IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 21 October 2023, accepted 8 December 2023, date of publication 13 December 2023,
date of current version 21 December 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3342698

RESEARCH ARTICLE

Improved Radial Movement Optimization With Fuzzy Neural Network Enabled Anomaly Detection for IoT Assisted Smart Cities

FATMA S. ALRAYES[1], WAFA MTOUAA[2], SUMAYH S. ALJAMEEL[3], MASHAEL MAASHI[4], MOHAMMED RIZWANULLAH[5], AND AHMED S. SALAMA[6]

[1]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[2]Department of Mathematics, Faculty of Sciences and Arts, King Khalid University, Muhayil, Asir 61421, Saudi Arabia
[3]Saudi Aramco Cybersecurity Chair, Department of Computer Science, College of Computer Science and Information Technology, Imam Abdulrahman bin Faisal University, Dammam 31441, Saudi Arabia
[4]Department of Software Engineering, College of Computer and Information Sciences, King Saud University, P.O. Box 103786, Riyadh 11543, Saudi Arabia
[5]Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam bin Abdulaziz University, Al-Kharj 16278, Saudi Arabia
[6]Department of Electrical Engineering, Faculty of Engineering & Technology, Future University in Egypt, New Cairo 11845, Egypt

Corresponding author: Mohammed Rizwanullah (r.mohammed@psau.edu.sa)

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through large group Research Project under grant number (RGP2/56 /44). Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R319), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. Research Supporting Project number (RSPD2023R787), King Saud University, Riyadh, Saudi Arabia. We Would like to thank SAUDI ARAMCO Cybersecurity Chair for funding this project. This study is supported via funding from Prince Sattam bin Abdulaziz University project number (PSAU/2023/R/1444). This study is partially funded by the Future University in Egypt (FUE).

ABSTRACT Recently, an extensive implementation of the recent Internet of Things (IoT) model has resulted in the development of smart cities. The network traffic of smart cities using loT systems has developed rapidly and established novel cybersecurity problems later these loT devices are linked to sensors that are directly linked to huge cloud servers. Unfortunately, IoT systems and networks can be identified as extremely exposed to security attacks that aim at service accessibility and data integrity. Additionally, the heterogeneity of data gathered in distinct IoT devices, composed of the disturbances acquired in the IoT systems, renders the recognition of anomalous performance and threatened nodes very difficult related to typical Information Technology (IT) networks. Accordingly, there is a critical requirement for reliable and effectual anomaly detection (AD) for identifying malicious data to promise that it could not be utilized in IoT lead to decision support systems (DSS). This manuscript offers an Improved Radial Movement Optimization with Fuzzy Neural Network Enabled Anomaly Detection (IRMOFNN-AD) technique for IoT Assisted Smart Cities. The main purpose of the IRMOFNN-AD algorithm lies in the accurate and automated detection of the anomalies that exist in the IoT environment. For the feature selection process, the IRMOFNN-AD technique uses the IRMO system to elect an optimum set of features. Additionally, the IRMOFNN-AD algorithm applies the FNN model for the detection and classification of anomalies. Besides, the sine cosine algorithm (SCA) has been employed for the parameter tuning of the FNN algorithm. The simulation value of the IRMOFNN-AD system has been tested on benchmark IDS datasets. The extensive results illustrate the better detection outcomes of the IRMOFNN-AD system interms of different measures.

INDEX TERMS Anomaly detection, smart cities, fuzzy neural network, Internet of Things, security, feature selection.

I. INTRODUCTION

The Internet of Things (IoT) has become a crucial module of several Information and Communications Technology (ICT) systems [1]. It has carried new service models through various domains namely diverse smart city applications, wearable medical devices, and autonomous transportation. IoT-based devices are embedded with sensors, which transfer data to the cloud for performing data analytics and producing control solutions relevant to cyber-physical systems (CPS) [2].

The associate editor coordinating the review of this manuscript and approving it for publication was Giovanni Pau.

In accordance with the current statistics, it is presently above 26 billion interconnected and dynamic IoT devices all over the world. Various IoT devices can be predicted to rise and attain 75 billion in 2025. Several IoT devices have been employed by organizations for improving productivity and security [3]. For instance, manufacturers utilize IoT-based solutions for analyzing massive quantities of data taken by sensor devices incorporated into manufacturer's tools to allow analysts and data scientists to prevent and predict serious and real-world issues like engine failures and other cases [4]. It permits manufacturers to considerably improve security and productivity. Recently, the security of IoT devices has involved enormous research work [5]. IoT systems are utilized for processing, collecting, and generating data that major cases including sensitive data, making them mainly vulnerable to major security attacks that are employed by attackers [6]. As a result, the reliability of the information collected by IoT devices must be secure in the real world, generating the development of efficient anomaly detection (AD) methods highly significant.

Several novel anomalies (both new and the mutation of a previous anomaly) are often produced because of the existence of a large quantity of data [7]. Therefore, an intrusion detection system (IDS) could be performed as another line of defence, which offers more safety to an IoT network against security threats. IDS is categorized depending on the identification technique and deployment approach [8]. IDS has a host-based IDS (HIDS) and network-based IDS (NIDS) relies on its utilization however, it also includes AD-based, specification-based, signature-based or hybrid detection dependent upon the identification technique. In this study, attention is to offering safety to the IoT at access points by modifying the NIDS by employing the AD-based identification approach [9]. The major issues in existing IDSs are improved in the False Alarm Rate (FAR) for identifying the zero-day anomalies. Researcher workers are currently examining the probability of utilizing DL and ML algorithms for enhancing identification accurateness and decreasing the FAR for NIDS. Researchers can determine both DL and ML approaches are effective tools to learn useful models from the network traffic for classifying the flows as normal or anomalies [10]. The DL method exhibited the effectiveness of learning useful features from the raw data because of their deep framework with no human intervention, emphasizing their important application within NIDS for IoT networks.

This manuscript offers an Improved Radial Movement Optimization with Fuzzy Neural Network Enabled Anomaly Detection (IRMOFNN-AD) technique for IoT Assisted Smart Cities. The main purpose of the IRMOFNN-AD system lies in the accurate and automated detection of the anomalies that exist in the IoT environment. For the feature selection (FS) process, the IRMOFNN-AD technique uses the IRMO system to elect an optimum set of features. Moreover, the IRMOFNN-AD methodology applies the FNN model for the identification and classification of anomalies. Additionally, the sine cosine algorithm (SCA) can be employed for the parameter tuning of the FNN algorithm. The simulation value of the IRMOFNN-AD algorithm has been tested on benchmark IDS datasets.

