FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 1 | Pages 219-227 | e-ISSN: 2347-470X

Improving Intrusion Detection using Satin Bowerbird Optimization with Deep Learning Model for IIoT Environment

E. Anbalagan[1], Dr P S V Srinivasa Rao[2], Dr. P. Vijayan[3], Dr Amarendra Alluri[4], Dr. D. Nageswari[5] and Dr. R. Kalaivani[6*]

[1]Professor Department of Computer science and Engineering Saveetha School of engineering, Saveetha Institute of medical and technical sciences, Kanchipuram, Chennai, India; anbalagane.sse@saveetha.com
[2]Professor Department of Cyber security Sphoorthy Engineering College, Nadargul (V), Saroornagar (M), Hyderabad, India; parimirao66@gmail.com
[3]Assistant Professor (SG), Department of Artificial Intelligence and Data Science, Saveetha Engineering College, Thandalam, Chennai, India; vijeyanpanneerselvam@gmail.com
[4] Professor EEE Department SR Gudlavalleru Engineering College, Gudlavalleru, India; amarendra@gecgudlavallerumic.in
[5]Assistant professor Department of Science and humanities (General engineering Division) R.M.K. College of Engineering and Technology, Puduvoyal, India; nageswari@rmkcet.ac.in
[6]Professor Department of Electronics &Communication Engineering Erode Sengunthar ENGINEERING college, India; kalaivaniassistantprofessor@gmail.com

*__Correspondence:__ Dr. R. Kalaivani; kalaivaniassistantprofessor@gmail.com

ABSTRACT- Intrusion Detection in the Industrial Internet of Things (IIoT) concentrations on the security and safety of critical structures and industrial developments. IIoT extends IoT principles to industrial environments, but linked sensors and devices can be deployed for monitoring, automation, and control of manufacturing, energy, and other critical systems. Intrusion detection systems (IDS) in IoT drive to monitor network traffic, device behavior, and system anomalies for detecting and responding to security breaches. These IDS solutions exploit a range of systems comprising signature-based detection, anomaly detection, machine learning (ML), and behavioral analysis, for identifying suspicious actions like device tampering, unauthorized access, data exfiltration, and denial-of-service (DoS) attacks. This study presents an Improving Intrusion Detection using Satin Bowerbird Optimization with Deep Learning (IID-SBODL) model for IIoT Environment. The IID-SBODL technique initially preprocesses the input data for compatibility. Next, the IID-SBODL technique applies Echo State Network (ESN) model for effectual recognition and classification of the intrusions. Finally, the SBO algorithm optimizes the configuration of the ESN, boosting its capability for precise identification of anomalies and significant security breaches within IIoT networks. By widespread simulation evaluation, the experimental results pointed out that the IID-SBODL technique reaches maximum detection rate and improves the security of the IIoT environment. Through comprehensive experimentation on both UNSW-NB15 and UCI SECOM datasets, the model exhibited exceptional performance, achieving an average accuracy of 99.55% and 98.87%, precision of 98.90% and 98.93%, recall of 98.87% and 98.80%, and F-score of 98.88% and 98.87% for the respective datasets. The IID-SBODL model contributes to the development of robust intrusion detection mechanisms for safeguarding critical industrial processes in the era of interconnected and smart IIoT environments.

Keywords: Industrial Internet of Things; Denial-of-Service; Echo State Network; Intrusion detection system; Cybersecurity.

ARTICLE INFORMATION

Author(s): E. Anbalagan, Dr P S V Srinivasa Rao, Dr. P. Vijayan, Dr Amarendra Alluri, Dr. D. Nageswari and Dr.R.Kalaivani;
Received: 30/10/2023; **Accepted**: 13/01/2024; **Published**: 20/03/2024;
e-ISSN: 2347-470X;
Paper Id: IJEER 3010-28;
Citation: 10.37391/IJEER.120131
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-12/ijeer-120131.html

Publisher's Note: FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

Industrial Internet of Things (IIoT) is a system of machine form IoT tools which discover uses in several areas in order to assist business system's effectiveness, enterprise real-time mechanization as well as decrease operative and maintenance prices [1]. Conventional IIoT is a system of industrial control methods which is termed Operational Technology (OT) through exclusive communication procedures [2]. General Electric (GE) labelled it as "an IoT, computers, machinery, and persons permitting intelligent processes by utilizing advanced data analytics in order to change business performance". However, resource-constrained industrial IoT devices need extra resources for implementing novel cybersecurity features [3]. Cybersecurity is anxious with the defines of software, data, and electronics together with the actions where the systems are retrieved. Generally, the security aims include privacy, in terms of data that is not improperly released to the individuals must be destroyed [4]. Hence, society is becoming helpless to

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 1 | Pages 219-227 | e-ISSN: 2347-470X

cyber-threats like denial-of-service (DoS) attacks by hackers because of the limitless present IoT-based connected devices [5]. For example, that reject direct access to devices, etc. In present scenario, technology is becoming one of the main points in everyone's daily lives that means cybersecurity and cybercrime tools develop parallel throughout the entire manufacturing sector that requires spending on cybersecurity but new tools are evolving for IoT cybersecurity management [6].

Additionally, cyber-attacks on smart networks act as key structure modules that are mainly defenceless and allow better costs [7]. Presently, there is a developing anxiety about cybersecurity as well as absence of real countermeasures [8]. In order to elaborate a little more, detection techniques can be categorized into knowledge-based and then anomaly-based models [9]. Whereas, the knowledge-based model depends upon off-the-shelf databases for the purpose of detection which cannot recognize unknown attacks while anomaly-based model naturally raises ML approaches in order to identify traffic. For the method of desi, the IDSs can be divided into 3 categories such as hybrid, centralized, and distributed [10]. Exactly, the distributed IDS works on every physical device in the network and conducts the intrusion detection individually.

This study presents an Improving Intrusion Detection using Satin Bowerbird Optimization with Deep Learning (IID-SBODL) model for IIoT Environment. The IID-SBODL technique initially pre-processes the input data for compatibility. Next, the IID-SBODL technique applies Echo State Network (ESN) model for effectual recognition and classification of the intrusions. Finally, the SBO algorithm optimizes the configuration of the ESN, boosting its capability for precise identification of anomalies and significant security breaches within IIoT networks. By widespread simulation evaluation, the experimental results pointed out that the IID-SBODL technique reaches maximum detection rate and improves the security of the IIoT environment.

