SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549 / https://doi.org/10.14445/23488549/IJECE-V10I4P101

Volume 10 Issue 4, 1-8, April 2023
© 2023 Seventh Sense Research Group®

Original Article

Selfish Herd Optimization with Improved Deep Learning based Intrusion Detection for Secure Wireless Sensor Network

S. Suma Christal Mary[1], E. Thenmozhi[2], K. Murugeswari[3], N. Senthamilarasi[4]

[1,2,4]Department of Information Technology, Panimalar Engineering College, India
[3]Department of Computer Science and Engineering, Panimalar Engineering College, India

[1]Corresponding Author : professorsumachristalmary@gmail.com

Received: 27 February 2023 Revised: 01 April 2023 Accepted: 13 April 2023 Published: 30 April 2023

Abstract *- Wireless sensor networks (WSNs) are becoming more frequently utilized in many applications like environmental monitoring, smart cities, and healthcare. But, security is an important problem in WSNs because of the possible vulnerability to attacks. Intrusion detection systems (IDS) are utilized for detecting and preventing attacks on WSNs. Typical IDS depend on rule-based or signature-based methods that are limited in their capability for detecting before unseen attacks. Deep learning (DL)-based IDS are exposed to promising outcomes in identifying novel attacks. DL-based IDS for WSNs are created utilizing an integration of supervised and unsupervised learning approaches. Therefore, this study designs a Selfish herd optimization with Improved Deep Learning based Intrusion Detection (SHOIDL-ID) technique for secure WSN. The presented SHOIDL-ID technique focuses on the process of identifying and classifying intrusions in the WSN. The presented SHOIDL-ID approach applies data preprocessing to normalize the input data to accomplish this. The SHOIDL-ID technique employs an attention-based bidirectional long short-term memory (ABiLSTM) approach for intrusion recognition and classification. Finally, the SHO approach was utilized for the optimal hyperparameter tuning of the ABiLSTM algorithm. The experimental validation of the SHOIDL-ID approach takes place on the WSN-DS dataset. The outcomes indicate the improved performance of the SHOIDL-ID methodology over other existing approaches in terms of different measures.*

Keywords *- Intrusion detection, Wireless sensor networks, Security, Deep learning, Selfish herd optimization.*

1. Introduction

Wireless Sensor Networks (WSN), the basic technology that allows the Internet of Things (IoT), has quickly increased in terms of application [1]. The small, intellectual sensor node (SN) is positioned to monitor physical phenomena or events. The node transmits the gathered information to the central node, named the base station (BS), for data fusion and processing [2] or to the IoT cloud for further analysis. WSN network is vulnerable to many critical cyberattacks because of the limited node resources and poor security capabilities [4]. This cyberattack has different goals: stealing, hacking, altering information the sensor has, flooding or collecting the targeted node with additional packets in an effort to drain the batteries of the sensor and disconnect them from the network, which prevents them from sensing or routing traffic and renders them inoperable [5]. Robust security measures, namely well-determined recognition and mitigation methods, should be prepared to resolve the challenge. WSN has a unique feature that grants traditional heavyweight security measures involving cryptography, spread spectrum, and insufficient and key administration, because of constrained resources like computation power, data storage, and packet buffering [7]. This detriment has constructed the necessity to search for an effective, lightweight security mechanism that balances node resource use in terms of memory, power, processing, and storage.

There exist various solutions that are used to protect WSNs, namely cryptography or authentication and key management [8]. Notwithstanding, this solution does not guarantee complete prevention of each attack. The challenging problem that the whole security division face is identifying and tackling forthcoming attacks. However, it is prominent that an intrusion detection system (IDS) is a highly efficient security mechanism for monitoring the network for unauthorized access or vicious attacks as a second line of defense and alert administrator on these subjects [9]. In summary, IDS is necessary to protect against WSN attacks. In the last decade, the applications of the Machine Learning (ML) algorithm for detecting maliciousness in WSN have mainly improved.

However, the general approach still considers the analysis as an offline-learning issue, where the model was trained only once on past information [10]. Due to the increasing quantity of information necessary to uncover increasingly sophisticated attack, and provide the massive quantity of information produced in real-time that gush through this network on a systematic basis [12], existing identification technique is inadequate to detect malicious network intrusion. The recognition of attacks needs a faster mechanism for the online investigation of thousands of events every second [13].

This study designs a Selfish herd optimization with Improved Deep Learning based Intrusion Detection (SHOIDL-ID) technique for secure WSN. The presented SHOIDL-ID technique focuses on the process of identifying and classifying intrusions in the WSN. The presented SHOIDL-ID approach applies data preprocessing to normalize the input data to accomplish this. The SHOIDL-ID technique employs an attention-based bidirectional long short-term memory (ABiLSTM) approach for intrusion recognition and classification. Finally, the SHO approach is utilized for the optimal hyperparameter tuning of the ABiLSTM algorithm. The experimental validation of the SHOIDL-ID method takes place on the WSN-DS dataset.

2. Related Works

Alruhaily and Ibrahim [15] suggest a multilayer Intrusion Detection (ID) structure for WSN, in which the authors practice a defence-in-depth safety policy, where two detection levels are arranged. The initial level is situated on the dispersed network core sensors and employs an NB categorizer for the real-time decision of the examined packets. The next level was situated on the cloud server and used a Random Forest (RF) multiclass categorizer to inspect the investigated packets deeply. Zhang and Xiao [16] propose a purifying selection prototype founded on spatial partition and enforced to ordered WSN. The prototype initially evaluates self-set dispersion in the real-valued space and later separates the real-valued space, and many subspaces were attained. Pan et al. [18] recommend a Lightweight Intelligent ID prototype for WSN. Integrating Sine Cosine Algorithm (SCA) and k-Nearest Neighbor (kNN) Algorithm can knowingly enhance the categorization precision and tremendously mitigate the rate of false alarms and, in a way, intellectually detect a range of outbreaks encompassing unidentified outbreaks. The compact mechanism was enforced to SCA (CSCA) to save the computation space and period from regulating the convolution of the prototype. The Polymorphic Mutation (PM) policy was employed to reimburse for the maximization precision losses.