In summary, the key contributions of the IRMOFNN-AD technique are given as follows.

- Develop an automated anomaly detection approach named the IRMOFNN-AD technique to accurately detect anomalies in IoT-assisted Smart Cities. To the best of our knowledge, the IRMOFNN-AD technique never existed in the literature.
- Design a new IRMO technique to select highly related and useful features from the IoT data, decreasing dimensionality and improving the efficiency of the anomaly detection process.
- Apply the FNN model for the identification and classification of anomalies, which is appropriate to handle uncertainty and non-linearity in data, which is mainly related to the IoT environment where data can be noisy and complex.
- To further enhance the performance of the FNN algorithm, the manuscript introduces the use of SCA for parameter tuning for better anomaly detection results.

II. RELATED WORKS

Khayyat [11] presented an Improved Bacterial Foraging Optimizer with optimal DL for AD (IBFO-ODLAD) from the IoT network. For the FS method, the IBFO-ODLAD approach develops the IBFO method to select optimum feature subsets. Additionally, the IBFO-ODLAD approach utilizes a multiplicative LSTM (MLSTM) algorithm for intrusion recognition and classification methods. Moreover, the BOA could be implemented for optimum hyperparameters by choosing the MLSTM technique. In [12], a new architecture was developed for AD through edge-assisted IoTs. A new effective and unsupervised DL approach was established to equalize accuracy and resource utilization for AD dependent upon the integration of an adversarial training and convolutional autoencoder (CAE).

Ragab and Sabir [13] designed the IoTs Assisted-DL Enabled AD approach for Smart City Infrastructures called (IoTAD-SCI) method. Furthermore, the IoTAD-SCI algorithm contains a Deep Consensus Network (DCN) framework developed for identifying the anomalies in input video frames. Additionally, AOA has been implemented for tuning the hyperparameters of the DCN framework. In [14], to overcome the IoT cybersecurity attacks in a smart city, the authors presented an AD-IoT technique, which has intelligent AD relies on RF and ML methods. This presented outcome can effectively recognize compromised IoT devices at allocated fog nodes.

The authors [15] introduced a novel green energy-efficient routing with a DL-based AD (GEER-DLAD) method for IoT applications. Additionally, the moth flame swarm optimizer (MSO) method was implemented for optimally select routes from the network. Further, the DLAD procedure occurs through the RNN-LSTM technique for AD from the

IoT communication networks. In [16], the authors focus on the AD issue of smart city facilities and differentiate various anomalies of communication in an efficient manner that has targeted to secure the data confidentiality of users. Besides, the authors introduced an AI-based Improved-LSTM (I-LSTM)-NN to enhance the time aspect and utilize a new smooth activation function that could increase the effectiveness of multi-classification for AD. Hazman et al. [17] suggested AD, robust IDS for IoT-based smart settings that employ Ensemble Learning. In general, the model provided an optimal AD technique, which integrates AdaBoost and combines numerous FS methods Boruta, mutual data, and correlation. Islam et al. [18] proposed an effective and robust system for identifying anomalies in monitoring huge video data. The CNN could be utilized as feature extraction in the input videos that are further stored to AE for feature enhancement and then ESN for anomalous activities detection and sequence learning.

Ullah et al. [19] examine an effectual and robust structure for recognizing anomalies in surveillance Big Video Data (BVD) utilizing AI of Things (AIoT). Smart surveillance is a vital application of AIoT and it can be presented as a 2-stream NN in this way. He et al. [20] present an Attention-based Convolution Recurrent Encoder-Decoder (ACRED) that is effective for addressing anomaly detection and predicting problems in time sequences. Chen et al. [21] proposed GTA, a novel structure for multiple variate time-series AD that automatically learns a graph design, graph convolutional, and modeling temporal dependency utilizing a transformer-based structure. In [22], the authors develop and design new anomaly-based IDS for IoT networks. Primarily, a CNN approach can be utilized for creating a multiple-class classifier model. The presented approach is then executed utilizing CNNs in 1D, 2D, and 3D.

Even though numerous techniques exist in the literature, a prominent research gap in the field of AD within the IoT platform is the serious requirement for efficient feature selection (FS) methods and superior parameter tuning algorithms. However, IoT systems produce massive quantities of data; the complex nature of these data streams often overcomes standard AD approaches. Recent techniques often shortage the ability to automatically select the major important features from this data overflow, which leads to computational inefficiency and possibly hiding genuine anomalies in the noise. Additionally, parameter tuning is a significant issue, as fine-tuning the hyperparameters of identification methods to ensemble the dynamic and variety of IoT data sources is a difficult and time-consuming method. Connecting this gap by evolving innovative approaches for FS and parameter tuning is essential for improving the effectiveness and accuracy of AD in IoT platforms, eventually confirming the security and reliability of interconnected devices and systems in the IoT.

III. THE PROPOSED MODEL

In this manuscript, we have devised an automated AD utilizing the IRMOFNN-AD algorithm for IoT Assisted Smart Cities. The main purpose of the IRMOFNN-AD approach lies in the accurate and automated detection of the anomalies that exist from the IoT platform. It comprises 3-phases of operations namely IMRFO feature subset selection, FNN classification, and SCA-based parameter tuning. Fig. 1 demonstrates the entire procedure of the IRMOFNN-AD algorithm.

