A Novel Learning-Based Attack Detection System for Enhancing Security in Cyber-Physical Environments

Ghulam Mohi-ud-din[1, *], Liu Zhiqiang[2], Zheng Jiangbin[1], Wang Sifei[3], Zeng Xinyu[4], Lai Zizheng[4], Lin Zhijun[1], Muhammad Asim[1]

[1]School of Software, Northwestern Polytechnical University, Xi'an 710072, P. R China
[2]School of Cybersecurity, Northwestern Polytechnical University, Xi'an 710129, P. R China
[3]Collage of Electrical and Information Engineering, Xian Jiaotong University, Xi'an 710049, P. R China
[4]School of International Education, Nanchang Hangkong University, Nanchang 330063, P. R China

Abstract: An Intrusion Detection System (IDS) is an essential part of the network as it contributes towards securing the network against various vulnerabilities and threats. Over the past decades, there has been a comprehensive study in the field of IDS, and various approaches have been developed to design intrusion detection and classification system. With the proliferation in the usage of Deep Learning (DL) techniques and their ability to learn data extensively, we aim to design Deep Neural Network (DNN) based IDS. In this study, we aim to focus on enhancing the performance of DNN-based IDS in Cyber-Physical Systems (CPS). CPS combine physical processes, networking, and computation. The integration of CPS components could seriously jeopardise the security of CPS settings because of the physical limitations. The vulnerability of CPS to cyberattacks has grown with the development of IoT and other physical systems. As cyber-physical systems refer to the intersection of your organization's technology and IT infrastructure and its physical assets, ensuring access and data security through advanced methods prevents any cyber-attack from damaging your physical assets and thereby disrupting your business flow. Conventional cyber and network security procedures fail to guarantee data privacy and security in CPS contexts. This research aims to provide a cutting-edge attack detection method based on learning for CPS environments. The paper suggests using MLP-based smart attack control systems to increase the CPSs' security. Performance analysis is presented in terms of different evaluation metrics such as accuracy, precision, recall, f-score, and False Positive Rate (FPR), and the results are compared with existing feature selection techniques. The effectiveness of the suggested model was confirmed by comparing the outcomes with those of other successful deep learning-based algorithms, including the Gaussian Naive Bayes algorithm, SVM, and logistic regression. Comparative results demonstrate that the suggested method outperforms existing learning models with an exceptional accuracy of 99.52%.

Keywords: Cyber-Physical Systems; Learning Model; Kernel Functions; Deep Learning; Multilayer Perceptron

DOI: 10.57237/j.cst.2022.01.003

1 Introduction

Cyber-Physical System (CPS) is a system that can effectively integrate cyber networks and physical devices using modern sensors and advanced computing systems. Due to the technological advancements in communication, networking, computing and other hardware technologies, there is a growing interest in the development of CPSs as

[*]Corresponding author: Ghulam Mohi-ud-din, 3474195255@qq.com

Received: September 20, 2022; Accepted: November 8, 2022; Published Online: December 1, 2022

discussed by Li & Li. [1] From a technological perspective, CPSs are a unification of different networking systems, ubiquitous computation, effective communication, physical mechanisms and efficient control. These functionalities play an important role in developing a robust networking infrastructure for different social and physical applications mentioned by Cao, Cheng, Chen, & Sun. [2] The basic illustration of a CPS is shown in Figure 1.

The application of CPS has been growing extensively in recent years across various sectors such as healthcare, industrial sector, smart transportation etc. Besides conventional applications, several physical and social applications have also been implemented given CPSs. These applications include advanced networking systems such as wireless sensor networks (WSNs), smart grids and network-controlled systems Ge et al, Ge et al, Giraldo et al, He & Chen et al, He at al, Zhang et al respectively. [22, 3-7] Considering the recent developments, various researchers have predicted that CPSs are expected to become one of the prominent components of the industrial revolution discussed Zhang et al. [18] Significant efforts have been made in this context to demonstrate the potential of CPS in the Industry 4.0 environment as discussed by (Kagermann, Wahlster, & Helbig, 2013). [8] It is to be noted that the performance analysis and evaluation of CPS have been explored extensively, especially concerning CPS organisation, growth and strength Wang et al. [19].

With the emergence of the Internet of Things (IoT), the physical devices linked with CPS have become more susceptible to adversary attacks. Some CPSs depend on the internet and ad hoc networks for exchanging data and control signals between the system components. This increases the system's vulnerability to attacks mainly launched in the network region mentioned by Humayed, Lin, Li, & Luo. [9] These attacks don't need to happen in the network domain, but there are chances that they can also occur in the physical environment. Ashibani & Mahmoud, says this makes CPS more sensitive to attacks on all components. [10] Hence, network or cyber security mechanisms are not enough to ensure the smooth and secure operation of the CPS. Advanced control systems are required to strengthen the network security protection of the CPSs discussed by Giraldo et al. [4] These systems can potentially strengthen the system to face security attacks and hence can be included in the design of intrusion detection systems (IDS) and compensation systems.

