Iraqi Journal for Computer Science and Mathematics

Journal Homepage: http://journal.esj.edu.iq/index.php/IJCM
e-ISSN: 2788-7421 p-ISSN: 2958-0544

An Intelligent Prairie Dog Optimization (IPDO) and Deep Auto-Neural Network (DANN) based IDS for WSN Security

D.Hemanand[1], P.Mohankumar[2], N.Manoj Kumar[3], S.Vaitheki[4] P. Saranya[5]

[1]Professor, Department of Computer Science and Engineering, S.A. Engineering College (Autonomous), Thiruverkadu, Chennai-600077, Tamil Nadu, India,
[2]Associate Professor School of Computer Science and Engineering, VIT University Vellore Tamil Nadu 632014 , **India**
[3]Associate Professor, Department of Electrical and Electronics Engineering, Panimalar Engineering College Chennai 600123, Tamil Nadu. **India**
[4]Assistant Professor, Department of Electronics and communication Engineering, P.S.R.R.College of Engineering, Sivakasi-626140, Taminadu, India.
[5]Assistant Professor, Department of Mathematics, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, Tamil Nadu-600062, India.

*Corresponding Author :**D.Hemanand**
DOI: https://doi.org/10.52866/ijcsm.2023.04.04.004
Received July 2023; Accepted September 2023; Available online October 2023

ABSTRACT: Wireless sensor networks (WSNs) are targets of intrusion, which seeks to make these networks less capable of performing their duties or even completely eradicate them. The Intrusion Detection System (IDS) is highly important for WSN, since it aids in the identification and detection of harmful attacks that impair the network's regular functionality. In order to strengthen the security of WSN, several machine learning and deep learning approaches are employed in the traditional works. However, its main drawbacks are computational burden, system complexity, poor network performance outcomes, and high false alarms. Therefore, the goal of this study is to develop an intelligent IDS framework for significantly enhancing WSN security through the use of deep learning model. Here, the min-max normalization and data discretization operations are carried out to produce the preprocessed dataset. Then, an Intelligent Prairie Dog Optimization (IPDO) algorithm is used to reduce the dimensionality of features by identifying the best optimal solution with a higher convergence rate. Moreover, a Deep Auto-Neural Network (DANN) based classification method is used to properly forecast the class of data with less false alarms and higher detection rate. For evaluation, a thorough analysis is conducted to evaluate the performance and detection results of the proposed IPDO-DANN model.

Keywords: Intrusion Detection System (IDS), Wireless Sensor Network (WSN), Min-Max Normalization, Data Preprocessing, Intelligent Prairie Dog Optimization (IPOD), and Deep auto Neural Network (DANN), and Attack Classification.

1. INTRODUCTION

Wireless Sensor Network (WSN) [1, 2] is a type of large-scale ad-hoc network that has small devices, sensors, and modern computing components. This network is properly monitored and controlled with the use of sensors, many wireless nodes, and low power computing devices. Moreover, self-healing, availability, adaptability, resilience, and security are the five primary factors that must be taken into account when developing WSN [3]. Also, it can be used in a wide range of applications, including monitoring the ocean, industrial production tooling, tracking earthquakes, different military missions and etc. WSNs have a number of benefits, one of which is the ability to transform un-organized raw data into organized information. In most cases [4-6], a base station serves as a gateway to some other network, as well as an access point for interpersonal interactions. It may also be leveraged as a bridge to retrieve data from the network and distribute control information. The sink has also been mentioned by the base station. The base station serves as the root of each tree in the routing forest that is created by all of the sink node. The WSN is a self-organizing network with limited resources that is primarily recommended for challenging and adverse environments. The WSN deployment pattern is particularly susceptible to various faults. These errors may occur for a variety of

 **Corresponding author: d.hemanand@gmail.com

reasons, including faulty hardware, software, node isolation, or environmental factors [7-9]. The WSNs' deployment in unsupervised situations raises the risk of attackers capturing nodes. Typically, the intrusions have the ability to modify a node's operation or contents, which can initiate a variety of internal attacks and give them control over the entire network. Since sensor nodes in WSN are distributed at random, the topology is unknown before deployment. The sensor nodes must reconfigure themselves and restart contact with the neighboring nodes in the event of any failure. Because each sensor node has limited resources, WSN security is particularly difficult. When creating security frameworks or protocols for the WSN [10-12], the scalability aspect should be taken into account.

The second line of network security protection is intrusion detection. An intrusion detection system (IDS) [13-15] can increase the system's vulnerabilities based on known threats in addition to thwarting network attacks from attackers. Monitoring network transactions and spotting malicious activity can be articulated as the role of an IDS. Anomaly and signatures are two different types of input parameters that can be used with IDS. When a transaction detracts from the norm, it might be classified as suspicious activity. Transaction behavior patterns are recorded as anomalies. When using a signature system, each activity is given a special ID-based pattern that may be used to separate a legitimate user from a fraudster. A key method for ensuring product security is intrusion detection technology. As a result, it is crucial to precisely recognize different network threats. There are now such well machine learning-based [16-18] intrusion detection methods have been developed for WSNs, which includes decision trees, random forests, naive Bayes, logistic regression, and deep learning models. Most of the existing works [19, 20] facing the problems associated to the factors of ineffective detection performance, high false positives, computational burden, and complexity in intrusion detection. Thus, the proposed work aims to develop an effective and competent IDS framework for assuring the security of WSNs. The original contributions of this paper are as follows:

- To generate the preprocessed dataset, the min-max normalization and data discretization operations are performed.
- To minimize the dimensionality of features by choosing the optimal attributes, an Intelligent Prairie Dog Optimization (IPDO) algorithm is employed, which identifies the best optimal solution with increased convergence rate.
- To accurately predict the class of data with reduced false alarms and increased detection rate, a Deep Auto-Neural Network (DANN) based classification algorithm is utilized.
- To assess the performance and detection outcomes of the proposed IPDO-DANN model, an extensive analysis is carried out.

The following sections make up the remaining parts of this paper: In Section 2, a thorough assessment of the literature on the current IDS frameworks is offered, along with an examination of the difficulties and issues posed by traditional security approaches. Section 3 presents the architecture model and description of the proposed IPDO-DANN based IDS framework. The effectiveness and comparative outcomes of the current and proposed IDS frameworks are validated in Section 4 using various metrics. In Section 5, the findings and future scope of the work are summarized.

2. RELATED WORKS

This section reviews some of the recent state-of-the-art security approaches used in WSNs. Also, it presents the comprehensive analysis on various optimization and classification methods used in the existing IDS frameworks.

