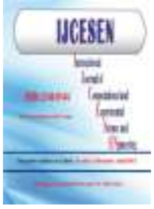
International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.1 (2025) pp. 1301-1313
http://www.ijcesen.com

ISSN: 2149-9144

Research Article



Deep Learning Models with Transfer Learning and Ensemble for Enhancing Cybersecurity in IoT Use Cases

Sivananda Hanumanthu[1]*, Gaddikoppula Anil Kumar[2]

[1]Research Scholar, Department of CSE, Bharatiya Engineering Science and Technology Innovation University (BESTIU), AP & Director of Enterprise Architecture at Rubrik, Bangalore, India
* **Corresponding Author Email:** siva.phd1984@gmail.com – **ORCID:** 0009-0003-3763-3952

[2]Principal and Professor of CSE, Scient Institute of Technology, Ibrahimpatnam, R.R. District, Telengana, India
Email: anil_deva@yahoo.com - **ORCID:** : 0000-0002-0448-102X

Article Info:

DOI: 10.22399/ijcesen.1037
Received : 22 November 2024
Accepted : 15 February 2025

Keywords :

Internet of Things,
Artificial Intelligence,
Cybersecurity,
Deep Learning Transfer Learning,
Hyperparameter Optimization.

Abstract:

Internet of Things (IoT) applications have made inroads into different domains, providing unique solutions—Internet of Things technology offers seamless integration of physical and digital worlds. However, the broad nature of the technologies and protocols used in IoT applications has increased vulnerability from malicious attackers. Hence, protecting IoT applications from cyber-attacks is imperative. Researchers have implemented intrusion detection systems to overcome this issue to improve cybersecurity in IoT scenarios. With the new threats of cybercrime emerging, a continuous effort is required to enhance the security of IoT applications. To address this pressing need, we present our study that proposes a deep learning-based framework to bolster cybersecurity at the IoT use cases level by exploiting the power of transfer learning and ensembling it from deep learning models pre-trained at larger datasets. Deep learning models attain high performance with the help of hyperparameter tuning, and we achieve that through PSO in our proposed system. Our ensemble system shows how individual models can outperform individual models by using the best-performing models as constituents in the ensemble approach. We introduce an algorithm called — Optimized Ensemble Learning-Based Intrusion Detection (OEL-ID). This algorithm leverages the present framework and corresponding optimization strategies to boost intrusion detection performance for improved cyber security in IoT scenarios. Using the UNSW-NB15 benchmark dataset, our empirical study demonstrates that our proposed method, compared to some of the existing deep learning models, obtained a detection accuracy of 98.89%, which, in turn, provided the highest comparative accuracy. Therefore, the proposed system can be used with IoT use cases as it allows for a significant level of security to the system's underlying applications.

1. Introduction

Technological innovations like the Internet of Things (IoT) have paved the way for many unprecedented applications previously thought impossible. With the integration of the physical and digital worlds, there is seamless communication among things on digital platforms, enabling higher control over monitored things, which was impossible earlier without IoT technology. However, the tremendous possibilities of IoT applications also brought about security issues due to the heterogeneous nature of the technology, which uses several existing techniques, protocols, applications, and interfaces with a kind of amalgamation. With the increased number of cyber attacks witnessed every year in cyberspace, including IoT use cases, it is vital that security mechanisms are continuously improved to withstand the pace at which adversaries exploit available technologies to perpetrate more sophisticated cyber attacks. The emergence of artificial intelligence has made it possible to exploit learning-based approaches instead of relying on heuristic-based approaches to enhance cybersecurity. With the help of artificial intelligence, security mechanisms can be improved to leverage the cybersecurity of various applications, including IoT use cases.