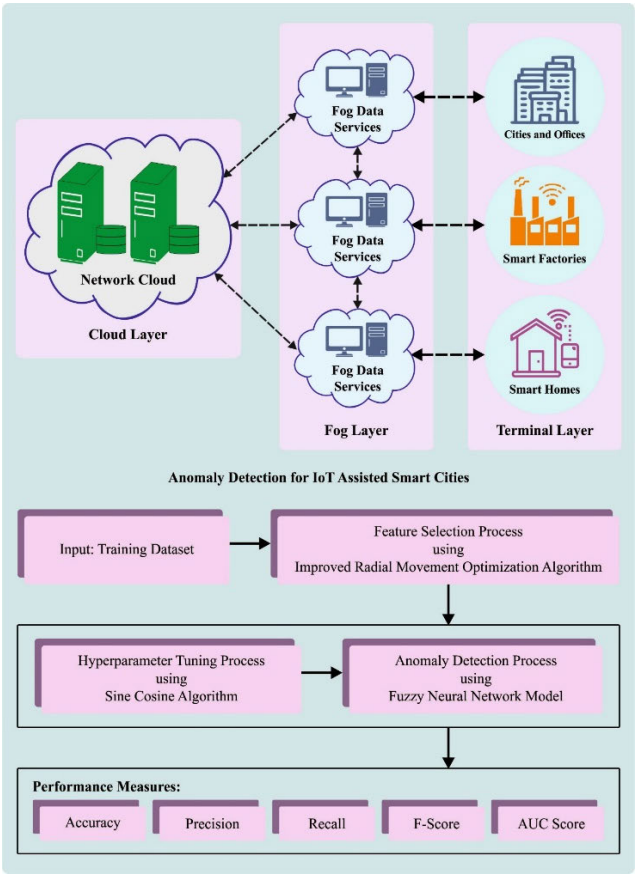

FIGURE 1. Overall flow of IRMOFNN-AD system.

A. STAGE I: IRMO-BASED FS APPROACH

For the FS process, the IRMOFNN-AD method uses the IRMO system to elect an optimum set of features. IRMO approach simulates a group of particles $[X_M, N]$ that moves with the centre particle towards the best location spontaneously [23]. The particles situated in the search space is N-dimensional vector assessed by fitness function (FF). IRMO can automatically update the centre and larger particles by comparing all the fitness values as generation upsurges. The outcomes are always upgraded as the generation increases and moves in the global optimum direction.

1) GENERATION OF THE INITIAL PARTICLE GROUP

In IRMO, a primary M particle, N-dimensional vectors are represented as a matrix $[X_{M,N}]$ for storing the location information of the particles about the FF variable. According to

Eq. (2) every dimension is generated randomly, where the upper limit max and x_j lower limit $\min x_j\,(1 \le j \le N)$ are set beforehand. By comparing and calculating the fitness values of initial particles, the optimum location in the primary particle group has been considered as the first global optimum location *Gbest* and the initial centre $Centre^1$.

$$X_{M,N} = \begin{bmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,N-1} & x_{1,N} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,N-1} & x_{2,N} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{M,1} & x_{M,2} & \cdots & x_{M,N-1} & x_{M,N} \end{bmatrix} \tag{1}$$

$$x_{ij} = \min x_j + rand\,(0,\,1) \times \left(\max x_j - \min x_j\right) \tag{2}$$

Update the particle group

Two random parameters r_1 & r_2 determine whether the newest particle location can be updated by the central location or directly inherited to optimize the self-feedback of particles. If $r_1 < MRorr_1 < w^k/w$, the newest position is generated by Eq. (3); or else, by Eq. (4). Evaluate the fitness value $f\left(X_i^k\right)$ of $x_{i,j}^k$, and the optimum fitness values of the novel group are kept as $Rbest^k$. If it can be greater than the present *Gbest* value, then upgrade the global optimum location *Gbest*.

$$x_{i,j}^k = w^k \cdot rand\,(-0.5,\,0.5) \times \left(\max x_j - \min x_j\right) + Centre_{j^{k-1}} \tag{3}$$

$$x_{ij}^k = x_{ij}^{k-1} \tag{4}$$

In Eq. (3), w^k refers to the inertia weight reducing with the increasing generation, and k indicates the present generation.

Radial movement of central position

The central location $Centre^k$ moves with the current optimum location $Rbest^{k-1}$ and global optimum location *Gbest*, the coefficients C_1 and C_2 affect the accuracy and convergence rate of the model., C_1 and C_2 are set to 0.4 and 0.5 correspondingly.

$$Centre^k = Centre^{k-1} + C_1\left(Gbest - Centre^{k-1}\right) + C_2\left(Rbest^{k-1} - Centre^{k-1}\right) \tag{5}$$

The computation stops once the final generation has been evaluated. The fitness values of global place *Gbest* are the optimum solution, with the fitness value and optimum location data.

2) DYNAMIC INERTIA WEIGHT APPROACH

The optimizing and searching solution of the model is usually controlled by inertia weighted. In the beginning, the model aims at global searching, while it achieves the best results in radial searching with the decreasing inertia weighted. The iterative procedure of implicit expression of slope F_S depends on the Rigorous Janbu technique is nonlinear and very challenging. Such a dynamic inertia-weighted model was introduced to replace the linearly reducing inertia-weight model as follows.

$$w^{k+1} = w_{\max} - (w_{\max} - w_{\min}) \cdot \left[\frac{2k}{G} - \left(\frac{k}{G}\right)^2\right], \quad \left(\frac{f\,(Gbest)}{f\left(Rbest^k\right)}\right) \ge W \tag{6}$$

$$w^{k+1} = w_{\max} - (w_{\max} - w_{\min}) \cdot \left(\frac{k}{G}\right)^2, \frac{f\,(Gbest)}{f\left(Rbest^k\right)} < W \tag{7}$$

where G indicates the overall iterations, $w_{\max}$ and $w_{\min}$ denote the upper and lower limits of inertia weight, $f\,(Gbest)$ shows the fitness values of global optima, $Rbest^k$ represents the fitness value of current optimal in existing generation k, W shows the judgment co-efficient set.

If the $f\,(Gbest)\,/f\left(Rbest^k\right)$ value is greater than judgment co-efficient W, then the particle group can be positioned in the best location. Using the dynamic inertia weight model, it adjusts the optimizing approach for adapting the nonlinear complex variation in resolving objective function in IRMO to enhance the optimization outcome for the multi-dimensional complex objective function.

In the IRMO algorithm, the average dimensions of the dataset for classification (viz., supervised learning) are $N_S \times N_F$, where N_S represents the overall amount of samples, and N_F denotes the amount of features. To achieve this, the FS model first splits the N_F subset of features into small set (S) whose combined dimension is smaller than N_F:

$$Fit = \lambda \times \gamma s + (1 - \lambda) \times \left(\frac{|S|}{N_F}\right) \tag{8}$$

In Eq. (8), The selected feature is represented as $|S|$, and the classification error can be represented as γ_S. The parameter λ is chosen between zero and one, and the balance between $\left(\frac{|S|}{N_F}\right)$ and γ_S.

