sensors

MDPI

Article

Development and Validation of a Cyber-Physical System Leveraging EFDPN for Enhanced WSN-IoT Network Security

Sundaramoorthy Krishnasamy [1], Mutlaq B. Alotaibi [2], Lolwah I. Alehaideb [2] and Qaisar Abbas [2,*]

[1] Department of Information Technology, Jerusalem College of Engineering (Autonomous) Pallikaranai, Chennai 600100, Tamil Nadu, India; sundaramoorthyit@jerusalemengg.ac.in
[2] College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh 11432, Saudi Arabia; motaibi@imamu.edu.sa (M.B.A.)
* Correspondence: qaabbas@imamu.edu.sa

Abstract: In the current digital era, Wireless Sensor Networks (WSNs) and the Internet of Things (IoT) are evolving, transforming human experiences by creating an interconnected environment. However, ensuring the security of WSN-IoT networks remains a significant hurdle, as existing security models are plagued with issues like prolonged training durations and complex classification processes. In this study, a robust cyber-physical system based on the Emphatic Farmland Fertility Integrated Deep Perceptron Network (EFDPN) is proposed to enhance the security of WSN-IoT. This initiative introduces the Farmland Fertility Feature Selection (F^3S) technique to alleviate the computational complexity of identifying and classifying attacks. Additionally, this research leverages the Deep Perceptron Network (DPN) classification algorithm for accurate intrusion classification, achieving impressive performance metrics. In the classification phase, the Tunicate Swarm Optimization (TSO) model is employed to improve the sigmoid transformation function, thereby enhancing prediction accuracy. This study demonstrates the development of an EFDPN-based system designed to safeguard WSN-IoT networks. It showcases how the DPN classification technique, in conjunction with the TSO model, significantly improves classification performance. In this research, we employed well-known cyber-attack datasets to validate its effectiveness, revealing its superiority over traditional intrusion detection methods, particularly in achieving higher F1-score values. The incorporation of the F3S algorithm plays a pivotal role in this framework by eliminating irrelevant features, leading to enhanced prediction accuracy for the classifier, marking a substantial stride in fortifying WSN-IoT network security. This research presents a promising approach to enhancing the security and resilience of interconnected cyber-physical systems in the evolving landscape of WSN-IoT networks.

Keywords: wireless sensor network (WSN); internet of things (IoT); security; cyber-physical system; intrusion detection; farmland fertility feature selection (F^3S); deep perceptron network (DPN); tunicate swarm optimization (TSO)

Citation: Krishnasamy, S.; Alotaibi, M.B.; Alehaideb, L.I.; Abbas, Q. Development and Validation of a Cyber-Physical System Leveraging EFDPN for Enhanced WSN-IoT Network Security. *Sensors* **2023**, *23*, 9294. https://doi.org/10.3390/s23229294

Academic Editors: Luca Vollero, Mario Merone and Anna Sabatini

Received: 21 September 2023
Revised: 14 November 2023
Accepted: 15 November 2023
Published: 20 November 2023

1. Introduction

A wireless sensor network (WSN) [1,2], which is made up of different kinds of sensors with limited resources, is an important part of monitoring an environment and sending important data to a designated node, also called a sink, through different communication protocols. These data are then relayed to a base station for meticulous analysis and processing, catered to the specific demands of contemporary applications. Renowned for their efficacy in remote monitoring, WSNs have a promising future, finding applicability in critical domains such as border surveillance, industrial inspection, commercial utilities, health monitoring, and environmental and infrastructure surveillance [3].

Conversely, the Internet of Things (IoT) [4,5] embodies an intricate network of interconnected smart devices tasked with the collection, processing, optimization, and dissemination of valuable data through internet channels. Each device, identifiable by a unique

IP address or identifier, facilitates autonomous data exchange, enhancing the convenience and efficiency of daily activities through technological advancements [6–8]. However, this burgeoning development is not devoid of challenges, predominantly concerning security [9].

The extensive integration of IoT into daily life and the surge in remote device operations necessitate a unified platform facilitating seamless communication amongst a diverse array of devices [10–12]. This prerequisite has spurred the creation of specific IoT frameworks, outlining the architectural blueprint for selected applications and thus working towards standardizing IoT security protocols.

WSN and IoT [13,14] stand as potent forces capable of spearheading a societal transformation towards a smarter, more connected world. Despite their distinctive characteristics, they are occasionally utilized interchangeably owing to similarities in their processing power, memory storage, and communication capabilities. Both networks hold remarkable potential in real-time applications [15–17], yet they suffer from persistent security challenges at the device level [18].

In this context, the adoption of lightweight, low-power security mechanisms is crucial, aiming to enhance network longevity by minimizing power consumption during the intrusion detection phase [19–21]. Traditional methods have endeavored to address security concerns using minimal power consumption strategies, albeit with varying degrees of success. As the IoT landscape expands, so does its vulnerability to external threats, making the development of robust security infrastructure imperative.

Current classifiers have trouble differentiating normal and unusual system behaviors because there are so many network traffic data, which have different features [22]. The presence of irrelevant features and network communication disturbances further exacerbate this challenge, leading to increased resource expenditure and diminished detection rates. Therefore, the nuanced selection of features has emerged as a vital aspect of machine learning designed to accurately encapsulate object properties while eliminating redundant data [2].

Existing research has extensively explored the potential of feature selection and machine learning algorithms in network security and traffic monitoring. Nevertheless, conventional intrusion detection approaches exhibit significant limitations, including increased computation time, reduced reliability, and heightened complexity. So, the goal of this study is to develop a new Intrusion Detection System (IDS) framework to protect WSN-IoT networks as shown in Figure 1. This was achieved by using new feature optimization and classification strategies to improve accuracy and detection rates while cutting down on time [23].

Figure 1. Security properties of WSN-IoT systems.

1.1. Research Contribution

The proposed Emphatic Farmland Fertility Integrated Deep Perceptron Network (EFDPN) aims to bolster WSN-IoT network security through an innovative cyber-physical system. This method involves a systematic workflow encompassing cyber-dataset collection, preprocessing, and feature extraction, followed by implementing the Farmland Fertility Feature Selection (F3S) technique and Deep Perceptron Network (DPN) classification. In the final step, Tunicate Swarm Optimization (TSO) is employed to refine the sigmoid transformation function, enhancing prediction accuracy in intrusion detection. The major contributions of this work are as follows:

(1) An Emphatic Farmland Fertility Integrated Deep Perceptron Network (EFDPN)-based cyber-physical system was developed for protecting WSN-IoT networks;
(2) By using the Farmland Fertility Feature Selection (F3S) algorithm, the processes of incursion identification and classification are streamlined, with reduced computing complexity;
(3) A Deep Perceptron Network (DPN) classification technique was used to accurately classify intrusion types, yielding great performance outcomes;
(4) A Tunicate Swarm Optimization (TSO) model was used to estimate the sigmoid transformation function for better classification;
(5) Using well-known cyber-attack datasets, the results of the proposed EFDPN model were validated and contrasted.

1.2. Paper Organization

The further portions of this paper are split into the following sections: Section 2 reviews the literature relevant to cyber-security and intrusion detection in WSN-IoT networks, along with their merits and demerits. Section 3 presents the overall explanation for the proposed EFDPN model with system workflow and stage-wise descriptions. Section 4 validates and contrasts the results of the proposed EFDPB-based security framework using several performance measures. Section 5 provides a summary of the entire paper along with the conclusions, results, and suggested next steps.

2. Related Works

This section investigates various intrusion detection approaches used to safeguard WSN-IoT networks, wherein the positives and negatives of each model are discussed based on their performance.

Pundir et al. [24] investigated the different types of security challenges in WSN-IoT networks. The different types of security requirements were also discussed in this study for protecting WSN-IoT networks from intrusions. The following categories of potential threats could greatly affect WSN-IoT networks: eavesdropping, impersonation attacks, DoS attacks, malware attacks, database attacks, and man-in-the-middle attacks. Baraneetharan et al. [25] discussed the impacts of using machine learning algorithms for intrusion detection in WSN-IoT systems. In this study, classification, regression, and clustering-based machine learning algorithms were discussed with regard to intrusion detection in WSN-IoT networks. Moreover, the suggested intrusion detection approaches were compared based on the parameters of prediction accuracy, memory requirements, network architecture, and energy consumption. Among other models, the hybrid IDS frameworks are more suitable for WSN due to their improved energy efficiency and precise detection operation. Jiang et al. [26] deployed a lightweight Gradient Boost Mechanism (GBM)-based cyber-physical system for smart-networking environments. Amouri et al. [27] designed a cross-layered IDS-framework-based linear regression model for increasing the security of WSN-IoT networks. The authors aim to detect common malicious activities like blackholes, flooding, and DDoS within networks [28]. The suggested model has the major drawbacks of an increased false-positive rate and time consumption for attack detection.

Singh et al. [29] presented a comprehensive review to examine the different types of machine-learning-based intrusion detection approaches. This paper covers a few well-known and recently developed ML algorithms to highlight their strengths and weaknesses. This will assist researchers in choosing the best algorithm for their studies. Damasevicius et al. [30] utilized a new annotated dataset named LITNET-2020 for classifying normal and

intrusive events pertaining to WSN-IoT systems. In addition, the authors suggested some other cyber-attack datasets for IoT security. Safaldin et al. [31] implemented a binary gray-wolf optimization algorithm incorporated with the standard SVM mechanism for detecting intrusions in WSNs. When recommending a fitness function for assessing each subset of the selected feature, the significance of accuracy and the overall number of features were taken into account. According to the total number of features, the prediction performance of the classifier was determined in the cited work. Here, the SVM uses a dimensionality-reduced feature set for intrusion identification and classification. Some of the merits of using SVM include better scalability, high process speed, and low complexity with a reduced feature set.

Krishnan et al. [32] introduced an anomalous intrusion detection and prevention protocol for WSN-IoT networks. The authors aimed to increase the reliability of a network and provide an expanded time frame for an organization. Jayanayudu et al. [33] utilized hybrid Shuffled Frog Leap (SFL) and Ant Lion Optimization (ALO) algorithms to develop an intrusion detection framework for protecting WSN-IoT systems. Typically, securing data while improving energy efficiency is one of the most challenging network problems in present times. Increased attention to security is necessary while monitoring IDS using IoT-WSN systems. The authors of the suggested paper presented a safe routing intrusion prevention architecture for IoT-WSN networks. Moreover, they concentrated on the enhancement of network efficiency and defense against fraudulent attacks. Here, the greedy strategy was used for data routing, offering energy efficient solutions with security. Hussain et al. [34] presented a comprehensive literature review examining various routing strategies for low-powered IoT systems. Here, the assessment was carried out based on identification, screening, eligibility, and inclusion. Moreover, their work investigated the strengths and limitations of several security-based routing methodologies used in WSN-IoT networks. Al Sawafi et al. [35] implemented a hybrid deep-learning-based intrusion detection framework for WSN-IoT networks. In this paper, the authors intended to mitigate security attacks by analyzing a network traffic dataset. According to the pre-trained features, the authors' framework categorizes normal and malicious networking traffic in the network. Maheswari and Karthika [36] constructed a multi-tiered intrusion detection (MDIT) framework for safeguarding WSN-IoT networks. Here, the Spotted Hyena Optimization (SHO) algorithm, integrated with the standard LSTM deep learning algorithm, was used to detect malicious events in cyber-data. Table 1 summarizes the limitations of state-of-the-art systems.

Table 1. The table below provides a brief overview of the state of the art.