Mittal et al. [19], to accomplish greater effectiveness and dependable procedures in accordance with the present application policies, two popularly known energy-effective procedures, that is, Energy–Efficient Sensor Routing (EESR) and Low-Energy Adaptive Clustering hierarchy (LEACH), are restructured in view of NNs. In particular, a Levenberg–Marquardt NN (LMNN) is incorporated to enhance the outcomes regarding energy effectiveness. Also, to enhance the accomplishment, a sub-cluster LEACH-derived procedure is suggested. Tan et al. [21] suggest a technique of implementing the Synthetic Minority Oversampling Technique (SMOTE) to normalize the database and later employ the RF protocol to train the categorizer for ID.

The authors [22] construct lightweight IDS founded on two ML methods, called feature classification and feature selection. The initial categorization protocol for the present scheme was recognized by comparing DT, LR, KNN, SVM, RF, NB, and multilayer perceptron (MLP). Alqahtani et al. [23] recommend a novel prototype to identify invasion outbreaks founded on a genetic protocol and an Extreme Gradient Boosting (XGBoot) categorizer named the GXGBoost prototype. The last is a GBoost prototype constructed to enhance the accomplishment of conventional prototypes to identify fewer classes of outbreaks in the hugely non-stabilized data traffic of WSN.

3. The Proposed Model

In this study, we have designed a new SHOIDL-ID approach for the automated identification and classification of intrusions in the WSN. The presented SHOIDL-ID technique focuses on the process of identifying and classifying the intrusions in the WSN. The presented SHOIDL-ID approach encompasses three operational stages: preprocessing, ABiLSTM-based intrusion detection, and SHO-based parameter optimization. Fig. 1 represents the overall process of the SHOIDL-ID approach.

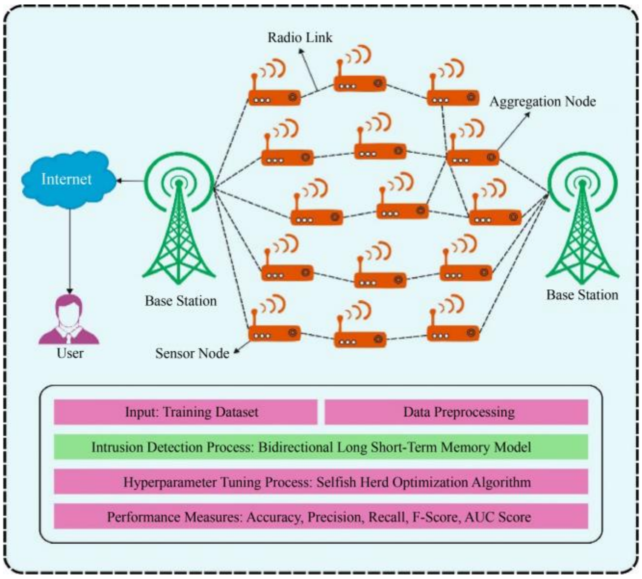

Radio Link
Aggregation Node
Internet
Base Station
Base Station
User
Sensor Node
Input: Training Dataset
Data Preprocessing
Intrusion Detection Process: Bidirectional Long Short-Term Memory Model
Hyperparameter Tuning Process: Selfish Herd Optimization Algorithm
Performance Measures: Accuracy, Precision, Recall, F-Score, AUC Score

Fig. 1 Overall Process of SHOIDL-ID Approach

3.1. Intrusion Detection using ABiLSTM Model

For intrusion recognition and classification, the SHOIDL-ID technique employed the ABiLSTM model. The RNN generate better performance of the network in modelling hidden sequential pattern of time-series dataset [25]. Typically, it can be resolved using 2 variations of RNN, namely GRU and LSTM. Theoretically, the architecture of LSTM is like RNN; however, a special unit memory cell" was presented in LSTM to replace the updating procedure of RNN. The memory cells of LSTM keep data for a long period. Consider the existing input vector x_t, the final hidden state h_{t-1}, and the final memory cell state c_{t-1}, the subsequent equation is used for implementing the LSTM model:

$$i_t = \sigma(W_{xi}x_t + W_{hi}h_{t-1} + W_{ci}c_{t-1} + b_i) \tag{1}$$

$$f_t = \sigma\left(W_{xf}x_t + W_{hf}h_{t-1} + W_{cf}c_{t-1} + b_f\right) \tag{2}$$

$$c_t = f_t c_{t-1} + i_t tanh(W_{xc}x_t + W_{hc}h_{t-1} + b_c) \tag{3}$$

$$o_t = \sigma(W_{xo}x_t + W_{ho}h_{t-1} + W_{co}c_t + b_o) \quad (4)$$

$$h_t = 0_t.tanb(c_t) \quad (5)$$

Where, 0, I, c, and f indicate the output gate, input gate, memory cell state, and forget gate at time t, correspondingly. σ signifies the sigmoid activation function; W and b demonstrate the weight and bias vector. For obtaining the entire context of any video, it can be significant to consider both directions, viz., the historical and upcoming context of the video. Thus, the BLSTM seems to be a relevant option in video classification since it keeps the data in both directions.

