrix} 1, if \mid p_r^d - p_s^d \mid \leq \gamma \\ 0, otherwise \end{Bmatrix} \tag{13}$$

$$e_{r,s} = 1 \Big/ \left(M + 1 - \sum_{M=1}^{M} e_{r,s}^d \right) \tag{14}$$

where, $e_{r,s} \in [0,1]$ designates the edge mass between nodes. $e_{r,s}$ is the component of the r row and s column of the edge restraint matrix. M is the quantity of hazard issues an M denotes the M_{th} risk factor. γ is the verge to calculate the likeness in the hazard issues structures among dual samples.

And (15) is used to update the node and accruing every rationalized result.

$$Gn\left(N^{(l)}\right) = Leaky - \mathrm{Re}\, Lu\left(\sum_{B \in A^l} BN^{(l)} \theta_B^{(l)}\right) \tag{15}$$

where $N^{(l)}$ characterizes the nodes in l . $\theta_B^{(l)}$ are trainable constraints. $Leaky - ReLu$ is an irregular stimulation. It is given in (16). The output $N^{(l+1)}$ is created by adding the result to the input of AGNN.

$$N^{(l+1)} = \left[N^{(l)}, (Gn(N^{(l)})) \right] \tag{16}$$

where $N^{(l)}$ characterizes the nodes in the layer. The regularized output is the last forecast of unidentified node.

- *Loss function (LF)*

The cross-entropy loss is considered as the LF. It is given in (17).

$$\ell\left(\widehat{C},C\right)=-\sum_{Z}c_{Z}\log P(|\,\widehat{C}=c_{Z}\mid I) \tag{17}$$

where, C is the estimated outcome of unfamiliar node, $\hat{C}$ is factual label, and Z is the sum of classes.

- *Training Scheme Based on Meta-learning*

In conclusion, the class of unidentified node is attained. The system parameters U can be reorganized by the loss function ℓ. It is given in (18).

$$U_{t+1}=f(\ell_{t},U_{t}) \tag{18}$$

where, f represents the procedure that update the constraints U_t founded on ℓ_t and t signifies the training approach.

From the above expressed (18), the data type is perceived effectively. After the execution of training, the constraints are updated and attain the last outcome that helps for classifies the data as attack and non-attack data [21]. After classification the data is given to EIBE for secure data transmission.

3.5. Enhanced Identity-based Encryption (EIBE) for Secure Data Transmission

The classified data is then given to EIBE for secure data transmission. In these approaches, the users can access the data using their individuality as a method of confirmation. Also, this EIBE approach provides a security layer to protect the data and decreases the time complexities. Further, EIBE is a symmetric encryption algorithm that proves effective in more applications. However, its simple and basic algebraic structure and the same replication method encrypt all the blocks in the signal, such as loopholes that make the signal vulnerable to different kinds of attacks. Thus, encryption and decryption techniques are implemented using the generated keys. This method is firstly employed in substitution waiters for cancelling the illegal operators. The authorized users' identity is stored in proxy servers. The authorized user gets rescinded as there is no matching key for that specific individuality when accessing the server's service. Hence, every operator has to register their identity to access the provision.

Initially, generate the public key and master key. A secret parameter is selected from the finite group α_p. Select a random generator g from the cyclic group $G^{"}$, then $g\in G^{"}$, fix $g_1\in g^{\alpha}$ and choose g_2 in $G^{"}$. After selecting all security parameters, choose a random amount u_1 hence $u_1\in G_1$ and a random m distance vector, then $U_1=u_1$. Lastly, g,g_1,g_2 and u_1 are referred as public keys and $g^{\gamma}2$ as master key.

In the private key generation phase, S denotes m bits identity user, then j^{th} bits of S is represented as s_j. Identity S is created by means of selecting a random value, and r represents the random number. Therefore, the private key with identity is given in (19),

$$d_s^n=\left(g^{\gamma}2\left(u_1\prod_{j\in s}s_j\right)^{r},g^{r}\right) \tag{19}$$

In the encryption phase, t is a random parameter selected in a_p and message $Mssg(Mssg\in G_1)$. Then the encryption key corresponding to the identity S can be expressed in (20),

$$T=\left(e(g_1,g_2)Mssg,g^{t},\left(u_1\prod_{j\in s}s_j\right)^{t}\right) \tag{20}$$

where e represents the bilinear map. In the decryption phase, $T=(T_1,T_2,T_3)$ is the legal cipher text for message $Mssg$ with the operator individuality s. Then, cipher text T can be decrypted by means of $d_s^{"}=(d_1^{"},d_2^{"})$ as formulated in (21),

$$Decryption=(e(g_1,g_2)^{t}\,Mssg)\frac{e(g,(u_1\prod_{j\in s}s_j)^{rt}}{e(g_1,g_2)^{t}e(g,(u_1\prod_{j\in s}s_j)^{rt})} \tag{21}$$