The IID-SBODL model addresses critical limitations in existing IIoT Intrusion Detection Systems by specifically targeting resource-constrained industrial IoT devices. Unlike conventional approaches, which struggle with computational constraints, the IID-SBODL technique optimizes intrusion detection without overburdening these devices. Furthermore, it tackles the challenge of recognizing unknown attacks that knowledge-based models often fail to address. By integrating the Satin Bowerbird Optimization with Deep Learning, the model enhances the effectiveness of anomaly-based detection using the Echo State Network model. This innovative approach aims to significantly improve the overall security of IIoT environments by precisely identifying anomalies and potential security breaches.

2. RELATED WORKS

In [11], an intelligent detection technique for detecting cyberattacks was introduced. This method employs the singular value decomposition (SVD) approach for decreasing data features and enhancing identification outcomes. Then, the SMOTE algorithm was employed to prevent under-fitting and over-fitting problems. Numerous ML and DL methods are applied to classify data for multi-class and binary classification. In [12], a semi-supervised DL system for intrusion detection (SS-Deep-ID) was presented. An enhanced traffic attention (TA) mechanism was developed for evaluating the significance score. This architecture could be simply incorporated as a fog-assisted IoT network to provide effective real-time intrusion detection.

Marzouk et al. [13] projected a new hybrid DL with meta-heuristics-assisted intrusion detection (HDL-MEID) method. This approach devises a novel chaotic mayfly optimizer (CMFO) based clustering model for efficiently selecting the CH and establishing clusters. Besides, equilibrium optimization with hybrid CNN-LSTM (HCNN-LSTM) assisted classification method could be obtained to recognize the intrusions. In [14], a network intrusion detection classification method (NIDS-CNNLSTM) depends on DL has been implemented. This approach integrates the robust learning capability of LSTM-NN in time series data, categorizes and learns the chosen features via the CNN, and confirms the applicability dependent upon multi-classification and binary classification conditions.

In [15], a DL-based WEMI IDS was implemented in this work. Primarily, this work presents the utilization of Kalman and changing average filters from the fingerprint removal phase. Secondarily, the time and frequency domain features have been removed. Lastly, the study examines the effectiveness of the WEMI-IDS. Alalayah et al. [16] used a Hunger Games Search Optimizer with DL-Driven Intrusion Detection (HGSODLID) method. The Sparrow Search Optimizer (SSO) could be exploited with GCN for classifying and recognizing intrusions. Next, the SSO algorithm has been employed for fine-tuning the hyper parameters included in the GCN architecture. This introduced HGSODL-ID technique could be empirically tested through a standard database. In Table 1, the Comparison of the Existing work is discussed.

Table 1: Comparison of the Existing work

Reference(s)	Methodology	Key Features and Contributions
[11]	SVD and SMOTE	Feature reduction with SVD, addressing under/over-fitting. Multiple ML and DL methods for classification.
[12]	SS-Deep-ID with enhanced TA	Semi-supervised DL for real-time intrusion detection in fog-assisted IoT networks.
[13]	HDL-MEID with CMFO and HCNN-LSTM	Hybrid DL with meta-heuristics-assisted intrusion detection. Utilizes chaotic mayfly optimizer for clustering and HCNN-LSTM for classification.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 1 | Pages 219-227 | e-ISSN: 2347-470X

[14]	NIDS-CNNLSTM	DL-based network intrusion detection. Integrates LSTM-NN and CNN for feature learning in multi/binary classification.
[15]	DL-based WEMI IDS	DL-based Wireless Electromagnetic Imaging Intrusion Detection System. Utilizes Kalman and changing average filters.
[16]	HGSODLID with SSO and GCN	Hunger Games Search Optimizer with DL-Driven Intrusion Detection. Empirically tested through a standard database.

3. THE PROPOSED METHOD

In this article, a novel IID-SBODL model for IIoT Environment. The IID-SBODL technique initially pre-processes the input data for compatibility. Next, the IID-SBODL technique applies ESN model for effectual recognition and classification of the intrusions. Finally, the SBO algorithm optimizes the configuration of the ESN model. *fig. 1* signifies the workflow of IID-SBODL method.

Consider conducting experiments with other publicly available IIoT datasets to provide a more comprehensive evaluation of the model's generalizability and robustness. This would allow for a comparative study and a clearer assessment of the precision of the proposed model. The UNSW-NB15 dataset, originating from a real-world industrial network, encompasses a variety of cyber threats, making it an ideal benchmark for evaluating the IID-SBODL model's ability to handle different types of intrusions. Its inclusion in the experiments would enable a comparative analysis, showcasing how the proposed model performs in comparison to existing methods under similar conditions. Similarly, the UCI SECOM dataset, which is designed for semiconductor manufacturing processes, introduces a different set of challenges. Evaluating the IID-SBODL model on this dataset would provide insights into its adaptability to distinct IIoT settings. Robustness and precision across datasets are crucial aspects for any intrusion detection model, and this expanded experimentation would contribute to a more thorough assessment. Conducting experiments on multiple datasets also allows for a better understanding of how well the IID-SBODL model generalizes to diverse environments and whether its performance improvements observed in one setting carry over to others. This comparative study would enhance the reliability of the findings and provide a clearer picture of the model's practical utility in industrial cybersecurity.