Safaldin, et al [21] deployed a binary grey wolf optimization based SVM model for predicting intrusions in WSNs. The purpose of this framework is to obtain an increased intrusion detection rate with reduced false alarm rate and execution time. In this framework, the dataset preparation and normalization processes are performed at the beginning to scale the data. Then, the grey wolf optimization algorithm is employed to obtain the optimal feature set for improving the overall intrusion detection performance. Here, the SVM classification model is used to predict the intrusion with reduced false positives. However, it has the major drawbacks of overfitting, high training and testing time. Mohapatra, et al [22] intended to detect the man-in-the-middle (MITM) attack with the use of IDS for WSN security. In an MITM attack, two legitimate users' conversations are secretly overheard by the attackers. When necessary, the hacker impersonates a legitimate user to manipulate information or data. During an MITM assault, the intruder typically focuses on real-time communications, operations, or transmission of data. Moreover, it implementing the attacking activities in the following ways:

1. Message delay
2. Data dropping
3. Message tampering

In the suggested framework, the LSTM based deep learning model is used to predict the MITM attack with high accuracy. Liu, et al [23] developed an intelligent intrusion detection model for WSNs with the use of arithmetic optimization and KNN algorithms. Here, a parallel method is deployed to improve communication between the populations and the Lévy flight strategy to modify the optimization in order to increase the model's accuracy. The key benefits of using this optimization algorithm are reduced local optimum and increased convergence rate. Maheswari, et al [24] introduced a unequal clustering protocol to detect intrusions in WSNs with improved Quality of Service (QoS). In this work, the Deer Hunting Optimization (DHO) algorithm is used to optimally select the CH based on the

parameters of residual energy and node distance. Moreover, the hybridized Adaptive Neuro Fuzzy Inference System (ANFIS) system is used to categorize the type of intrusion based on feature learning. The performance of this model is assessed in terms of network lifetime, average residual energy, and delay. However, the suggested mechanism required to reduce the performance of classification with minimal processing time, which could be the major limitation of this work. Pundir, et al [25] presented a comprehensive review to examine the challenges and problems associated to intrusion detection in WSNs. Here, some of the major security requirements, potential applications and impacts of deploying IDS have been discussed in detail. The major security requirements of WSNs are as follows: integrity, confidentiality, authentication, secrecy, and non-repudiation. Moreover, some of the most popular attacks that may degrade the performance of WSNs are also discussed in this work, which includes eavesdropping, packet analysis, replay, impersonation, and DoS. Farooq, et al [26] presented a comprehensive survey to investigate the different types of security breaches in WSNs. Here, some of the recent data mining techniques such as NB, LR, DT, SVM, RF and etc have been discussed for developing an IDS. An anomaly detection based IDS framework was proposed by Sushant et al [27]. Typically, the WSN environment is homogeneous in nature, where all sensor nodes behave similarly. In the suggested technique, the IDS agent is chosen based on internal node congestion and given a matrix. The authors in [28] implemented a smart security architecture employing random neural networks to develop an intrusion detection system. The suggested security solution is applied for an existing WSN system to evaluate its viability, and its functioning is nearly proven by successfully identifying any suspicious sensor nodes and unusual behavior in the base station with high accuracy and little overhead. In this work, the efficiency and overheads are assessed by integrating the suggested model into the base station application

Through the use of the genetic K-means algorithm [29], the authors presented a conceptual framework for recognizing intrusions. The algorithm divides instances into a set quantity of clusters. Pattern analysis techniques are used by intrusion detection systems to identify useful patterns in system properties. With the help of the right combination of system features, anomalies are detected in this work. The classification algorithms [30] that use the resulting patterns as inputs rely on statistical and machine learning pattern recognition methods. The selection of the appropriate IDS should be made by taking into account the requirements of the intended application, such as the desired precision, detection rate, adequate false alarms rate, etc. Since there are numerous proposed IDS frameworks available, each with some strengths and weaknesses. These recently proposed IDS frameworks for WSN have been evaluated and compared in this study. On the basis of energy efficiency, accuracy, strengths, and shortcomings, the examined IDS models have been examined [31, 32]. The IDS has also been discussed, along with its structures, detection methods, and design difficulties.[36,37] This study shows that while numerous effective designs for intrusion detection have been put out recently, there are still significant gaps in the current solutions that are caused by the WSN's resource constraints. Due to the self-organizing and random nature of sensor nodes, securing Wireless Sensor Networks (WSN) has become a more difficult task in recent years.[38][39][40].

3. PROPOSED METHODOLOGY

The computational design and procedures used to create the proposed IDS framework are described in this section. The original contribution of this paper is to develop a novel and effective IDS framework for securing WSNs with less computational burden and increased attack detection rate. For this purpose, the novel optimization and deep learning based classification models are employed in this work. As shown in Fig 1, the data collection and preprocessing operations are carried out at first. Here, the min-max normalization technique is used to preprocess the dataset, which includes the stages of normalization and discretization. After that, an Intelligent Prairie Dog Optimization (IPDO) algorithm is used to choose the best features from the normalized dataset for improving the performance of classification. Typically, finding the top feature in a piece of data is the goal of feature selection. After that, a set of features are used by the classification approaches for categorizing the class of data. In the existing works, the utilization of unnecessary and irrelevant variables are reduced in a number of ways. Also, the feature selection operations enhances the performance of classification with reduced processing requirements, minimized dimensionality of features, and better data comprehension. Furthermore, the Deep Auto Neural Network (DANN) is employed to categorize the data into the class of normal or intrusion. The benefits of using this framework are increased convergence rate, high attack detection rate, low false alarms, and computationally efficient. Moreover, the proposed work include the following operations:

- Min-Max Normalization based preprocessing
- Intelligent Prairie Dog Optimization (IPDO) algorithm based feature selection
- Deep Auto Neural Network (DANN) based classification