In BLSTM, there exist two dissimilar hidden layers represented as backward hidden layers (h_t^b) and forward hidden layer $\left(h_t^f\right)$. Where h_t^f consider backwards hidden layer h_t^b in descending sequence viz., $t = T, T-1, T-2, \dots, 1$ and the input vector x_t in ascending sequence viz., $t = 1,2,3, \dots, T$. Finally, the output y_t is produced by integrating the outcomes of h_t^f and h_t^b:

$$h_t^f = \tanh\ (W_{xh}^f x_t + W_{hh}^f hi_{t-1} + \mathrm{b}_h^{\mathrm{f}} \quad (6)$$

$$h_t^b = tanh\left(W_{xh}^b x_t + W_{hh}^b h_{t+1}^b + b_h^b\right) \quad (7)$$

$$y_t = W_{hy}^f h_{\mathrm{t}}^{\mathrm{f}} + W_{hh}^b h_t^b + b_y \quad (8)$$

Note that adding an extreme amount of layers of BLSTM raises the difficulty and reduces the training procedure. Therefore, this work applied two layers of BLSTM for understanding video representations. Fig. 2 represents the framework of BLSTM.

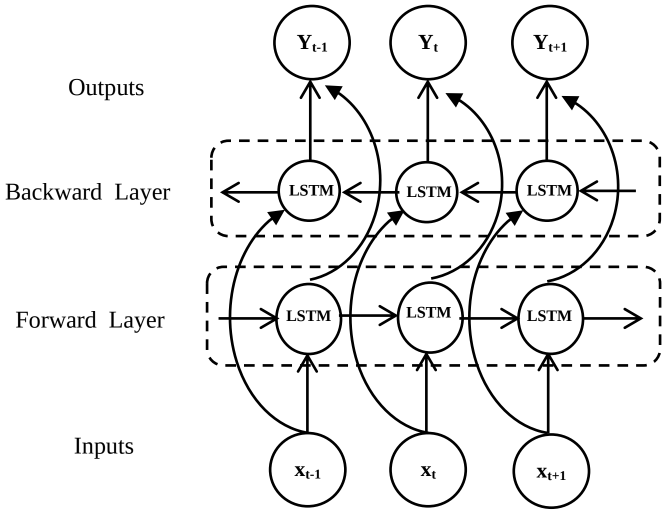


Fig. 2 Architecture of BLSTM

A NN structure with the attention model decides when to look into the dataset (segment of videos) by providing a higher focus level to the feature vector with useful data than the feature vector with lesser valuable data. Consider the last hidden state of $i\text{-}th$ BLSTM as h_{it}, which can be evaluated as follows:

$$h_{it} = \left[h_t^f, h_t^b\right] \quad (9)$$

Next, the attention model can be evaluated by the subsequent formula:

$$e_{it} = tanh(W_a h_{it} + b_a) \quad (10)$$

$$a_{it} = \frac{\exp(e_{it})}{\sum_{j=1}^{T} e\,xp(\mathrm{e})} \quad (11)$$

$$v_t = \sum_{t=1}^{T} a_{it} \,.\, h_{it} \quad (12)$$

The attention model allocates attention weight a_{it} to $i\text{-}th$ BiLSTM output vector at t time. b_a and W_a denotes the bias and weight from the attention layer. Lastly, output from the attention layer produces an attention vector v_t that can be evaluated as the weighted sum of multiplication in-between attention weight a_{it} and $i\text{-}th$ BLSTM output vector at t time.

3.2. Parameter Tuning using SHO Algorithm

In this work, the SHO algorithm is utilized for the optimal hyperparameter tuning of the ABiLSTM approach. SHO algorithm begins by setting the number of iterations (itr_{max}) and population $\left(N_p\right)$ [26]. The individual position is formulated in Eq. (13). The (N_p) can be splitted into prey (N_{pr}) and predator(N_{pd}).

$$a_{ij}^0 = x_j^{low} + rand(0,1)\left(x_j^{high} - x_j^{low}\right) \quad (13)$$

The survival with the worst and best values are expressed as follows.

$$SV_{ai} = \frac{f(a_i) - f_{best}}{f_{best} - f_{worst}} \quad (14)$$

$$f_{best/worst} = \min_{j\varepsilon\{1,2,\dots,\mathrm{K}\}} / \, max\left(\left(\min_{j\varepsilon\{1,2,\dots,\mathrm{N}\}}\left(f(a_i)\right)\right)_j\right) (15)$$

3.2.1. Structuration Stage

The member with maximum surviving or aggression factors is promoted as a leader. By using Eq. (16), the leader can be chosen. During the challenging moment, each attempt to be safe; thus, all the members upgrade the location based on the near optimum location. This new and nearest neighboring value can be defined using Eq. (17).

$$h_{Ld}^K = \left(h_j^{\mathrm{k}} \varepsilon H^{\mathrm{k}} \middle| SV_{h_i^k} = \max_{j\varepsilon\{1,2,\dots,\mathrm{N_h}\}} \left(SV_{h_j^k}\right)\right) \quad (16)$$

$$\begin{aligned} h_{N_i}^{\mathrm{k}} &= (h_j^{\mathrm{k}} \varepsilon H^k, h_j^k \neq [h_i^k, h_{Ld}^k] | SV_{hd_j^k} > SV_{\mathrm{h}_i^{\mathrm{k}}}, \mathrm{r_{ij}} \\ &= \min_{j\epsilon\{1,2,\dots,\mathrm{N_h}\}} \left(\|h_i^k - h_j^k\right) \quad (17) \end{aligned}$$

In the chasing process, the herding group can be split into two sub-groups, namely deserted herds and leader followers. Furthermore, the leader-follower is broken into two subgroups subordinate member and dominant member.