However, it can be inferred from the existing works that the cyber-attacks in CPS might also result in faults and can result in the failure of the physical systems. One of the prominent challenges faced by the researchers is to compensate for the effects of faults in these systems automatically. Also, it is challenging to maintain the consistency of the system‘s performance under fault occurrences. These attacks or faults affect the system process and sensors. Hence it is essential to develop robust attack detection systems to enhance the security of CPSs. The main objective of the attack detection model is to strengthen the availability of the system using various control algorithms, which can improve the performance and stability of the system under the existence of CPS attacks or faults. In this context, this research aims to enhance security in cyber-physical environments using a potential attack detection system.

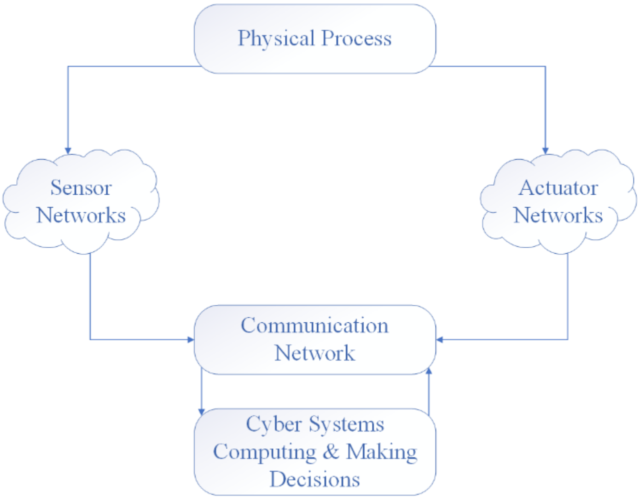

Figure 1 A basic illustration of a CPS Gunes et al. [21]

The main contributions of this paper are:

1) This paper proposes a deep learning-based attack detection model to enhance security in CPS environments.
2) This paper proposes a novel controller design by mapping the Multilayer perceptron network (MLP) with a combination of kernel functions.
3) The proposed research differs from conventional deep learning (DL) approaches in implementing a Robust Attack Control System (RACS) online estimating possible attacks.
4) The learning model's performance was improved using novel kernel functions and neural networks. An active controller compensates for the effects of malicious attacks and maintains the system's

reliability.

5) Performance validation of the proposed attack detection module was performed by comparing it with the Gaussian Naive Bayes algorithm, SVM and logistic regression algorithms.

The rest of the paper is organized as follows: Section II briefly reviews existing techniques related to the attack detection system. Section III discusses the main problem of the CPSs. Section IV discusses the main research methodology that describes the workflow of the proposed methodology. It briefs about CPS architecture, data and control exchange and detection process of attacks. Section V deals with the details of the software used, parameters of parameter settings, comparative techniques and performance measures such as accuracy and precision, and experimental results. Section 6 concludes the paper with experimental observations and future scope.

2 Literature Review

With the growing interest in the security of CPS systems, various techniques have been proposed in recent years. A comprehensive review of recent advancements and development in the domain of CPSs is presented by Khaitan & McCalley. [11] The review analysis also discusses the illustrations of different types of CPSs. The main objective of the review analysis is to provide a detailed analysis which enables the researchers to obtain insights into the functioning and applications of CPSs and to actuate them to develop novel solutions for developing a wide-range implementation of CPS. The development of mobile CPS, its applications and associated challenges are discussed by Guo. et al. [12] The study mainly distinguishes the mobile CPS from conventional CPS and discusses three prominent application areas such as mobile education, healthcare systems and vehicular networking systems. The challenges associated with mobile CPS were categorized into four main areas: Security, power utilization, dynamic environment of mobile CPS and its stability. The study also analyses different alternative techniques which address the research challenges and evaluates the relation between them.

Ding et al presented a survey on security control and attack detection for industrial CPS. [13] The study was conducted from the perspective of control theory and provides a brief overview of technological advancements related to security control and the detection of cyber-attacks on industrial CPSs in recent times. The survey comprises modelling CPS systems for catering to the performance analysis requirement. Furthermore, three different types of cyber-attacks: deception attacks, replay attacks and denial-of-service attacks (DoS). The study also analyses the potential, security, adaptability and stability for governing the strength of CPS to withstand different attacks. The survey was conducted based on different categories of detection mechanisms. Additionally, the control of the security systems and state estimation were investigated in detail.

Xiang, Wang, & Liu discuss coordinated attacks on electric power systems in a cyber-physical environment and investigate possible coordinated attack scenarios. [14] The research mainly focuses on two important attack coordination scenarios: the coordination between load redistribution (LR) attack and attacking generators; and the coordination between LR attack and attacking lines. These attacks are evaluated as bi-level optimization issues where the attacker presents at the higher state targets to increase the load retrenchment, and the defender presents at the lower level to minimize the load retrenchment. The case studies considered in the research are based on a modified IEEE 14-bus system to demonstrate the effects of significant damage caused by coordinated attacks. It was observed from the analysis that coordinated attacks are responsible for higher load retrenchment compared to standalone attacks. The proposed research provides useful insights regarding the prevention and mitigation of high-impact, low-frequency (HILF) coordinated attacks.