Reference	Methodology	Results	Limitations
Pundir et al. [24]	Investigated security challenges and requirements in WSN-IoT networks.	Identification of potential threats like eavesdropping, DoS, etc.	Low performance in various models.
Baraneetharan et al. [25]	Explored machine learning algorithms (classification, regression, clustering) for intrusion detection.	Comparative analysis based on prediction accuracy, energy, etc.	High false positive rate; increased time consumption for attack detection.
Jiang et al. [26]	Implemented a lightweight GBM-based cyber-physical system.	Enhanced smart-networking environment.	Low performance in various models.
Amouri et al. [27]	Cross-layered IDS framework using a linear regression model.	Detection of malicious activities like blackholes, DDoS, etc.	High false positive rate; increased time consumption for attack detection.
Singh et al. [29]	Comprehensive review of machine-learning-based intrusion detection approaches.	Highlighted strengths and weaknesses of various ML algorithms.	Low performance in various models; insufficient memory use during classification.
Damasevicius et al. [30]	Utilized LITNET-2020 dataset for classifying events; suggested other datasets.	Identification of normal and intrusive events in WSN-IoT systems.	Inability to handle massive datasets.
Safaldin et al. [31]	Binary grey-wolf optimization with SVM for intrusion detection, considering feature set reduction.	SVM with reduced feature set achieved efficient intrusion identification.	High curse of dimensionality.
Krishnan et al. [32]	Anomalous intrusion detection and prevention protocol for WSN-IoT.	Increased network reliability.	Excessive memory use during classification.
Jayanayudu et al. [33]	Hybrid SFL and ALO algorithms for an IDS framework; authors focused on energy efficiency with a greedy routing strategy.	Enhanced network efficiency; defence against fraudulent attacks.	Low performance in various models.

The following are some of the major drawbacks of the current approaches that were identified in the literature review [37,38]:

- Low performance in various models;
- Excessive memory use during classification;
- High curse of dimensionality;
- Inability to handle massive datasets.

In order to create a highly effective cyber-physical system for WSN-IoT networks, in the proposed work, we make use of innovative optimization and classification approaches.

3. Proposed Methodology

The proposed strategy describes how to build a cyber-physical system based on the EFDPN in order to improve the security of WSN-IoT networks. Our intention in this initiative is to adeptly identify security breaches in these networks by leveraging state-of-the-art feature selection and classification algorithms. Commencing with the acquisition of pertinent cyber datasets, the methodology transitions into a preprocessing and feature extraction phase where data are refined and pivotal features are isolated to facilitate effective intrusion detection. This is followed by the application of the Farmland Fertility Feature Selection (F3S) technique, a pivotal process designed to alleviate computational complexity by homing in on critical features. Subsequently, the Deep Perceptron Network (DPN) takes the helm, functioning as a vital tool in the precise categorization of data points and thereby playing an instrumental role in the meticulous identification of intrusions. This structured approach culminates in the integration of the Tunicate Swarm Optimization (TSO) model, fine-tuning the sigmoid transformation function in the classification phase to potentially elevate prediction accuracy. Consequently, this holistic methodology envisages a fortified security landscape for WSN-IoT networks, with a particular emphasis on enhancing the accuracy and efficiency of intrusion detection systems.

In this section of the paper, a cyber-physical system based on Emphatic Farmland Fertility Integrated Deep Perceptron Network (EFDPN) designed as a way of protecting WSN-IoT networks is described in detail. The EFDPN is utilized to enhance security in WSN-IoT environments by integrating advanced machine learning techniques, optimizing computational efficiency, reducing false positives, and demonstrating readiness for real-world applications. It offers accurate intrusion detection and quantitative performance evaluations, making it a valuable asset in safeguarding interconnected cyber-physical systems. With the aid of cutting-edge feature selection and classification algorithms, in the proposed work, we created an efficient security framework for WSN-IoT systems. The proposed EFDPN system's workflow model is depicted in Figure 2, which consists of the following operations:

- Cyber-dataset collection;
- Preprocessing and feature extraction;
- Farmland Fertility Feature Selection (F3S);
- Deep Perceptron Network (DPN) classification;
- Tunicate Swarm Optimization (TSO) for sigmoid transformation function estimation.

In the proposed EFDPN framework, the emerging public intrusion detection datasets are acquired at the beginning. The next step is to conduct dataset normalization and feature extraction in order to extract the appropriate features from the given dataset [32]. The recently introduced F3S algorithm is used to select the best features by lowering dimensionality after the set of features has been extracted. This algorithm is designed to produce accurate classification results with minimal time and computational overhead. By using the features that are carefully chosen from the dataset, the DPN classifier can predict malicious events. During this process, the TSO model is utilized to optimally compute the sigmoid transfer function, which enhances the classifier's performance in attack detection.

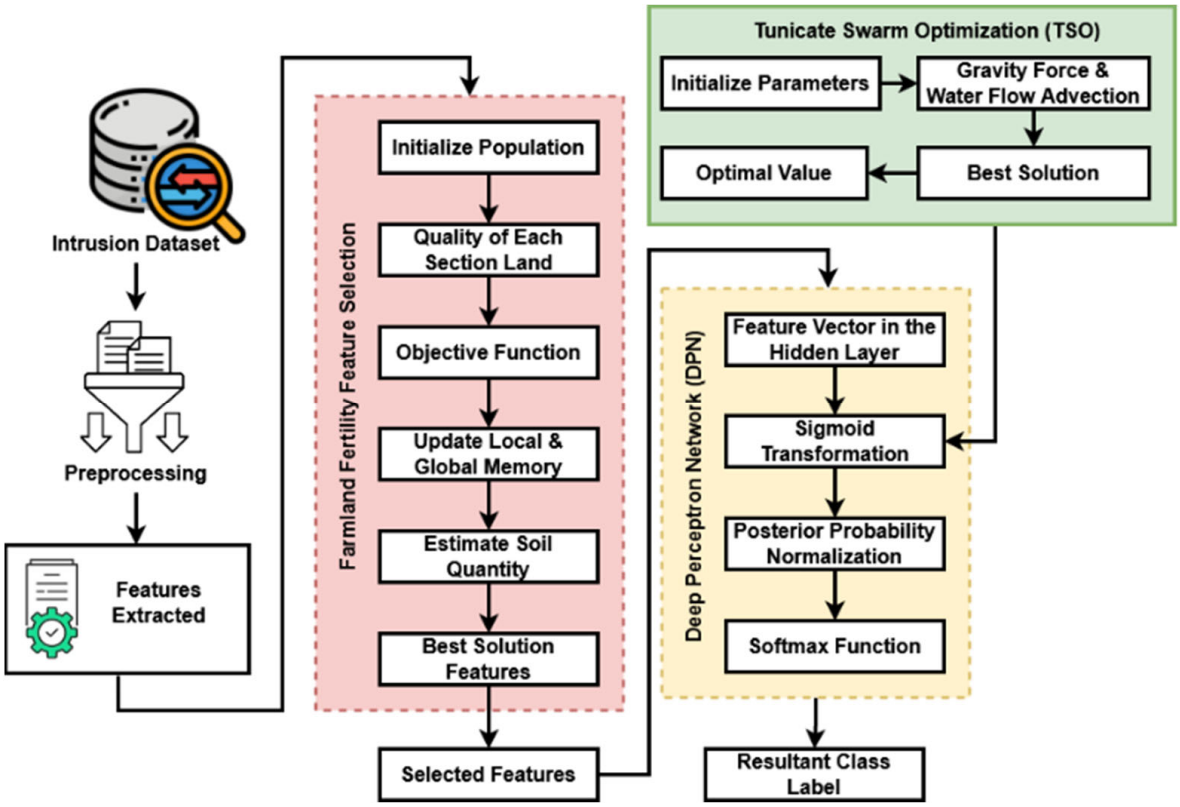

Figure 2. Workflow model.

3.1. Farmland Fertility Feature Selection (F^3S)

In this stage, a number of features are selected from the original feature set with the use of F^3S algorithm. Feature selection or optimization is the most crucial operation in the intrusion detection system since the classifier's detection performance is highly dependent on the features used for training and testing. A summary of earlier studies on IDS reveals that the technique of integrating predictive classifiers plays a crucial role in IDS. In contrast, the large set of data in this detection system decreases the precision as well as speed of classifiers. Hence, meta-heuristic techniques are increasingly being employed by researchers to minimize the features of data. In order to detect network assaults, the hybridization of the classifiers and the subsequent choice of useful features are essential. Here, a successful strategy for choosing the features based on F^3S is introduced, which substantially lowers the dimensionality of features with improved accuracy. In this algorithm, the soil quality of each portion of the farm can vary from that of the others because farmers typically split various parts of a farm into distinct soil types. The quality of the soil in each segment can be changed by adding specific compounds. Therefore, farmers apply specific materials that the soil requires in order to maximize the area of each segment of the farm. Farmers alter each area of their farm in accordance with this model and by monitoring each sector's state of the soil. Then, they may determine the feasible ways of enhancing each portion's soil. After that, the most effective and essential materials are then distributed to each sector in order to enhance the quality of the soil. The advantages of the F^3S algorithm are its low processing time, high convergence, and ability to reach the best solution in the searching space with minimal iterations. Initially, the feature set F_s is obtained as the input, and the estimated δ_f is delivered as the output of this algorithm. After obtaining the original set of features, the number of solutions is estimated for each portion of a farm, as shown below:

$$H = (\beta \times \mathfrak{y}) \quad (1)$$

where β indicates a constant variable, and η is an integer number. After defining the initial population, the quality of each portion of the farm is determined using the following model:

$$Q_{section} = F_s(\alpha \times d),\ \alpha = \eta \times (r-1)\ : (\eta \times r)\ r = \{1, 2, \ldots, \beta\},\ k = \{1, 2, \ldots, 4\} \quad (2)$$

The average of each part is independently estimated using the aforementioned equation, where d with the interval $[1, \ldots, D]$ is determined using the variable F_s. Then, the fitness of quality is estimated for each section as shown below:

$$fit_{section} = avg\left(objective\left(F_s^{ik}\right) in\ section_r\right)\ r = \{1, 2, \ldots, \beta\},\ i = \{1, 2, \ldots, \eta\} \quad (3)$$

where objective(.) indicates the objective function, and avg(.) represents the average of the solutions within each section of land. Consequently, local L^{mem} and global memory G^{mem} updation are performed, and the best solution obtained from each portion is maintained in the local memory as represented below:

$$G^{mem} = round(t \times H);\ 0.1 < t < 1 \quad (4)$$

$$L^{mem} = round(t \times \eta);\ 0.1 < t < 1 \quad (5)$$

Moreover, the soil quality of each portion is changed and determined using the solutions of global memory in the farm's worst section as represented in the following models:

$$\rho = \tau \times rand(-1, 1) \quad (6)$$

$$F_s^{new} = \rho \times \left[F_s^{ik} - F_s^G\right] + c \quad (7)$$

where F_s^G randomly selects one of the global memory solutions, and τ is a random number between 0 and 1 that is initiated at the beginning of the algorithm. Furthermore, the solutions based on both local and global memory are updated, providing the feasible solutions in each portion, but they are not integrated with the local memory. However, some of the solutions are integrated with the best solution for improving quality, as illustrated below:

$$\delta_f = \begin{cases} F_s^{new} = F_s^{ik} + \varphi_1 \times \left[F_s^{id} - G^{best}\right]\ R > rand \\ F_s^{new} = F_s^{ik} + rand(0, 1) \times \left[F_s^{id} - G^{best}\right]\ else \end{cases} \quad (8)$$

where R indicates a random number ranging from o to 1 that represents the extent to which the solutions are combined with best global, and φ_1 is an integer determined at the beginning of optimization. Finally, the optimized feature set δ_f is obtained as the output of this algorithm, which is further used by the classifier for intrusion detection and classification. The description of F^3S technique is presented in Algorithm 1.