Finally, the EIBE method transmits the data more safely. Hence, the achieved consequences designate that the EIBE technique has efficient data transmission. After predicting the outcome with EIBE, they are sent to the user [22]. To get more secure data transmission, the secret parameter a_p of EIBE technique is optimized using advanced WHO. The WHO algorithm is explained below,

Wild Horse Optimizer for Optimizing EIBE

WHO is used to enhance the parameters of the EIBE procedure to get the ideal parameters. Hence, these parameters are enhanced by computing the ideal parameters for protected data transmission. Firstly, the WHO creates a uniform distribution initial population. The parameters are produced randomly, and afterward initialization, it computes the suitability function. While using the foraging and navigation behaviour of the WHO optimizes the weight parameters a_p of EIBE Techniques for efficient data transmission in IoT environment. The WHO updates the finest result. Then, the procedure is repetitive until the possible best result is met. The step by step process is specified below, and the flow chart for WHO is given in Fig. 2.

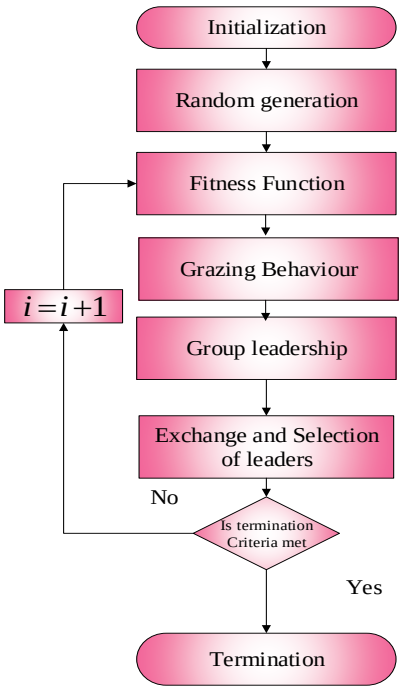

Fig.2. Flowchart of WHO

Step 1: Initialization

Initialize the parameters of the WHO. First, split this initial populace into numerous collections. If A is the number of associates of the populace, the sum of group is $B=[A\times SP]$. The SP is the ratio of stallions in the entire populace. Leader B, according to the number of groups, and the enduring followers $(A-B)$ are separated equally amongst the clusters. The leader of the clusters is erratically designated at the commencement of the procedure, and in the advanced phases, they are designated based on the group members' fitness.

Step 2: Random generation

The input restrictions are produced randomly. Hence, the values of greatest suitability for WHO are nominated based on the condition.

Step 3: FF

FF is utilized to derive the objective function. The secret parameter α_p is enhanced for effectual data transmission in IoT environment. Fitness function is measured using (22),

$$Fitness\ \ function = optimization(\alpha_p) \tag{22}$$

Step 4: Grazing behavior

To implement the grazing behavior, take stallion as the midpoint of the browsing part, and followers of the group

exploration about the midpoint. Equation (23) causes group associates to transfer and pursuit everywhere the leader with a dissimilar range.

$$\bar{X}_{i,G}^{j} = 2Z\cos(2\Pi RZ)\times(Stallion^{j} - X_{iG}^{i}) + Stallion^{j} \tag{23}$$

where Z is an adapted mechanism, $Stallion^{j}$ is the position of the stallion, R is an even random quantity that reasons the horses grazing at dissimilar perspectives of group spearhead, $\prod$ is the similar as the pi value (3.14). The cos purpose by uniting $\prod$ and R reasons movement in unlike ambit, and lastly $X_{i,G}^{i}$ is the novel location of the group affiliate when grazing. Z is an adaptive device evaluated by (24)-(26),

$$P_P = \vec{R}_1 < Td_r \tag{24}$$

$$Id_X = (P == 0); \tag{25}$$

$$Z = R_2 \Theta IDX + \vec{R}_3 \Theta(\sim IDX) \tag{26}$$

where P_P is a route equivalent to the sizes of the problematic, $\vec{R}_1$ and $\vec{R}_3$ are random paths with unchanging circulation in the range [0,1], R_2 is an arbitrary amount with undeviating circulation, Id_X index of the random path $\vec{R}_1$ proceeds which gratify the states $(P == 0)$. Td_r is an accommodate restriction that begins with a value of 1 and reductions through the implementation.