The subordinate or dominant members were evaluated by comparing with the mean survival value of herds that are shown as follows.

$$h_{Fol}^{\mathrm{k}} = \left\{h_i^{lc} \neq h_{Ld}^{k} \middle| SV_{hd_i^k} \geq rand(O,1)\right\} \tag{18}$$

$$h_{Des}^{\mathrm{k}} = \left\{h_i^{k} \neq h_{Ld}^{\mathrm{k}} \middle| SV_{hd_i^{\mathrm{k}}}, < rand(O,1)\right\} \tag{19}$$

$$h_{dom}^{k} = \left\{h_i^{k} \in h_{Fol}^{k} \middle| SV_{hd_j^{\mathrm{k}}}, \geq SV_{H_\mu^k}\right\} \tag{20}$$

$$h_{sub}^{\mathrm{k}} = \left\{h_i^{\mathrm{k}} \in h_{Fol}^{\mathrm{k}} \middle| SV_{hd_i^k} < SV_{H_\mu^k}\right\} \tag{21}$$

Where mean $survival, SV_{H_\mu^k} = \frac{\sum_{i=1}^{N} SV_{hd_i^k}}{N_{hd}}$

In this work, afterwards, forming the herd member, the centre of mass of the predator, and the herd were evaluated by the following equations representing the relative riskier or safer position.

$$hd_{cm}^{\mathrm{k}} = \frac{\sum_{i=1}^{N} S\,V_{hd_i^k} hd_i^k}{\sum_{j=1}^{N_h} S\,V_{hd_j^k}} \tag{22}$$

$$pd_{cm}^{k} = \frac{\sum_{i=1}^{N_p} S\,V_{pd_i^k} pd_i^k}{\sum_{j=1}^{N_p} S\,V_{pd_j^k}} \tag{23}$$

During chasing, the predator tries to hunt, and instantaneously, the herding group get closer towards the safer location. The leader of the herd, updating of the predator, and other members are shown in the following.

$$pd_i^{\mathrm{k}+1} = pd_i^k + 2\rho(hd_i^k - pd_i^k \tag{24}$$

$$h_{Ld}^{lc+1} = \begin{cases} h_{Ld}^k + c^{\mathrm{k}}\ if\ SV_{hd_L^k} = 0 \\ h_{Ld}^k + S^k\ if\ SV_{hd_L^{\mathrm{k}}} > 0 \end{cases} \tag{25}$$

$$h_{Ld}^{k+1} = \begin{cases} hd_i^{\mathrm{k}} + f_i^{\mathrm{k}}\ if hd_i^{\mathrm{k}} \in h_{Fol}^k \\ hd_i^{\mathrm{k}} + d_i^k\ if hd_i^{\mathrm{k}} \in h_{Dom}^k \end{cases} \tag{26}$$

Where $c^{\mathrm{k}} = 2\alpha\phi_{h_L P_M}^{\mathrm{k}}(P_M^k - h_L^k, S^k = 2\alpha\psi_{h_L X_{best}}^k(x_{best}^k - h_L^k)$

$$d_i^{\mathrm{k}} = 2\left(\beta\psi_{h_i h_{best}}^k\left(x_{best}^k - h_i^k\right) + \gamma\left(1 - SV_{h_i^k}\right)\hat{r}\right)$$

and

$$f_i^k = \begin{cases} 2\ (\beta\psi_{h_{\mathrm{i}} h_L}^{\mathrm{k}}\left(h_L^{\mathrm{k}} - h_i^{\mathrm{k}} + \gamma\psi_{h_t h_N}^k\left(h_N^k - h_i^{\mathrm{k}}\right)\right)\ if\ h_i^k \in H_d^k \\ 2\delta\psi_{h_i h_L}^k(h_M^k - h_i\ if\ h_i^{\mathrm{k}} \in H_s^k \end{cases}$$

Now, α, β, γ, and δ denote the random value differs within [0,1]. The radius of the domain of danger is expressed in Eq. (27):

$$R = \frac{\sum_{j=1}^{n} |\ x_j^{low} - x_j^{high}|}{2n} \tag{27}$$

Threatened prey of the predator can be represented as follows:

$$T_{Pi} = \left\{h_j \in h \middle| SV_{hdj} < SV_{Pi}, \left\|pd_i - hd_j\right\| \leq R, hd_j \notin \kappa\right\} \tag{28}$$

Finally, the new members are created by mating probability for restoring the size of the herding group unchanged as:

$$M_{h_j} = \frac{SV_{hd_j}}{\sum_{(hd_m \epsilon M)} S\,V_{hd_m}}, hd_j \in M \tag{29}$$

Where $M = \{h_j \notin K\}$

According to mating probability, a set of 'n' arbitrarily selected individuals from the matrix M exchange their location using the roulette selection technique. With that regard, a new solution can be created. The procedure is continued until the stopping condition is reached, viz., each herd member with maximum survival value than the predator.

The SHO approach produces a fitness function (FF) to accomplish better classifier results. It explains a positive integer to exemplify the good efficiency of candidate results. Here, the minimal classifier rate of errors regards that FF is written in Eq. (24).

$$fitness(x_i) = ClassifierErrorRate(x_i)$$

$$= \frac{number\ of\ misclassified\ samples}{Total\ number\ of\ samples} * 100 \tag{30}$$