Alguliyev et al analyses and classifies existing literary works done on the security of CPSs. [15] The study also focuses on philosophical issues related to CPSs, the operating principle and their impact on people's lives. The prominent research challenges and solutions raised while evaluating the consequences of attacks on modelling, detection, cyber-attacks, and the construction of security architecture were analyzed. The three significant threats and attacks against CPSs are evaluated, and a tree of attacks on CPSs is proposed.

Wu, Song, & Moon discussed the application of machine learning methods for detecting cyber-physical attacks in Cyber manufacturing systems. The study applies machine learning techniques to physical data for detecting cyber-physical attacks. [16] Experimental analysis was conducted considering two examples, a 3D printing malicious attack and a CNC milling machine malicious attack, which were developed using simulation tools. It was observed from the experimental analysis that the implementation of ML-based methods in physical data enabled the anomaly detection algorithm to achieve a detection accuracy of 96.1% in identifying cyber-physical attacks in the 3D printing process. Another efficient machine learning algorithm, the Random Forest algorithm, achieved an accuracy of 91.1% in the detection of cyber-physical attacks in the CNC milling process.

Chen et al discussed the application of deep learning methods for securing mobile edge computing in Cyber-Physical Transportation Systems. The proposed research employs unsupervised learning to establish the active learning mechanism. [17] The proposed model contributes significantly to enhancing the accuracy of the detection process compared to other machine learning-based algorithms due to its active feature learning. It can be observed from the experimental analysis that the proposed model achieved superior accuracy in the attack detection process. It was observed that the model achieved an overall 12.61 percent higher accuracy compared to softmax-regression-based algorithms, 5.76 percent higher compared to the decision-tree-based algorithm, 3.20 percent higher compared to the support-vector machine-based algorithm, and 2.61 percent higher compared to the random forest-based algorithm.

3 Problem Statement

Cyber-Physical Systems (CPS) have the Internet of Things (IoT) as one of their prominent substitutes because of their effectiveness in establishing communication between various physical entities. Certain CPSs depend on wireless or ad hoc networks, making these approaches sensitive to attacks. The cyber-attacks on CPS can significantly harm the performance of CPS, thereby reducing its feasibility and robustness when applied for cyber applications. CPS is more vulnerable to external attacks, and information/cyber security techniques are not enough to ensure the security of CPS. Besides, cyber-attacks in CPS can also cause disruption and failure in physical systems. There are certain prominent research challenges associated with the security of CPSs. One such issue is that it is essential in CPS to compensate for the effects of shortcomings and maintain the presentation of the approach at some desired level. The main target of cyber-attacks or threats is sensors and actuators. These techniques are implemented as an impromptu attack, where the attacker targets the sensors present in the system process, disrupting CPS architecture's complete working. However, there are certain limitations associated with neural network-based approaches. Though they can achieve desired detection accuracy for a trained, known cyber-attack, it is not ensured to work for an unknown new cyber-attack unless it shares similar properties with known cyber-attacks. This work emphasizes four types of attacks, namely Denial of Service (DoS), probing, User to Root (U2R), and Root to Local (R2L). DoS attacks are cyber-attacks that disrupt the operation of a machine or a network and make it unavailable for users. DoS attacks terminate all services of the host connected to that network. Similarly, DDoS attacks disrupt the data traffic by introducing malicious attacks into the network system. The U2R attack allows unauthorized access to the user network and later access to the network's root by exploiting the system's vulnerability. Similar to the U2R network, the R2L attack exploits the network's vulnerabilities and gains unauthorized access to sensitive information by sending malicious network packets into the system.

4 Research Methodology

The preliminary aim of the proposed research is to develop a novel learning-based robust attack detection system for enhancing the security of CPSs. The attack detection and control systems' main objective is to strengthen the system's availability using various control algorithms capable of improving the performance and stability of the system under the existence of CPS attacks or faults. The study employs a Multilayer perceptron (MLP) classifier for implementing a robust attack control system. The proposed methodology will be implemented using the following stages: A cyber-physical scenario simulation built in this first stage. The environment is constructed with a required number of physical and computational objects and is configured appropriately. In the second step, the data and the control signal exchange of the CPS over the ad hoc network are simulated. A RACS is constructed in the third stage, using a smart estimator and active controller for the online estimation of attacks. The fourth and last stage simulated a scenario of cyber-physical attacks. The proposed attack detection process is briefly described in the following subsections.