Several existing works aim to improve cybersecurity with the help of learning-based approaches. Existing research has revealed that deep learning models can be appropriately used to realize intrusion detection systems for protecting IoT use cases [1]. Furthermore, deep learning approaches use enhanced neural networks that mimic human brain functionality, which could leverage the intrusion detection procedure while protecting IoT networks. It has been found that deep learning models could analyze the data in a better way towards automatically detecting possible intrusions [2]. Learning-based approaches that use AI have continued to be popular in the recent past as they could provide enhanced capabilities in the intrusion detection process. Another important fact is that explainable AI has the potential to benefit the intrusion detection process, aid systems, and network security professionals as it could provide an additional layer of security [3]. Concerning IoT applications, deep learning and radio frequency fingerprinting associated with intrusion detection have also been investigated and found beneficial. Such learning-based mechanisms protect IoT devices from various cyber-attacks. The deep learning models could perform even better with optimizations like hyperparameter tuning and enhanced transient search optimization towards leveraging their performance [4,5]. The existing literature also provided that identifying efficient deep-learning models and making them into ensembles is essential in improving attack detection performance [6]. Based on these literature findings, we propose a deep learning-based framework for leveraging cyber attack detection performance in IoT use cases in this paper.

Our paper introduces several key contributions. Our proposed system utilizes Particle Swarm Optimization (PSO) for hyperparameter tuning, enhancing the performance of deep learning models. By incorporating the best-performing models as components in an ensemble approach, our system shows the potential to surpass individual models. We introduce an algorithm named Optimized Ensemble Learning Based Intrusion Detection (OEL-ID), which leverages the proposed framework and optimization mechanisms to enhance intrusion detection, thus bolstering cybersecurity in IoT use cases. Our empirical study, conducted using the UNSW-NB15 benchmark dataset, demonstrated that our method achieved the highest accuracy of 98.65%, outperforming many existing deep learning models. Consequently, our proposed system holds promise for integrating IoT use cases, offering enhanced security to safeguard the underlying applications. The remainder of the paper is structured as follows: Section 2 reviews literature on various existing deep learning models utilized for intrusion detection in IoT use cases. In contrast, section 3 presents the proposed intrusion detection system that utilizes pre-trained models with transfer learning and ensembles them to harness the strengths of the best-performing models. Section 4 presents the results of our experiments, and Section 5 discusses the research besides providing limitations of the study. Section 6 concludes our research work in this paper, providing opportunities for future endeavors.

2. Related work

Numerous approaches are found in the literature for detecting intrusions using deep learning approaches. Ibitoye et al. [1] concentrated on strengthening SNN resilience and comprehending the influence of its self-normalizing features on IoT dataset protection to improve deep learning-based IDS performance against adversarial assaults. Madhu et al. [2] improved IoT security by utilizing deep learning and machine learning in conjunction with enhanced DIDS models to provide more precise attack detection and categorization and have 95% accuracy. Keshk et al. [3] improved the SPIP framework's 92.46% accuracy in intrusion detection systems by honing feature extraction and locating targeted attack vulnerabilities. Bassey et al. [4] included t-SNE hyperparameter optimization for reliable dimension reduction in RF fingerprinting. Fatani et al. [5] expanded TSODE to additional optimization problems and investigated other IoT IDS metaheuristic optimizers.

Lazzarini et al. [6] tested DIS-IoT with actual IoT devices to evaluate real-time performance and computational overhead. Ferrag et al. [7] investigated fresh deep-learning models and datasets for intrusion detection in cyber security. Bakhsh et al. [8] investigated CNNs, RNNs, Transformers, federated learning, ensemble methods, and hybrid architectures to advance DL-based IDS for IoT. Jayalaxmi et Al. [9] incorporated ML and DL IoT security techniques to advance IDS and IPS platforms. Bovenzi et al. [10] extended attack classes, investigating privacy-preserving distributed H2ID implementations and improving threshold design for specific IoT use scenarios.

Vishwakaram and Kesswani [11] focused on enhancing real-time training capabilities for the IDS model and increasing datasets to cover new sorts of attacks. Soliman et al. [12] included a decision-making unit for reaction activities and extended the model to identify new forms of cyberattacks by training on various datasets. Rezvy et al. [13] focused on mobile and IoT security solutions with intelligent agents, expanding the algorithm's coverage to encompass a broader spectrum of assaults. Saleem and Chishti [14] concentrated on lowering DL models' computational complexity for Internet of Things applications without sacrificing accuracy. Akgun et al. [15] focused on increasing processing speed in real time and investigating resilience against novel attack forms.