B. STAGE II: FNN-BASED CLASSIFICATION

At this stage, the FNN model is used for the classification of anomalies. FNN is a powerful and effectual mechanism to recognize supervised learning and modelling [24]. FNN contains of membership function (MF) layer, rule layer, input layer, and output layer. Fig. 2 depicts the infrastructure of FNN.

Input layer: The input layer receives $x = [x_1, x_2, \ldots, x_n]$, and the size of the input vector signifies the neuron counts from the input layer.

Membership function layer: In the MF layer, all the neurons are lingual variables which evaluate the degree of membership. The MF layer is as follows:

$$f_{ij} = e^{-\frac{(x_i - c_{ij})^2}{\sigma_{ij}^2}}, \tag{9}$$

Here c_{ij} and σ_{ij} represent the center and width of the j^{th} membership Gaussian function of x_i, correspondingly. The MF f_{ij} represents the i^{th} input belonging to the j^{th} fuzzy set.

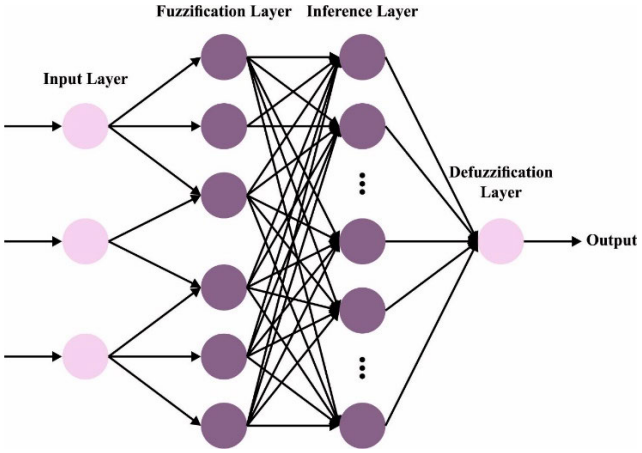

FIGURE 2. Architecture of FNN.

Rule layer: All the neurons are a fuzzy rule, where the outcome is activation intensity as follows:

$$a_j = f_{1j}(x_1) f_{2j}(x_2) \cdots f_{nj}(x_n), \tag{10}$$

$$\overline{a}_j = \frac{a_j}{\sum_{j=1}^{r} a_j}, \tag{11}$$

where $\overline{a}$ is the normalized value, and$r$ refers to the neuron counts from the rule layer.

Output layer: The output layer identifies the last output computation, it can be expressed as:

$$y = \sum_{j=1}^{r} w_j \overline{a}_j \tag{12}$$

In Eq. (12), y refers to the resultant of FNN, and w_j indicates the weighted connection rule and output layers.

In this work, the objective is to train the weight-connected rule and resultant layers w_j, center c_{ij} and width σ_{ij} of j^{th} membership Gaussian function of x_i.

C. STAGE III: PARAMETER TUNING USING SCA

Lastly, the parameter tuning of the FNN method takes place using the SCA. SCA follows an SC oscillate function is vital to determining the optimum position of the solution [25]. The following random variable is used to express SC operations.

- The direction of motion.
- The position of the movements.
- Emphasize/de-emphasize the destination effects.
- The swapping amongst the sines and cosines modules.

Using the following equation, the updating procedure of the candidate solution is performed.

$$P(t+1) = \begin{cases} P(t) + r_5.sin(r_6).\left|r_7 S^*(t) - S(t)\right| \\ P(t) + r_5.cos(r6).\left|r_7 S^*(t) - S(t)\right| \\ rr_4 4 \geq 0.5 < 0.5 \end{cases} \tag{13}$$

In Eq. (13), t denotes the number of search iterations . This method tracks two significant performances: the best performance, represented as S^*, and the current performance, represented as S. Random parameters r_4, r_6, and r_7 are assigned values within [0, 1]. As they affect the solution's position, this random variable plays an essential role in the algorithm. Particularly, the equation shows that the position of the obtained best solution affects the present solution. This impact enables the exploration of searching space and upsurges the probability of converging toward an optimum performance. In the iteration process, the values of r_4 are updated dynamically based on Eq. (14), further improving the search process.

$$r_4 = a - \frac{a \times t}{t_{\max}} \tag{14}$$

In Eq. (14), a refers to a constant, t and $t_{\max}$ correspondingly indicates the existing and maximal iterations.

The SCA is a resilient meta-heuristic technique that uses a single optimum solution for guiding the other solutions. This method contributes toward a noticeable decline in memory usage and convergence time, which distinguishes it from other approaches.

The fitness optimal is a key aspect of the SCA algorithm. Solution encoding has been employed to assess the better of candidate results. Presently, the accuracy value is the major condition deployed to design an FF.

$$Fitness = \max(P) \tag{15}$$

$$P = \frac{TP}{TP + FP} \tag{16}$$

whereas, FP and TP denote the false and true positive values.

IV. RESULTS AND DISCUSSION

The simulation validation of the IRMOFNN-AD approach has been tested using the UNSW NB-15 database [26] and the UCI SECOM database [27]. The data contains 42 features and the proposed approach elected a group of 16 features. Also, the data takes 10 classes composed of 1 normal and 9 attacks. Afterwards, the UCI SECOM database was collected in semiconductor industries. The data take 1567 instances with 591 features. The data contains 2 class labels that fail and pass with 104 and 1463 instances. The proposed methodology has elected a group of 198 features in the data.

Table 1 and Fig. 3 represent the AD outcome of the IRMOFNN-AD system on the dataset1.

The result highlighted the proficient recognition of all anomalies. On the 70% TR set, the IRMOFNN-AD technique offers average $accu_y$,$prec_n$, $reca_l$, F_{score}, and AUC_{score} of 99.06%, 95.29%, 95.29%, 95.28%, and 97.38% respectively. Also, on the 30% TS set, the IRMOFNN-AD system attains average $accu_y$,$prec_n$, $reca_l$, F_{score}, and AUC_{score} of 98.93%, 94.70%, 94.64%, 94.66%, and 97.03% respectively.