4.1 Data Collection

The data for the experimental analysis was collected from the NSL-KDD CUP99 dataset. The NSL-KDD data set is highly multidimensional with 41 training features, as metioned in Table 1 and comprises two subsets: KDDTrain+ and KDDTest+. For the training dataset, 125973 instances and 18793 instances were used for testing. The data type is split into the feature and label data, wherein the feature data has a data type of string. The string data type is converted into integer format. The null values in the data type are removed by preprocessing. Among the total samples, 67% of the data is used as training data, and 33% is used for testing. An MLP neural network is applied to train the dataset for predicting accuracy. The NSL-KDD dataset in the proposed research is used to detect four types of attacks Denial of Service (DoS), probing, User to Root (U2R), and Root to Local (R2L). Table 1 shows the attack classes and the number of sample sizes for attack detection.

Table 1 Dataset description of the NSL-KDD dataset

NSL−KDD	**Total**	**Normal**	**DoS**	**Probe**	**R2L**	**U2R**
KDDTrain+	125973	67343	45927	11656	995	52
KDDTest+	18793	9710	5741	1106	2199	37

4.2 Creation of CPS environment for Cyber-attack Detection

This research focuses mainly on the detection of three different types of cyber-attacks in the CPS environment, namely: Denial of Service (DoS), probing, User to Root (U2R), and Root to Local (R2L). A prototype of the attack detection module is created for simulation purposes. In this proposed simulation module, various attack scenarios are generated to analyse the vulnerabilities of the CPS and to understand the cascading effects of the attacks. The vulnerabilities associated with the network are identified by evaluating the possible paths an attacker can take for launching an attack. For this purpose, the possible attack scenarios are created by creating a CPS environment.

The architecture of the CPS consists of various sensors and actuator networks fused into an intelligent decision system. Their effectiveness distinguishes CPSs in analysing cross-domain sensors, divergent data flow and intelligent decision making. Integration of multiple CPS components is performed based on the robustness of the connectivity. CPS environment includes a fusion of different key functions based on their applications. CPS environment consists of computational components which employ basic statistics and guidance from physical processes.

The system architecture of CPS is developed considering various layers. The architecture is divided into seven basic layers, from the physical to the application layer.

1) Physical Layer: The physical layer is the fundamental and base layer of the CPS architecture. In this layer, sensors and actuators are connected through wireless networks such as Wifi networks, Bluetooth, RFID tags and wired networks such as PLC etc. The components in this layer are connected to other systems using the Internet. These devices generally possess low memory and processing power, and this layer is prone to attacks from external sources.
2) Data Link Layer: The data link layer consists of different system components to create, transmit and receive data frames. This layer is used to process the request of the network layer, and the information is exchanged by sending and receiving the packets through the physical layer. The data link layer is mainly categorised into two sub-layers: the logical channel management (LLC) sublayer and the media access control (MAC) sublayer. The service request of the network layer is processed using LLC, and the MAC sublayer is used to control the accessibility of the physical environment. The attacks on the data link layer result in MAC addresses exploitation, which can disrupt the device identification.
3) Network Layer: In the network layer, data packets are routed by converting MAC addresses to network addresses. This layer uses different routing protocols to establish secure and reliable communication between different layers of the architecture. The attacks on this layer disrupt the working of sensors and actuators, changing the address of source and information, and resulting in mechanical failure.
4) Transport Layer: The data packets are divided into small segments in the transport layer. This layer consists of fundamental protocols such as TCP, UDP, and ICMP. The attacks on this layer affect the network's computational speed, ultimately causing

system process failure.

5) Session Layer: This layer handles the exchange of information between different layers. This layer monitors the range of data transmitted over the network layer. This layer is an integral part of the architecture and plays an important role in ensuring the proper functioning of the CPS.

6) Application Layer: This layer consists of different domains. The application layer is meant for storing, processing and updating the data obtained from previous layers. This layer provides control decisions, which can be monitored using the virtual prototype interface. This layer aims to achieve data privacy which is one of the important aspects of CPS architecture. The proposed research performs an online estimation of the possible attacks in a CPS environment. For this purpose, this work proposes the implementation of a Robust Attack Control System (RACS).

4.2.1 Multilayer Perceptron (MLP)

MLP is a feed-forward artificial network branch that maps the input data to the desired output. MLP is constituted by a network of small neurons known as the perceptron. This perceptron will evaluate an individual output using different real value inputs by forming a linear combination of input and output functions. MLP networks are mainly employed in applications that require supervised learning.

An MLP consists of neurons in the MLP network that are considered a single input layer with multiple hidden layers and a single output layer, as shown in Figure 2.

The neurons in the MLP network can be activated using an activation function. In this work, the neurons are activated using a sigmoid activation function. A sigmoid activation function is similar to the tanh activation function, wherein it uses a data function that ranges between 0 and 1, unlike other activation functions whose range is between - 1 and 1.

The number of layers and neurons in the MLP network is considered hyperparameters while training the network. These parameters must be appropriately tuned to achieve better performance and improve the MLP network's accuracy. The neural network weights and parameter tuning are performed using a backpropagation algorithm. The backpropagation algorithm is a supervised learning method in which the variance between the estimated and actual outcome is calculated and communicated back to the neural network layers by adjusting the neurons' weights. The process involved in MLP learning is detailed in the below steps:

1) Initially, the data is propagated from the input layer to the output layer. This step is called forward propagation.
2) Based on the difference between the estimated and actual output, the error is calculated and minimised to improve the attack detection accuracy.
3) The error is back propagated, and its derivative is calculated considering each weight in the network. The parameters of the MLP are further updated with the new values.