Ullah et al. [16] investigate deep learning techniques such as FFN, RNN, and GAN for IoT anomaly detection. Qiu et al. [17] improved the model's resilience to mitigate adversarial assaults on DL-based NIDS. Kasongo [18] concentrated on augmenting the resilience and expandability of the IDS framework by utilizing sophisticated RNNs and feature selection methods. Rahman et al. [19] improved model accuracy and efficiency and concentrated on enhancing client selection in Federated Learning for IoT intrusion detection. Hnamte and Hussain [20] enhanced the DCNNBiLSTM model's training effectiveness for network intrusion detection, investigated zero-day attack detection, and investigated real-time deployment capabilities.

Cassales et al. [21] improved current procedures, extending the architecture for IoT intrusion detection, testing various approaches, and conducting comparative performance evaluations with more enormous datasets. Anushiya et al. [22] focused on expanding dataset exploration, refining feature selection methods for increased accuracy and scalability, and refining the GA-FR-CNN approach for IoT intrusion detection. Yahyaoui et al. [23] extended the hierarchical anomaly detection technique to a broader range of WSN and IoT network abnormalities beyond Selective Forwarding Attacks. Li et al. [24] improved cybersecurity and concentrated on expanding DeepFed to federate data across several industrial CPS domains. Hazman et al. [25] added deep learning methods to IDS-SIoEL to improve IoT intrusion detection and extend it for multi-class categorization.

Singh et al. [26] specialized IoT and edge network datasets, improving packet feature resilience, automating feature engineering, and building a mitigation framework. Hasan et al. [27] created reliable detection algorithms beyond traditional machine learning, concentrating on real-time IoT data and handling significant data issues. Campos et al. [28] tackled non-iid data issues, implementing FL-enabled IDS in actual IoT environments and investigating customized FL for increased attack detection precision. For better classification accuracy, Pecori et al. [29] consider increasing the integrated IoT traffic dataset, improving the DL model's complexity, and investigating feature selection strategies. Catillo et al. [30] extended the investigation of CPS-GUARD to several systems to better comprehend its limits. Improved detection against zero-day threats and investigating federated learning for IDS are essential objectives.

Amanullah et al. [31] presented a unique Internet of Things security architecture that addresses recognized issues by combining big data and deep learning technology. Saleem and Chishti [32] investigated the possibilities of deep learning for Internet of Things data analytics, resolving existing issues and improving model efficacy. Verma and Ranga [33] created lightweight security solutions for IoT and deploying and assessing ELNIDS on intelligent nodes. Vishwakarma and Kesswani [34] applied IoT devices to network traffic analysis in real-time deployment, improving multiclass classification and feature engineering. Elmasry et al. [35] improved the feature selection and hyperparameter optimization twofold PSO-based technique in IDS. Enhancing model performance across various datasets and assessing real-world deployment situations will be the main goals of the research.

Telikani and Gandomi [36] used CSSAE to handle class imbalance and optimize IDS for IoT networks. Subsequent investigations will concentrate on augmenting velocity and scalability using parallel deep learning for extensive data examination. Altunay and Albayrak [37] combined synthetic data and boosting model accuracy with sophisticated feature selection techniques to improve the IIoT IDS. Nguyen et al. [38] extended the reach of IOT to encompass a wider variety of IoT devices and developing attack methods. Gumusbas et al. [39] developed unique methodologies and increased assessment of various benchmark datasets to advance machine learning and deep learning approaches in cybersecurity. Cybersecurity is also widely studied in literature [40-43]. Ahmed et al. [44] employed weighted sub-sample selection for intrusion detection datasets and entropy-based active learning to optimize SDN load balancing for vehicle sensors. From the literature, it was understood that improving deep learning models with optimizations is very important in her research area for leveraging performance in intrusion detection in IoT use cases.