Algorithm 1: Farmland Fertility Feature Selection (F^3S)

Input : Feature set F_s
Output : Selected Features δ_f
Step 1: → H for each section of land, as shown in Equation (1);
Step 2: → Initialize the populations, and determine the soil quality $Q_{section}$ of each portion of the farm using Equation (2);
Step 3: → Compute the fitness of quality solution in each portion $fit_{section}$ using Equation (3);
Step 4: → Perform local (L^{mem}) and global (G^{mem}) memory updation, where the best solutions in each portion are stored in the local memory using Equations (4) and (5);
Step 5: → Change the quality of soil in each portion of the farm, which is determined with global memory solutions in the farm's worst section, as shown in Equations (6) and (7);
Step 6: → Update the solutions based on local memory and lobal memory L^{best}, providing the feasible solutions in each section.
Step 7: → Improve the quality of solutions, as depicted in Equation (8), for obtaining the optimized set of features δ_f.

3.2. Deep Perceptron Network (DPN)

After choosing the features, the DPN classifier model is applied to classify the malicious activities in a network according to their pertinent features. This is a deep learning model developed based on the multilayer perceptron neural network. The structure of the DPN is shown in Figure 3; it comprises more than three layers, including input and output layers. In this model, the network is first constructed with the number of hidden layers, and the output vector of the layer (i.e., feature map) is estimated, as shown in the following model

$$F_m^l = f\left(\vartheta^l\right) = f\left(W^l \times F_m^{l-1} + bias^l\right) \tag{9}$$

where $\vartheta^l \in \mathbb{R}^{N^l}$ is the activation vector of the l^{th} layer with N^l neurons, $W^l \in \mathbb{R}^{N^l * N^{l-1}}$ is the weight matrix, and $bias^l \in \mathbb{R}^{N^l}$ represents the bias vector. Consequently, the sigmoid transfer function is estimated, as shown in the following model:

$$f(\vartheta) = \frac{1}{(1 + e^{-\vartheta})} \tag{10}$$

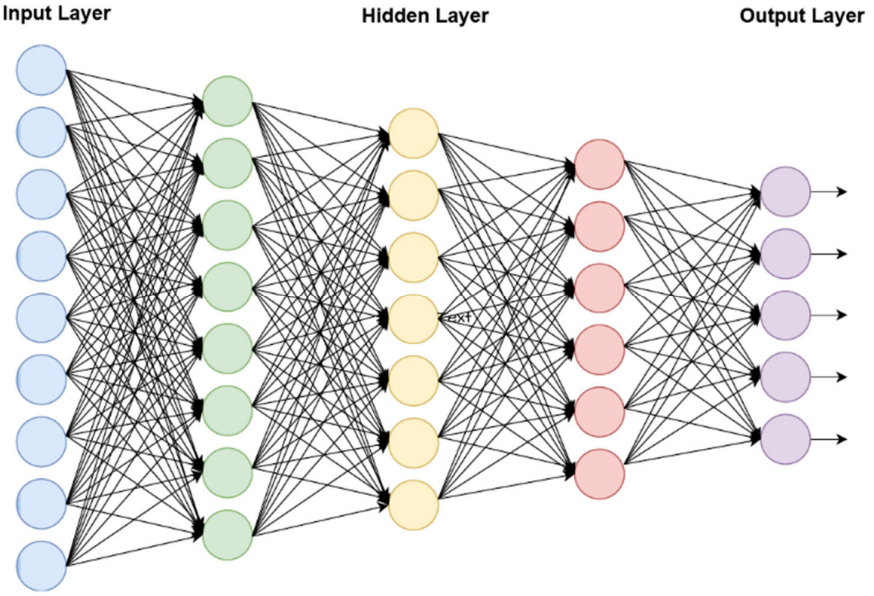

Figure 3. Structure of DPN.

Typically, the activation function must be properly selected according to the type of prediction application. In the proposed framework, the activation function is optimally computed using the TSO algorithm. The posterior probability of class $j \in \{1, \ldots, C\}$ was determined to be $Pr(cls_j|y)$. Here, the softmax function is used to satisfy the posterior probability function, as represented below:

$$F_m^L = Pr\left(cls_j\,|y\right) = softmax\left(\vartheta^L\right) = \frac{e^{\vartheta_j^L}}{\sum_{k=1}^{C} e^{\vartheta_k^L}} \tag{11}$$

where ϑ_j^L is the element with j^{th} index in the activation of vector ϑ^L. Moreover, the training process is carried out with the optimized cost function, as represented in the following equation:

$$Q\left(W^l, bias^l\right) = \frac{1}{S}\sum_{a=1}^{S} Q_{CE}\left(W^l, bias^l, y_a, l_f\right) + \beta\left|W^l\right|_F^2 \tag{12}$$

Finally, the predicted classified label can be produced, as shown in the following form:

$$Q_{CE}\left(W^{l}, bias^{l}, y_{a}\right) = -\sum_{k=1}^{C} y_{a}\left[F_{m}^{l}\right] \tag{13}$$

$$cls_{f} = Q_{CE}\left(W^{l}, bias^{l}, l_{f}\right) \tag{14}$$

Based on this prediction operation, normal and attacking events are precisely classified in the proposed framework. Moreover, the steps to develop DPN architecture is described in Algorithm 2.

Algorithm 2: Deep Perceptron Network (DPN)

Input : Selected Features δ_{f}, Label data l_{f};
Output : Classified output cls_{f};
Procedure:
Step 1 : Compute the feature map F_{m} using Equation (9);
Step 2: → Estimate the Sigmoid transformation as an activation function $f(\vartheta)$, as shown in Equation (10);//Tunicate Swarm Optimization;
Step 3: Compute the posterior probability of class,
$j \in \{1, \ldots, \mathcal{C}\}$ as $Pr(cls_{j}|y)$;
Step 4: → The softmax function is used to satisfy the posterior probability normalization requirement F_{m}^{L} as shown in Equation (11);
Step 5: → The training process is carried out with the optimized cost function as represented in Equation (12);
Step 6: → The classified output is predicted as shown in the form of Equations (13) and (14);

3.3. Tunicate Swarm Optimization (TSO)

During classification, the sigmoid transfer function is optimally computed by using the TSO algorithm, which helps to improve the intrusion detection rate of the classifier. In general, tunicates produce a bright, pale, blue-green bioluminescent light that can be seen from a few meters away. When they reach a size of a few millimeters, these cylindrical creatures have to crack at one of their ends. Each tunicate is made up of a developing gelatinous tunic that helps to bind all the organisms together. These tunicates can grow up to a few millimeters in length and only have an opening at one of their ends. Every tunicate develops a gelatinous tunic that aids in the unification of all the individuals. By drawing water from the sea surrounding them, each tunicate uses an atrial syphon to produce jet propulsions from its aperture. A tunicate needs to meet three requirements in order to satisfy the operations of jet propulsion using the statistical model: they need to avoid collisions between possible solutions, to move further in the direction of the best solution, and to stay close to the best solution. In this technique, the feature map result F_{m} is obtained as the input, and the optimal value $\vec{\varphi}_{r}$ is produced as the output. In the beginning, the parameters such as the constant $(\breve{\mathcal{F}})$, gravity force $(\breve{\mathcal{G}})$, water flow advection in the deep ocean $(\breve{\mathfrak{w}}_{f})$, social force $\breve{M}_{I}$, and the maximum number of iterations are initialized as shown below:

$$\breve{\mathcal{F}} = \frac{\breve{\mathcal{G}}}{\breve{M}_{I}} \tag{15}$$

$$\breve{\mathcal{G}} = r_{2} + r_{3} - \breve{\mathfrak{w}}_{f} \tag{16}$$

$$\breve{\mathfrak{w}}_{f} = 2 \times r_{1} \tag{17}$$

$$\breve{M}_{I} = [\rho_{mn} + r_{1} \times \rho_{mx} - \rho_{mn}] \tag{18}$$

where r_{1}, r_{2}, and r_{3} are random numbers in the range [0, 1], and ρ_{mn} and ρ_{mx} are considered to equal 1 and 4, respectively. After successfully avoiding a dispute with their neighbors, the search agents move towards the best neighbors, as represented below:

$$_{d} = |F_{m} - rand \times \vec{\varphi}_{r}(x)| \tag{19}$$

where $_{d}$ is the total distance between the search agent and food source, rand is a random number in the range [0, 1], x indicates the current iteration, F_m indicates the position of the food source, and $\vec{\varphi_r}$ is the position of the tunicates. The search agent may establish itself as the top search agent, as represented below:

$$\vec{\varphi_r}(x) = \begin{cases} F_m + \check{\mathcal{F}} \times {}_{d}\,, \text{ if rand} \geq 0.5 \\ F_m - \check{\mathcal{F}} \times {}_{d}\,, \text{ if rand} \geq 0.5 \end{cases} \tag{20}$$

Moreover, the position of all tunicates can be updated according to the position of the first two tunicates, as shown in the following model:

$$\vec{\varphi_r}(x+1) = \frac{\vec{\varphi_r}(x) + \vec{\varphi_r}(x+1)}{2 + r_1} \tag{21}$$

where $\vec{\varphi_r}(x+1)$ represents the updated position of the tunicates. Overall steps of TSO technique is described in Algorithm 3.

Algorithm 3: Tunicate Swarm Algorithm (TSO)

Input : Feature map result F_m;
Output: Optimal Value $\vec{\varphi_r}$;
Procedure:
Step 1 : The parameters $\check{\mathcal{F}}$(constant), gravity force ($\check{\mathcal{G}}$), water flow advection in the deep ocean ($\check{w}_f$), social force $\check{M}_I$, and the maximum number of iterations are initialized as represented in Equation (15) to (18);
Step 2: → After successfully avoiding a dispute with their neighbors, the search agents are directed towards the best neighbors, as shown in Equation (19);
Step 3: → The search agent can even establish its position as the leading search agent $\vec{\varphi_r}(x)$, as shown in Equation (20);
Step 4: → Update the position of all tunicates in accordance with the position of first two tunicates $\vec{\varphi_r}(x+1)$ using Equation (21);
Step 5: → Obtain the optimal value $\vec{\varphi_r}$ as the output;

4. Experimental Results

4.1. Experimental Setup

The effectiveness of the EEDPN was experimentally assessed, as shown in this section. This section contains detailed descriptions of the evaluation dataset, the experimental settings, and the experimental methods, as well as comparisons to traditional approaches, imbalanced data-processing algorithms, and cutting-edge intrusion detection techniques. To ensure efficient data handling and model training, hardware with the following specifications was used. An Intel Core i7 8th Gen processor (or higher) with a clock speed of at least 3.5 GHz was used. An NVIDIA GeForce RTX 2080 Ti GPU with 11 GB of GDDR6 VRAM was used due to its excellent deep-learning performance. The system has 16 GB of DDR4 RAM (2400 MHz) and a high-speed SSD with a 500 GB storage capacity for storing datasets, code, and model checkpoints. To support the specified hardware tools, the following software was used. The system operates on Windows 10 (64-bit). Keras 2.13 with TensorFlow as a backend for deep learning model development and MATLAB R2023b with the Statistics and Machine Learning Toolbox for machine learning algorithms were installed. Python 3.7 was used for data preprocessing and analysis. NumPy (v1.18.5) was used for numerical computations, pandas (v1.0.5) was used for data manipulation, scikit-learn (v0.23.1) was used for machine learning tasks, Matplotlib (v3.2.2) was used for data visualization, and Jupyter Notebook (v6.0.3) was used as the integrated development environment (IDE) for coding and experimentation.