The steps are repeated over multiple epochs to learn ideal weights. As a final step, the output is obtained using a threshold value and this value is used to obtain the predicted class labels.

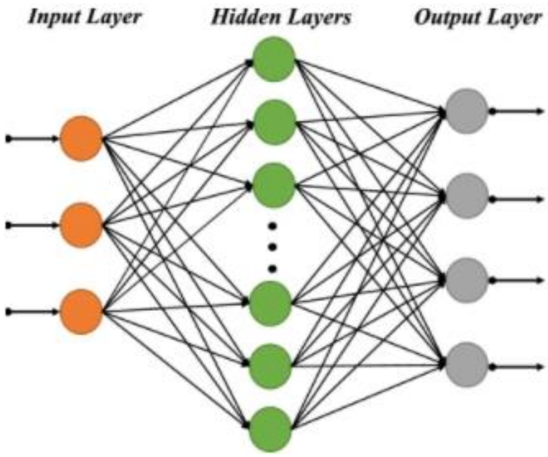

Figure 2 The architecture of a multilayer perceptron

4.2.2 Implementation of RACS system

The RACS was constructed using a smart estimator and active controller. The smart estimator will perform an online estimation of possible attacks. Novel kernel functions and neural networks are proposed to improve the learning model's performance. The Active Controller component compensates for the effects of malicious attacks and maintains the system’s performance. This research developed the learning model using a Multilayer perceptron network (MLP) combined with kernel functions to enhance the learning model's potential.

1) Smart Estimator

The MLP is developed as a smart estimator for estimating the state models and possible sensor attack signals. The estimator is defined as Eq (1):

$$\hat{f} = \omega^T M(z, c, \sigma) \quad (1)$$

Where z = $(z1, z2, \ldots, zm)^T \in R_n$ is defined as the input vector, $\omega = (\omega_1, \omega_2, \ldots, \omega_m)^T$ is defined as the weighting vector of the output layer. The MLP function is given as M = $(M1, M2, \ldots, M3)^T$ where σ = $(\sigma 1, \sigma 2, \ldots, \sigma m)^T$ is defined as the standard deviation and c = $(c1, c2, \ldots, cm)^T$ is defined as the mean vector of the MLP function. The ideal neural network smart estimator as per the universal approximation theorem is given as Eq (2):

$$f^*(t) = \hat{f}(t) + \epsilon = \omega^{*T} M(z(t), c^*, \sigma^*) \quad (2)$$

Where ∈ is defined as the approximation error considered to be bounded, and w*, c*, σ* is deemed optimal values that can provide the appropriate approximation of the nonlinear function f. Determining the values of all these parameters is a complex task. Hence, the approximation function is given as Eq (3):

$$\hat{f}(t) = \hat{\omega}^T M(z(t), c, \sigma) \quad (3)$$

Where $\hat{\omega}$ is defined as the estimation value of the respective optimal value of the parameters. These optimal values are different for different functions and are not the same. This research focuses on calibrating the weighting vectors. The error between the optimal values and the estimated weighting vectors is given as Eq (4):

$$\vec{\omega} = \omega^* - \hat{\omega} \quad (4)$$

In this research, Gaussian kernel-based MLP is employed, which dictates the major contribution of the proposed system is given as Eq (5) and Eq (6):

$$\hat{f}_a(t) = \hat{\omega}^T T_a M(z(t), c, \sigma) \times C_k(a_m, a_n) \quad (5)$$

$$the\ C_k(a_m, a_n) = \sum C_{KL}(a_m, a_n) \cdot C_{KG}(a_m, a_n) \quad (6)$$

Where,

C_{KL} is Local Kernel, and CKG is a global kernel

2) Active controller:

The dynamic functioning of the attack in CPS environment A(t) is not known but is assumed to be predictable. Hence an active controller is designed to predict the attack function. The controller was designed by mapping the MLP to predict the possible attacks. In this research, the MLP is mapped with kernel functions to enhance the learning model's performance by mapping the nonlinear function from the input domain X to an implicit intermediate Hilbert space H which is further mapped to the hidden layer domain 0. The implicit kernel mapping (θ) is defined as:

$$\theta : X \rightarrow H$$

$$x \rightarrow \theta(x) \quad (7)$$

Eq (7) states that a feature vector of x is modified into a feature vector of θ(x). This map cannot be determined explicitly.

5 Results and Discussion

The proposed learning model was evaluated in terms of various performance evaluation parameters, and the obtained results are compared with another effective Gaussian Naive Bayes algorithm for validating the effectiveness of the proposed approach.