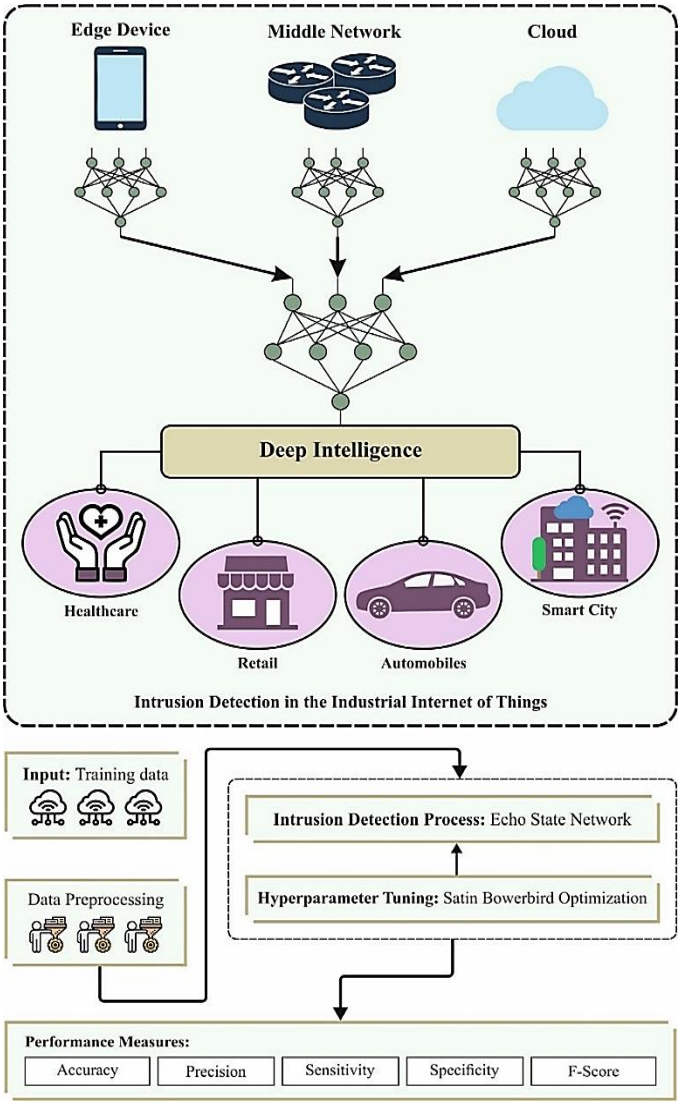


Figure 1. Workflow of IID-SBODL algorithm

4. DATA PRE-PROCESSING

Min-max normalization is also called feature scaling. It is data pre-processing method that is utilized to change mathematical features within an exact range, normally between 0 and 1. This procedure includes rescaling the information by subtracting the least value of the feature and then separating it by the range (variance among maximum and minimum values). Min-max normalization is highly beneficial in machine learning (ML) because it safeguards all features which have a similar scale, avoiding assured attributes from leading others at the time of model training and enhancing the merging as well as performance of diverse algorithms, chiefly those sensitive to the extent of input features.

Prior to any analysis, the dataset undergoes a comprehensive data cleaning process to identify and rectify errors, missing values, and inconsistencies. This ensures the dataset's integrity and reliability for subsequent processing. The dataset is subjected to min-max normalization, a widely utilized method

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 1 | Pages 219-227 | e-ISSN: 2347-470X

in machine learning. This process scales mathematical features to a specific range, typically between 0 and 1. By rescaling the data through subtracting the minimum feature value and dividing it by the range (difference between maximum and minimum values), min-max normalization ensures uniform scales across all features. This is crucial for preventing certain features from dominating others during model training, promoting algorithm convergence, and improving the overall performance of various machine learning algorithms. Beyond normalization, the methodology incorporates feature engineering techniques to extract relevant information, enhance model interpretability, and potentially improve predictive performance. Feature engineering may involve creating new features, transforming existing ones, or selecting a subset of features that contribute most effectively to the predictive task.

4.1 ESN based Classification

The model of ML requires numerous calculations and continues for a long time. The integrated learning method makes the technique plan extra struggle which is not helpful in upgrading the method [17]. ESN is considered an effective technique for training RNNs which is more beneficial than a simply tested process as well as short time consumption. It defines the $u(n) = [u_1(n) \cdots u_k(n)]^T$ as input example at period n. $y(n)$ denotes to the subsequent equal to(n). An input matrix W_{in} and $\widehat{W}$ is reservoir layer biased matrix are regularly circulated between [-1, 1] which sustained endlessly. In the verified process, by example input, the reservoir level can be updated by employing following expression.

$$x(n+1) = f\left(W_{in}u(n+1) + \widehat{W}x(n)\right) \quad (1)$$

Whereas $\widehat{W}$ denotes to the reservoir state link matrix, f signifies the initiation work in the reservoir state is normally attained severely as hyperbolic curve tasks, and W_{in} indicates the input link matrix. Depending on the above-mentioned state of reservoir layers, subsequent ESN is considered using following formulation.

$$y(n+1) = f_{out}\left(W_{out}x(n+1)\right) \quad (2)$$

W_{out} Stands for resultant association matrix, and f_{out} signifies the consequential excitation function. During the verified process, the reservoir state has been combined as a state matrix X. The final system output weighted W_{out} has been calculated by employing consequent formula.

$$W_{out} = (X^T X)^{-1} X^T Y \quad (3)$$

Whereas T denotes the matrix transpose and -1 means inverse of matrix. X States the matrix process of input reservoir layer, and Y validates the outcome matrix model. An optimal result of subsequent matrix has been introduced by consuming smallest squares or MSE only. *Figure. 2* depicts the architecture of ESN.

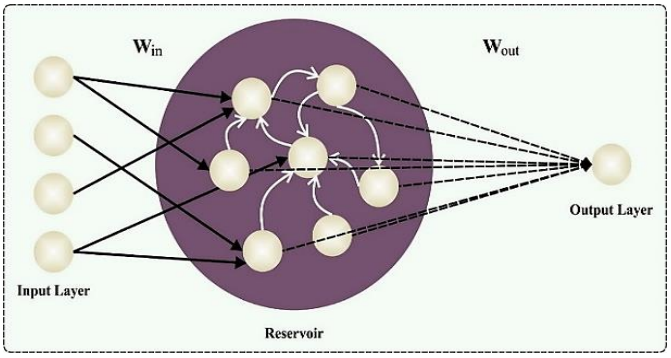


Figure 2. Structure of ESN

4.2 SBO based Parameter Tuning

SBO method begins by creating even arbitrary people which includes a group of locations to bower [18]. Every location (pop(i), Pos) which is definite to the unstable that is supposed will increase as mentioned in *eq. (5)*. It is determined that the cost of original populace lies between current least as well as greatest limit of improving parameter.

$$pop\,(i)\,.Pos\; = rand(1, n_{var}) \cdot (Var_{\text{Max}} - Var_{\text{Min}}) + Var_{\text{Min}}, \forall i \in n_{Pop} \quad (4)$$

Moderately, connected to ABC, the possibility of absorbing female/male (Prob_i) to bower is estimated via:

$$Prob_i = \frac{cost_i}{\sum_{k=1}^{n_{Pop}} c\,ost_i}, \forall i \in n_{Pop} \quad (5)$$

$$\cos t_i = \begin{cases} \frac{1}{1+f(x_i)}, f(x_i) \geq 0 \\ 1 + |f(x_i)|, f(x_i) < 0 \end{cases} \quad (6)$$