At this stage, emerging benchmarking datasets like UNSW-NB 15 (intrusion dataset IS-1) and NSL-KDD (intrusion dataset IS-2) were taken into consideration for testing and validating this system. The Australian Centre for Cyber Security (ACCS) produced the UNSW-NB15 dataset in 2015. It comprises a wide range of deep-structure network communication data as well as minimal incursion information. As a result, it is better suited to imitating the complicated modern network environment. It depicts the modern network traffic mode. It has one unique attack category designation and 47 attributes. There are

2,540,044 samples in the collection, representing nine different attack methods, including fuzzers, DoS, analysis, reconnaissance, exploitation, shellcode, worm, backdoor, and generic. The NSL-KDD and UNSW-NB15 datasets, which exhibit high feature dimensions along with substantial data volume, are typical examples of high-dimensional imbalanced datasets. The majority of the data contained in them are typical network data, with only a trace quantity of attack data. Lower detection accuracy and longer training and detection times are precipitated by duplicated features and unbalanced data. The test set encompasses unidentified attacks, which puts the capacity for generalization under greater strain. Descriptions of the datasets are given in Table 2.

Table 2. Dataset details.

Attacking Classes	No of Samples
IS-1	
Normal	77,054
DoS	53,385
Probe	14,077
R2L	3749
U2R	252
UNSW-NB 15	
Normal	2,218,761
Generic	215,481
Exploits	44,525
Fuzzers	24,246
DoS	16,353
Reconnaissance	13,987
Analysis	2677
Backdoor	2329
Shellcode	1511
Worms	174

The NSL-KDD Dataset requires approximately 2 GB of storage space, while the UNSW-NB15 Dataset, being larger, requires around 4 GB of storage space. During deep-learning model training, the GPU memory usage ranges from 6 GB to 10 GB. This is to accommodate the model's architecture and batch size. The NVIDIA GeForce RTX 2080 Ti provides ample memory for efficient training. The bulk of CPU usage primarily occurs during data preprocessing, where multiple CPU cores are used for parallel data processing. The extent of CPU utilization varies but typically stays below 50%. RAM usage during model training depends on the batch size and model complexity. With a batch size of 32–64, the RAM usage remains within the available 16 GB, ensuring smooth model training. The training time for the EFDPN model using the specified hardware ranges from several hours to a day. This is related to the dataset's size, model complexity, and the number of training epochs. Adequate storage space (500 GB) is available for storing datasets, code, model checkpoints, and experiment results. Multiple experiments were conducted to assess the impact of hyperparameters and configurations. Computational overhead is incurred for each experiment. Data preprocessing, including cleaning, normalization, and feature engineering, primarily utilizes CPU resources and requires a few hours for completion, depending on the dataset's size.

4.2. Performance Metrics

The standard parameters such as accuracy, precision, recall, f1-score, and training time were computed in this study in order to validate the proposed EFDPN model. These parameters determine the overall performance of the security framework, which is estimated using the following models:

$$\text{Accuracy} = \frac{T_{+ve} + T_{-ve}}{T_{+ve} + T_{-ve} + F_{+ve} + F_{-ve}} \tag{22}$$

$$\text{Precision} = \frac{T_{+ve}}{T_{+ve} + F_{+ve}} \tag{23}$$

$$\text{Recall or TPR} = \frac{T_{+ve}}{T_{+ve} + F_{+ve}} \tag{24}$$

$$F1 - \text{score} = 2 \times \left(\frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \right) \tag{25}$$

$$\text{FPR} = \frac{F_{+ve}}{F_{+ve} + T_{-ve}} \tag{26}$$

$$\text{FNR} = \frac{F_{-ve}}{T_{+ve} + F_{-ve}} \tag{27}$$

where T_{+ve} indicates a true positive, T_{-ve} represents a true negative, F_{+ve} is a false positive, and F_{-ve} is a false negative. Figure 4 evaluates the performance of the proposed EFDPN model using IS-1 with and without the F^3S mechanism.

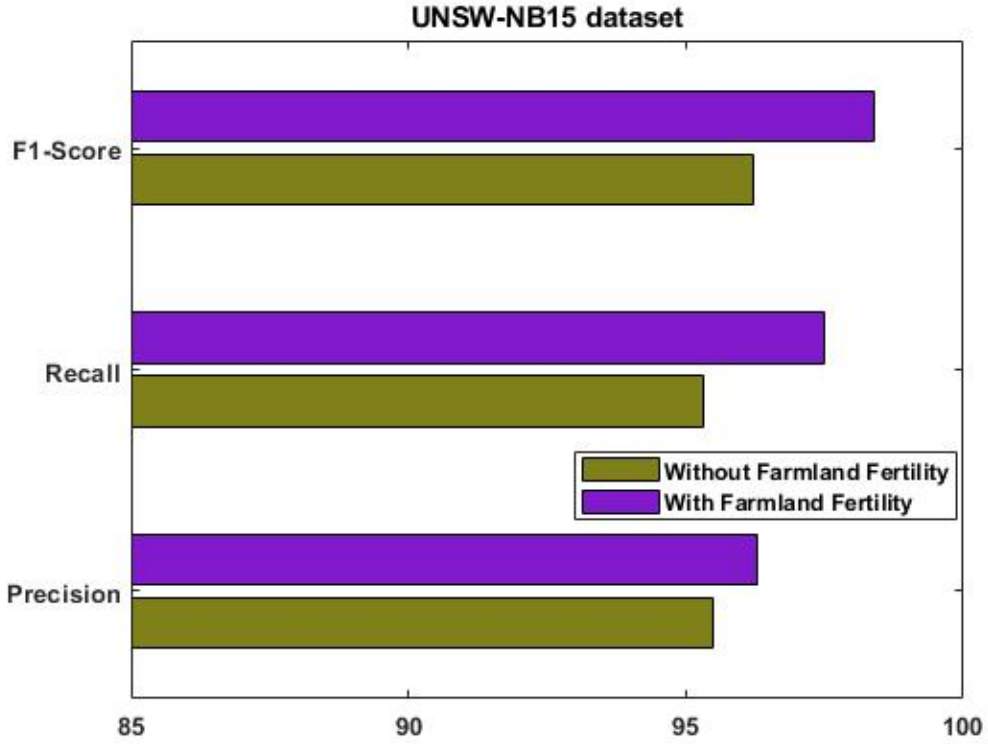

Figure 4. Performance analysis with and without optimization algorithms for IS-1.

4.3. Results Analysis

This section validates the performance and results of the proposed EFDPN cyber-physical system using a variety of measures and public datasets. The sample network environment created in this analysis is shown in Figure 5, where the green-colored nodes are considered normal, and other colors indicate the different types of intrusions. By using the combination of F^3S + DPN + TSO models, intrusions can be accurately predicted in the proposed framework. For the testing and validation of this system, emerging benchmarking datasets such as UNSW-NB 15 (Intrusion dataset IS-1) and NSL-KDD (Intrusion dataset IS-2) were considered.

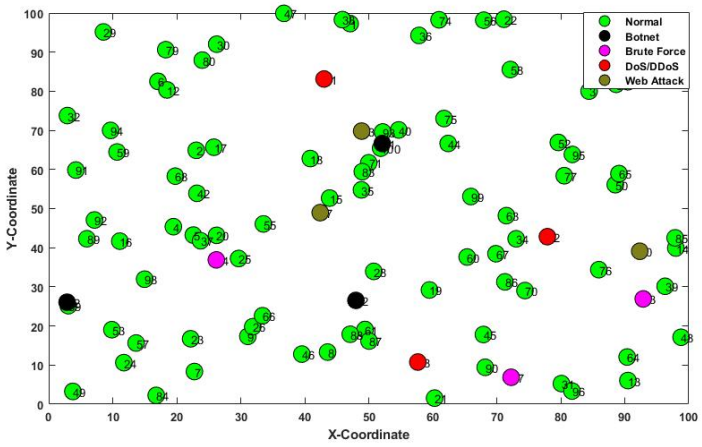

Figure 5. Network deployment.

Similarly, the results were estimated for IS-2, as shown in Figure 6. This analysis was mainly carried out to determine the importance of using the F3S mechanism in the intrusion detection approach. The results reveal that performance was greatly improved with the use of the F3S algorithm for both datasets. As the increased dimensionality of features may affect the performance of a classifier with low accuracy, it is essential to squeeze the feature dimensionality for improved detection results. Figures 7–10 show the results of the validation and comparison of the accuracy, precision, recall, and f1-score parameters for both conventional [39] and the proposed intrusion detection approaches with respect to the different types of attacks. These results include the following attack categories: normal attack, brute force attack, botnet attack, and web attack. A subset of the model's performance was used to evaluate the accuracy of the algorithm. One of the metrics used to evaluate the classification models was accuracy, as computed in Equation (22). Precision implies a high rate of accurate estimation. It is a percentage of all genuine positives that the model claims are connected with all positives that the model expects, and it is estimated using Equation (23). Recall is also referred to as the true positive rate (as computed in Equation (24)), which compares the total positives in all the system states to the actual total of positives in the data. Additionally, model performance can be estimated using the F1 score, which is the weighted average of precision and recall, as computed in Equation (25). The obtained results reveal that the proposed EFDPN-based security model provides an effective attack detection result when compared to the other techniques. Due to the inclusion of the TSO and F3O algorithms, the security performance results are greatly enhanced in the proposed cyber-physical system.

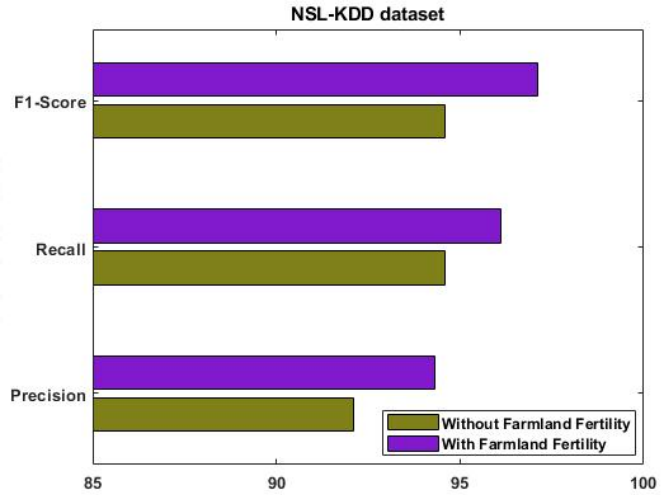

Figure 6. Performance analysis with and without optimization algorithms for IS-2.