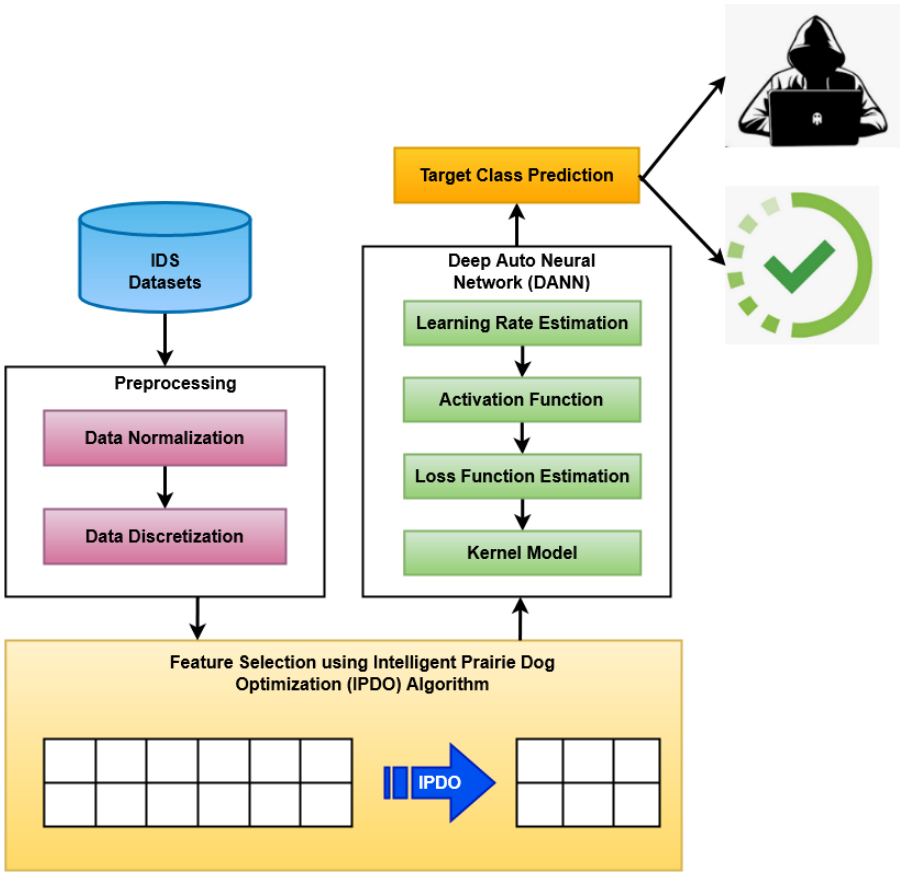

Fig 1. Workflow of the proposed IDS framework

A. Dataset Preprocessing

The goal of preprocessing data is to convert the raw data into a format that will be simpler and more useful for subsequent stages of processing. We standardize data using the min-max approach in the initial stage. Because all training data, for instance those in the range of 0 and 1, have the same scale, normalization might reduce training time. The normalized data is generated by using the following equation:

$$DS_N = \frac{DS - DS_{mn}}{DS_{mx}} \quad (1)$$

Where, DS_N indicates the normalized dataset, DS is the raw dataset, DS_{mn} denotes the minimum value, and DS_{mx} denotes the maximum value. Consequently, the data discretization is also performed, which is defined as the process of turning the value of a continuous data attribute into a sequence of finite intervals by reducing the information loss.

B. Intelligent Prairie Dog Optimization (IPDO) based Feature Selection

After preprocessing, a novel IPDO algorithm is used to choose the features for classifier training. The existing IDS frameworks use different types of meta-heuristic models for dimensionality reduction or optimal feature selection. But, the techniques have the major problems of low convergence rate, high processing time, searching complexity, and maximal number of iterations. Thus, the proposed work intends to use a new nature inspired optimization algorithm, named as, IPDO for optimal feature selection. In order to solve unrestrained mathematical optimization problems, a novel, nature-inspired technique called as, prairie dog optimization (PDO) is developed in recent days. To accomplish optimization, the suggested algorithm models the behavior of four prairie dogs. The foraging and tunnel behaviors of prairie dogs are used to study the optimal solution space. A plentiful food source serves as the foundation for the prairie dogs' tunnels. As the food source runs out, they look for a new one, dig additional tunnels surrounding it, and explore the entire colony or problem area to find food sources or solutions. The difference between the prairie dogs' reactions to two different alert or communication noises is used in this instance to achieve the desired outcome. When a predator is around or when food is available, prairie dogs will produce specific noises or emit specific signals. The extraordinary communication abilities of prairie dogs help them meet their dietary needs and protect themselves from predators. The stages involved in this optimization algorithm are as follows:

- Parameter initialization
- Fitness function evaluation

- Exploration
- Exploitation

Initially, PDO creates a set of decision variables that are generated and distributed randomly. The algorithm then repeatedly employs its preset methods to investigate every potential position for near-optimal solutions. Each time, the algorithm replaces the previously discovered solution with the best one yet discovered in accordance with the given rule. Moreover, the algorithm accomplishes exploration and exploitation using four prairie dog actions. The PDO starts the exploration phase when the iteration is lesser than the maximum iteration, and the exploitation phase is carried out when the iteration is greater than the maximum iteration. The exploration and exploitation operations are represented in Fig 2 (a) and (b) respectively. Finally, the algorithm comes to end, when the stopping criterion is met. The best ideal parameters are chosen using this optimization approach and provided to the classifier for training and testing.

Algorithm 1 – Intelligent Prairie Dog Optimization (IPDO) Algorithm

Step 1: Parameter initialization;

1. Initialize the parameters such as w, t, ρ, α;
2. Set the parameters as global best and current best solution H_{GB} and H_{CB} as $\emptyset$ respectively;
3. Set the candidate solutions of all coteries and prairie dogs as K & L;

Step 2: While $h < Xw_{it}$ do

For $(i = 1\ to\ t)$ do

For $(j = 1\ to\ w)$ do

Step 3: Discover the prairie dogs' best fitness ratings;

Step 4: Update the global best function H_{GB};

Step 5: Update the value of randomized cumulative effect $R_{i,j}$ by using:

$$R_{i,j} = \frac{H_{GB_{i,j}} - r\delta_{i,j}}{H_{GB_{i,j}} + \Delta} \quad (2)$$

Where, r - random number, $\delta_{i,j}$ - i[th] prairie dog at j[th] dimension;

Step 6: According to the quality of the food source and random value, the coterie's digging strength is estimated.

Step 7: $$\alpha_{i+1,j+1} = H_{GB_{i,j}} \times \tau \times r1 \forall 3\frac{Xw_h}{4} \leq h \leq Xw_h \quad (3)$$

Where, τ - effect of predator, and $r1$ - random number.