4. Results and Discussion

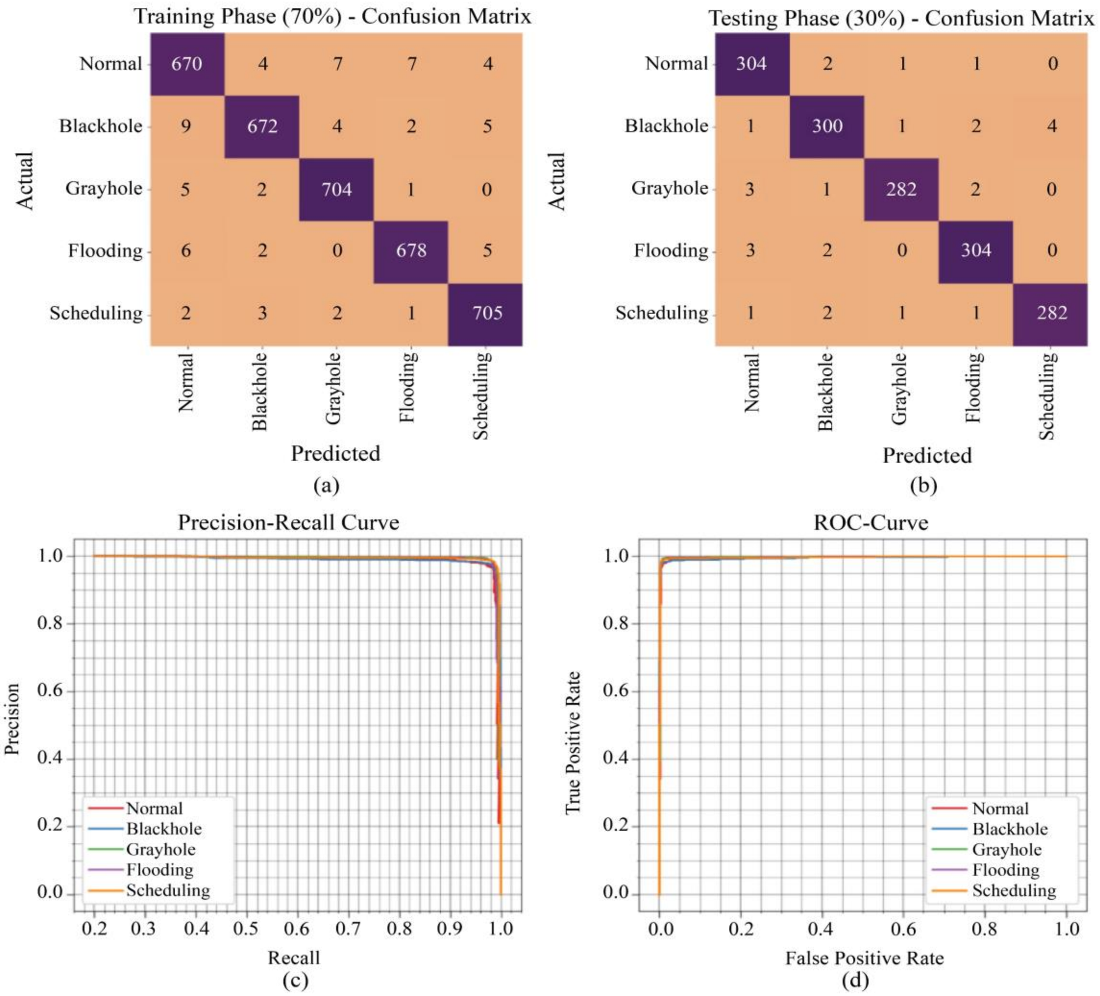
In this section, the results of the SHOIDL-ID technique are studied on the WSN-DS Public Dataset [27], comprising 5000 instances with five classes, as defined in Table 1.

Table 1. Details of dataset

Class	No. of Instances
Normal	1000
Blackhole	1000
Grayhole	1000
Flooding	1000
Scheduling	1000
Total Number of Instances	**5000**

Fig. 3 exhibits the classifier results of the SHOIDL-ID technique under the test dataset. Fig. 3a portrays the confusion matrix obtainable by the SHOIDL-ID method on 70% of TRP. The figure denoted that the SHOIDL-ID model has detected 670 instances under normal, 672 instances under blackhole, 704 instances on grayhole, 678 instances on flooding, and 705 samples on scheduling. Besides, Fig. 3b displays the confusion matrix offered by the SHOIDL-

ID technique on 30% of TSP. The figure denoted that the SHOIDL-ID method has identified 304 samples on normal, 300 samples on blackhole, 282 samples on grayhole, 304 samples on flooding, and 282 samples on schedule. Likewise, Fig. 3c demonstrates the PR analysis of the SHOIDL-ID model. The figures stated that the SHOIDL-ID method had obtained maximum PR performance in all classes. Finally, Fig. 3d illustrates the ROC investigation of the SHOIDL-ID model. The figure depicted that the SHOIDL-ID approach has proficient results with higher ROC values on five class labels.



(a)

(b)

(c)

(d)

Fig. 3 Classifier outcome of (a-b) Confusion matrices of 70:30, (c) PR curve, and (d) ROC curve

Table 2. Intrusion outcome of SHOIDL-ID approach on 70% of TRP with varying classes

Training Phase (70%)					
Labels	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	**AUC Score**
Normal	98.74	96.82	96.82	96.82	98.02
Blackhole	99.11	98.39	97.11	97.75	98.36
Grayhole	99.40	98.19	98.88	98.53	99.21
Flooding	99.31	98.40	98.12	98.26	98.86
Scheduling	99.37	98.05	98.88	98.46	99.19
Average	**99.19**	**97.97**	**97.96**	**97.96**	**98.73**

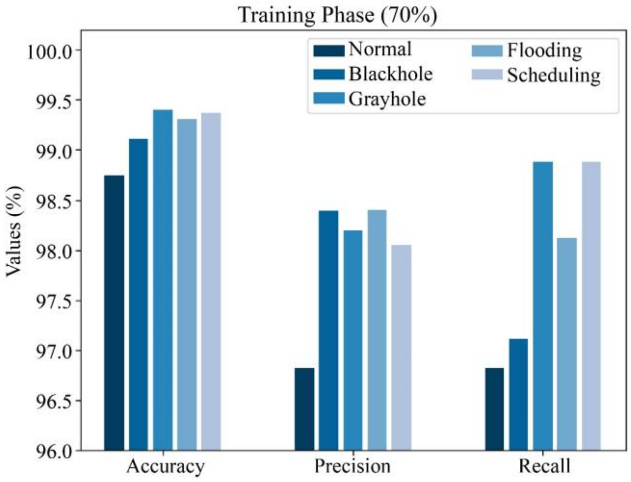


Fig. 4 $Accu_y$, $prec_n$, and $reca_l$ the outcome of the SHOIDL-ID approach on 70% of TRP