3. Proposed Framework

To detect different kinds of assaults in Internet of Vehicles (IoV) systems, a new, enhanced CNN and transfer learning approach intrusion detection system is suggested in this study. The time-based segments of external network and intra-vehicle data are transformed into images using the quantile transform technique. The resulting picture collection is then trained using five cutting-edge CNN models (VGG16, VGG19, Xception, Inception, and

InceptionResnet) to create base learners. PSO is an HPO technique that optimizes the CNN models by automatically adjusting the hyper-parameters. Subsequently, the fundamental CNN models for constructing the ensemble learning models are selected from the three best-performing CNN models. Finally, concatenation and confidence averaging are the two ensemble procedures used to build ensemble models for ultimate detectionFigure 1 CNN is a popular deep-learning model, often utilized in image identification and classification tasks [7]. Figure 2 provides a summary of the recommended IDS framework. No additional feature extraction or data reconstruction steps are required when using the photos as inputs into CNN models. Pooling, fully connected, and convolutional layers are the three types of layers that make up a conventional CNN [7]. Convolution procedures allow for the automated extraction of picture feature patterns in convolutional layers. To avoid over-fitting, local correlations are utilized. The data complexity in pooling layers may be decreased without sacrificing crucial information. The output is generated, and all features are coupled through fully connected layers. For Deep Neural Network (DL) models, Transfer Learning (TL) is the process of shifting the weights of a CNN model trained on one dataset to another [16]. Numerous image