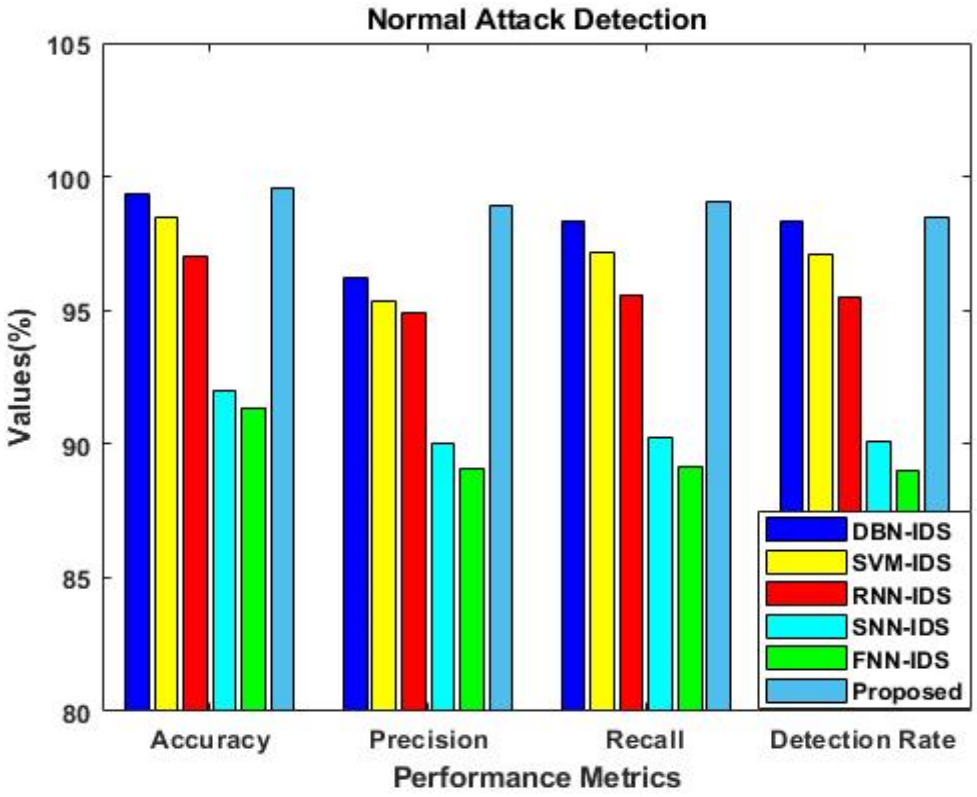

Figure 7. Comparative analysis with other IDS approaches for normal attacks.

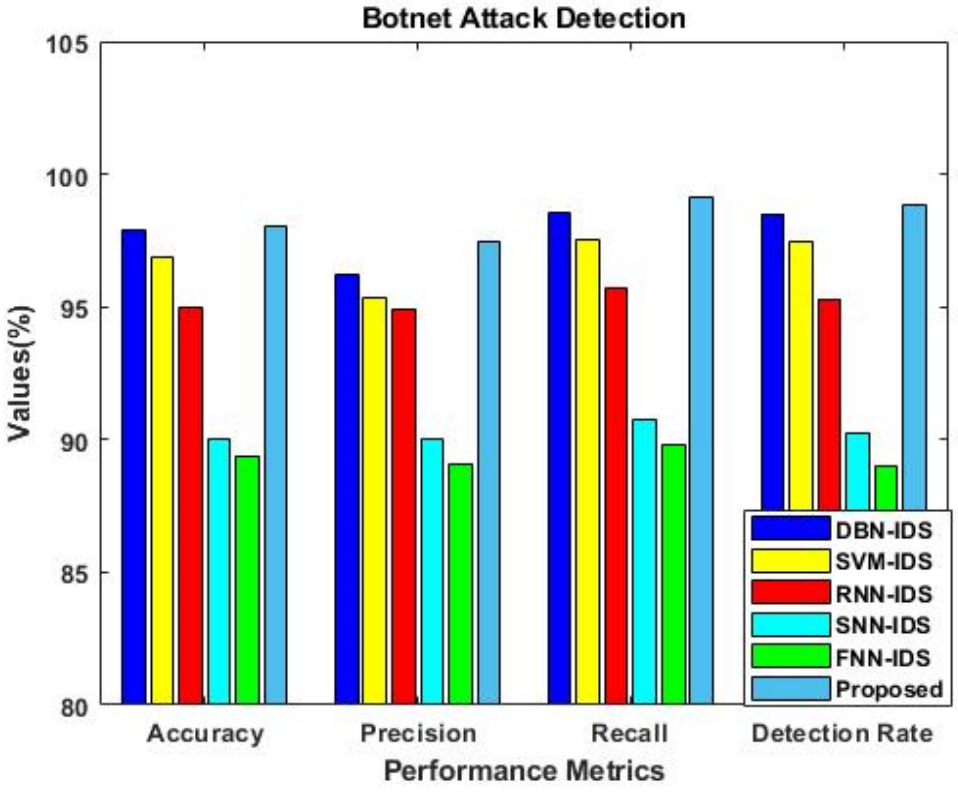

Figure 8. Comparative analysis with other IDS approaches for Botnet attacks.

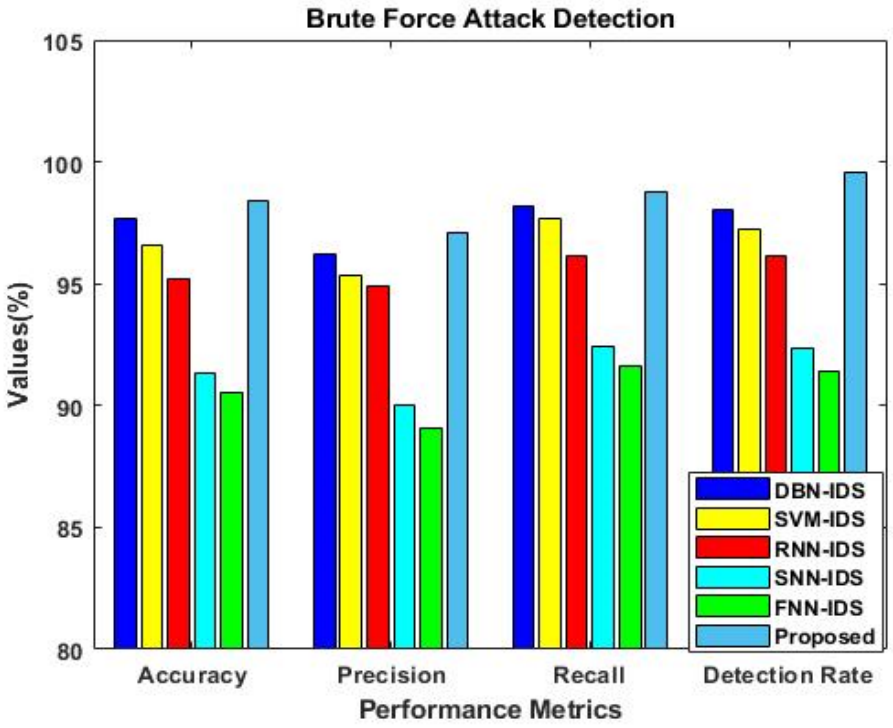

Figure 9. Comparative analysis with other IDS approaches for brute-force attacks.

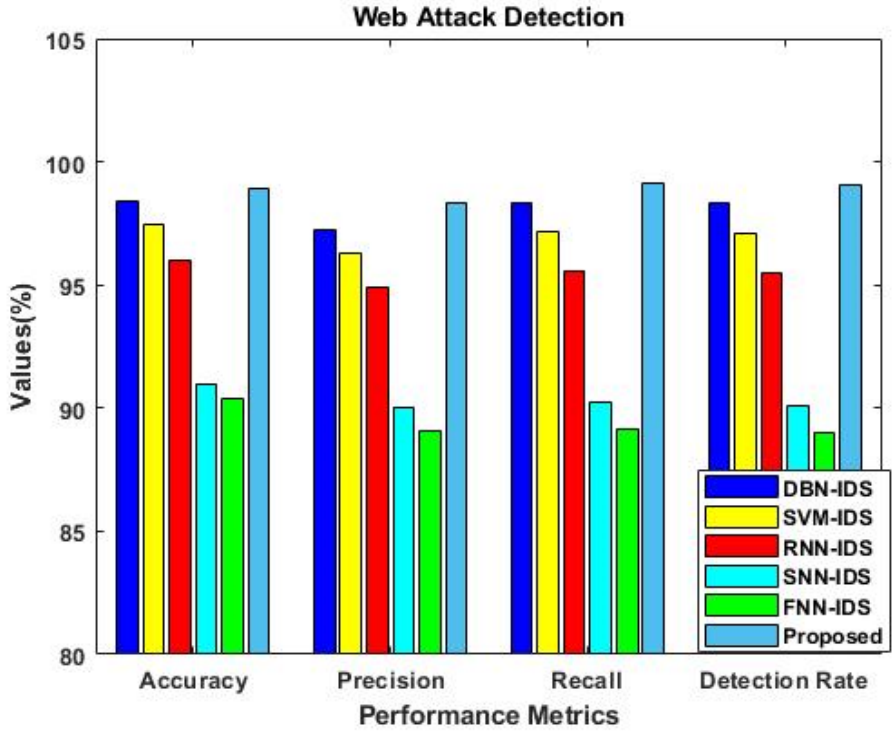

Figure 10. Comparative analysis with other IDS approaches for web attacks.

Figure 11 validates the F1-score values of all the existing intrusion detection approaches in accordance with the different types of attacks. The estimated results indicate that the proposed EFDPN model triumphs over the conventional DBN-, SVM-, RNN-, SNN-, and FNN-based intrusion detection approaches, presenting an increased F1-score value. The F3S algorithm plays a vital role in obtaining better prediction results in the proposed framework since it eliminates irrelevant features in order to improve the prediction process of the classifier.

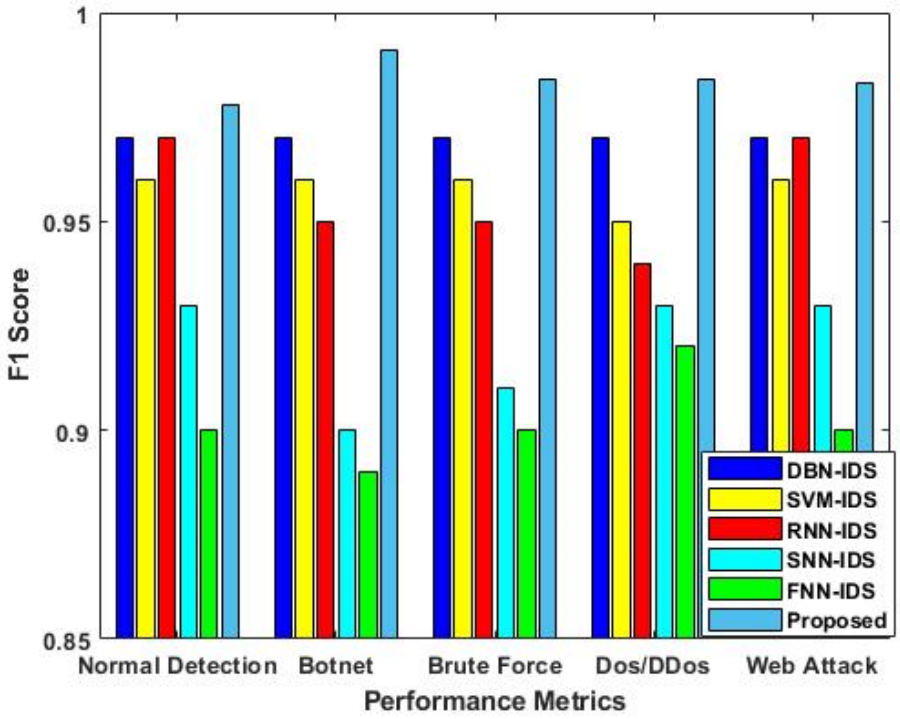

Figure 11. F1-score analysis with respect to different types of attacks.

Figures 12 and 13 show the results of the validation and comparison of the existing [40] and proposed security methodologies performed using the IS-1 dataset. The obtained results also indicate that the proposed EFDPN model outperforms the other models, yielding high performance results. The deployed cyber-physical system represents a more advanced and intelligent approach to intrusion detection, integrating cutting-edge techniques and optimizing the classification process. It offers improved adaptability, efficiency, and performance compared to traditional IDSs.