Step 8: if $\left(h < \frac{Xw_h}{4}\right) then$ //foraging activities

$$\delta_{i+1,j+1} = H_{GB_{i,j}} - eH_{CB_{i,j}} \times \partial - CE_{i,j} \times Levy\ (y); \quad (4)$$

Where, ∂ - specialized food source;

Step 9: Else if $\left(\frac{Xw_h}{4} \leq h < \frac{Xw_h}{2}\right)$ then //Burrowing activities;

$$\delta_{i+1,j+1} = H_{GB_{i,j}} \times eH_{CB_{i,j}} \times L \times Levy\ (t); \quad (5)$$

Where, L - digging strength;

Step 10: Else if $\left(\frac{Xw_{it}}{2} \leq it < 3\frac{Xw_{it}}{4}\right)$ then //Food Alarm;

$$\delta_{i+1,j+1} = H_{GBi,j} \times eH_{CBi,j} \times \vartheta - H_{CBi,j} \times r1; \quad (6)$$

Step 11: Else //Anti-predation alarm

$$\delta_{i+1,j+1} = H_{GBi,j} \times K \times r1; \quad (7)$$

End if;

End for;

End for;

Step 12: $h = h + 1$;

Step 13: End while;

Step 14: Return best solution H_{GB};

Step 15: End;

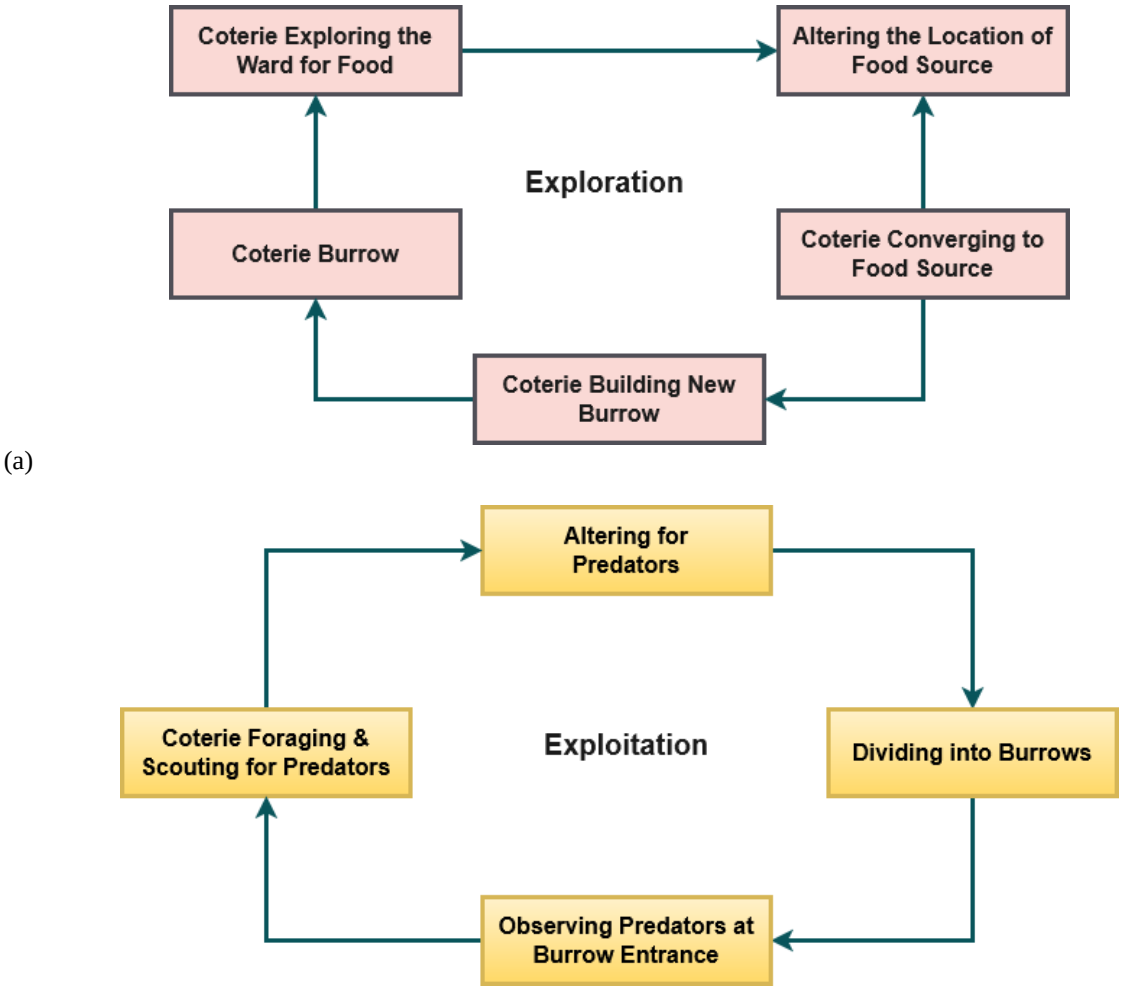

Fig 2 (a). Exploration phase and (b). Exploitation phase

Deep Auto Neural Network (DANN) based Classification

In this stage, the optimal set of selected features are fed to the classifier for training and testing. For this purpose, a Deep Auto Neural Network (DANN) classification technique is employed, which predicts the normal and intrusion with reduced false alarm rate and error rate. The existing IDS frameworks use the machine learning and deep learning based classification approaches like SVM, NB, DT, ELM, and etc for categorizing the class of intrusion. Still, it has the problems with the factors of over fitting, high time consumption, and computational burden. Therefore, the proposed work motivates to implement a new deep learning algorithm for categorizing the class of intrusion. The output of the extracted feature is transmitted to the DANN framework for fine-tuning with the bias and weight values in the form of an encoding structure. The model does not receive the structure and data from the decoding layer. Then, it trains the data based on the optimized features, and the optimal model is constructed during the hyperparameter tuning phase by tracking the attack classification detection rate. The main goal of this work is to create an effective IDS by choosing features from raw data to reflect low-dimensional features more accurately. The feature selection procedure seeks to improve the detection and classification of binary (normal or anomalous) and multiclass assaults with increased efficiency and accuracy. The inclusion of hidden layers in the DANN model enables auto-encoder to learn more intricate mathematical data patterns. Typically, encoding is the step where layer inputs are mapped to hidden layers on an auto-encoder with a single hidden layer. The decoding process involves mapping the hidden layer to the output layer. Additional encoder and decoder pairs could be found in a DANN with several hidden layers.

In this model, the vector encoding function is estimated at first by using the following model:

$$K^{(p+1)} = f(\omega^p \times K^p + (\beta^p)) \quad (8)$$

Where, p indicates the hidden layer, K is the encoding function, ω denotes the weight matrix, and β is the bias value. Consequently, the cost function is estimated, which is defined as the distance function between the input and

reconstructed data. With mean squared error loss for the activation function, cost also known as a loss can be computed by using the following model:

$$D(\omega, \beta, a^i, \hat{a}^i) = \frac{1}{2}||a^i - \hat{a}^i||^2 \quad (9)$$

Where, $D(.)$ is the cost function, and a^i is the input vector. A nonlinear sigmoid function is further used to perform the preparation process on the hidden layers. After that, the binary cross-entropy is utilized as a loss function with a binary integer. The loss value is also estimated for the overall training data by using the following equation:

$$D(\omega, \beta) = \frac{1}{G}\sum_{i=1}^{G}[a^i \log(\hat{a}^i) + (1 - a^i)\log(1 - \hat{a}^i)] \quad (10)$$

The cost of backpropagation is decreased by updating the weight and bias values of each node in each layer, and the value near to zero is the best cost for the smallest loss value. After that, the retraining procedure is carried out to learn the output based on the weight and bias values. Finally, the output label is produced as follows:

$$\hat{o} = f(\omega^p \times K^p + \beta^p) = f(y^{p+1}) \quad (11)$$

Where, $\hat{o}$ indicates the output label, y represents the encoding structure, and $p + 1$ is the last layer. Finally, the output label is categorized into the class of normal and intrusion with reduced false positives and increased detection accuracy.