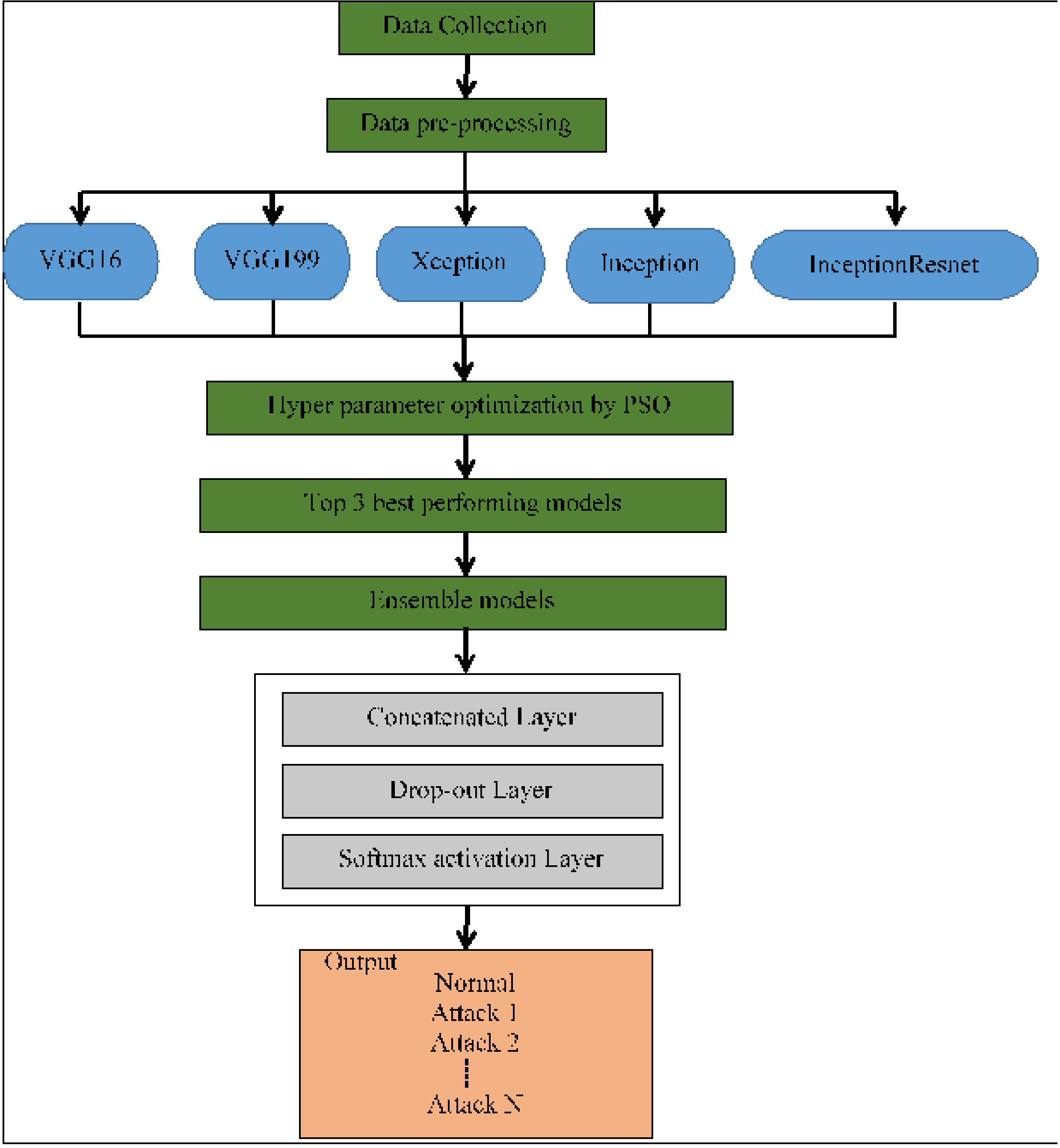


Figure 1. *Proposed Deep Learning-Based Framework with Optimizations for Intrusion Detection in IoT Use Cases.*

processing jobs have seen the practical application of the TL approach. This is because only features learned particular characteristics for a specific dataset are represented by the upper layers of CNN models. However, feature patterns picked up by CNN models' lower layers are frequently general patterns that may be used for various purposes [16]. Consequently, the lowest layers of CNN models may be used right away in multiple applications. Fine-tuning can be used to improve the effectiveness of the TL process for DL models. A portion of the top layers are unfrozen to retrain, while the majority of the pre-trained model's layers stay frozen (i.e., their weights are kept) during the fine-tuning process. The learning model can adjust the pre-trained model's higher-order attributes to suit the target task or dataset better [16]. Our selection of VGG16, VGG19, Xception, Inception, and InceptionResnet as the core CNN models in the proposed system is based on their strong performance in most photo classification tasks [9]. These CNN models have shown excellent results on various picture classification tasks after prior training on the ImageNet dataset. With over a million photos over 1,000 classifications, the ImageNet dataset is a standard for picture manipulation [9]. The 16- and 19-layer VGG16 and VGG19 models presented in [17] for the ImageNet Challenge had an error rate of 7.3% lower. Compared to the VGG16 design's five convolutional layer blocks, the VGG19 architecture has three more convolutional layers. The Inception network, initially introduced in [18], uses convolutional feature extractors that combine several contexts to produce a variety of feature patterns, therefore reducing the computational cost through dimensionality reduction. In Xception [19], depthwise separable convolutions are used instead of regular network convolutions, making it a network extension for Inception. Comparing Xception to Inception, the former requires somewhat less memory—First appearance. By integrating the leftover linkages between Resnet and the Inception network, Resnet further expands Inception [9]. The first appearance of image classification tasks is that Resnet models perform better than Inception models but also need twice as much work and memory. The vehicle network datasets train five state-of-the-art CNN models via fine-tuning and transfer learning. The following paragraph displays the ensemble models constructed using the top three CNN models as the foundation.

3.1 Proposed Ensemble Learning Model

By combining many base learning models, ensemble learning creates an ensemble model that performs better overall. Ensemble learning is often applied in data analytics difficulties due to its tendency to produce better results than a single learner [2]. To determine which class has the highest confidence value, base learners' classification probability values are combined in an ensemble learning technique called confidence averaging [20]. Softmax layers in DL models can provide a posterior probability list, including each class's classification confidence. According to the confidence averaging technique, which first calculates the average classification probability of base learners for each class, the class label with the most significant average confidence value is the final classification result. Each class's confidence value is ascertained using the softmax function [20]:

$$softmax(z)_i = \frac{e^{z_i}}{\sum_{j=1}^{C} e^{z_j}} \qquad (1)$$

Assuming that C is the number of classes in the dataset and z is the input vector, e^{z_i} and e^{z_j} Where the vectors representing the input and output, respectively, are the conventional exponential functions. The confidence averaging method's anticipated class label may be expressed as follows:

$$\hat{y} = \underset{i\in\{1,\ldots\ldots,c\}}{\operatorname{argmax}} \frac{\sum_{j=1}^{k} p_j(y=i \mid B_j, x)}{k} \qquad (2)$$