5.1 Performance Evaluation

The experimental data used for simulation consists of 41 attributes which are listed in Protić et al [20] with main data split into training data and testing data for the training dataset, 125973 instances were used and 18793 instances were used for testing. The features in this dataset are categorised into three groups; (i) fundamental input features related to network connection, such as the number of bytes from source or destination IP address, prototype and duration, (ii) network connection features, and (iii) statistical input features which can be analysed using a time window function.

The proposed model was simulated, and the stability and resilience of the system after the attack were investigated. Furthermore, the effectiveness of the smart estimator is determined by calculating the measures such as Precision, Recall, f1 score, and Support and the obtained values are tabulated in Table 2, Table 3.

5.2 Performance Metrics

The performance measures are calculated as follows:

Accuracy defines the percentage of several correctly identified CPS attacks and is calculated as:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (8)$$

Recall for a function is determined as the ratio of the CPS attacks that are accurately classified and is given as:

$$Recall = \frac{TP}{TP+FN} \quad (9)$$

F1 score is also defined as the F-measure, which is determined as the weighted harmonic mean of its precision and recall. F1 score is used for measuring the accuracy, which can possess values between 1 and 0. Where 1 represents the best value, and 0 represents the worst value. Correspondingly, the F1 score is defined as:

$$F1\ score = \frac{2*Precision*Recall}{Precision*Recall} \qquad (10)$$

Similarly, precision is defined as the accuracy of positive predictions. It is calculated as shown in Eq (11).

$$Precision = \frac{TP}{TP+FP} \qquad (11)$$

And support is the number of actual class occurrences in the specified dataset. It defines the total number of samples of the true response in the training data, which is used to evaluate the performance of the classification process.

The experimental data used for simulation consists of 41 attributes, with main data split into training and testing data. For the training dataset, 125973 instances and 18793 instances were used for testing. The proposed model was simulated, and the stability and resilience of the system after the attack were investigated. Furthermore, the effectiveness of the smart estimator is determined by calculating the measures such as Precision, Recall, f1 score, and Support and the obtained values are tabulated in Table 2.

The average accuracy obtained by the learning model using MLP for attack detection is 99.52%.

To evaluate the effectiveness of the proposed learning model, the results of the learning model were compared with another deep learning-based Gaussian NB algorithm. The obtained results for the Gaussian NB algorithm are tabulated in Table 3.

The average accuracy obtained by the learning model using Gaussian NB for attack detection is 87.83%. A graphical representation of the comparative analysis is illustrated in Figure 3.

To validate the work efficiency of the proposed approach, we compare the final accuracy achieved from our proposed method with a few other relevant approaches, which are illustrated in Table 4 and Figure 4, Figure 5.

Table 2 Parameter values for the MLP learning model

	Precision	**Recall**	**f1-score**	**Support**
DoS	1 00	1 00	1 00	129130
normal	0.99	1.00	0.99	32154
probe	0 78	0 80	0 79	1337
r2l	0.00	0.00	0.00	387
u2r	0.00	0.00	0.00	19
Accuracy	-	-	1.00	163027
Macro Average	0.55	0.56	0.56	163027
Weighted Average	0.99	1.00	0.99	163027

Table 3 Parameter values for the Gaussian NB learning model

	Precision	**Recall**	**f1-score**	**Support**	
DoS	0.98	0.94	0.96	129130	
normal	0 97	0 63	0.77	32154	
probe	0.09	0.99	0.17	1337	
r2l	0 30	0 38	0 34	387	
u2r	0.00	0.68	0.01	19	
Accuracy	-	-	0.88	163027	
Macro Average	0.47	0.73	0.45	163027	
Weighted Average	0.97	0.88	0.91	163027	

Table 4 Comparative analysis of weighted accuracy computational time

Weighted	**Accuracy (%)**	**Computational time (microsecond)**
SVM	91.3	1230
Logistic regression	89.01	1670
Artificial Neural Network	95.6	1107
Random Forest	94.1	936
Proposed Method (Kernel MLP)	99.52	890