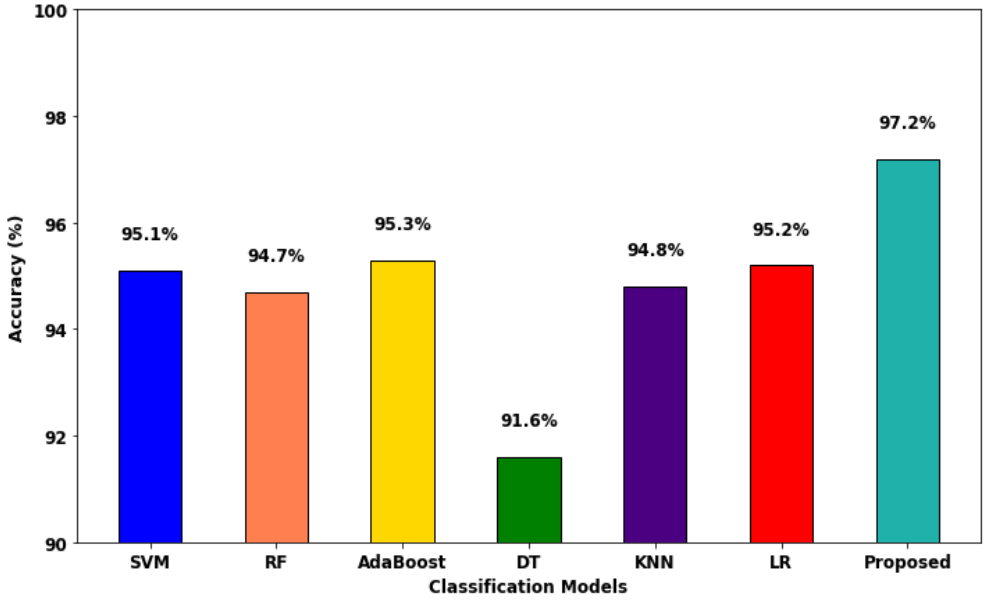

Figure 12. Comparative analysis with other IDS approaches based on accuracy.

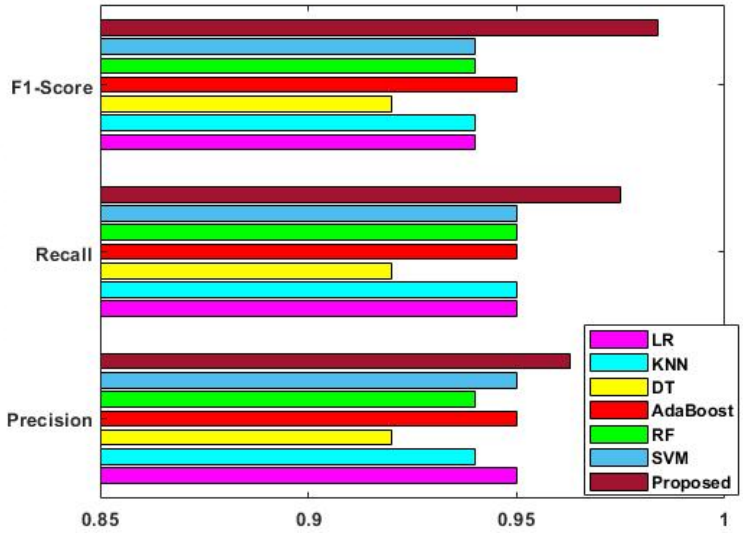

Figure 13. Intrusion detection performance analysis with other IDS approaches.

Figure 14 compares the conventional PSO-based classification [41] and the proposed EFDPN models using the IS-1 dataset. In order to demonstrate the effectiveness of optimization in the security framework, the optimization-integrated classifier models are compared in this study. For this assessment, standard machine learning algorithms, including RF, DT, KNN, and RC, are considered, which predict intrusions in the dataset according to the features chosen via PSO. In contrast to these algorithms, the proposed EFDPN algorithm yields improved detection results. Since the F3S technique provides the best solution with an increased convergence rate, it effectively reduces the dimensionality of features before the training and testing processes. Therefore, the proposed F3S incorporated with the DPN model greatly outperforms the other classification approaches. A comparative analysis based on the classifier's training time was performed, as shown in Figure 15. A good classification model should minimize the training time and offer an increased attack detection rate. Typically, the classifier's training time can be increased with the use of high-dimensionality features, which also increases the computational complexity of classification. Therefore, the input feature set used for the classifier's training must be optimized for better predictions. According to the results, the proposed EFDPN model could effectively reduce the training time with the use of the F3S algorithm.

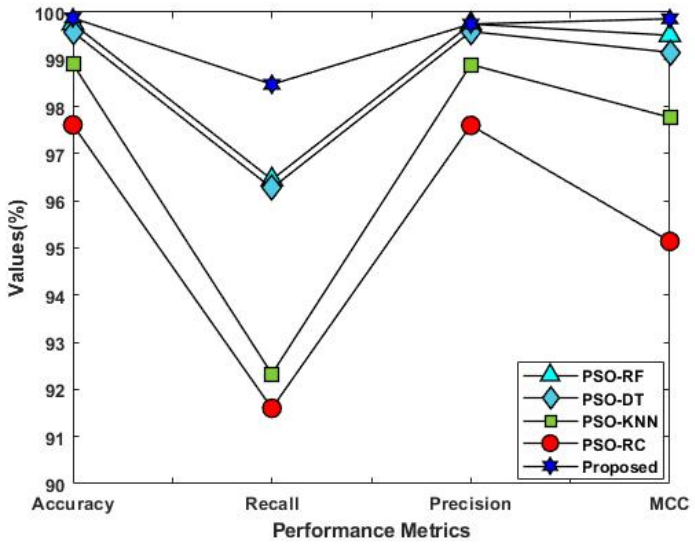

Figure 14. Overall comparative analysis with optimization-based intrusion detection approaches.

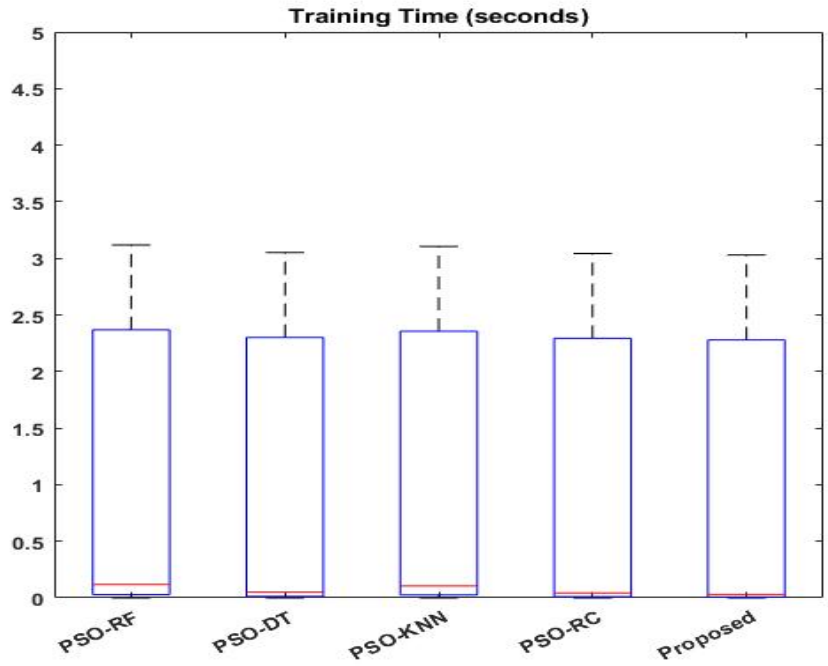

Figure 15. Comparative analysis with other IDS approaches based on training time (s).

Figure 16 compares the accuracy of various machine learning and deep learning techniques [42] used for intrusion detection. In addition, the classifier's detection accuracy is estimated and compared for both IS-1 and IS-2, as shown in Figures 17 and 18, respectively. In addition, a qualitative security analysis [31] was also performed in this study, as shown in Table 3, based on the following parameters: false acceptance rate, accuracy, detection rate, number of features, and time consumption. Overall, the estimated results demonstrate that the proposed EFDPN cyber-physical system provides effective prediction results when compared with the existing algorithms due to the inclusion of the F3S and TSO algorithms. This is because effective dimensionality reduction was achieved with the use of the F3S technique and the classifier sigmoid function was computed with the use of the TSO algorithm.

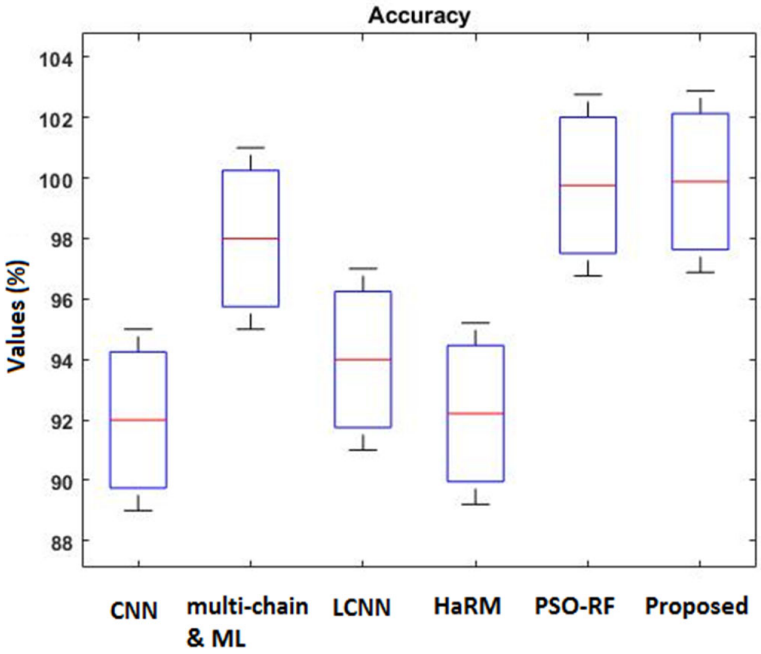

Figure 16. Comparative analysis based on accuracy.

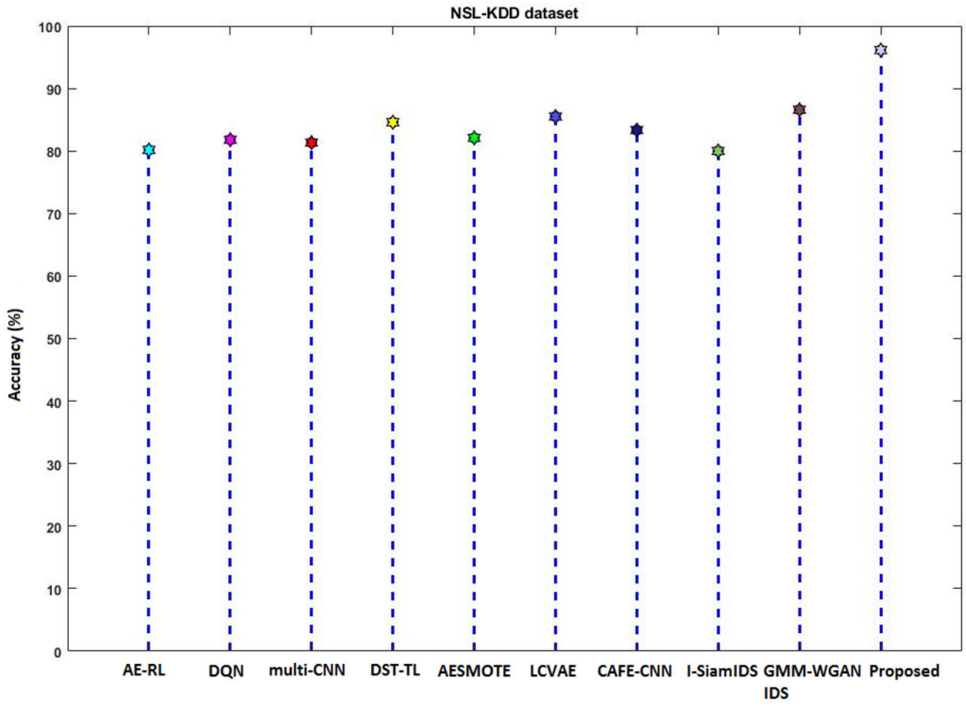

Figure 17. Accuracy analysis using IS-1.