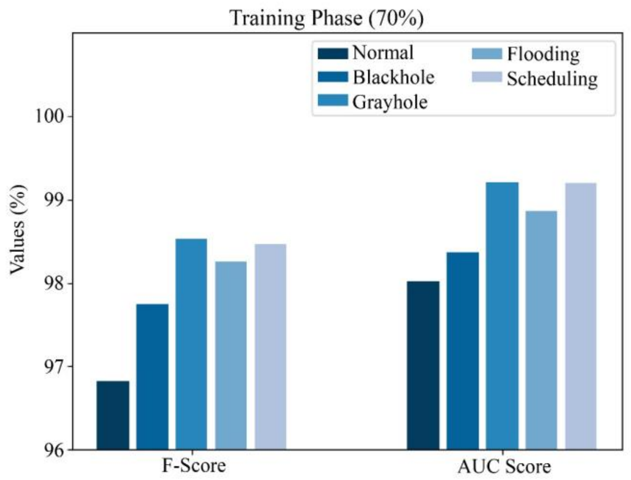


Fig. 5 F_{score} and AUC_{score} the outcome of the SHOIDL-ID approach on 70% of TRP

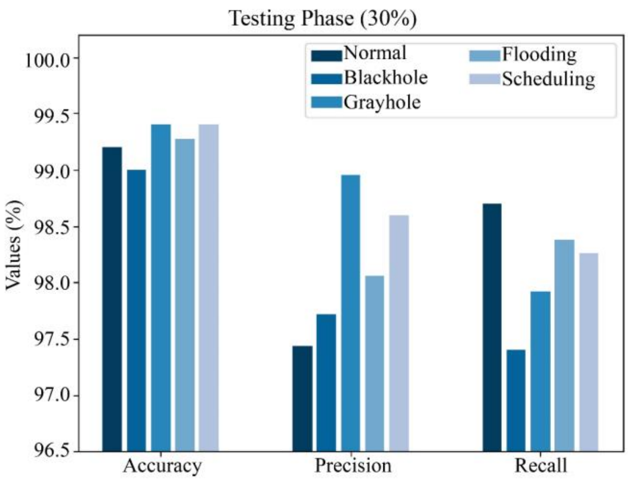


Fig. 6 $Accu_y$, $prec_n$, and $reca_l$ the outcome of the SHOIDL-ID approach on 30% of TSP

In Table 2, the overall intrusion outcomes of the SHOIDL-ID technique are reported under 70% of TRP. Fig. 4 inspects the results of the SHOIDL-ID technique in terms of $accu_y$, $prec_n$, and $reca_l$. In a normal class, the SHOIDL-ID technique reaches $accu_y$, $prec_n$, and $reca_l$ of 98.74%, 96.82%, and 96.82% respectively. Also, in the grayhole class, the SHOIDL-ID method reaches $accu_y$, $prec_n$, and $reca_l$ of 99.40%, 98.19%, and 98.88% respectively. Meanwhile, on scheduling class, the SHOIDL-ID method reaches $accu_y$, $prec_n$, and $reca_l$ of 99.37%, 98.05%, and 98.88% correspondingly.

Fig. 5 scrutinizes the results of the SHOIDL-ID method in terms of F_{score} and AUC_{score}. In a normal class, the SHOIDL-ID technique reaches F_{score} and AUC_{score} of 96.82% and 98.02%, respectively. In addition, in the grayhole class, the SHOIDL-ID technique reaches F_{score} and AUC_{score} of 98.53% and 99.21%, respectively. In the meantime, on scheduling classes, the SHOIDL-ID technique reaches F_{score} and AUC_{score} of 98.46% and 99.19%, respectively.

In Table 3, the complete intrusion outcomes of the SHOIDL-ID technique are reported under 30% of TSP. Fig. 6 illustrates the outcomes of the SHOIDL-ID technique in terms of $accu_y$, $prec_n$, and $reca_l$. In a normal class, the SHOIDL-ID technique reaches$accu_y$, $prec_n$, and $reca_l$ of 99.20%, 97.44%, and 98.70% correspondingly.

Table 3. Intrusion outcome of SHOIDL-ID approach on 30% of TSP with varying classes

Testing Phase (30%)					
Labels	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	**AUC Score**
Normal	99.20	97.44	98.70	98.06	99.02
Blackhole	99.00	97.72	97.40	97.56	98.41
Grayhole	99.40	98.95	97.92	98.43	98.83
Flooding	99.27	98.06	98.38	98.22	98.94
Scheduling	99.40	98.60	98.26	98.43	98.96
Average	**99.25**	**98.15**	**98.13**	**98.14**	**98.83**

Similarly, in the grayhole class, the SHOIDL-ID technique reaches $accu_y$, $prec_n$, and $reca_l$ of 99.40%, 98.95%, and 97.92% respectively. In the meantime, on scheduling class, the SHOIDL-ID approach reaches $accu_y$, $prec_n$, and $reca_l$ of 99.40%, 98.60%, and 98.26% respectively.

Fig. 7 examines the outcomes of the SHOIDL-ID scheme in terms of F_{score} and AUC_{score}. In a normal class, the SHOIDL-ID technique reaches F_{score} and AUC_{score} of 98.06% and 99.02%, respectively. Further, in grayhole class, the SHOIDL-ID technique reaches F_{score} and AUC_{score} of 98.43% and 98.83%, respectively. In the meantime, on scheduling classes, the SHOIDL-ID technique reaches F_{score} and AUC_{score} of 98.43% and 98.96% correspondingly.

Fig. 8 examines the accuracy of the SHOIDL-ID technique during the training and validation process on the test database. The figure reports that the SHOIDL-ID method reaches increasing accuracy values over increasing epochs. In addition, the increasing validation accuracy over training accuracy exhibits that the SHOIDL-ID technique learns efficiently on the test database.