Fig. 4 shows the training accuracy TR_accu_y and VL_accu_y of the IRMOFNN-AD technique on dataset1. The TL_accu_y is determined by the assessment of the IRMOFNN-AD approach on the TR database while the VL_accu_y is calculated by evaluating the outcome on a discrete testing database. The outcomes exhibit that TR_accu_y and VL_accu_y increase

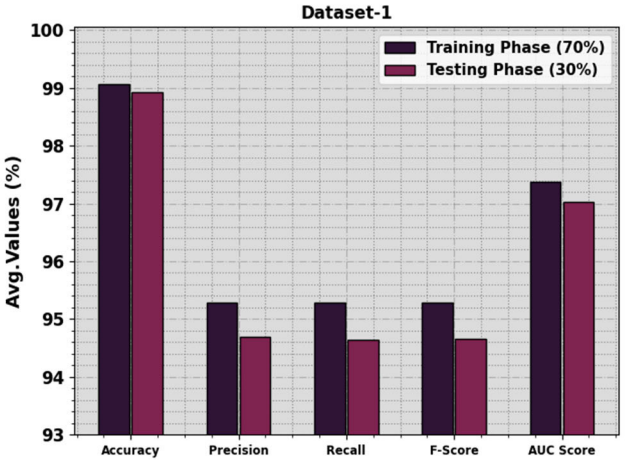

FIGURE 3. Average of IRMOFNN-AD methodology on dataset1.

TABLE 1. AD outcome of IRMOFNN-AD system on dataset1.

Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}	AUC_{Score}
TR set (70%)					
Normal	99.03	95.68	94.59	95.13	97.06
Generic	99.29	95.28	97.72	96.48	98.59
Exploits	99.31	96.33	96.88	96.60	98.23
Fuzzers	99.26	97.14	95.51	96.32	97.59
DoS	98.86	94.87	93.80	94.33	96.62
Reconnaissance	99.03	94.69	95.76	95.22	97.58
Analysis	99.00	93.82	96.25	95.02	97.78
Backdoor	98.97	95.77	93.51	94.63	96.53
Shellcode	99.06	94.19	96.14	95.15	97.76
Worms	98.77	95.13	92.74	93.92	96.10
Average	99.06	95.29	95.29	95.28	97.38
TS set (30%)					
Normal	98.87	94.59	93.96	94.28	96.68
Generic	98.93	94.04	95.30	94.67	97.32
Exploits	98.73	94.48	92.57	93.52	95.99
Fuzzers	99.13	96.45	94.44	95.44	97.04
DoS	99.07	94.56	95.86	95.21	97.64
Reconnaissance	99.07	93.42	97.26	95.30	98.26
Analysis	98.67	95.24	91.50	93.33	95.49
Backdoor	98.73	92.26	96.27	94.22	97.65
Shellcode	99.20	96.32	96.32	96.32	97.94
Worms	98.93	95.65	92.96	94.29	96.26
Average	98.93	94.70	94.64	94.66	97.03

with an upsurge in epochs. As a result, the performance of the IRMOFNN-AD technique improves on the TR and TS database with an upsurge in the count of epochs.

In Fig. 5, the *TR_loss* and *VR_loss* results of the IRMOFNN-AD technique on dataset1 are shown. The *TR_loss* defines the error between the predictive performance and original values on the TR data. The *VR_loss* represent the measure of the performance of the IRMOFNN-AD methodology on separate validation data. The results indicate that

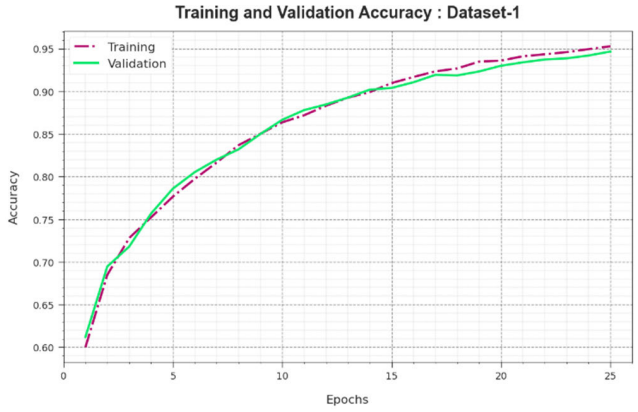

FIGURE 4. $Accu_y$ curve of IRMOFNN-AD methodology on dataset1.

FIGURE 5. Loss curve of IRMOFNN-AD methodology on dataset1.

the *TR_loss* and *VR_loss* tend to decrease with rising epochs. It represented the better solution of the IRMOFNN-AD method and its ability to create a correct classification. The lesser value of *TR_loss* and *VR_loss* reveals the enhanced outcome of the IRMOFNN-AD technique on capturing designs and relationships.

Table 2 and Fig. 6 represent the AD outcome of the IRMOFNN-AD algorithm on the dataset2. The simulation value denoted the proficient detection of all anomalies. On 70% TR set, the IRMOFNN-AD system attains average $accu_y$,$prec_n$, $reca_l$, F_{score}, and AUC_{score} of 98.26%, 98.31%, 98.26%, 98.28%, and 98.26% correspondingly. Similarly, on the 30% TS set, the IRMOFNN-AD approach gains average $accu_y$,$prec_n$, $reca_l$, F_{score}, and AUC_{score} of 99.02%, 98.96%, 99.02%, 98.99%, and 99.02% correspondingly.

Fig. 7 illustrates the training accuracy TR_accu_y and VL_accu_y of the IRMOFNN-AD algorithm on dataset2. The TL_accu_y is defined by the estimate of the IRMOFNN-AD approach on the TR database but the VL_accu_y is calculated by evaluating the outcome on a distinct testing dataset. The outcomes exhibit that TR_accu_y and VL_accu_y increase with an upsurge in epochs. Consequently, the solution of the IRMOFNN-AD system improves the TR and TS database with an upsurge in the count of epochs.

TABLE 2. AD outcome of IRMOFNN-AD system on dataset2.

Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}	AUC_{Score}
TR set (70%)					
Class-1	98.90	97.83	98.90	98.37	98.26
Class-2	97.61	98.79	97.61	98.20	98.26
Average	98.26	98.31	98.26	98.28	98.26
TS set (30%)					
Class-1	99.26	98.53	99.26	98.89	99.02
Class-2	98.79	99.39	98.79	99.09	99.02
Average	99.02	98.96	99.02	98.99	99.02

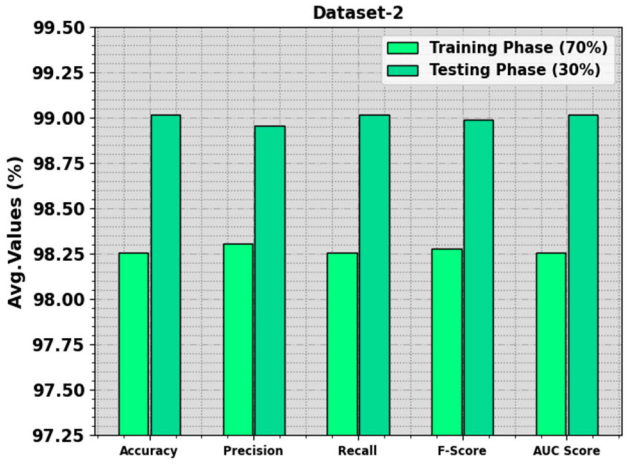

FIGURE 6. Average of IRMOFNN-AD methodology on dataset2.