4.RESULTS AND DISCUSSION

This section presents the results and discussion of the existing and proposed security methodologies used for securing WSNs. Additionally, the dataset used for model training and model testing determines the appropriate performance parameters for every classifier. The different types of IDS datasets used to assess the performance of this work are listed in Table 1. Also, the parameters used to validate the outcomes of the security approaches are described in below:

Table 1. Dataset details

Dataset	Description
Dataset 1	NSL-KDD
Dataset 2	UNSW-NB 15
Dataset 3	IoT-23
Dataset 4	BoT-IoT

Attack Detection Rate (ADR): It is also termed as True Positive Rate (TPR) estimated based on the total number of packets that are precisely identified as attacks rather than the total number of packets that are actually transmitted. Then, its mathematical model is represented as follows:

$$ADR = TPR = \frac{TP}{TP+FN} \quad (12)$$

Where, the TP indicates the true positives, TN indicates the true negatives, and FN is the false negatives.

Accuracy: The accuracy of the attack detection and categorization system is often validated using one of the most widely used performance measures. It is computed as shown in below:

$$Accuracy = \frac{TP+TN}{TP+FP+FN+TN} \quad (13)$$

False Positive Rate (FPR): The FPR is calculated using the following formula based on the ratio between the number of data packets that were incorrectly identified and all of the data packets that were transmitted:

$$FPR = \frac{FP}{FP+TN} \quad (14)$$

Precision, Recall, and F1-score: The effectiveness of the IDS is validated according to the parameters of precision, recall and f-measure, which determines the entire performance of the security framework. The parameters are computed by using the following equations:

$$Precision = \frac{TP}{FP+TP} \quad (15)$$

$$\text{Recall} = \frac{TP}{FN+TP} \quad (16)$$

$$F1-\text{measure} = 2 * \frac{\text{Precision} \times \text{Recall}}{\text{Precision}+\text{Recall}} \quad (17)$$

Table 2 and Fig 3 validates the performance of the existing [33] and proposed IPDO-DANN based IDS frameworks using dataset 1, where the parameters such as accuracy, precision, recall and f1-score are considered. Consequently, the detection accuracy is also validated and compared as shown in Table 3 and Fig 4. The findings show that the proposed IPDO-DANN model overwhelms the other approaches with increased performance values. Since, the IPDO technique helps to enhance the training and validation operations, which increases the accuracy of intrusion detection.

Table 2. Comparative analysis using dataset 1

Methods	*Accuracy (%)*	*Precision (%)*	*Recall (%)*	*F1-score (%)*
RF	83	81	91	86
SVM	84	87	86	87
DT	81	82	87	84
LGBM	78	80	84	82
EC	80	78	91	84
GBC	77	88	70	78
ABC	78	83	76	80
KNN	82	80	94	86
MLP	83	81	91	86
GNB	81	79	91	85
LR	80	81	86	83

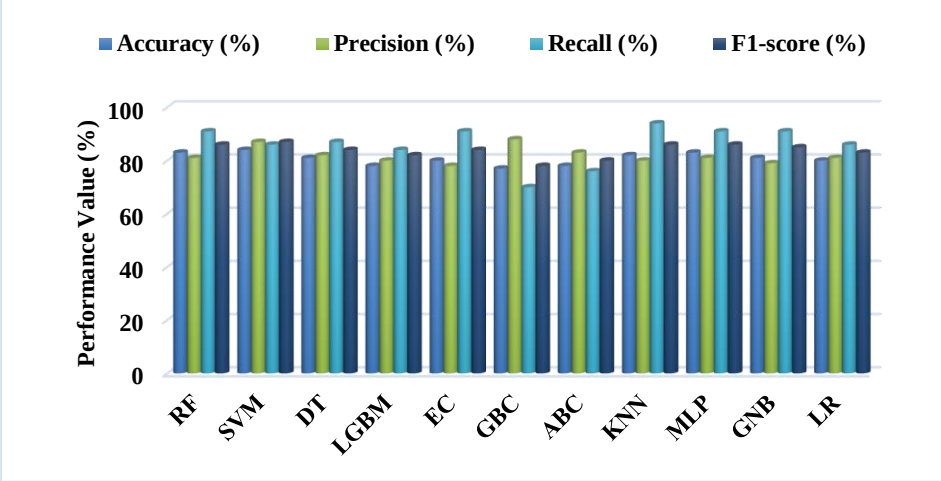

Fig 3. Comparative analysis using dataset 1

Table 3. **Detection accuracy using dataset 1**

Methods	Accuracy (%)
Deep Model	98.27
Shallow Model	96.75
kFN-KNN	99
CFS-DT	90.3
DBN	97.5
RNN	83.28
CNN-LSTM	99
AE	87
B-Stacking	98.5
Proposed IPDO-DANN	99.5

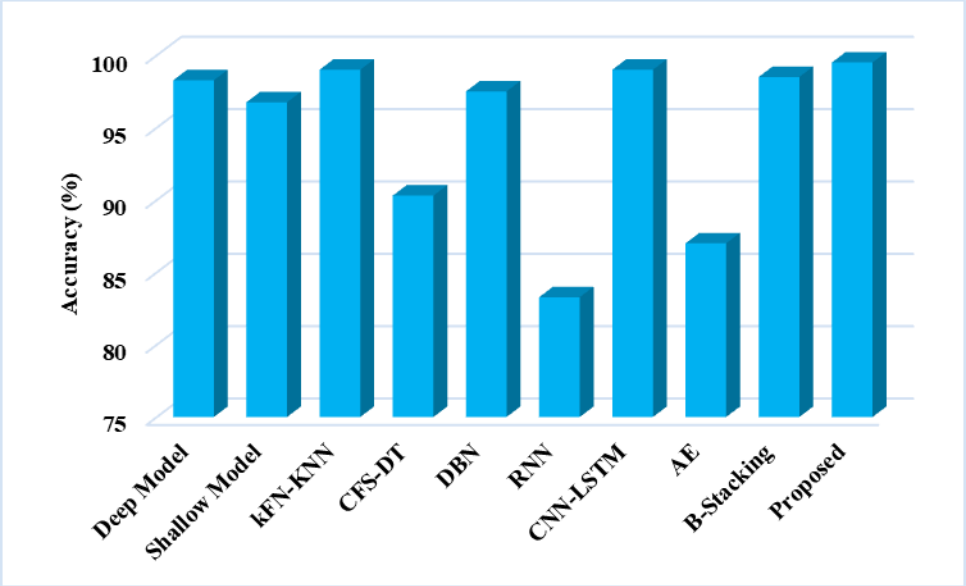

Fig 4. **Detection accuracy using dataset 1**

Table 4 and Fig 5 validates the overall detection performance and efficacy of the existing [34] and proposed IPDO-DANN based IDS models using dataset 2. Furthermore, choosing the best combination of characteristics to train the classifier is crucial to the accuracy of the attack classification technique. This analysis makes it clear that, when compared to other procedures, the suggested IPDO-DANN technique has a higher accuracy value.