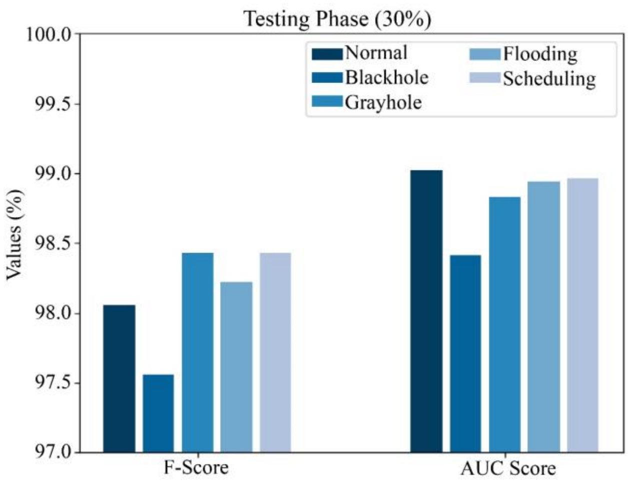


Fig. 7 F_{score} and AUC_{score} the outcome of the SHOIDL-ID approach on 30% of TSP

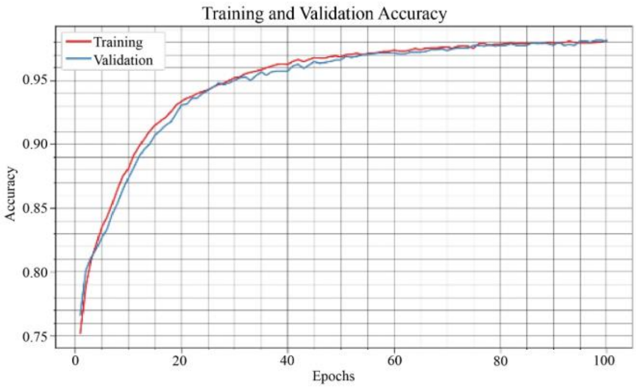


Fig. 8 Accuracy curve of the SHOIDL-ID approach

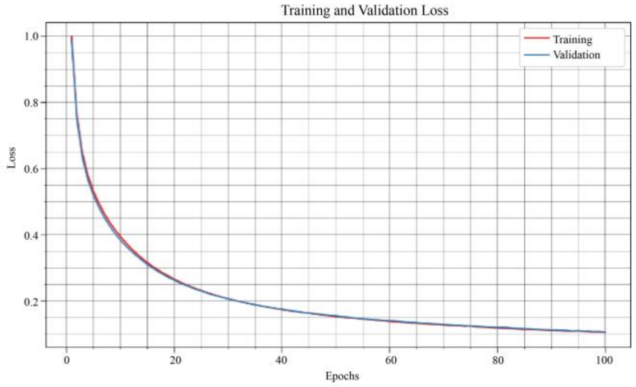


Fig. 9 Loss curve of the SHOIDL-ID approach

The loss analysis of the SHOIDL-ID technique at the time of training and validation is demonstrated on the test database in Fig. 9. The figure indicates that the SHOIDL-ID technique reaches closer values of training and validation loss. The SHOIDL-ID method learns efficiently on the test database.

Table 4 reports the overall comparative study of the SHOIDL-ID system is reported clearly [28]. The results indicate that the SVM, LR, and NB models obtain poor performance over other models. Next, the DT model has tried to report moderately improved outcomes.

Table 4. Comparative outcome of SHOIDL-ID method with existing systems

Methods	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}
SHOIDL-ID	99.25	98.15	98.13	98.14
NB Algorithm	96.34	75.29	84.96	76.51
SVM Algorithm	95.79	82.77	82.87	81.70
LR Algorithm	95.83	85.08	83.69	84.50
DT Algorithm	97.01	96.78	97.89	96.90
XG-Boost	98.71	95.99	97.10	97.65
SLGBM	98.89	97.23	97.19	97.31

Although the XGBoost and SLGBM models highlight reasonable results, the SHOIDL-ID technique gains maximum $accu_y$ of 99.25%, $prec_n$ of 98.15%, $reca_l$ of 98.13%, and F_{score} of 98.14%. These outcomes show the enhanced outcome of the SHOIDL-ID method over other present techniques.

5. Conclusion

In this article, we have designed a new SHOIDL-ID methodology for automated classification and identification of intrusions in the WSN. The presented SHOIDL-ID technique focuses on the process of classifying and identifying the intrusions in the WSN. The presented SHOIDL-ID approach applies data preprocessing to normalize the input data to accomplish this. For intrusion recognition and classification, the SHOIDL-ID technique employed the ABiLSTM model. Finally, the SHO technique is exploited for the optimal hyperparameter tuning of the ABiLSTM method. The experimental validation of the SHOIDL-ID algorithm takes place on the WSN-DS database. The outcomes indicate the improved performance of the SHOIDL-ID method over other existing approaches in terms of different measures. In the future, feature selection approaches can boost the SHOIDL-ID technique's performance.

References

[1] Abhilash Singh et al., “LT-FS-ID: Log-Transformed Feature Learning and Feature-Scaling-Based Machine Learning Algorithms to Predict the K-Barriers for Intrusion Detection Using Wireless Sensor Network,” *Sensors*, vol. 22, no. 3, p. 1070, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] Nitin Goyal, Jasminder Kaur Sandhu, and Luxmi Verma, “Machine Learning based Data Agglomeration in Underwater Wireless Sensor Networks,” *International Journal of Management, Technology and Engineering*, vol. 9, no. 6, pp.240-245, 2019. [Google Scholar]

[3] V. Subburaj et al., “DDoS Defense Mechanism by Applying Stamps using Cryptography,” *International Journal of Computer Applications*, vol. 1, no. 6, pp. 48-52, 2010.