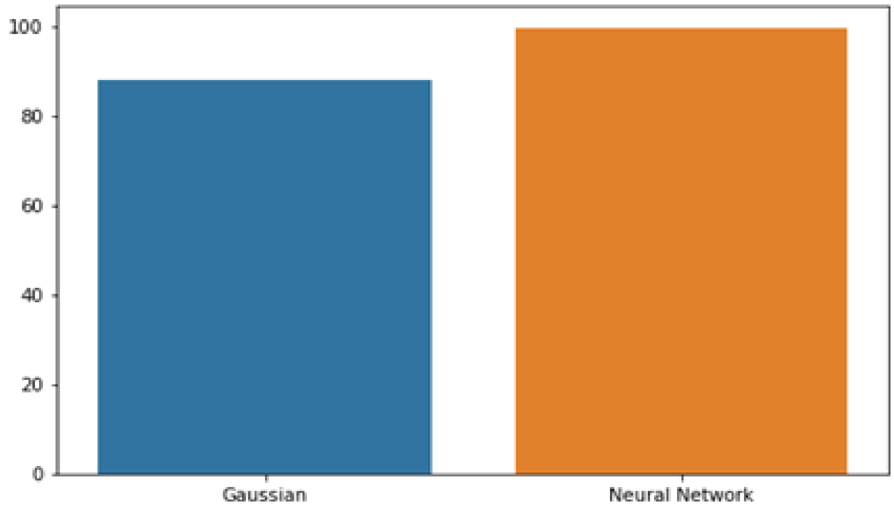

Figure 3 Graphical representation of the comparative analysis

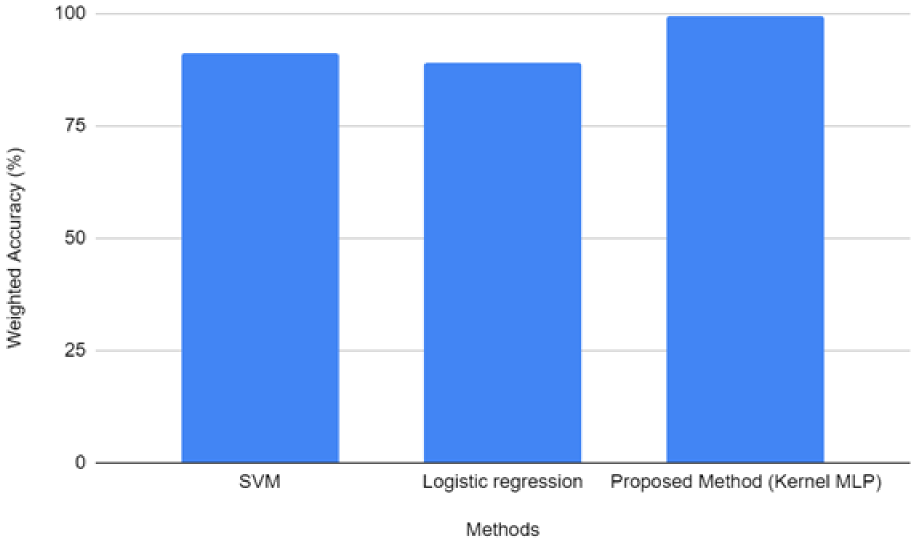

Figure 4 Comparison of weighted accuracy achieved by different techniques

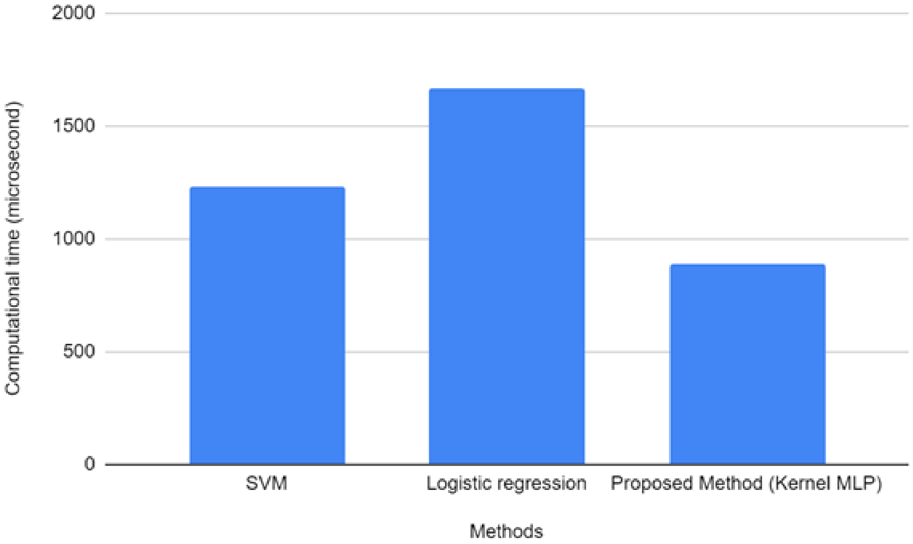

Figure 5 Graphical representation of the comparative analysis

It can be observed from the results that the attack detection accuracy in the CPS environment using the proposed MLP learning model achieved higher accuracy compared to other approaches with less computational time. Results show the proposed approach's effectiveness and the adaptability of the proposed approach for other environments apart from the CPS environment.

6 Conclusion

This research aims to develop a learning-based attack detection system for improving security in CPS environments. In this research, the learning model was implemented using a smart estimator and active controller to estimate possible attacks online. The smart estimator was developed using a neural network-based Multilayer perceptron (MLP). The study employs novel kernel functions to enhance the learning model's performance. The MLP framework was mapped with kernel functions, and the active controller was used to compensate for the effects of malicious attacks and maintain the system's performance. The model was simulated, and the results were compared with other deep learning algorithms such as Gaussian Naive Bayes algorithm, SVM and Logistic regression to validate the proposed model's effectiveness. It can be observed from the results that the proposed approach achieved an attack detection accuracy of 99.52% with the less computational time, and the learning model using Gaussian NB attained an accuracy of 87.83% for attack detection. The results show the efficacy of the proposed model and can be used for other environments apart from CPS environments. As a part of future research, the study intends to integrate different deep learning models to strengthen the performance of the attack detection models.