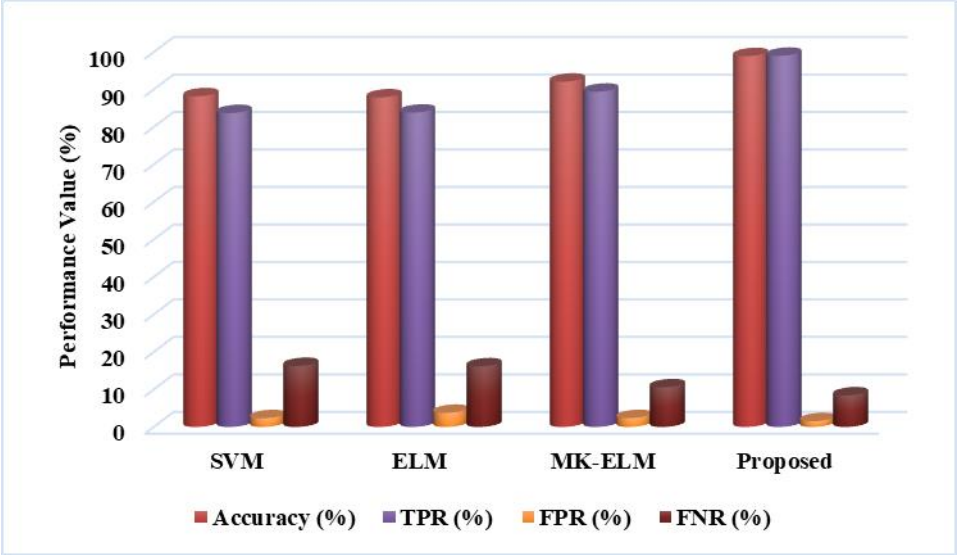

Fig 5. **Detection performance analysis using dataset 2**

Table 4. **Comparative analysis using dataset 2**

Methods	Accuracy (%)	TPR (%)	FPR (%)	FNR (%)
SVM	88.20	83.73	2.34	16.27
ELM	87.90	83.84	3.76	16.16
MK-ELM	92.10	89.42	2.37	10.58
Proposed	98.9	99	1.53	8.41

Moreover, the overall intrusion detection performance of the proposed IPDO-DANN is validated by using all the datasets such as NSL-KDD, UNSW-NB15, IoT-23 and BoT-IoT as shown in Table 5 and Fig 6. The observed results state that the IPDO-DANN technique provides a highly improved detection results for all the datasets. Due to the inclusion of IPDO, the DANN classifier could accurately spots the attacks with reduced false alarms. Thus, the performance of the proposed IDS framework is efficiently improved in this work.

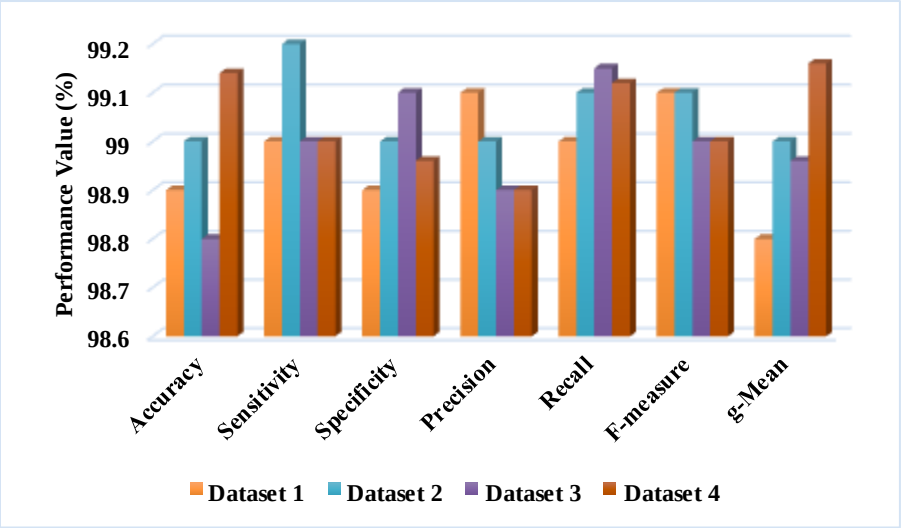

Fig 6. Overall performance analysis using different datasets

Table 5. Performance analysis of the proposed framework using different datasets

Measures	Dataset 1	Dataset 2	Dataset 3	Dataset 4
Accuracy	98.9	99	98.8	99.9
Sensitivity	99	99.2	99	99
Specificity	98.9	99	99.1	998.96
Precision	99.1	99.4	98.9	100
Recall	99	99.1	99.15	100
F-measure	99.1	99.1	99	99.99
g-Mean	98.8	99	98.96	99.9

Table 6 validates the performance of existing IDS-SIoEL [35] and proposed IPDO-DANN mechanisms by using dataset 3 and dataset 4. By accurately identifying the attacking packets based on the set of optimal features, the IPDO-DANN technique performs better than the other strategy. Consequently, the results of other machine learning, deep learning and proposed IDS models are validated and compared using IoT-23 and BoT-IoT datasets as shown in Fig 7 and 8 respectively. Here, the techniques of data normalization and missing data replacement aid in enhancing the classifier's accuracy in identifying all sorts of assaults present in the IDS dataset. Similar to this, the best attributes are chosen to accurately anticipate the categorized label. Studies on numerous datasets and performance comparisons have shown that our model is the most effective and reliable, with the lowest computational complexity.