Step 5: Group leadership

The group must be led to the proper location by the group leader. Consider the water hole to be this appropriate location. This water hole must be approached by the group. In a same manner, other groups approach this water hole. Until the domination group leaves, not extra groups permitted to employ the water hole. The group leaders must direct their members to the watering hole, utilize it if their group is the dominant one, and migrate away. Equation (27) helps to approach and distance.

$$\overline{Stallion_{Gi}} = \begin{Bmatrix} 2Z\cos(2\Pi RZ)\times(WH - Stallion_{Gi}) + WH & if\ R_3 > 0.5 \\ 2Z\cos(2\Pi RZ)\times(WH - Stallion_{Gi}) - WH & if\ R_3 \le 0.5 \end{Bmatrix} \tag{27}$$

where $\overline{Stallion_{Gi}}$ is the group leaders upcoming post, WH is the water hole's position, $Stallion_{Gi}$ is the current location and an adaptive mechanism Z.

Step 6: Selection of leaders

If one of the group leaders, the situation of the spearhead and the consistent associate altered according to (28),

$$Stallion_{Gi} = \begin{Bmatrix} X_{G,i} if\ \cos(X_{G,i}) < \cos t(Stallion_{Gi}) \\ Stallion_{Gi} if\ \cos(X_{G,i}) > \cos t(Stallion_{Gi}) \end{Bmatrix} \tag{28}$$

where $Stallion_{Gi}$ is the present location of the spearhead of the i group. The weight parameter is optimized with the help of above equation, which helps to rise the effectiveness of the data transmission in the IoT environment.

Step 7: Termination

The wild horse optimizer saves the best solution. Until met the conclusion, the algorithm repeats step 5 to step 3 till the criteria time iteration $i = i + 1$ is met. Finally, EIBE transmits data more securely with the help of WHO [23].

4. Results and Discussion

In this phase, the performance of AGNN-AWHSE-ST-IoT is discussed. Hence, the AGNN-AWHSE-ST-IoT is performed in python language. Performance metrics are examined, such as accuracy, cumulative accuracy, computational time, decryption time, encryption time, and security level. The performance of the proposed AGNN-AWHSE-ST-IoT is likened with the present methods like SBAS-ST-IoT, BDN-GWMNN-ST-IoT and DNN-LSTM-ST-IoT, respectively.

4.1. Dataset Description

The NSL-KDD dataset is normally used in the field of the interruption finding system. The train and test set have unlimited records that make executing the experiments along the whole set easier. It contains 1,29,156 records for training and 19,371 records for testing. From this dataset, 50% is used for training, and 50% is employed for testing.

4.2. Performance Metrics

Several metrics are utilised to assess system performance and run tests. Performance metrics, including accuracy, cumulative accuracy, computational time, encryption time, decryption time and security level, are evaluated. Mathematical expressions and the definition of performance metrics are given below to calculate the confusion matrix,

True Positive (tp): Non-attack data is properly recognized as non-attack data.

True Negative (tn): Attack data is properly recognized as attack data.

False Positive (fp): Attack data is properly recognized as non-attack data.

False Negative (fn): Non-attack data properly recognized as attack data.

Accuracy

Accuracy is the proportion of exact prediction to the entire sum of records in the dataset, and it is determined in (29),

$$Accuracy = \frac{tp + tn}{tp + tn + fp + fn} \tag{29}$$

ET

ET is based on the encipher time of the algorithm with different data size.

DT

DT is based on the decipher time of the algorithm with different data size.

Computational Time(CT)

CT is known as the time taken to organize the data as attack and non-attack data. It is shown in (30) as follows,

$$Computational\ Time = J * CPI / P \tag{30}$$

where J denotes the sum of attacks, CPI is the cycle per instruction, and P represents the computational time.

4.3. Comparison of Proposed AGNN-AWHSE-ST-IoT with Various Existing Methods

In this section, the accuracy, cumulative accuracy, computational time, decryption time, encryption time and security level for secure data transmission in an IoT environment are analysed. Then the efficiency of the proposed AGNN-AWHSE-ST-IoT method is compared with SBAS-ST-IoT, BDN-GWMNN-ST-IoT and DNN-LSTM-ST-IoT, respectively. To predict the efficiency of the proposed design, the proposed AGNN-AWHSE-ST-IoT method is compared with the existing method using (31).

$$Performance\ of\ the\ proposed\ method = \frac{\Pr oposed - Existing}{Existing} \times 100 \tag{31}$$