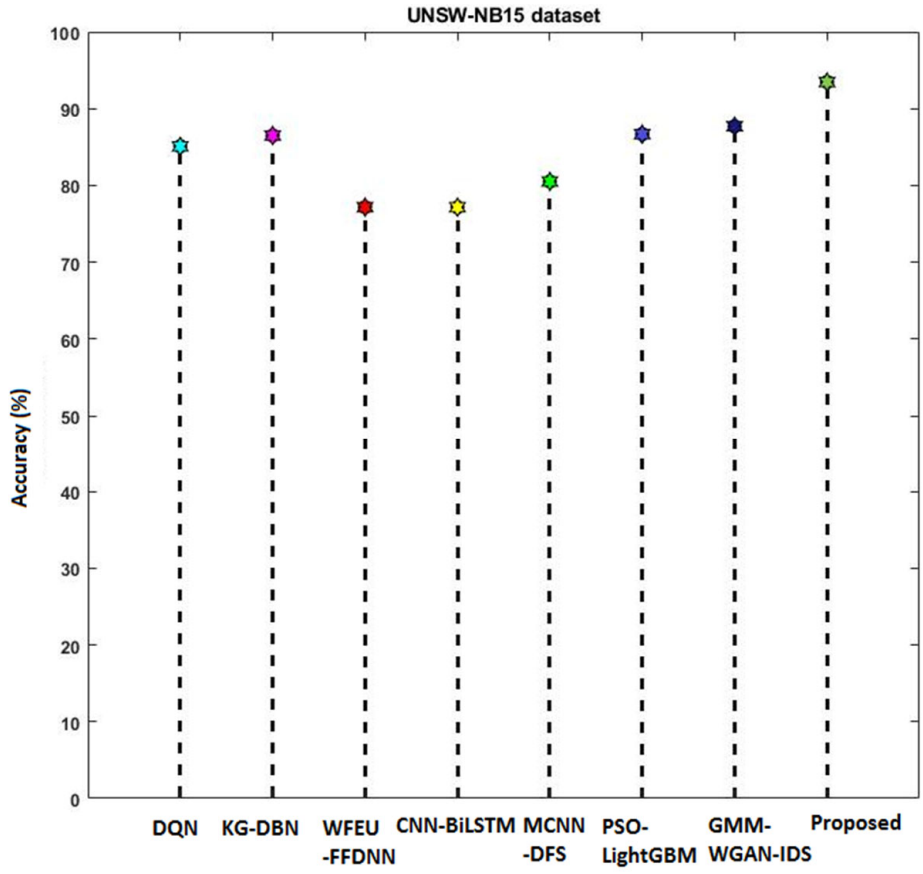

Figure 18. Accuracy analysis using IS-2.

Table 3. Security analysis.

Methods	FAR	Accuracy	DR	No of Features	Time
Multi-agent IDS	L	L	VH	NA	NA
ARIMA-IDS	L	L	VH	NA	H
Lightweight IDS	VL	H	VH	NA	NA
Sensor IDS	L	H	VH	NA	NA
PSO-IDS	H	H	L	VH	NA
Evolutionary NN—MO IDS	VH	VH	VH	L	NA
GWO-SVM	VL	H	H	VL	VL
Proposed	VL	VH	VH	VL	VL

L—Low, VH—Very High, NA—Not applicable, H—High, and VL—Very Low.

5. Discussion

In this study, we embarked on a rigorous exploration of potential enhancements in intrusion detection mechanisms within the framework of WSN-IoT networks through the development and evaluation of an Emphatic Farmland Fertility Integrated Deep Perceptron Network (EFDPN)-based cyber-physical system. Our investigative journey was grounded in a substantial body of previous studies, which mapped out the present landscape of intrusion detection systems, along with their respective merits and challenges ([24,25,29,30,35–38]). The proposed EFDPN model represents a significant stride towards the fortification of WSN-IoT networks, primarily anchored by its innovative Farmland Fertility Feature Selection (F3S) mechanism and a potent classification stage leveraging a Deep Perceptron Network (DPN) followed by fine-tuning with Tunicate Swarm Optimization (TSO) for sigmoid transformation function estimation. This innovative concoction of methodologies not only hones the accuracy of intrusion detection but also astutely manages feature dimensionality, thereby mitigating computational complexity and enhancing the efficiency of the system.

When juxtaposed against existing models documented in previous studies, such as DBN-, SVM-, RNN-, SNN-, and FNN-based approaches, our model exhibits a significant escalation in performance metrics such as accuracy, precision, recall, and F1-score, as evidenced by the results derived from utilizing the benchmark datasets UNSW-NB 15 and NSL-KDD ([39–42]). Notably, the implementation of the F3S algorithm resulted in being a crucial factor in boosting the predictive efficacy of the classifier via allowing for the meticulous filtering of irrelevant features, thereby facilitating an improved prediction process and a commendable reduction in training time. However, it is imperative to acknowledge potential limitations that might encumber the proposed framework. Future studies might focus on further optimizing the computational efficiency of the EFDPN model alongside exploring its applicability and performance across diverse, more complex network environments. Additionally, a deeper dive into addressing potential vulnerabilities to newer, sophisticated attack vectors would be a prudent avenue to tread.

While the results are promising, we recognize the need for continuous evolution in optimizing computational efficiency and in tailoring the framework to counter newer, sophisticated attack vectors. Future research trajectories should also explore the scalability of the EFDPN in real-time environments with diverse infrastructures to fully realize its robustness and adaptability.

Furthermore, the scalability of the proposed model should be tested in real-time scenarios, spanning across diverse infrastructures and varying scales, to rigorously assess its robustness and adaptability. Parallelly, fostering collaborations with industry stakeholders could foster the refinement of the model to meet specific, real-world requirements and standards. In conclusion, our study stands as a testament to the viable advancements in securing WSN-IoT networks through intelligent, data-driven mechanisms. The EFDPN model, with its innovative blend of feature selection and classification methodologies, marks a promising precedent in the realm of cyber-physical systems security. As we venture forth, it holds immense potential to spearhead a new generation of resilient, efficient, and

intelligent intrusion detection systems, fostering a safer and more secure cyber-physical landscape.

5.1. Advantages of EFDPN Model

Our study offers a novel strategy for protecting WSN-IoT networks using clever, data-driven approaches. The EFDPN model, with its novel convergence of feature selection and classification strategies, heralds a promising frontier in the security of cyber-physical systems, promising a robust, effective, and intelligent infrastructure capable of fending off the constantly evolving cyberthreats and fostering a safer and more secure cyber-physical landscape. The following are the primary advantages of the proposed system:

(1) The model can precisely identify different types of incursions by combining F3S and DPN, reducing false positives;
(2) The F3S method makes it easier to extract pertinent information, improving the model's capacity to pinpoint threats with greater accuracy while requiring less computational effort;
(3) By including tunicate swarm optimization (TSO), the sigmoid transformation function can be adjusted, improving the model's ability to detect intrusions;
(4) Thanks to better feature selection and decreased dimensionality, the EFDPN model efficiently decreases training time, boosting efficiency without compromising the detection rate;
(5) The architecture of the EFDPN model allows for scalable deployment, making it adaptable to various network sizes and complexities;
(6) The model is capable of identifying and mitigating a wide range of attack categories, including brute force, botnet, and web attacks, thereby providing a robust defense mechanism;
(7) The model's compatibility with established benchmark datasets (UNSW-NB 15 and NSL-KDD) showcases its readiness for real-world applications and further testing;
(8) Given its feature set and capabilities, the EFDPN model has substantial potential for implementation in real-time environments, offering a timely response to security breaches;
(9) The model is designed to minimize the usage of resources, such as memory, through intelligent design choices in the classification and feature selection phases, which contribute to overall system efficiency.

5.2. Future Works

The proposed EFDPN model heralds a promising frontier in the security landscape of WSN-IoT networks. In the future, the following trajectories can be pursued to further its potential:

(1) Conduct pilot studies to assess the model's adaptability and performance in real-time environments, with a focus on scaling the model to accommodate larger and more complex network infrastructures;
(2) Further refine the F3S and TSO algorithms to enhance computational efficiency and accuracy, possibly integrating it with other optimization techniques to forge a more robust system;
(3) Continually update and adapt the model to identify and counteract emerging and sophisticated attack vectors, fostering a dynamic security framework that evolves with the threat landscape;
(4) Develop multi-layered security protocols within the EFDPN framework, which can work in synergy with existing security infrastructures, to provide a comprehensive security solution;
(5) Explore the potential applications of the EFDPN model in other domains, such as industrial control systems and healthcare networks, tailoring the model to meet the unique security requirements of these sectors;
(6) Engage with the user and broader community to gather feedback and insights, fostering a collaborative approach to further refine and enhance the model;

(7) Develop educational initiatives and training programs to foster awareness and skill development, equipping individuals and organizations with the tools to effectively deploy and manage EFDPN-based security systems.

By pursuing these trajectories, we envision the EFDPN model evolving into a cornerstone of cybersecurity in WSN-IoT networks, setting a new standard in resilience, efficiency, and intelligence in the face of escalating cyber threats.

6. Conclusions

This paper introduces novel EFDPN-based cyber-physical systems designed to increase the security of WSN-IoT systems. In this study, the combination of F3S, DPN, and TSO mechanisms was implemented to construct a computationally effective and accurate intrusion detection framework. The emerging public intrusion detection datasets IS-1 and IS-2 were obtained first for processing. To extract the necessary features from the given dataset, dataset normalization and feature extraction processes were carried out. After the set of features was retrieved, the new F3S algorithm was utilized to choose the best features by reducing dimensionality. The objective of this technique is to generate precise categorization results with little computational overhead. The DPN classifier can then forecast malicious occurrences using the attributes that were carefully selected from the dataset. In this instance, the sigmoid transfer function is optimally computed using the TSO model, which improves the classifier's effectiveness in attack detection. Moreover, standard performance measures such as accuracy, precision, recall, f1-score, and training time were estimated and compared during evaluation to demonstrate the effectiveness of the EFDPN model. Then, recent state-of-the-art models were compared with the EFDPN mechanism using IS-1 and IS-2. Overall, the obtained results reveal that the EFDPN model provides improved prediction performance over other algorithms following the inclusion of F3S and TSO algorithms. In the future, the current security framework will be enhanced to protect IoMT or IoHT from network intrusions with low complexity.