Similar to last evolutionary that is generated on optimizer, superiority was demoralized in order to supply an optimum answer at each iteration. At the time of mating, males alike all bird uses their energies for garnishing as well as constructing the bower. Extraordinarily, skilled and adult males are concerned attention of others to the bower. Additionally, these bowers have extra fitness when compared to other bowers. In SBO procedure, place of optimum bower created by bird was evaluated as elite of k^{th} iteration $(x_{elite,k})$ viz., maximum fitness and capable of upsetting other places. In every iteration, a new alteration at definite bower intended depends on subsequent equation:

$$\chi_{ik}^{new} = \chi_{i,k}^{old} + \beta_k \left[\left(\frac{x_{jk} + x_{elite,k}}{2}\right) - \chi_{i,k}^{old}\right] \quad (7)$$

Remember that roulette wheel discerning model was irregular for picking bower with improved possibility(x_{jk}). Variable β_k defines the step count choice objective bower which is estimated to every adaptable in SBO model as:

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 1 | Pages 219-227 | e-ISSN: 2347-470X

$$\beta_k = \frac{\alpha}{1 + Prop_i} \quad (8)$$

Arbitrary modification was realized to x_{ik} with definite possibility, where (N) defines normal distribution was used by alteration of σ and then average of $x_{i,k}^{old}$ as follows:

$$X_{ik}^{neω} \sim X_{ik}^{old} + \sigma \cdot N(0,1) \quad (9)$$
$$\sigma = Z \cdot (Var_{\text{Max}} - Var_{\text{Min}})$$

Finally, every cycle an elderly populace and people gained as mentioned beyond were organized, combined, and evaluated as well a new populace was produced.

Algorithm 1: Pseudocode SBO Model

Input: Population $\overrightarrow{P_{sp}}$
Output: Optimal searching agent, $\overrightarrow{P_{bst}}$
Procedure SOA
Parameter Initialized: C_A and C_B
Describe the fitness of every penetrating agent
$\overrightarrow{P_{bst}} \leftarrow$ optimal searching agent
While $(z < Max_{iterations})\ do$
for every search agent do
Update the searching agent's place
end for
Update parameters C_A and C_B
Term fitness value of all the searching agent
Update $\overrightarrow{P_{bst}}$ if optimal solution occurs above prior optimum solution
$z \leftarrow z + 1$
End while
Return $\overrightarrow{P_{bst}}$
End process

The Satin Bowerbird Optimization (SBO) algorithm is a nature-inspired optimization technique outlined in the pseudocode. In this algorithm, a population of potential solutions, denoted as (P_sp) $^{\rightarrow}$, undergoes iterative updates to identify the optimal searching agent (P_bst) $^{\rightarrow}$. The process begins with initializing control parameters C_A and C_B that influence the behavior of search agents during the optimization. The optimal searching agent is initially set based on the current optimal solution. he main iterative loop involves updating the positions of each search agent, adjusting control parameters, evaluating fitness, and updating the optimal searching agent if a superior solution is found. The algorithm explores the solution space through the adjustment of search agent positions, aiming to strike a balance between exploration and exploitation. The termination criterion is based on a predefined maximum number of iterations (Max_iterations).

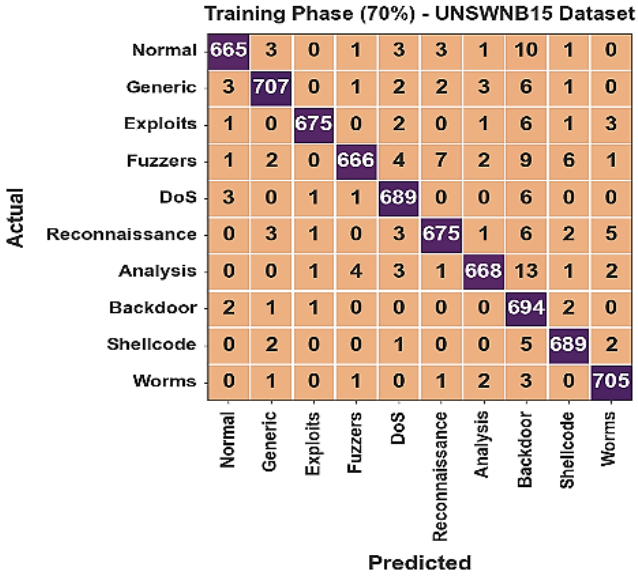
The model of SBO resultant a fitness function (FF) takes improved classification algorithm result. It defined optimistic values for suggesting greater outcomes of the applicant solutions. The decreased classification algorithm error level is FF in this article which is provided in *eq. (10)*.

$$fitness(x_i) = ClassifierErrorRate(x_i) = \frac{number\ of\ misclassified\ samples}{Total\ number\ of\ samples} * 100 \quad (10)$$

The Echo State Network (ESN) model, strategically employed for intrusion detection in Industrial Internet of Things (IIoT) environments, exhibits distinct functionalities that enhance its efficacy in recognizing and classifying intrusions. Operating on a reservoir computing architecture, ESN leverages a reservoir of neurons with recurrent connections, creating a dynamic memory capable of capturing temporal dependencies in sequential data. Through nonlinear mapping, the model transforms input data into a high-dimensional space, allowing it to discern intricate patterns. The echo state property ensures the preservation of historical information, enabling ESN to effectively recognize temporal patterns in network traffic. With an efficient training process that involves adjusting output weights, ESN emerges as a powerful tool for precise and adaptive intrusion detection in the complex and dynamic landscape of IIoT environments.