References

[1] M. Li and P. Li, "Crowdsourcing in Cyber-Physical Systems: Stochastic Optimization With Strong Stability," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, pp. 218-231, 2013.

[2] X. Cao, P. Cheng, J. Chen and Y. Sun, "An Online Optimization Approach for Control and Communication Codesign in Networked Cyber-Physical Systems," *IEEE Transactions on Industrial Informatics*, vol. 9, pp. 439-450, 2013.

[3] X. Ge, F. Yang and Q.-L. Han, "Distributed networked control systems: A brief overview," *Information Sciences*, vol. 380, pp. 117-131, January 2017.

[4] J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos and M. Kantarcioglu, "Security and Privacy in Cyber-Physical Systems: A Survey of Surveys," *IEEE Design Test*, vol. 34, pp. 7-17, 2017.

[5] W. He, G. Chen, Q.-L. Han and F. Qian, "Network-based leader-following consensus of nonlinear multi-agent systems via distributed impulsive control," *Information Sciences*, vol. 380, June 2015.

[6] W. He, F. Qian, J. Lam, G. Chen, Q.-L. Han and J. Kurths, "Quasi-synchronization of heterogeneous dynamic networks via distributed impulsive control: Error estimation, optimization and design," *Automatica*, vol. 62, pp. 249-262, December 2015.

[7] X.-M. Zhang, Q.-L. Han and X. Yu, "Survey on Recent Advances in Networked Control Systems," *IEEE Transactions on Industrial Informatics*, vol. 12, pp. 1740-1752, 2016.

[8] H. Kagermann, W. Wahlster and J. Helbig, "Recommendations for Implementing the Strategic Initiative INDUSTRIE 4.0 – Securing the Future of German Manufacturing Industry," München, 2013.

[9] A. Humayed, J. Lin, F. Li and B. Luo, "Cyber-Physical Systems Security—A Survey," *IEEE Internet of Things Journal*, vol. 4, pp. 1802-1831, 2017.

[10] Y. Ashibani and Q. Mahmoud, "Cyber Physical Systems Security: Analysis, Challenges and Solutions," *Computers and Security*, vol. 68, p. 81–97, April 2017.

[11] S. K. Khaitan and J. D. McCalley, "Design Techniques and Applications of Cyberphysical Systems: A Survey," *IEEE Systems Journal*, vol. 9, pp. 350-365, 2015.

[12] Y. Guo, X. Hu, B. Hu, J. Cheng, M. Zhou and R. Y. K. Kwok, "Mobile Cyber Physical Systems: Current Challenges and Future Networking Applications," *IEEE Access*, vol. 6, pp. 12360-12368, 2018.

[13] D. Ding, Q.-L. Han, Y. Xiang, X. Ge and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674-1683, January 2018.

[14] Y. Xiang, L. Wang and N. Liu, "Coordinated attacks on electric power systems in a cyber-physical environment," *Electric Power Systems Research*, vol. 149, pp. 156-168, 2017.

[15] R. Alguliyev, Y. Imamverdiyev and L. Sukhostat, "Cyber-physical systems and their security issues," *Computers in Industry*, vol. 100, pp. 212-223, September 2018.

[16] M. Wu, Z. Song and Y. Moon, "Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods," *Journal of Intelligent Manufacturing,* vol. 30, March 2019.

[17] Y. Chen, Y. Zhang, S. Maharjan, M. Alam and T. Wu, "Deep Learning for Secure Mobile Edge Computing in Cyber-Physical Transportation Systems," *IEEE Network*, vol. 33, pp. 36-41, 2019.

[18] X.-M. Zhang, Q.-L. Han and B.-L. Zhang, "An Overview and Deep Investigation on Sampled-Data-Based Event-Triggered Control and Filtering for Networked Systems," *IEEE Transactions on Industrial Informatics*, vol. 13, pp. 4-16, 2017.

[19] L. Wang, M. Törngren and M. Onori, "Current status and advancement of cyber-physical systems in manufacturing," *Journal of Manufacturing Systems,* vol. 37, 2015.

[20] D. Protic, "Review of KDD Cup '99, NSL-KDD and Kyoto 2006+ datasets," *Vojnotehnicki glasnik*, vol. 66, pp. 580-596, July 2018.

[21] V. Gunes, S. Peter, T. Givargis and F. Vahid, "A Survey on Concepts, Applications, and Challenges in Cyber-Physical Systems," *KSII Transactions on Internet and Information Systems*, vol. 8, pp. 4242-4268, December 2014.

[22] X. Ge and Q.-L. Han, "Consensus of Multiagent Systems Subject to Partially Accessible and Overlapping Markovian Network Topologies," IEEE Transactions on Cybernetics, vol. 47, pp. 1807-1819, 2017.