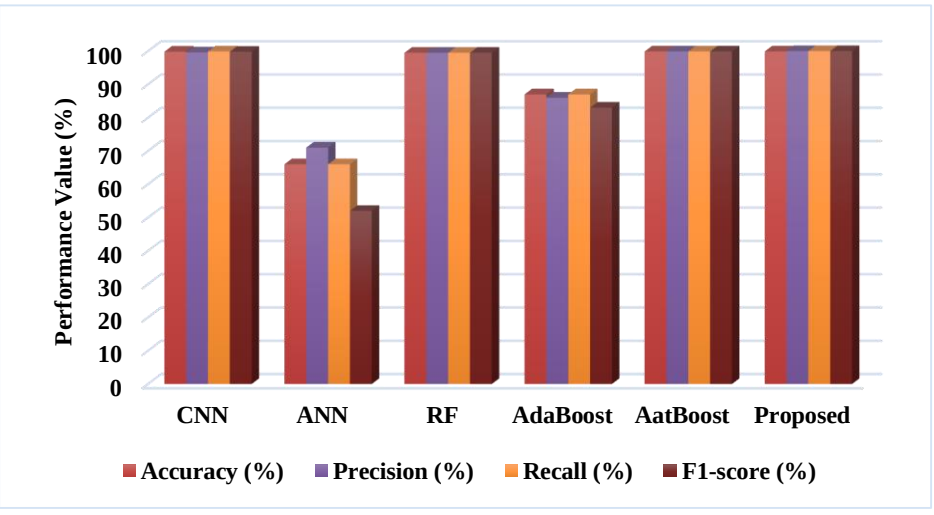

Fig 7. Comparative analysis using dataset 3

Table 6. Comparative analysis using dataset 3 and dataset 4

Measures	IoT-23		BoT-IoT	
	IDS-SIoEL	Proposed	IDS-SIoEL	Proposed
Accuracy	99.98	99.95	99.99	99.99
Precision	99.98	99.91	99.99	100
Recall	99.91	99.9	100	100
F1-score	99.99	100	99.99	99.99
AUC	100	100	100	100

5. CONCLUSION

In order to spot threatening network intrusions, this article suggested an intelligent IDS framework by using an advanced IPDO-DANN models. The contribution of this paper is to implement one of the most efficient and reliable feature selection algorithms, named as, IPDO for choosing the most crucial features to increase classification precision and intrusion detection rate. The existing IDS frameworks use the machine learning and deep learning based classification approaches like SVM, NB, DT, ELM, and etc for categorizing the class of intrusion. Still, it has the problems with the factors of over fitting, high time consumption, and computational burden. Therefore, the proposed work motivates to implement a new deep learning algorithm for categorizing the class of intrusion. In the proposed framework, the dataset is first preprocessed using the min-max normalization method, which involves normalizing and discretization steps. The best features from the normalized dataset are then selected using the IPDO algorithm to enhance classification performance. The objective of feature selection is often to identify the most important feature in a set of data. The classification approaches then classify the class of data using a set of features. The use of pointless and unimportant variables is minimized in the existing works in a variety of methods. Additionally, the feature selection operations improve classification performance by reducing processing demands, reducing feature dimensionality, and improving data comprehension. Finally, the DANN is used to classify the data into the class of normal or intrusion. Various measures are used during experimentation to compare and validate the effectiveness of different strategies. The results indicate that the proposed outperforms the other strategies, according to the compared results by successfully identifying the attacker packets from the IDS datasets.

In future, the proposed work can be enhanced by implementing a hybrid met-heuristic model for strengthening the security of IoT integrated WSN framework.

Funding

None

ACKNOWLEDGEMENT

None

CONFLICTS OF INTEREST

None

REFERENCES

[1] Y. Zhang, "The WSN intrusion detection method based on deep data mining," Journal of Cyber Security Technology, pp. 1-19, 2023.
[2] H. Li, J. Ou, H. Cui, S. Zhao, D. Zeng, and Y. Wang, "GKFCR: An Improved Clustering Routing Algorithm for Wireless Sensor Networks," in 2022 IEEE International Conference on Sensing, Diagnostics, Prognostics, and Control (SDPC), 2022, pp. 222-227.
[3] H. Echoukairi, A. Idrissi, and F. Omary, "New Hierarchical Routing Protocol Based on K-Means Clustering with Exploiting Free Time Slot for Wireless Sensor Networks," International Journal of Interactive Mobile Technologies, vol. 16, 2022.
[4] K. Ramana, A. Revathi, A. Gayathri, R. H. Jhaveri, C. L. Narayana, and B. N. Kumar, "WOGRU-IDS—An intelligent intrusion detection system for IoT assisted Wireless Sensor Networks," Computer Communications, vol. 196, pp. 195-206, 2022.
[5] M. Maheswari and R. Karthika, "A Novel Hybrid Deep Learning Framework for Intrusion Detection Systems in WSN-IoT Networks," Intelligent Automation & Soft Computing, vol. 33, 2022.
[6] P. Biswas, T. Samanta, and J. Sanyal, "Intrusion detection using graph neural network and Lyapunov optimization in wireless sensor network," Multimedia Tools and Applications, pp. 1-12, 2022.