Fig. 3 represents the accuracy analysis of the AGNN-AWHSE-ST-IoT method for attacked and non-attacked data. For attacked data, at node 20, the AGNN-AWHSE-ST-IoT method attains 1.123%, 2.272% and 5.882% higher accuracy than the present methods. At node 40, AGNN-AWHSE-ST-IoT method attains 2.222%, 6.976% and 9.523% higher accuracy than the present methods. At node 60, AGNN-AWHSE-ST-IoT method attains 5.617%, 10.588% and 11.253% higher accuracy than the current methods. At node 80, AGNN-AWHSE-ST-IoT method attains 6.666%, 12.941% and 16.662% higher accuracy the present methods. At node 100, the AGNN-AWHSE-ST-IoT method attains 8.888%, 13.953% and 19.512% higher accuracy than the existing methods such as SBAS-ST-IoT, BDN-GWMNN-ST-IoT and DNN-LSTM-ST-IoT, respectively.

For non-attacked data, at node 20, the AGNN-AWHSE-ST-IoT method attains 3.448%, 7.142% and 5.882% higher accuracy than the present methods. At node 40, AGNN-AWHSE-ST-IoT method attains 4.597%, 5.883% and 8.333% higher accuracy than the current methods. At node 60, the AGNN-AWHSE-ST-IoT method attains 2.222%, 5.747% and 8.235% higher accuracy than the current methods. At node 80, AGNN-AWHSE-ST-IoT method attains 2.197%, 4.494% and 13.414% higher accuracy than the present methods. At node 100, AGNN-AWHSE-ST-IoT

method attains 4.444%, 10.588% and 14.634% higher accuracy than the existing methods such as SBAS-ST-IoT, BDN-GWMNN-ST-IoT and DNN-LSTM-ST-IoT, respectively.

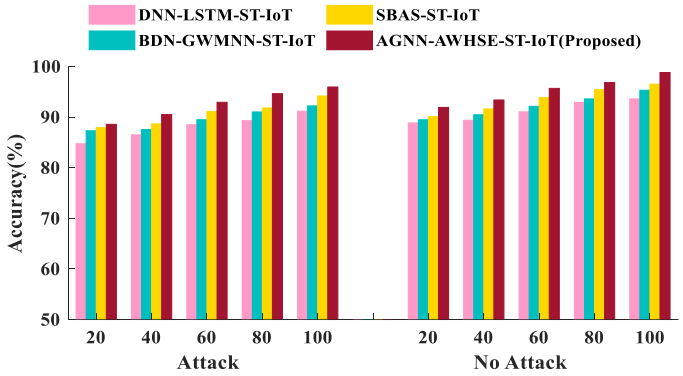

Fig.3. Accuracy analysis

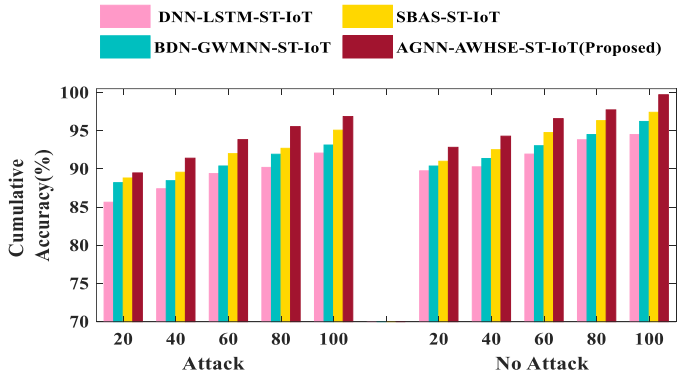

Fig.4. Cumulative accuracy analysis

Fig. 4 represents the cumulative accuracy analysis of the AGNN-AWHSE-ST-IoT method for attacked and non-attacked data. For attacked data, at node 20, the AGNN-AWHSE-ST-IoT method attains 2.298%, 3.488% and 4.705% higher cumulative accuracy than the existing methods. At node 40, the AGNN-AWHSE-ST-IoT method attains 4,545%, 5.747% and 6.976% higher cumulative accuracy than the existing methods. At node 60, the AGNN-AWHSE-ST-IoT method attains 3.296%, 6.818% and 9.302% higher cumulative accuracy than the existing methods. At node 80, the AGNN-AWHSE-ST-IoT method attains 4.395%, 5.555% and 10.465% higher cumulative accuracy than the existing methods. At node 100, the AGNN-AWHSE-ST-IoT method attains 4.347%, 6.666% and 11.344% higher cumulative accuracy than the present methods such as SBAS-ST-IoT, BDN-GWMNN-ST-IoT and DNN-LSTM-ST-IoT, respectively.