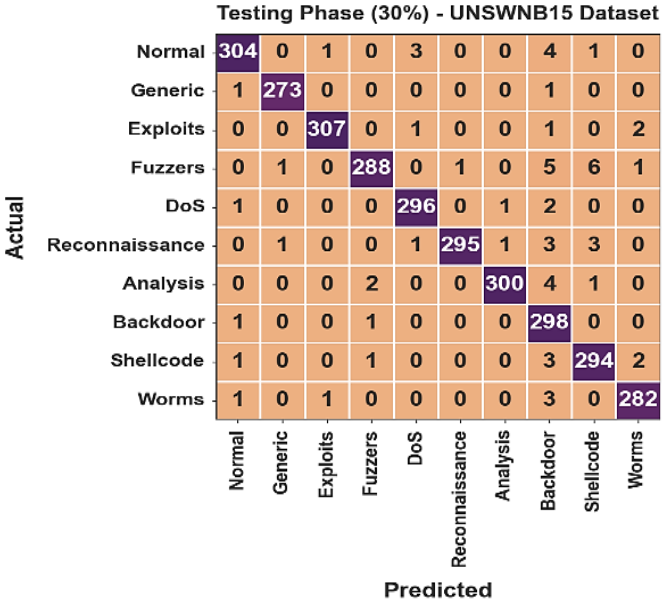
4.3 Experimental validation

The experimental evaluation of the IID-SBODL methodology is tested using 2 datasets: UNSW-NB15 dataset and UCI SECOM dataset. *Figure 3* defines the classifier performances of the IID-SBODL method on UNSWNB15 database. *Figures 3a-3b* illustrates the confusion matrices attained by the IID-SBODL system at 70:30 of TR phase/TS phase. The simulation value referred that the IID-SBODL methodology has detected and ordered all 10 classes. Afterward, *figure 3c* represents the PR outcome of the IID-SBODL system. The simulation results inferred that the IID-SBODL approach has attained better values of PR on 10 classes. However, *figure 3d* depicts the ROC analysis of the IID-SBODL method. The outcome defined that the IID-SBODL approach led to effective performance with better outcomes of ROC on 10 classes.

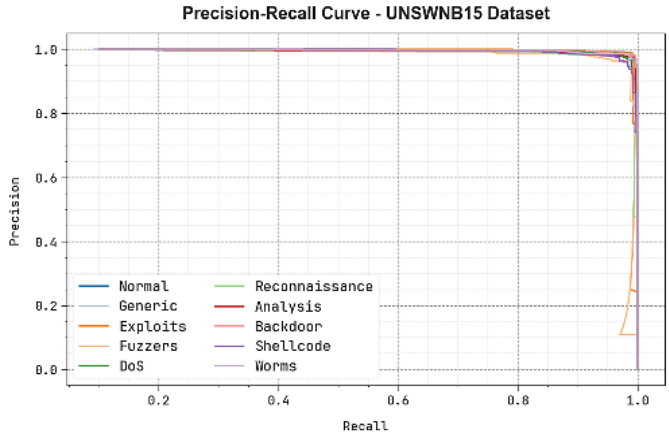


(a)

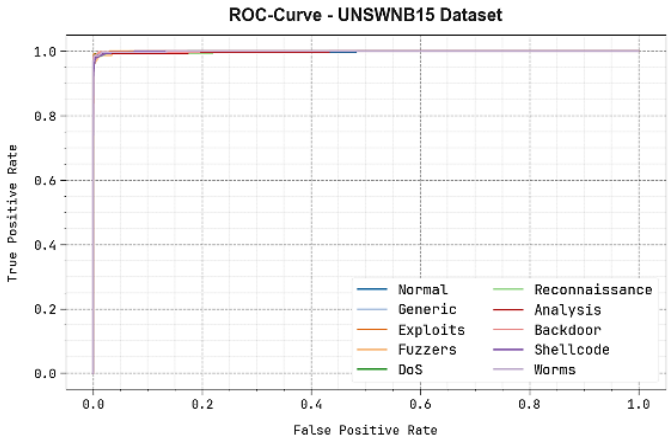
FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 1 | Pages 219-227 | e-ISSN: 2347-470X



(b)



(c)



(d)

Figure 3. UNSWNB15 dataset (a-b) Confusion matrices, (c) PR curve, and (d) ROC

The intrusion detection outcome of the IID-SBODL methodology is tested on the UNSWNB15 database, which is reported in *table 2* and *fig. 4*. The experimental values stated that the IID-SBODL system appropriately identifies the intrusions. With 70% of TR phase, the IID-SBODL technique offers average $accu_y$ of 99.52%, $prec_n$ of 97.68%, $sens_y$ of 97.61%, $spec_y$ of 99.73%, and F_{score} of 97.62%. In addition, with 30% of TS phase, the IID-SBODL methodology attains average $accu_y$ of 99.58%, $prec_n$ of 97.96%, $sens_y$ of 97.92%, $spec_y$ of 99.77%, and F_{score} of 97.92%.

Table 2 Intrusion detection outcome of IID-SBODL system on UNSWNB15 database

UNSWNB15 Dataset					
Classes	$Accu_y$	$Prec_n$	$Sens_y$	$Spec_y$	F_{Score}
TR Phase (70%)					
Normal	99.54	98.52	96.80	99.84	97.65
Generic	99.57	98.33	97.52	99.81	97.92
Exploits	99.74	99.41	97.97	99.94	98.68
Fuzzers	99.43	98.81	95.42	99.87	97.08
DoS	99.59	97.45	98.43	99.71	97.94
Reconnaissance	99.50	97.97	96.98	99.78	97.47
Analysis	99.50	98.53	96.39	99.84	97.45
Backdoor	99.00	91.56	99.14	98.98	95.20
Shellcode	99.66	98.01	98.57	99.78	98.29
Worms	99.70	98.19	98.88	99.79	98.53
Average	99.52	97.68	97.61	99.73	97.62
TS Phase (30%)					
Normal	99.53	98.38	97.12	99.81	97.75
Generic	99.87	99.27	99.27	99.93	99.27
Exploits	99.80	99.35	98.71	99.93	99.03
Fuzzers	99.40	98.63	95.36	99.85	96.97
DoS	99.70	98.34	98.67	99.81	98.50
Reconnaissance	99.67	99.66	97.04	99.96	98.33
Analysis	99.70	99.34	97.72	99.93	98.52
Backdoor	99.07	91.98	99.33	99.04	95.51
Shellcode	99.40	96.39	97.67	99.59	97.03
Worms	99.67	98.26	98.26	99.82	98.26
Average	99.58	97.96	97.92	99.77	97.92

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 1 | Pages 219-227 | e-ISSN: 2347-470X