Where B_j is the j_{th} Base learner, where k is the total number of base CNN learners chosen, and in the suggested IDS, k = 3; $p_j(y = i \mid B_j, x)$ demonstrates the class value's prediction confidence in a data sample x utilizing B_j.By employing classification confidence, confidence averaging allows the ensemble model to identify ambiguous classification outcomes and rectify the misclassified samples, in contrast to the traditional voting technique, which considers the class labels. Although the confidence averaging strategy itself has a temporal complexity of just O(NKC), where N denotes the number of instances, K the number of base CNN models, and C the number of classes, the computing cost of a whole ensemble model is dependent on the complexity of its base learners [21]. Because K and C are often small, the confidence averaging approach executes quickly.A further ensemble technique for DL models is concatenation [22]. Using concatenate techniques, a concatenated CNN aims to create a new concatenated layer with all the features, combining the highest-order features generated from the top dense layer of basic CNN models. Following the concatenated layer, a drop-out layer is applied to remove redundant features, and a softmax layer is added to construct a new CNN model. Concatenation allows the highest-level elements to be combined to create a whole new model. It adds to the model training time, though, as the new model has to be re-trained using the entire dataset. The computing cost of the concatenation approach is O(NF), where N and F are the number of data samples and features, respectively, that have been extracted from the dense layers of the basic CNN models.

3.2 Hyper-Parameter Optimization (HPO)

To enhance the models' performance and more closely match the base models to the chosen datasets, CNN models' hyper-parameters must be adjusted and refined. As with other deep learning models, CNN models feature many hyper-parameters that require tuning. These hyperparameters fall into two categories: those used for model creation and those used for model training [10]. It is essential to specify hyper-parameters throughout the model design process, which are called hyper-parameters in the model design. The proposed tunneling theory framework's model-design hyper-parameters are the number of frozen layers (expressed as a percentage), the learning rate, and the dropout rate. The batch size, epoch count, and early stop patience are hyper-parameters used for model training to strike a compromise between training speed and model performance. The hyper-parameters above directly impact CNN models' structure, efficacy, and efficiency. HPO is an automated procedure that uses optimization approaches to adjust the hyper-parameters of ML or DL models [10]. PSO is one of the most popular metaheuristic optimization approaches for HPO problems. It finds the ideal hyper-parameter values by utilizing swarming particles' cooperation and information exchange [10]. Each group member is assigned a place at the beginning of PSO. $\overrightarrow{x_\iota}$ and velocity $\overrightarrow{u_\iota}$ Following every cycle, each particle's velocity is modified according to its optimal location. $\overrightarrow{p_\iota}$ as well as the present worldwide ideal position $\vec{p}$ shared by further people:

$$\overrightarrow{u_\iota} \coloneqq \overrightarrow{u_\iota} + \cup\,(0,\varphi_1)(\overrightarrow{p_\iota}-\overrightarrow{x_\iota}) + \cup\,(0,\varphi_2)(\vec{p}-\overrightarrow{x_\iota}), \quad (3)$$

where U(0, ϕ) is the constant acceleration distribution that is continuous and uniform φ_1 and φ_2. Eventually, the particles might progressively approach the potential areas to find the global optimum. O(NlogN) time complexity and support for many hyper-parameters are why PSO is selected in the suggested framework [10].

3.3 Proposed Algorithm

We have developed an algorithm called Optimized Ensemble Learning Based Intrusion Detection (OEL-ID). This algorithm aims to improve the nitrogen detection process by leveraging multiple pre-trained deep learning models through transfer learning. We also utilized an ensemble approach to maximize the benefits of combining models, enhancing the cyber attack detection process to safeguard IoT use cases.