Author Contributions: Conceptualization, S.K., M.B.A., L.I.A. and Q.A.; Data curation, S.K., M.B.A. and Q.A.; Formal analysis, S.K. and M.B.A.; Funding acquisition, M.B.A. and L.I.A.; Investigation, L.I.A. and Q.A.; Methodology, S.K., M.B.A. and Q.A.; Project administration, M.B.A. and L.I.A.; Resources, M.B.A., L.I.A. and Q.A.; Software, S.K., M.B.A., L.I.A. and Q.A.; Validation, S.K. and M.B.A.; Visualization, S.K. and Q.A.; Writing—original draft, S.K., M.B.A. and Q.A.; Writing—review and editing, Q.A. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported and funded by the Deanship of Scientific Research at Imam Mohammad Ibn Saud Islamic University (IMSIU) (grant number IMSIU-RG23129).

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Acknowledgments: This work was supported and funded by the Deanship of Scientific Research at Imam Mohammad Ibn Saud Islamic University (IMSIU) (grant number IMSIU-RG23129).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Hasan, M.Z.; Hanapi, Z.M. Efficient and Secured Mechanisms for Data Link in IoT WSNs: A Literature Review. *Electronics* **2023**, *12*, 458. [CrossRef]
2. Begum, B.A.; Nandury, S.V. Data Aggregation Protocols for WSN and IoT Applications–A Comprehensive Survey. *J. King Saud Univ. Comput. Inf. Sci.* **2023**, *35*, 651–681. [CrossRef]
3. Sudha, I.; Mustafa, M.A.; Suguna, R.; Karupusamy, S.; Ammisetty, V.; Shavkatovich, S.N.; Ramalingam, M.; Kanani, P. Pulse jamming attack detection using swarm intelligence in wireless sensor networks. *Optik* **2023**, *272*, 170251. [CrossRef]
4. Ramana, K.; Revathi, A.; Gayathri, A.; Jhaveri, R.H.; Narayana, C.L.; Kumar, B.N. WOGRU-IDS—An intelligent intrusion detection system for IoT assisted Wireless Sensor Networks. *Comput. Commun.* **2022**, *196*, 195–206. [CrossRef]

5. Biswas, P.; Samanta, T.; Sanyal, J. Intrusion detection using graph neural network and Lyapunov optimization in wireless sensor network. *Multimed. Tools Appl.* **2023**, *82*, 14123–14134. [CrossRef]
6. Reddy, G.; Kadiyala, S.; Potluri, C.S.; Saravanan, P.S.; Athisha, G.; Mukunthan, M.; Sujaritha, M. An Intrusion Detection Using Machine Learning Algorithm Multi-Layer Perceptron (MlP): A Classification Enhancement in Wireless Sensor Network (WSN). *Int. J. Recent Innov. Trends Comput. Commun.* **2022**, *10*, 139–145. [CrossRef]
7. Choudhary, V.; Srivastava, A.; Kumar, A.; Taruna, S. Comparative Analysis of Security Issues and Trends in IoT and WSN. *SAMRIDDHI J. Phys. Sci. Eng. Technol.* **2022**, *14*, 216–222.
8. Alwan, M.H.; Hammadi, Y.I.; Mahmood, O.A.; Muthanna, A.; Koucheryavy, A. High Density Sensor Networks Intrusion Detection System for Anomaly Intruders Using the Slime Mould Algorithm. *Electronics* **2022**, *11*, 3332. [CrossRef]
9. Ahmed, S.H.; Rani, S. A hybrid approach, Smart Street use case and future aspects for Internet of Things in smart cities. *Future Gener. Comput. Syst.* **2018**, *79*, 941–951. [CrossRef]
10. Zrelli, A.; Nakkach, C.; Ezzedine, T. Cyber-Security for IoT Applications based on ANN Algorithm. In Proceedings of the 2022 International Symposium on Networks, Computers and Communications (ISNCC), Shenzhen, China, 19–22 July 2022; pp. 1–5.
11. Kumar, A.; Agrawal, K.K. Energy-Efficient Resource Allocation and Routing Protocols for IoT-based WSN: A Review. In Proceedings of the 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Bengaluru, India, 27–28 January 2023; pp. 363–369.
12. Samara, A.M.; Bennis, I.; Abouaissa, A.; Lorenz, P. A survey of outlier detection techniques in IoT: Review and classification. *J. Sens. Actuator Netw.* **2022**, *11*, 4. [CrossRef]
13. Vishnu, V.M. ProSD-edgeIoT: Protected cluster assisted SDWSN for tetrad edge-IoT by collaborative DDoS detection and mitigation. *Cyber-Phys. Syst.* **2023**, *9*, 144–173.
14. Kumar, A.; Dhabliya, D.; Agarwal, P.; Aneja, N.; Dadheech, P.; Jamal, S.S.; Antwi, O.A. Cyber-internet security framework to conquer energy-related attacks on the internet of things with machine learning techniques. *Comput. Intell. Neurosci.* **2022**, *2022*, 8803586. [CrossRef] [PubMed]
15. Sheron, P.F.; Sridhar, K.; Baskar, S.; Shakeel, P.M. A decentralized scalable security framework for end-to-end authentication of future IoT communication. *Trans. Emerg. Telecommun. Technol.* **2019**, *31*, e3815a. [CrossRef]
16. VenkataRao, S.; Ananth, V. A Hybrid Optimization Algorithm and Shamir Secret Sharing Based Secure Data Transmission for IoT based WSN. *Int. J. Intell. Eng. Syst.* **2021**, *14*, 498–506.
17. Ismail, S.; Reza, H. Evaluation of Naïve Bayesian Algorithms for Cyber-Attacks Detection in Wireless Sensor Networks. In Proceedings of the 2022 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 6–9 June 2022; pp. 283–289.
18. Subburayalu, G.; Duraivelu, H.; Raveendran, A.P.; Arunachalam, R.; Kongara, D.; Thangavel, C. Cluster based malicious node detection system for mobile ad-hoc network using ANFIS classifier. *J. Appl. Secur. Res.* **2021**, *18*, 402–420. [CrossRef]
19. Islam, M.S.; Dey, G.K. Precision agriculture: Renewable energy based smart crop field monitoring and management system using WSN via IoT. In Proceedings of the 2019 International Conference on Sustainable Technologies for Industry 4.0 (STI), Dhaka, Bangladesh, 24–25 December 2019; pp. 1–6.
20. Tama, B.A.; Lim, S. Ensemble learning for intrusion detection systems: A systematic mapping study and cross-benchmark evaluation. *Comput. Sci. Rev.* **2021**, *39*, 100357. [CrossRef]
21. Zrelli, A.; Ezzedine, T. A new approach of WSN deployment, K-coverage and connectivity in border area. *Wirel. Pers. Commun.* **2021**, *121*, 3365–3381. [CrossRef]
22. Iwendi, C.; Maddikunta, P.K.R.; Gadekallu, T.R.; Lakshmanna, K.; Bashir, A.K.; Piran, J. A metaheuristic optimization approach for energy efficiency in the IoT networks. *Softw. Pract. Exp.* **2021**, *51*, 2558–2571. [CrossRef]
23. Rajeswari, A.; Kulothungan, K.; Ganapathy, S.; Kannan, A. Trusted energy aware cluster based routing using fuzzy logic for WSN in IoT. *J. Intell. Fuzzy Syst.* **2021**, *40*, 9197–9211. [CrossRef]
24. Pundir, S.; Wazid, M.; Singh, D.P.; Das, A.K.; Rodrigues, J.J.; Park, Y. Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: Survey and future challenges. *IEEE Access* **2019**, *8*, 3343–3363. [CrossRef]
25. Baraneetharan, E. Role of machine learning algorithms intrusion detection in WSNs: A survey. *J. Inf. Technol. Digit. World* **2020**, *2*, 161–173. [CrossRef]
26. Jiang, S.; Zhao, J.; Xu, X. SLGBM: An intrusion detection mechanism for wireless sensor networks in smart environments. *IEEE Access* **2020**, *8*, 169548–169558. [CrossRef]
27. Amouri, A.; Alaparthy, V.T.; Morgera, S.D. A machine learning based intrusion detection system for mobile Internet of Things. *Sensors* **2020**, *20*, 461. [CrossRef] [PubMed]
28. Gopalakrishnan, S. Performance analysis of malicious node detection and elimination using clustering approach on MANET. *Circuits Syst.* **2016**, *7*, 748–758. [CrossRef]
29. Singh, G.; Khare, N. A survey of intrusion detection from the perspective of intrusion datasets and machine learning techniques. *Int. J. Comput. Appl.* **2022**, *44*, 659–669. [CrossRef]
30. Damasevicius, R.; Venckauskas, A.; Grigaliunas, S.; Toldinas, J.; Morkevicius, N.; Aleliunas, T.; Smuikys, P. LITNET-2020: An annotated real-world network flow dataset for network intrusion detection. *Electronics* **2020**, *9*, 800. [CrossRef]
31. Safaldin, M.; Otair, M.; Abualigah, L. Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks. *J. Ambient. Intell. Humaniz. Comput.* **2021**, *12*, 1559–1576. [CrossRef]

32. Hemanand, D.; Reddy, G.V.; Babu, S.S.; Balmuri, K.R.; Chitra, T.; Gopalakrishnan, S. An Intelligent Intrusion Detection and Classification System using CSGO-LSVM Model for Wireless Sensor Networks (WSNs). *Int. J. Intell. Syst. Appl. Eng.* **2022**, *10*, 285–293.
33. Jayanayudu, D.; Sudhir, A.C. Shuffled Frog Leap and Ant Lion Optimization for Intrusion Detection in IoT-Based WSN. In *Proceedings of Fourth International Conference on Computer and Communication Technologies*; Springer: Singapore, 2023; pp. 17–26.
34. Hussain, M.Z.; Hanapi, Z.M. Efficient Secure Routing Mechanisms for the Low-Powered IoT Network: A Literature Review. *Electronics* **2023**, *12*, 482. [CrossRef]
35. Al Sawafi, Y.; Touzene, A.; Hedjam, R. Hybrid Deep Learning-Based Intrusion Detection System for RPL IoT Networks. *J. Sens. Actuator Netw.* **2023**, *12*, 21. [CrossRef]
36. Maheswari, M.; Karthika, R. A Novel Hybrid Deep Learning Framework for Intrusion Detection Systems in WSN-IoT Networks. *Intell. Autom. Soft Comput.* **2022**, *33*, 365–3822022. [CrossRef]
37. Maldonado, J.; Riff, M.C.; Neveu, B. A review of recent approaches on wrapper feature selection for intrusion detection. *Expert Syst. Appl.* **2022**, *198*, 116822. [CrossRef]
38. De Souza, C.A.; Westphall, C.B.; Machado, R.B. Two-step ensemble approach for intrusion detection and identification in IoT and fog computing environments. *Comput. Electr. Eng.* **2022**, *98*, 107694. [CrossRef]
39. Manimurugan, S.; Al-Mutairi, S.; Aborokbah, M.M.; Chilamkurti, N.; Ganesan, S.; Patan, R. Effective attack detection in internet of medical things smart environment using a deep belief neural network. *IEEE Access* **2020**, *8*, 77396–77404. [CrossRef]
40. Chaganti, R.; Mourade, A.; Ravi, V.; Vemprala, N.; Dua, A.; Bhushan, B. A Particle Swarm Optimization and Deep Learning Approach for Intrusion Detection System in Internet of Medical Things. *Sustainability* **2022**, *14*, 12828. [CrossRef]
41. Saheed, Y.K.; Arowolo, M.O. Efficient cyber attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms. *IEEE Access* **2021**, *9*, 161546–161554. [CrossRef]
42. Cui, J.; Zong, L.; Xie, J.; Tang, M. A novel multi-module integrated intrusion detection system for high-dimensional imbalanced data. *Appl. Intell.* **2023**, *53*, 272–288. [CrossRef]