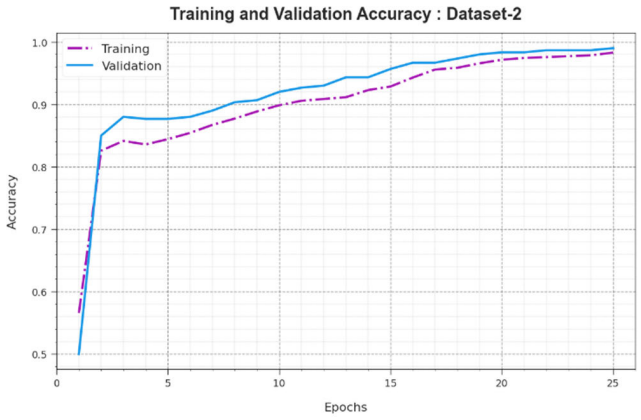

FIGURE 7. $Accu_y$ curve of IRMOFNN-AD methodology on dataset2.

In Fig. 8, the *TR_loss* and *VR_loss* outcomes of the IRMOFNN-AD method on dataset2 are exposed. The *TR_loss* determines the error between the predictive outcome and original values on the TR data. The *VR_loss* signify the measure of the performance of the IRMOFNN-AD algorithm on individual validation database. The results indicate that the *TR_loss* and *VR_loss* tend to decline with rising epochs. It depicted the higher solution of the IRMOFNN-AD algorithm and its ability to generate exact classification. The lesser value of *TR_loss* and *VR_loss* exhibits the enhanced

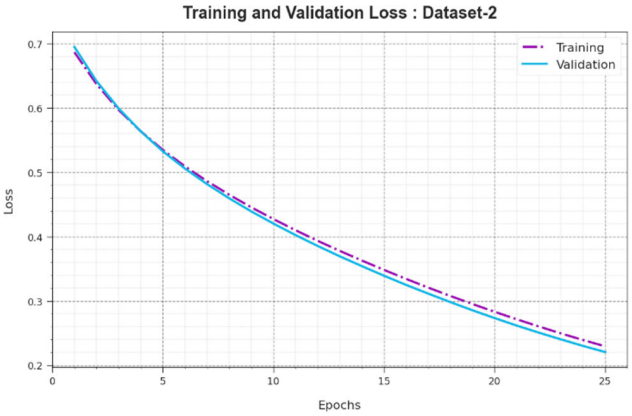

FIGURE 8. Loss curve of IRMOFNN-AD methodology on dataset2.

outcome of the IRMOFNN-AD technique on capturing patterns and relationships.

Fig. 9 illustrates the classifier performance of IRMOFNN-AD methodology on dataset1 and dataset2. Figs. 9a-9c defines the PR outcome of the IRMOFNN-AD model on dataset1 and dataset2. The result demonstrated that the IRMOFNN-AD algorithm performs in increasing PR values. Afterwards, it can be clear that the IRMOFNN-AD approach reaches superior values of PR values on all class labels. Finally, Figs. 9b-9d exhibits the ROC outcome of the IRMOFNN-AD system on dataset1 and dataset2. The simulation value defined that the IRMOFNN-AD technique resulted in greater values of ROC. Next, it could be clear that the IRMOFNN-AD methodology achieved greater values of ROC on all class labels.

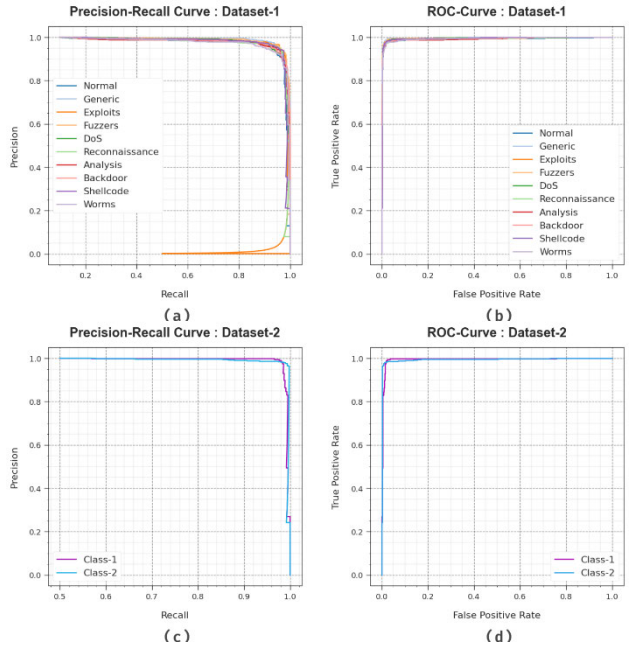

FIGURE 9. Dataset1: (a-b) PR and ROC curve, Dataset2: (c-d) PR and ROC curve.

The comparison results of the IRMOFNN-AD technique on dataset1 are reported in Table 3 and Fig. 10 [11]. The outcome value signifies that the ANN and SVM approaches report lesser results whereas the LR, KNN, DT, and SSA-CRNN models achieve considerable performance. Along with that, the IBFO-ODLAD model reaches near-optimal outcomes with $prec_n$, $reca_l$, $accu_y$, and F_{score} of 94.34%, 94.46%, 98.89%, and 94.28%, the IRMOFNN-AD technique gains maximum outcomes with $prec_n$, $reca_l$, $accu_y$, and F_{score} of 95.29%, 95.29%, 99.06%, and 95.28% respectively.

TABLE 3. Comparative outcome of IRMOFNN-AD system with other methods on dataset1.