[7] G. Bakshi and H. Sahu, "WSN Security: Intrusion Detection Approaches Using Machine Learning," in Computational Intelligence for Wireless Sensor Networks, ed: Chapman and Hall/CRC, 2023, pp. 151-174.
[8] M. Sirajuddin and B. Sateesh Kumar, "Collaborative Security Schemes for Wireless Sensor Networks," in ICCCE 2021: Proceedings of the 4th International Conference on Communications and Cyber Physical Engineering, 2022, pp. 343-354.
[9] A. Singh, J. Amutha, J. Nagar, and S. Sharma, "A deep learning approach to predict the number of k-barriers for intrusion detection over a circular region using wireless sensor networks," Expert Systems with Applications, vol. 211, p. 118588, 2023.
[10] K. Hussain, Y. Xia, A. N. Onaizah, T. Manzoor, and K. Jalil, "Hybrid of WOA-ABC and proposed CNN for intrusion detection system in wireless sensor networks," Optik, vol. 271, p. 170145, 2022.
[11] M. Sadeghizadeh, "A lightweight intrusion detection system based on RSSI for sybil attack detection in wireless sensor networks," International Journal of Nonlinear Analysis and Applications, vol. 13, pp. 305-320, 2022.
[12] G. Nagalalli and G. Ravi, "A Novel MegaBAT Optimized Intelligent Intrusion Detection System in Wireless Sensor Networks," Intelligent Automation & Soft Computing, vol. 35, 2023.
[13] S. Saif, K. Karmakar, S. Biswas, and S. Neogy, "MLIDS: Machine Learning Enabled Intrusion Detection System for Health Monitoring Framework Using BA-WSN," International Journal of Wireless Information Networks, pp. 1-12, 2022.
[14] R. Krishnan, R. S. Krishnan, Y. H. Robinson, E. G. Julie, H. V. Long, A. Sangeetha, et al., "An intrusion detection and prevention protocol for internet of things based wireless sensor networks," Wireless Personal Communications, vol. 124, pp. 3461-3483, 2022.
[15] P. Gulganwa and S. Jain, "EES-WCA: energy efficient and secure weighted clustering for WSN using machine learning approach," International Journal of Information Technology, vol. 14, pp. 135-144, 2022.
[16] V. Ponnusamy, M. Humayun, N. Jhanjhi, A. Yichiet, and M. F. Almufareh, "Intrusion Detection Systems in Internet of Things and Mobile Ad-Hoc Networks," Comput. Syst. Sci. Eng., vol. 40, pp. 1199-1215, 2022.
[17] D.-W. Huang, F. Luo, J. Bi, and M. Sun, "An Efficient Hybrid IDS Deployment Architecture for Multi-Hop Clustered Wireless Sensor Networks," IEEE Transactions on Information Forensics and Security, vol. 17, pp. 2688-2702, 2022.
[18] G. Kalnoor and S. Gowrishankar, "A Framework Using Markov-Bayes' Model for Intrusion Detection in Wireless Sensor Network," in ICDSMLA 2020: Proceedings of the 2nd International Conference on Data Science, Machine Learning and Applications, 2022, pp. 73-80.
[19] A. G. Putrada, N. Alamsyah, S. F. Pane, and M. N. Fauzan, "XGBoost for IDS on WSN Cyber Attacks with Imbalanced Data," in 2022 International Symposium on Electronics and Smart Devices (ISESD), 2022, pp. 1-7.
[20] T. Sood, S. Prakash, S. Sharma, A. Singh, and H. Choubey, "Intrusion detection system in wireless sensor network using conditional generative adversarial network," Wireless Personal Communications, vol. 126, pp. 911-931, 2022.
[21] M. Safaldin, M. Otair, and L. Abualigah, "Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks," Journal of ambient intelligence and humanized computing, vol. 12, pp. 1559-1576, 2021.
[22] H. Mohapatra, S. Rath, S. Panda, and R. Kumar, "Handling of man-in-the-middle attack in wsn through intrusion detection system," International journal, vol. 8, pp. 1503-1510, 2020.
[23] G. Liu, H. Zhao, F. Fan, G. Liu, Q. Xu, and S. Nazir, "An enhanced intrusion detection model based on improved kNN in WSNs," Sensors, vol. 22, p. 1407, 2022.
[24] M. Maheswari and R. Karthika, "A novel QoS based secure unequal clustering protocol with intrusion detection system in wireless sensor networks," Wireless Personal Communications, vol. 118, pp. 1535-1557, 2021.
[25] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. Rodrigues, and Y. Park, "Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: Survey and future challenges," IEEE Access, vol. 8, pp. 3343-3363, 2019.
[26] Y. Farooq, H. Beenish, and M. Fahad, "Intrusion detection system in wireless sensor networks-a comprehensive survey," in 2019 Second International Conference on Latest trends in Electrical Engineering and Computing Technologies (INTELLECT), 2019, pp. 1-6.
[27] S. K. Pandey, P. Kumar, J. P. Singh, and M. Singh, "Intrusion detection system using anomaly technique in wireless sensor network," in 2016 International Conference on Computing, Communication and Automation (ICCCA), 2016, pp. 611-615.
[28] A. Yadav and A. Kumar, "Intrusion detection and prevention using RNN in WSN," in Inventive Computation and Information Technologies: Proceedings of ICICIT 2021, ed: Springer, 2022, pp. 531-539.
[29] L. Lakshmanan, A. Jesudoss, and V. Ulagamuthalvi, "Cluster based routing scheme for heterogeneous nodes in WSN–A genetic approach," in International Conference on Intelligent Data Communication Technologies and Internet of Things (ICICI) 2018, 2019, pp. 1013-1022.
[30] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, "CNN-LSTM: hybrid deep neural network for network intrusion detection system," IEEE Access, vol. 10, pp. 99837-99849, 2022.

[31] V. Ravi, R. Chaganti, and M. Alazab, "Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system," Computers and Electrical Engineering, vol. 102, p. 108156, 2022.
[32] S. Amaran and R. M. Mohan, "Intrusion detection system using optimal support vector machine for wireless sensor networks," in 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), 2021, pp. 1100-1104.
[33] S. Roy, J. Li, B.-J. Choi, and Y. Bai, "A lightweight supervised intrusion detection mechanism for IoT networks," Future Generation Computer Systems, vol. 127, pp. 276-285, 2022.
[34] A. B. Abhale and S. Manivannan, "Supervised machine learning classification algorithmic approach for finding anomaly type of intrusion detection in wireless sensor network," Optical Memory and Neural Networks, vol. 29, pp. 244-256, 2020.
[35] C. Hazman, A. Guezzaz, S. Benkirane, and M. Azrour, "lIDS-SIoEL: intrusion detection framework for IoT-based smart environments security using ensemble learning," Cluster Computing, pp. 1-15, 2022.
[36] Taseer Muhammad, & Hamayoon Ghafory. (2022). SQL Injection Attack Detection Using Machine Learning Algorithm. Mesopotamian Journal of CyberSecurity, 2022, 5–17. https://doi.org/10.58496/MJCS/2022/002
[37] Siti Nur Fathin Najwa Binti Mustaffa, & muhammad Farhan. (2022). Detection of False Data Injection Attack using Machine Learning approach. Mesopotamian Journal of CyberSecurity, 2022, 38–46. https://doi.org/10.58496/MJCS/2022/005
[38] Hemanand, D., Reddy, G. ., Babu, S. S. ., Balmuri, K. R. ., Chitra, T., & Gopalakrishnan, S. (2022). An Intelligent Intrusion Detection and Classification System using CSGO-LSVM Model for Wireless Sensor Networks (WSNs). International Journal of Intelligent Systems and Applications in Engineering, 10(3), 285–293. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2167
[39] P. Satyanarayana, T. Sushma, M. Arun, V. S. Raiu Talari, S. Gopalakrishnan and V. G. Krishnan, "Enhancement of Energy Efficiency and Network Lifetime Using Modified Cluster Based Routing in Wireless Sensor Networks," *2023 International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS)*, Coimbatore, India, 2023, pp. 127-132, doi: 10.1109/ICISCoIS56541.2023.10100580.
[40] Gopalakrishnan Subburayalu, Hemanand Duraivelu, Arun Prasath Raveendran, Rajesh Arunachalam, Deepika Kongara & Chitra Thangavel (2023) Cluster Based Malicious Node Detection System for Mobile Ad-Hoc Network Using ANFIS Classifier, Journal of Applied Security Research, 18:3, 402-420, DOI: 10.1080/19361610.2021.2002118