For non-attacked data, at node 20, the AGNN-AWHSE-ST-IoT method attains 2.272%, 2.298% and 3.488% higher cumulative accuracy than the existing methods. At node 40, AGNN-AWHSE-ST-IoT method attains 4.494%, 5.681% and 6.896% higher cumulative accuracy than the existing methods. At node 60, the AGNN-AWHSE-ST-IoT method attains 2.173%, 5.617% and 9.045% higher cumulative accuracy than the present methods. At node 80, the AGNN-AWHSE-ST-IoT method attains 2.156%, 4.395% and 9.195% higher cumulative accuracy than the existing methods. At node 100, the AGNN-AWHSE-ST-IoT method attains, attains 2.105%, 6.593% and 9.988% higher cumulative accuracy than the present methods such as SBAS-ST-IoT, BDN-GWMNN-ST-IoT and DNN-LSTM-ST-IoT, respectively.

Fig. 5 signifies the encryption time analysis of the AGNN-AWHSE-ST-IoT method for attacked and non-attacked data. At node 10, AGNN-AWHSE-ST-IoT method attains 50%, 66.666% and 61.538% lower encryption time than the present methods. At node 20, AGNN-AWHSE-ST-IoT method attains 60%, 64.705% and 71.428% lower encryption time than the existing methods. At node 30, the AGNN-AWHSE-ST-IoT method attains 52.173%, 56% and 54.166% lower encryption time than the present methods. At node 40, AGNN-AWHSE-ST-IoT method attains 54.285%, 54.285% and 52.941% lower encryption time than the existing methods. At node 50, the AGNN-AWHSE-ST-IoT method attains 44.444%, 46.808% and 47.916% lower encryption time than the existing methods such as SBAS-ST-IoT, BDN-GWMNN-ST-IoT and DNN-LSTM-ST-IoT, respectively.