Dataset-1				
Methods	$Prec_n$	$Reca_l$	$Accu_y$	F_{Score}
ANN Model	58.36	58.95	78.85	55.10
LR Algorithm	67.37	54.96	62.84	57.49
kNN Model	62.69	52.55	71.34	52.13
SVM Model	50.94	53.18	64.45	53.11
DT Model	64.42	53.27	70.67	48.23
SSA-CRNN	66.70	58.46	98.25	60.18
IBFO-ODLAD	94.34	94.46	98.89	94.28
IRMOFNN-AD	**95.29**	**95.29**	**99.06**	**95.28**

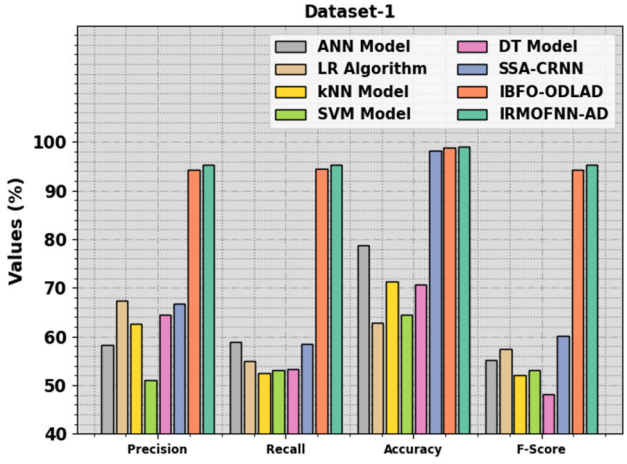

FIGURE 10. Comparative outcome of IRMOFNN-AD algorithm on dataset1.

The comparison outcomes of the IRMOFNN-AD methodology on the dataset1 are reported in Table 4 and Fig. 11. The simulation value signifies that the DNN Layer2 and Ensemble Models report lesser outcomes while the DNN Layer1, DNN Layer3, PSO Ensemble, and SSA-CRNN approaches accomplish considerable performance. Next, the IBFO-ODLAD system reaches near optimum outcomes with $prec_n$, $reca_l$, $accu_y$, and F_{score} of 96.81%, 97.88%, 98.66%, and 95.47%, the IRMOFNN-AD methodology obtains maximal outcomes with $prec_n$, $reca_l$, $accu_y$, and F_{score} of 98.96%, 99.02%, 99.02%, and 98.99% correspondingly.

TABLE 4. Comparative outcome of IRMOFNN-AD algorithm with other methodologies on dataset2.

Dataset2				
Methods	$Prec_n$	$Reca_l$	$Accu_y$	F_{Score}
DNN Layer1	91.23	84	92.09	90.44
DNN Layer2	89.06	86.58	93.37	91.15
DNN Layer3	90.75	87.72	83.42	87.07
Ensemble Model	89.47	88.07	90.87	90.07
PSO Ensemble	91.88	86.76	93.19	90.59
SSA-CRNN	91.66	88.61	97.62	90.43
IBFO-ODLAD	96.81	97.88	98.66	95.47
IRMOFNN-AD	**98.96**	**99.02**	**99.02**	**98.99**

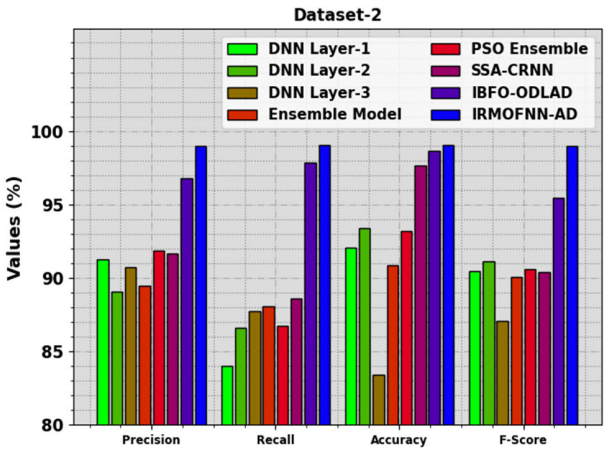

FIGURE 11. Comparative outcome of IRMOFNN-AD algorithm on dataset2.

These outcomes confirmed the better solution of the IRMOFNN-AD methodology for the anomaly detection process.

V. CONCLUSION

In this manuscript, we have devised an automated AD using the IRMOFNN-AD system for IoT Assisted Smart Cities. The main purpose of the IRMOFNN-AD system lies in the accurate and automated detection of the anomalies that exist in the IoT environment. It comprises 3-phases of operations namely IMRFO feature subset selection, FNN classification, and SCA-based parameter tuning. For the FS process, the IRMOFNN-AD technique uses the IRMO system to elect an optimum set of features. Furthermore, the IRMOFNN-AD methodology applies the FNN model for the detection and classification of anomalies. Furthermore, the SCA can be employed for the parameter tuning of the FNN algorithm. The simulation validation of the IRMOFNN-AD algorithm illustrates the improved detection performances of the IRMOFNN-AD methodology with maximum accuracy of 95.28% and 99.02% on UNSW NB-15 and UCI SECOM datasets, respectively. Future work can examine the computation complexity of the proposed model. Besides, the scalability and real-time abilities of the IRMOFNN-AD model can be boosted to accommodate the increasing

complexity and volume of data created by IoT devices in ever-expanding smart cities. Besides, future work can focus on the interpretability of the DL model. The integration of fault frequencies as prior knowledge into the model, particularly in offshore wind turbine applications, highlights the significance of this aspect. Acknowledging the critical role of interpretability could find a suitable place in the introduction section, underlining its relevance in real-world scenarios.

ACKNOWLEDGMENT

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through large group Research Project under grant number (RGP2/56 /44). Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R319), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. Research Supporting Project number (RSPD2023R787), King Saud University, Riyadh, Saudi Arabia. We Would like to thank SAUDI ARAMCO Cybersecurity Chair for funding this project. This study is supported via funding from Prince Sattam bin Abdulaziz University project number (PSAU/2023/R/1444). This study is partially funded by the Future University in Egypt (FUE).

REFERENCES

[1] Y. K. Saheed, O. H. Abdulganiyu, and T. A. Tchakoucht, "A novel hybrid ensemble learning for anomaly detection in industrial sensor networks and SCADA systems for smart city infrastructures," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 35, no. 5, May 2023, Art. no. 101532.

[2] D. K. Reddy, H. S. Behera, J. Nayak, P. Vijayakumar, B. Naik, and 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, Jul. 2021, Art. no. e4121.