[4] I. Gethzi Ahila Poornima, and B. Paramasivan, “Anomaly Detection in Wireless Sensor Network Using Machine Learning Algorithm,” *Computer Communications*, vol. 151, pp. 331-337, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[5] Dongxian Yu, Jiatao Kang, and Junlei Dong “Service Attack Improvement in Wireless Sensor Network Based on Machine Learning,” *Microprocessors and Microsystems*, vol. 80, p. 103637, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[6] S. Gavaskar, R. Surendiran, and E. Ramaraj, “Three Counter Defense Mechanism for TCP SYN Flooding Attacks,” *International Journal of Computer Applications*, vol. 6, no. 6, pp. 12-15, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[7] Periasamy Nancy et al., “Intrusion Detection using Dynamic Feature Selection and Fuzzy Temporal Decision Tree Classification for Wireless Sensor Networks,” *IET Communications*, vol. 14, no. 5, pp. 888-895, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[8] Lansheng Han et al., “Intrusion Detection Model of Wireless Sensor Networks Based on Game Theory and an Autoregressive Model,” *Information Sciences*, vol. 476, pp. 491-504, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[9] Rui-Hong Dong, Hou-Hua Yan, and Qiu-Yu Zhang, “An Intrusion Detection Model for Wireless Sensor Network Based on Information Gain Ratio and Bagging Algorithm,” *International Journal of Network Security*, vol. 22, no. 2, pp. 218-230, 2020. [CrossRef] [Google Scholar]

[10] Gaoming Yang et al., “An Intrusion Detection Algorithm for Sensor Network Based on Normalized Cut Spectral Clustering,” *PloS one*, vol. 14, no. 10, p. e0221920, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[11] R. Surendiran, and K. Alagarsamy, “A Crtitical Approach for Intruder Detection in Mobile Devices,” *SSRG International Journal of Computer Science and Engineering*, vol. 1, no. 4, pp.6-14, 2014. [CrossRef] [Publisher Link]

[12] Abhishek Raghuvanshi et al., “Intrusion Detection Using Machine Learning for Risk Mitigation in Iot-Enabled Smart Irrigation in Smart Farming,” *Journal of Food Quality*, pp. 1-8, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Bandar Almaslukh et al., “Deep Learning and Entity Embedding-Based Intrusion Detection Model for Wireless Sensor Networks,” *Computers, Materials & Continua*, vol. 69, pp. 1343-1360, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] Prabhdeep Singh, Navdeep Kaur, and Ravneet Kaur, "A Review: Comparative Analysis of Routing Protocols in Wireless Sensor Network," *International Journal of P2P Network Trends and Technology*, vol. 3, no. 1, pp. 12-17, 2013. [Google Scholar] [Publisher Link]

[15] Nada M. Alruhaily, and Dina M. Ibrahim, “A Multi-Layer Machine Learning-Based Intrusion Detection System for Wireless Sensor Networks,” *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 4, pp. 281-288, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[16] Ruirui Zhang, and Xin Xiao, “Intrusion Detection in Wireless Sensor Networks with an Improved NSA Based on Space Division,” *Journal of Sensors*, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[17] Ravneet Kaur, Deepika Sharma, and Navdeep Kaur, "Comparative Analysis of Leach and its Descendant Protocols in Wireless Sensor Network," *International Journal of P2P Network Trends and Technology*, vol. 3, no. 1, pp. 22-27, 2013. [Google Scholar] [Publisher Link]

[18] Jeng-Shyang Pan et al., “A Lightweight Intelligent Intrusion Detection Model for Wireless Sensor Networks,” *Security and Communication Networks*, pp. 1-15, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[19] Mohit Mittal et al., “Machine Learning Techniques for Energy Efficiency and Anomaly Detection in Hybrid Wireless Sensor Networks,” *Energies*, vol. 14, no. 11, p. 3125, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[20] Aashima Singla, and Ratika Sachdeva, "Review on Energy Conservation in Wireless Sensor Network," *International Journal of P2P Network Trends and Technology*, vol. 3, no. 2, pp. 1-3, 2013. [Publisher Link]

[21] Xiaopeng Tan et al., “Wireless Sensor Networks Intrusion Detection Based on SMOTE and the Random Forest Algorithm,” *Sensors*, vol. 19, no. 1, p. 203, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[22] Samir Fenanir, Fouzi Semchedine, and Abderrahmane Baadache, “A Machine Learning-Based Lightweight Intrusion Detection System for the Internet of Things,” *Revue d'Intelligence Artificielle*, vol. 33, no. 3, pp. 203-211, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[23] Mnahi Alqahtani et al., “A Genetic-Based Extreme Gradient Boosting Model for Detecting Intrusions in Wireless Sensor Networks,” *Sensors*, vol. 19, no. 20, p. 4383, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[24] S. Gavaskar, E. Ramaraj, and R. Surendiran, “A Compressed Anti IP Spoofing Mechanism Using Cryptography,” *International Journal of Computer Science and Network Security*, vol. 12, no. 11, pp. 137-140, 2012. [Google Scholar]

[25] Kanwal Yousaf, and Tabassam Nawaz, “A Deep Learning-Based Approach for Inappropriate Content Detection and Classification of Youtube Videos,” *IEEE Access*, vol. 10, pp. 16283-16298, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[26] Narendra Kumar Jena et al., “Fuzzy Adaptive Selfish Herd Optimization Based Optimal Sliding Mode Controller for Frequency Stability Enhancement of a Microgrid,” *Engineering Science and Technology, An International Journal*, vol. 33, p. 101071, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[27] Iman Almomani, Bassam Al-Kasasbeh, and Mousa AL-Akhras, “WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks,” *Journal of Sensors*, pp. 1–16, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[28] Shuai Jiang, Juan Zhao, and Xiaolong Xu “SLGBM: An Intrusion Detection Mechanism for Wireless Sensor Networks in Smart Environments,” *IEEE Access*, vol. 8, pp. 169548-169558, 2020. [CrossRef] [Google Scholar] [Publisher Link]