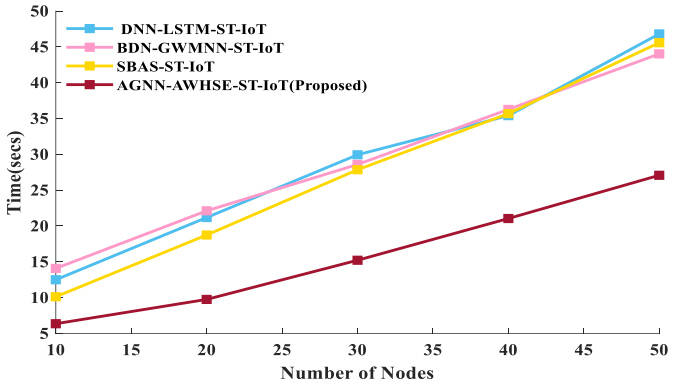

Fig.5. Encryption time analysis

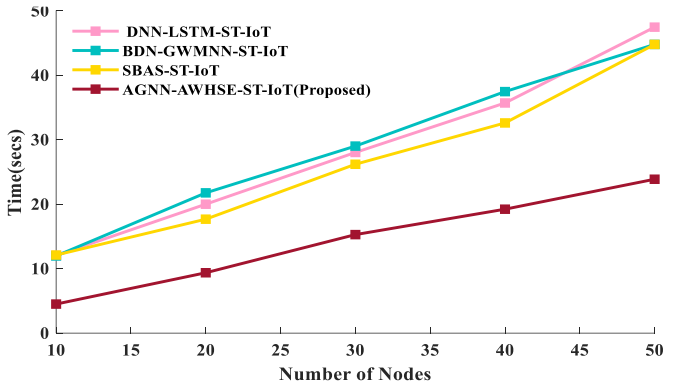

Fig.6. Decryption time analysis

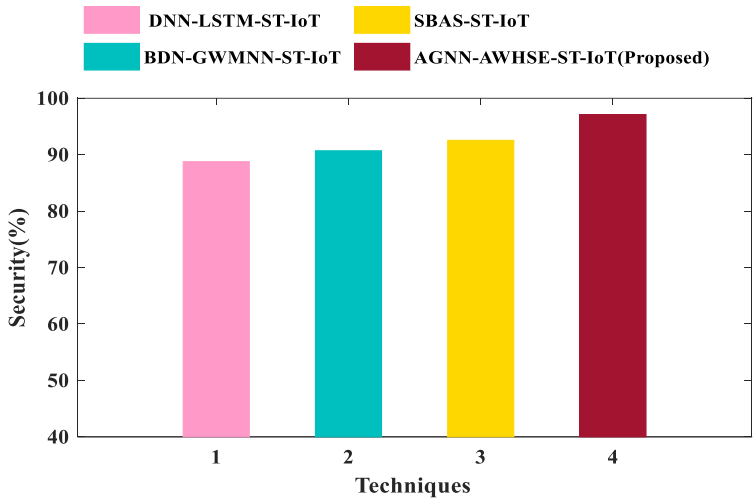

Fig.7. Security analysis

Fig. 6 denotes the decryption time analysis of AGNN-AWHSE-ST-IoT method for attacked and non-attacked data. At node 10, the AGNN-AWHSE-ST-IoT method attains 50%, 50% and 50% lower decryption time than the current methods. At node 20, the AGNN-AWHSE-ST-IoT method 50%, 64.705% and 70% lower decryption time than the present methods. At node 30, the AGNN-AWHSE-ST-IoT method attains 35.294%, 45% and 54.166% lower decryption time than the current methods. At node 40, the AGNN-AWHSE-ST-IoT method attains 27.272%, 36% and 46.666% lower decryption time than the current methods. At node 50, the AGNN-AWHSE-ST-IoT method attains 28.571%, 37.5% and 40.476% lower decryption time than the present methods such as SBAS-ST-IoT, BDN-GWMNN-ST-IoT and DNN-LSTM-ST-IoT, respectively.

Fig. 7 represents the security analysis of AGNN-AWHSE-ST-IoT with various existing methods. The proposed AGNN-AWHSE-ST-IoT method provides 11.627%, 10.344% and 6.666% higher security compared with existing methods like SBAS-ST-IoT, BDN-GWMNN-ST-IoT and DNN-LSTM-ST-IoT respectively.

Fig. 8 represents the computational time analysis of AGNN-AWHSE-ST-IoT with various methods. The proposed AGNN-AWHSE-ST-IoT method provides 60.869%, 70% and 64% lower computational time compared with existing methods like SBAS-ST-IoT, BDN-GWMNN-ST-IoT and DNN-LSTM-ST-IoT respectively.

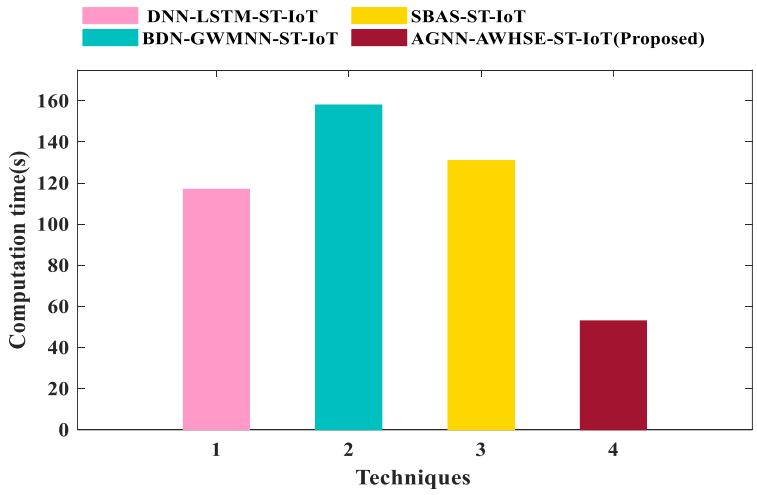

Fig.8. Computational time analysis

4.4. Overall Accuracy Analysis of Proposed Method

Table 2 shows the comparison of overall accuracy of AGNN-AWHSE-ST-IoT for attacked and non-attacked data.

Table 2. Comparison of overall accuracy of proposed method for attacked and non-attacked data

Number of nodes	AGNN-AWHSE-ST-IoT	
	Attacked Data (%)	Non-attacked data (%)
20	88	90
40	89	93
60	93	95
80	95	96
100	97	98

5. Conclusions

In this manuscript, AGNN-AWHSE-ST-IoT is effectively executed for Attack Detection and Secure Data Transmission using Optimized Enhanced Identity-Based Encryption in IoT. The AGNN-AWHSE-ST-IoT method is executed in the PYTHON platform. Further, the dataset of NSL-KDD is utilized for evaluating the performance of the AGNN-AWHSE-ST-IoT method. Here, the performance metrics, like, accuracy, computational time, encryption time, decryption time, and security level, are analyzed. And the AGNN-AWHSE-ST-IoT approach is compared with the current approaches such as SBAS-ST-IoT, BDN-GWMNN-ST-IoT and DNN-LSTM-ST-IoT respectively. The AGNN-AWHSE-ST-IoT method achieved improved performance with high accuracy compared with the existing techniques. The efficiency of the method can be improved in the future by adding new optimizations. The proposed method attains 98% accuracy, 96% cumulative accuracy, computational time-50s, encryption time-20s, decryption time-23s and 98% security level. Some unique applications, including third-party analysis of log files and detection output, which is already rather popular, may also find use for privacy improving strategies.