[3] S. Yaqoob, A. Hussain, F. Subhan, G. Pappalardo, and M. Awais, "Deep learning based anomaly detection for fog-assisted IoVs network," *IEEE Access*, vol. 11, pp. 19024–19038, 2023.

[4] A. S. Rajawat, P. Bedi, S. B. Goyal, R. N. Shaw, A. Ghosh, and S. Aggarwal, "Anomalies detection on attached IoT device at cattle body in smart cities areas using deep learning," in *AI and IoT for Smart City Applications*, 2022, pp. 223–233.

[5] T. Lai, F. Farid, A. Bello, and F. Sabrina, "Ensemble learning based anomaly detection for IoT cybersecurity via Bayesian hyperparameters sensitivity analysis," 2023, *arXiv:2307.10596*.

[6] R. Al-Amri, R. K. Murugesan, E. M. Alshari, and H. S. Alhadawi, "Toward a full exploitation of IoT in smart cities: A review of IoT anomaly detection techniques,"in *Proc. Int. Conf. Emerg. Technol. Intell. Syst. (ICETIS)*, vol. 2. Cham, Switzerland: Springer, 2022, pp. 193–214.

[7] Y. Guo, T. Ji, Q. Wang, L. Yu, G. Min, and P. Li, "Unsupervised anomaly detection in IoT systems for smart cities," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 4, pp. 2231–2242, Oct. 2020.

[8] S. Manimurugan, "IoT-fog-cloud model for anomaly detection using improved Naïve Bayes and principal component analysis," *J. Ambient Intell. Humanized Comput.*, to be published.

[9] Y. Liu, Z. Pang, M. Karlsson, and S. Gong, "Anomaly detection based on machine learning in IoT-based vertical plant wall for indoor climate control," *Building Environ.*, vol. 183, Oct. 2020, Art. no. 107212.

[10] R. Vangipuram, R. K. Gunupudi, V. K. Puligadda, and J. Vinjamuri, "A machine learning approach for imputation and anomaly detection in IoT environment," *Expert Syst.*, vol. 37, no. 5, Oct. 2020, Art. no. e12556.

[11] M. M. Khayyat, "Improved bacterial foraging optimization with deep learning based anomaly detection in smart cities," *Alexandria Eng. J.*, vol. 75, pp. 407–417, Jul. 2023.

[12] Y. Liu, H. Wang, X. Zheng, and L. Tian, "An efficient framework for unsupervised anomaly detection over edge-assisted Internet of Things," *ACM Trans. Sensor Netw.*, to be published.

[13] M. Ragab and M. Farouk S. Sabir, "Arithmetic optimization with deep learning enabled anomaly detection in smart city," *Comput., Mater. Continua*, vol. 73, no. 1, pp. 381–395, 2022.

[14] I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy, and H. Ming, "AD-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning," in *Proc. IEEE 9th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2019, pp. 0305–0310.

[15] E. L. Lydia, A. A. Jovith, A. F. S. Devaraj, C. Seo, and G. P. Joshi, "Green energy efficient routing with deep learning based anomaly detection for Internet of Things (IoT) communications," *Mathematics*, vol. 9, no. 5, p. 500, Mar. 2021.

[16] R. Xu, Y. Cheng, Z. Liu, Y. Xie, and Y. Yang, "Improved long short-term memory based anomaly detection with concept drift adaptive method for supporting IoT services," *Future Gener. Comput. Syst.*, vol. 112, pp. 228–242, Nov. 2020.

[17] C. Hazman, S. Benkirane, A. Guezzaz, M. Azrour, and M. Abdedaime, "Building an intelligent anomaly detection model with ensemble learning for IoT-based smart cities," in *Proc. Advanced Technology for Smart Environment and Energy*. Cham, Switzerland: Springer, 2023, pp. 287–299.

[18] M. Islam, A. S. Dukyil, S. Alyahya, and S. Habib, "An IoT enable anomaly detection system for smart city surveillance," *Sensors*, vol. 23, no. 4, p. 2358, Feb. 2023.

[19] W. Ullah, A. Ullah, T. Hussain, K. Muhammad, A. A. Heidari, J. Del Ser, S. W. Baik, and V. H. C. De Albuquerque, "Artificial intelligence of things-assisted two-stream neural network for anomaly detection in surveillance big video data," *Future Gener. Comput. Syst.*, vol. 129, pp. 286–297, Apr. 2022.

[20] J. He, M. Dong, S. Bi, W. Zhao, and X. Liao, "A deep neural network for anomaly detection and forecasting for multivariate time series in smart city," in *Proc. IEEE 9th Annu. Int. Conf. CYBER Technol. Autom., Control, Intell. Syst. (CYBER)*, Jul. 2019, pp. 615–620.

[21] Z. Chen, D. Chen, X. Zhang, Z. Yuan, and X. Cheng, "Learning graph structures with transformer for multivariate time-series anomaly detection in IoT," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9179–9189, Jun. 2022.

[22] I. Ullah and Q. H. Mahmoud, "Design and development of a deep learning-based model for anomaly detection in IoT networks," *IEEE Access*, vol. 9, pp. 103906–103926, 2021.

[23] L. Jin, J. Wei, C. Luo, and T. Qin, "Slope stability analysis based on improved radial movement optimization considering seepage effect," *Alexandria Eng. J.*, vol. 79, pp. 591–607, Sep. 2023.

[24] G. Wang, Q.-S. Jia, J. Qiao, J. Bi, and C. Liu, "A sparse deep belief network with efficient fuzzy learning framework," *Neural Netw.*, vol. 121, pp. 430–440, Jan. 2020.

[25] A. A. Abdelhamid, E.-S.-M. El-Kenawy, A. Ibrahim, M. M. Eid, D. S. Khafaga, A. A. Alhussan, S. Mirjalili, N. Khodadadi, W. H. Lim, and M. Y. Shams, "Innovative feature selection method based on hybrid sine cosine and dipper throated optimization algorithms," *IEEE Access*, vol. 11, pp. 79750–79776, 2023.

[26] *UNSW-NB15*. Accessed: Jul. 14, 2023. [Online]. Available: https://www.kaggle.com/mrwellsdavid/unsw-nb15

[27] *UCI SECOM Dataset*. Accessed: Jul. 17, 2023. [Online]. Available: https://www.kaggle.com/paresh2047/uci-semcom