Algorithm: Optimized Ensemble Learning Based Intrusion Detection (OEL-ID)
Input: UNSW-NB15 dataset *D*, deep learning models M
Output: Attack detection results R, performance statistics P

```
Begin
$D'$ ← Preprocess($D$)
($T1$, $T2$) ← SplitData($D'$)
For each model m in M
   Configure m with TL
   Compile m
   Optimize m with PSO
   m' ← TrainModel(T1)
End For
ensembleModel ← FindBestModels(M)
Save ensembleModel
Load ensembleModel
$R$ ← TestTheModel(ensembleModel, $T2$)
$P$ ← Evaluation($R$, ground truth)
Display $R$
Display $P$
End
```

Algorithm 1. *Optimized Ensemble Learning Based Intrusion Detection (OEL-ID).*

The UNSW-NB15 dataset is an input for different deep-learning models based on the algorithm described in this paper. It preprocesses the data and splits it into two sets: a training dataset (T1) and a testing dataset (T2) at a ratio of 80%-20%. For T1, the algorithm sets up multiple deep learning models using transfer learning to harvest the ability of performance. The algorithm identifies the best-performing models and ensembles the top three to improve IoT security. An ensemble method that combines the strengths of the most performant models to enhance intrusion detection capabilities. Then, a basic model is saved for later use. In this phase, when new network traffic arrives, the ensemble model is loaded to perform the intrusion detection in real-time. The suggested framework of deep learning employs a learning approach in the training phase to learn the attack signatures and to apply its knowledge in the attack detection process.

3.4 Dataset Details

It is used in this research because it has diversified attack flows suitable for cyberattack detection

Table 1. *Details Of Dataset in Terms of Different Attack Classes, Labels and Network Flows.*

Traffic Class	**Label**	**# Samples**	**Composition**
BENIGN	BENIGN	2273097	80.301%
Brute Force	FTP-Patator	7938	0.281%
	SSH-Patator	5897	0.209%
Botnet	Bot	1966	0.07%
DDoS	DDoS	128027	4.523%
	DoS GoldenEye	10293	0.364%
	DoS Hulk	231073	8.163%
DoS	DoS Slowhttptest	5499	0.195%
	DoS slow loris	5796	0.205%
Heartbleed	Heartbleed	11	0.001%
Infiltration	Infiltration	36	0.002%
PortScan	PortScan	158930	5.615%
	Web Attack- Brute Force	1507	0.054%
Web Attack	Web Attack – SQL Injection	21	0.001%
	Web Attack - XSS	652	0.024%
Total		2830743	100%

Table 2. *Performance Metrics of Different Models.*

Model	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**
VGG16	96.54	94.85	94.29	94.57
VGG19	93.59	93.87	92.59	93.23
Inception	94.08	94.01	90.87	92.41
Xception	93.67	95.74	93.29	94.50
InceptionResNet	96.54	94.56	96.56	95.55
Proposed Model (OEL-ID)	**98.89**	**96.89**	**98.74**	**97.81**

experiments. Table 1 shows different attack classes and data distribution dynamics.The UNSW-NB15 dataset encapsulates real-time network traffic flows. It includes benign network flows and attack flows of various categories. Each network flow has 78 features.