References

[1] S. Manimurugan, S. Al-Mutairi, M.M. Aborokbah, N. Chilamkurti, S. Ganesan, R. Patan, “Effective attack detection in internet of medical things smart environment using a deep belief neural network,” *IEEE Access*, vol. 8, pp.77396-77404, April 2020.

[2] P.K. Keserwani, M.C. Govil, E.S. Pilli, P. Govil, “A smart anomaly-based intrusion detection system for the Internet of Things (IoT) network using GWO–PSO–RF model,” *J. Reliab. Intell. Environ.* vol. 7, no. 1, pp. 3-21, March 2021.

[3] Z.A. Baig, S. Sanguanpong, S.N. Firdous, T.G. Nguyen, C. So-In, “Averaged dependence estimators for DoS attack detection in IoT networks,” *Future Gener. Comput. Syst.*, vol. 102, pp. 198-209, January 2020.

[4] V.R. Kebande, S. Alawadi, F.M. Awaysheh, J.A. Persson, “Active machine learning adversarial attack detection in the user feedback process,” *IEEE Access*, vol. 9, pp. 36908-36923, March 2021.

[5] M. Waqas, K. Kumar, A.A. Laghari, U. Saeed, M.M. Rind, A.A. Shaikh, F. Hussain, A. Rai, A.Q. Qazi, “Botnet attack detection in Internet of Things devices over cloud environment via machine learning,” *Concurr. Comput. Pract. Exp.* vol. 34, no. 4, pp. e6662, February 2022.

[6] S. Venkatraman, P. Muthusamy, B. Balusa, T. Jayasankar, G. Kavithaa, K.R. Sekar, C. Bharatiraja, “Time dependent anomaly detection system for smart environment using probabilistic timed automaton,” *J. Ambient Intell. Humaniz. Comput.* pp. 1-9, January 2021.

[7] S.V. Simpson, G. Nagarajan, "A fuzzy based co-operative blackmailing attack detection scheme for edge computing nodes in MANET-IOT environment," *Future Gener. Comput. Syst.* vol. 125, pp. 544-563, December 2021.
[8] M.J. Awan, U. Farooq, H.M. Babar, A. Yasin, H. Nobanee, M. Hussain, O. Hakeem, A.M. Zain, "Real-time DDoS attack detection system using big data approach," *Sustainability*, vol. 13, no. 19, pp. 10743, September 2021.
[9] A.A. Malibari, S.S. Alotaibi, R. Alshahrani, S. Dhahbi, R. Alabdan, F.N. Al-wesabi, A.M. Hilal, "A novel metaheuristic with deep learning enabled intrusion detection system for secured smart environment," *Sustain. Energy Technol. Assess.* vol. 52, pp. 102312, August 2022.
[10] N. Chamara, M.D. Islam, G.F. Bai, Y. Shi, Y. Ge, "Ag-IoT for crop and environment monitoring: Past, present, and future," *Agric. Syst.*, vol. 203, pp. 103497, December 2022.
[11] V.M. Manikandan, "A secure biometric authentication system for smart environment using reversible data hiding through encryption scheme," *Machine Learning for Biometrics Academic Press*, pp. 201-216, January 2022.
[12] S. Peneti, M. Sunil Kumar, S. Kallam, R. Patan, V. Bhaskar, M. Ramachandran, "BDN-GWMNN: internet of things (IoT) enabled secure smart city applications," *Wirel. Pers. Commun.* vol. 119, no. 3, pp. 2469-2485, August 2021.
[13] M. Al Razib, D. Javeed, M.T. Khan, R. Alkanhel, M.S. Muthanna, "Cyber Threats Detection in Smart Environments Using SDN-Enabled DNN-LSTM Hybrid Framework," *IEEE Access*, vol. 10, pp. 53015-53026, May 2022.
[14] R. Selvaraj, V.M. Kuthadi, S. Baskar, P.M. Shakeel, A. Ranjan, "Creating security modelling framework analysing in internet of things using EC-GSM-IoT," *Arab. J. Sci. Eng.* pp. 1-3, June 2021.
[15] A. Duraisamy, M. Subramaniam, "Attack Detection on IoT Based Smart Cities using IDS Based MANFIS Classifier and Secure Data Transmission Using IRSA Encryption," *Wirel. Pers. Commun.* vol. 119, no. 2, 2021, pp. 1913-1934.
[16] D.K. Reddy, H.S. Behera, J. Nayak, P. Vijayakumar, B. Naik, P.K. Singh, "Deep neural network based anomaly detection in Internet of Things network traffic tracking for the applications of future smart cities," *Trans. Emerg. Telecommun. Technol.* vol. 32, no. 7, 2021, p. e4121.
[17] M.A. Rahman, A.T. Asyhari, L.S. Leong, G.B. Satrya, M.H. Tao, M.F. Zolkipli, "Scalable machine learning-based intrusion detection system for IoT-enabled smart cities. *Sustain. Cities Soc.* vol. 61, 2020, p. 102324.
[18] A. Maseleno, D. Abdullah, E. Satria, F.N. Souisa, R. Rahim, An Intelligent Intrusion Detection for Smart Cities Application Based on Random Optimization with Recurrent Network. In *Artificial Intelligence Applications for Smart Societies*, Springer, Cham, 2021, pp. 119-133.
[19] W. Xu, J. Jang-Jaccard, A. Singh, Y. Wei, F. Sabrina, "Improving performance of autoencoder-based network anomaly detection on nsl-kdd dataset," *IEEE Access*, vol. 9, pp. 140136-140146, September 2021.
[20] M. Zaeimi, A. Ghoddosian, "Color harmony algorithm: an art-inspired metaheuristic for mathematical function optimization," *Soft Comput.* vol. 24, no. 16, pp. 12027-12066, August 2020.
[21] X. Song, M. Mao, X. Qian, "Auto-Metric Graph Neural Network Based on a Meta-Learning Strategy for the Diagnosis of Alzheimer's Disease," *IEEE J. Biomed. Health Inform.* vol. 25, no. 8, pp. 3141-3152, January 2021.
[22] R.K. Gupta, K.K. Almuzaini, R.K. Pateriya, K. Shah, P.K. Shukla, R. Akwafo, "An improved secure key generation using enhanced identity-based encryption for cloud computing in large-scale 5G," *Wirel. Commun. Mob. Comput.* 2022.
[23] I. Naruei, F. Keynia, "Wild horse optimizer: A new meta-heuristic algorithm for solving engineering optimization problems," *Eng. Comput.* pp.1-32, June 2021.