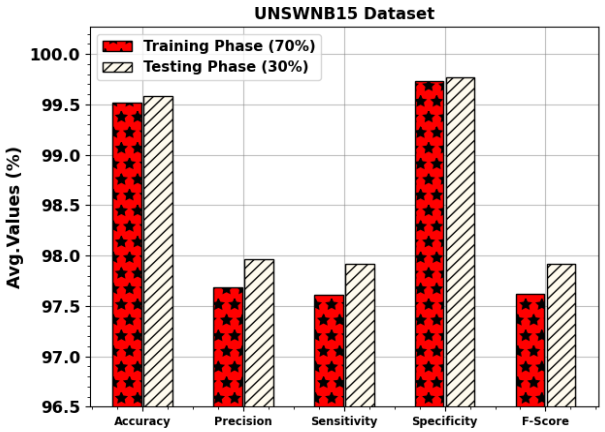


Figure 4. Average of IID-SBODL methodology on UNSWNB15 database

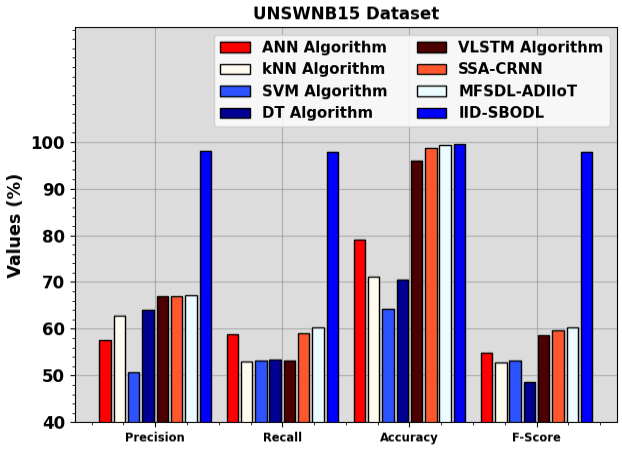
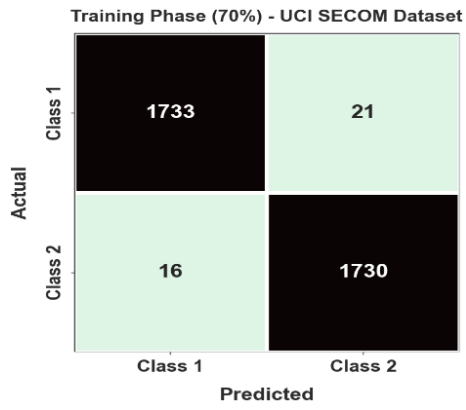
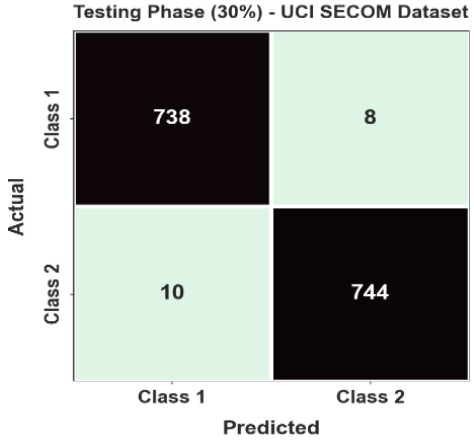


Figure 5. Comparative outcome of IID-SBODL algorithm on UNSWNB15 dataset

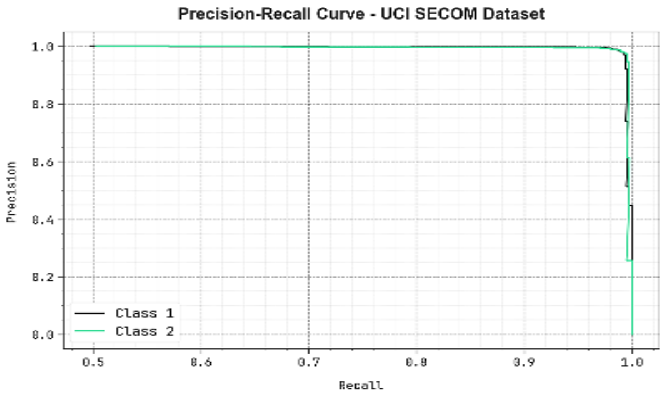
The comparative outcome of the IID-SBODL system with other approaches on the UNSWNB15 database is illustrated in *fig. 5* [21-24]. The outcome defines that the ANN and SVM systems accomplish least result. Besides, the kNN, DT, VLSTM, and SSA-CRNN models obtain somewhat improved results. Although the MFSDL-ADIIoT model reaches considerable performance. Bu the IID-SBODL methodology shows the other systems with maximal $prec_n$ of 97.96%, $reca_l$ of 97.92%, $accu_y$ of 99.58%, and F_{score} of 97.92%.



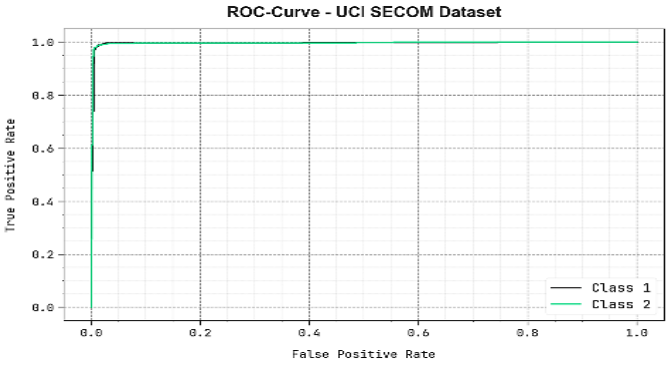
(a)



(b)



(c)



(d)

Figure 6. UCISECOM dataset (a-b) Confusion matrices, (c) PR curve, and (d) ROC

Figure. 6 defines the classifier result of the IID-SBODL methodology on UCISECOM database. *Figures. 6a-6b* represents the confusion matrices achieved by the IID-SBODL algorithm at 70:30 of TR phase/TS phase. The outcome implied that the IID-SBODL algorithm has classified and detected all 2 classes correctly. Also, *fig. 6c* exhibits the PR outcome of the IID-SBODL system. The simulation value inferred that the IID-SBODL system has gained higher values of PR on 2 classes. Besides, Fig. 6d defines the ROC outcome of the IID-SBODL methodology. The outcome exhibited that the IID-SBODL system led to effective performances with higher values of ROC in 2 classes.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 1 | Pages 219-227 | e-ISSN: 2347-470X

The intrusion detection outcomes of the IID-SBODL algorithm are tested on the UCISECOM database is defined in *table 3* and *figure. 7*. The simulation outcome stated that the IID-SBODL algorithm properly identifies the intrusions. With 70% of TR phase, the IID-SBODL approach gains average $accu_y$ of 98.94%, $prec_n$ of 98.94%, $sens_y$ of 98.94%, $spec_y$ of 98.94%, and F_{score} of 98.94%. Moreover, with 30% of TS phase, the IID-SBODL system reaches average $accu_y$ of 98.80%, $prec_n$ of 98.80%, $sens_y$ of 98.80%, $spec_y$ of 98.80%, and F_{score} of 98.80%.