Authors' Profiles

Mr. Ranganath Yadawad is an Assistant Professor at SDM College of Engineering and Technology, Dharwad, Karnataka, India. He obtained his Bachelor of Engineering (BE) in Computer Science and Engineering and Master's degree (M.Tech) in Computer Science and Engineering from Visvesvaraya Technological University, Belguam, Karnataka, India. He has supervised more than 30 number of Under Graduate and Post Graduate students' projects. Currently he is a member of Board of Studies in Department of Computer Science and Engineering, SDM College of Engineering and Technology, Dharwad, Karnataka, India He is pursuing his Ph.D in the area of Internet of Things form Visvesvaraya Technological University, Belguam, Karnataka, India.

Dr. Umakant P Kulkarni is a Professor at SDM College of Engineering and Technology, Dharwad, Karnataka, India. He is coordinating NBA & IQAC activities @ Institute level. He is in teaching profession since 1989 and his expertise in teaching includes the areas like: Software Engineering, Object Oriented System Design, and Principles of Programming languages, Operating Systems, Unix Operating Systems and Distributed Systems. His research interest includes: Smart Space/ Intelligent systems and Distributed Systems. Ten research scholars have completed their PhD under his guidance. He has 50 + publications including 8 copyrights. He gives consultancy to various Institutions for preparing accreditation for NBA and NAAC under OBE framework. His special interest includes exploring more on Human Values and spiritual journey.

Jafar A. Alzubi is an Associate Professor at Al-Balqa Applied University, School of Engineering, Jordan. He received his Ph.D. degree in Advanced Telecommunications from Swansea University, Swansea – UK (2012). Jafar works and researches in multi and interdisciplinary environment involving Machine Learning, classifications and detection of Web scams, Internet of Things, Wireless Sensor Networks, and using Algebraic–Geometric theory in channel coding for wireless networks. Managed and directed few projects funded by the European Union. A cumulative research experience for over ten years, resulted in publishing more than thirty papers in highly impacted journals.

How to cite this paper: Ranganath Yadawad, Umakant P. Kulkarni, Jafar A. Alzubi, "Auto-metric Graph Neural Network for Attack Detection on IoT-based Smart Environment and Secure Data Transmission using Advanced Wild Horse Standard Encryption Method", International Journal of Computer Network and Information Security(IJCNIS), Vol.16, No.3, pp.1-15, 2024. DOI:10.5815/ijcnis.2024.03.01