Table 3 Intrusion detection outcome of IID-SBODL approach on UCISECOM database

UCI SECOM Dataset					
Classes	$Accu_y$	$Prec_n$	$Sens_y$	$Spec_y$	F_{Score}
TR Phase (70%)					
Class 1	98.80	99.09	98.80	99.08	98.94
Class 2	99.08	98.80	99.08	98.80	98.94
Average	**98.94**	**98.94**	**98.94**	**98.94**	**98.94**
TS Phase (30%)					
Class 1	98.93	98.66	98.93	98.67	98.80
Class 2	98.67	98.94	98.67	98.93	98.80
Average	**98.80**	**98.80**	**98.80**	**98.80**	**98.80**

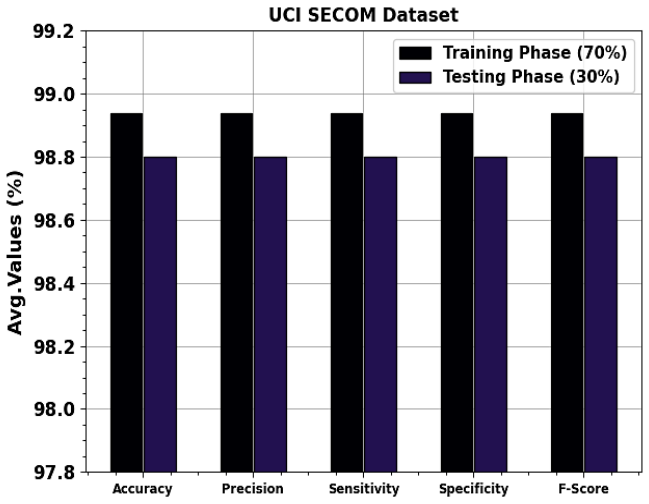


Figure 7. Average of IID-SBODL approach on UCISECOM database

The comparison outcome of the IID-SBODL system with other algorithms on the UCISECOM database is illustrated in Fig. 8. The outcome inferred that the DNN Layer2 and Ensemble approaches attain worse outcomes. Besides, the DNN Layer1, DNN Layer3, PSO Ensemble, and SSA-CRNN systems reach somewhat enhanced outcomes. However, the MFSDL-ADIIoT system attains considerable outcomes. However, the IID-SBODL methodology outperforms the other systems with maximal $prec_n$ of 98.94%, $reca_l$ of 98.94%, $accu_y$ of 98.94%, and F_{score} of 98.94%. Thus, the IID-SBODL system can be applied for automated intrusion recognition process.

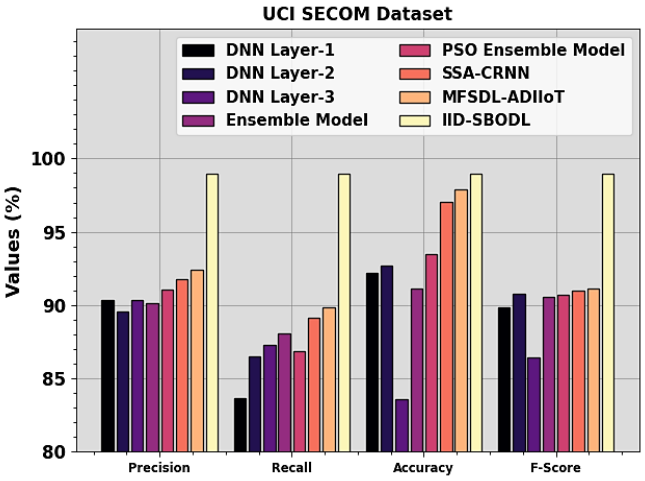


Figure 8. Comparative outcome of IID-SBODL algorithm on UCISECOM dataset

The exceptional performance of the IID-SBODL model can be attributed to the synergistic contribution of its key components. Firstly, the preprocessing phase ensures that input data is appropriately formatted, enhancing compatibility for subsequent stages. The utilization of the Echo State Network (ESN) model facilitates effective intrusion recognition and classification. ESN's inherent ability to capture complex temporal dependencies in data contributes to the model's robustness in detecting anomalous patterns within IIoT environments. The optimization process through the Successive Binary Optimization (SBO) algorithm plays a crucial role in fine-tuning the ESN's configuration. SBO enhances the model's adaptability by optimizing parameters to better suit the specific characteristics of the industrial network, thereby improving precision in identifying security breaches. The collective impact of these components results in a model that excels in accurately detecting and classifying intrusions, showcasing its effectiveness in enhancing the security posture of IIoT environments. Furthermore, the IID-SBODL model's success can be attributed to its ability to learn from dynamic and evolving threats. The iterative optimization mechanism, coupled with the ESN's capacity to handle temporal variations, contributes to the model's resilience against emerging intrusion patterns. This adaptability enables IID-SBODL to outperform conventional methods, demonstrating its efficacy in safeguarding critical industrial processes.

5. CONCLUSION

This study presents an IID-SBODL model for IIoT Environment. The IID-SBODL technique initially preprocesses the input data for compatibility. Next, the IID-SBODL technique applies ESN model for effectual recognition and classification of the intrusions. Finally, the SBO algorithm optimizes the configuration of the ESN, boosting its capability for precise identification of anomalies and significant security breaches within IIoT networks. By widespread simulation evaluation, the experimental results pointed out that the IID-SBODL technique reaches maximum detection rate and improves the security of the IIoT environment. The IID-SBODL model gives to the development of robust intrusion

detection mechanisms for safeguarding critical industrial processes in the era of interconnected and smart IIoT environments. Through comprehensive experimentation on both UNSW-NB15 and UCI SECOM datasets, the model exhibited exceptional performance, achieving an average accuracy of 99.55% and 98.87%, precision of 98.90% and 98.93%, recall of 98.87% and 98.80%, and F-score of 98.88% and 98.87% for the respective datasets. These results underscore the IID-SBODL model's prowess in accurately identifying and classifying intrusions, surpassing existing methods. The significant improvements in detection rates and overall security posture make IID-SBODL a valuable contribution to safeguarding critical industrial processes in interconnected and smart IIoT environments.

While the IID-SBODL model exhibits remarkable performance, it is essential to acknowledge its limitations. One constraint lies in its sensitivity to the characteristics of the training datasets, potentially leading to challenges when confronted with novel, unseen threats. Additionally, the computational complexity associated with the ESN model and SBO algorithm may impact real-time applicability in large-scale IIoT networks.
For future work, addressing these limitations could involve refining the model's adaptability to dynamic and evolving threats by incorporating continual learning mechanisms. Exploring techniques to optimize computational efficiency without compromising accuracy would enhance the model's scalability. Moreover, extending the evaluation to diverse IIoT environments and datasets would provide a more comprehensive understanding of IID-SBODL's generalizability. These endeavors aim to propel the IID-SBODL model towards increased robustness and applicability in real-world industrial scenarios.

REFERENCES

[1] Li, F.; Lin, J.; Han, H. FSL: Federated sequential learning-based cyberattack detection for Industrial Internet of Things. Ind. Artif. Intell. 2023, 1, 4.
[2] Khan, F.; Jan, M.A.; Alturki, R.; Alshehri, M.D.; Shah, S.T.; ur Rehman, A. A Secure Ensemble Learning-Based Fog-Cloud Approach for Cyberattack Detection in IoMT. IEEE Trans. Ind. Inform. 2023, 19, 10125–10132.
[3] Alkahtani, H.; Aldhyani, T.H. Intrusion detection system to advance Internet of Things infrastructure-based deep learning algorithms. Complexity 2021, 2021, 5579851.
[4] Alatawi, T.; Aljuhani, A. Anomaly Detection Framework in Fog-to-Things Communication for Industrial Internet of Things. Comput. Mater. Contin. 2022, 73, 1067–1086.
[5] Rouzbahani, H.M.; Bahrami, A.H.; Karimipour, H. A snapshot ensemble deep neural network model for attack detection in the industrial internet of things. In AI-Enabled Threat Detection and Security Analysis for Industrial IoT; Springer: Cham, Switzerland, 2021; pp. 181–194.
[6] Hinton, G.E.; Osindero, S.; Teh, Y.W. A fast-learning algorithm for deep belief nets. Neural Comput. 2006, 18, 1527–1554.
[7] Moustafa, N.; Slay, J. UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, Australia, 10–12 November 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 1–6.
[8] Chopra, N.; Ansari, M.M. Golden jackal optimization: A novel nature-inspired optimizer for engineering applications. Expert Syst. Appl. 2022, 198, 116924.
[9] Zhou, M.G.; Cao, X.Y.; Lu, Y.S.; Wang, Y.; Bao, Y.; Jia, Z.Y.; Fu, Y.; Yin, H.L.; Chen, Z.B. Experimental quantum advantage with quantum coupon collector. Research 2022, 2022, 798679.
[10] Trojovský, P.; Dehghani, M. Pelican optimization algorithm: A novel nature-inspired algorithm for engineering applications. Sensors 2022, 22, 855.
[11] Soliman, S., Oudah, W. and Aljuhani, A., 2023. Deep learning-based intrusion detection approach for securing industrial Internet of Things. *Alexandria Engineering Journal*, *81*, pp.371-383.
[12] Abdel-Basset, M., Hawash, H., Chakrabortty, R.K. and Ryan, M.J., 2021. Semi-supervised spatiotemporal deep learning for intrusions detection in IoT networks. *IEEE Internet of Things Journal*, *8*(15), pp.12251-12265.
[13] Marzouk, R., Alrowais, F., Negm, N., Alkhonaini, M.A., Hamza, M.A., Rizwanullah, M., Yaseen, I. and Motwakel, A., 2022. Hybrid deep learning enabled intrusion detection in clustered IIoT environment. *Computers, Materials & Continua*, *72*(2), pp.3763-3775.
[14] Du, J., Yang, K., Hu, Y. and Jiang, L., 2023. Nids-cnnlstm: Network intrusion detection classification model based on deep learning. *IEEE Access*, *11*, pp.24808-24821.
[15] Wang, T., Li, J., Wei, W., Wang, W. and Fang, K., 2022. Deep-learning-based weak electromagnetic intrusion detection method for zero touch networks on industrial IoT. *IEEE Network*, *36*(6), pp.236-242.
[16] Alalayah, K.M., Alrayes, F.S., Alzahrani, J.S., Alaidarous, K.M., Alwayle, I.M., Mohsen, H., Ahmed, I.A. and Al Duhayyim, M., 2023. Optimal Deep Learning Based Intruder Identification in Industrial Internet of Things Environment. *Computer Systems Science & Engineering*, *46*(3).
[17] Yao, X., Shao, Y., Fan, S. and Cao, S., 2022. Echo state network with multiple delayed outputs for multiple delayed time series prediction. *Journal of the Franklin Institute*, *359*(18), pp.11089-11107.
[18] Chen, X., Cao, B. and Pouramini, S., 2023. Energy cost and consumption reduction of an office building by Chaotic Satin Bowerbird Optimization Algorithm with model predictive control and artificial neural network: A case study. *Energy*, *270*, p.126874.
[19] https://www.kaggle.com/mrwellsdavid/unsw-nb15
[20] https://www.kaggle.com/paresh2047/uci-semcom
[21] Kasongo, S.M. and Sun, Y., 2020. Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset. *Journal of Big Data*, *7*(1), pp.1-20.
[22] Kotecha, K.; Verma, R.; Rao, P.V.; Prasad, P.; Mishra, V.K.; Badal, T.; Jain, D.; Garg, D.; Sharma, S. Enhanced Network Intrusion Detection System. Sensors 2021, 21, 7835. https://doi.org/10.3390/ s21237835
[23] Zhou, X., Hu, Y., Liang, W., Ma, J. and Jin, Q., 2020. Variational LSTM enhanced anomaly detection for industrial big data. *IEEE Transactions on Industrial Informatics*, *17*(5), pp.3469-3477.
[24] Moldovan, D., Anghel, I., Cioara, T. and Salomie, I., 2020, September. Particle Swarm Optimization Based Deep Learning Ensemble for Manufacturing Processes. In *2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP)* (pp. 563-570). IEEE.