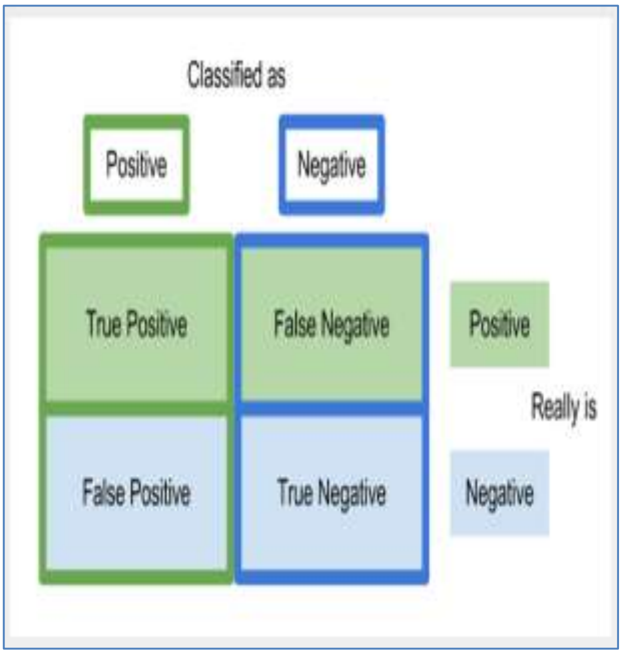


Figure 2. *Confusion Matrix*

3.5 Performance Evaluation

Confusion matrix is conceptually illustrated in Figure 2. It reflects four possible cases when the proposed system detects a given test sample. When there is an attack in the given sample and if the proposed algorithm detects it as such, this case is known as True Positive (TP). When there is no attack in the given sample and if the proposed algorithm detects it as usual, this case is known as True Negative (TN). When there is no attack in the given sample and if the proposed algorithm detects it as having an attack, this case is known as False Positive (FP). When an actual attack is in the given sample, and the proposed algorithm detects it as usual, this case is known as a False Negative (FN). Based on the confusion matrix and the four cases described above, different performance metrics are derived and used to evaluate the proposed system. Precision, recall, F1-score, and accuracy are widely used metrics for performance evaluation. These metrics are expressed in Eq. 2, Eq. 3, Eq. 4, and Eq. 5.

$$Precision\ (p) = \frac{TP}{TP+FP} \qquad (4)$$

$$Recall\ (r) = \frac{TP}{TP+FN} \qquad (5)$$

$$F1\text{-}score = 2 * \frac{(p * r)}{(p+r)} \qquad (6)$$

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \qquad (7)$$

All these metrics result in a value between 0.0 and 1.0, reflecting the least and highest performance, respectively.

4. Experimental Results

The experiments were conducted on a high-performance computing environment equipped with an Intel Core i9-12900K processor, NVIDIA RTX 3090 GPU with 24GB VRAM, 64GB DDR5 RAM, and running on Ubuntu 20.04 LTS. The deep learning models were implemented using TensorFlow 2.9, Keras, Scikit-learn, PyTorch, NumPy, Pandas, and Matplotlib. The UNSW-NB15 dataset containing diverse network traffic data was used for training and evaluation. A few data preprocessing steps were performed to have good quality input features. Values that were missing and redundant were removed. First, this was standardized using the StandardScaler function within the Python package Scikit-learn. To preserve a balanced evaluation, we did a stratified split of the dataset where 80 percent of it was used for training and the remaining 20 percent for testing. Principal Component Analysis (PCA) was performed to minimize the data complexity and enable its characteristics highlights.

The OEL-ID is an ensemble model that combines transfer learning and hyperparameter optimization using PSO. We have chosen five pre-trained CNNs, namely, VGG16, VGG19, Xception, Inception, and InceptionResNet, for extracting features. They unfreezed and configured the top layers of these trained models on the UNSW-NB15 dataset. Key hyper-parameters (batch size, learning rate, dropout rate, number of frozen layers) were optimized with PSO. The top 3 models were then ensembled by merging their feature extraction layers, followed by a dropout layer and a softmax classifier. In addition, the performance of the models is the accuracy, recall, precision, and F1-score.

We followed the particular setup of hyperparameter settings and training configurations for replication. The batch size was optimized in the range of 16 — 256 further using PSO and the learning rate was initialized to 1e-3 but tuned to the range of 1e-5 — 1e-2. Dropout was tuned between 0.2 and 0.5, and the Adam optimizer was applied with a decay rate 1e-6. The training was performed for 50 epochs and was stopped early without improvement for five consecutive epochs. Hidden layers used ReLU activation functions, softmax for the output, and sparse categorical cross-entropy as the loss function.

A prototype intrusion detection application was developed to demonstrate real-time implementation. Network traffic data from UNSW-NB15 was processed in real time, and feature extraction was performed using pre-trained CNN models. The trained OEL-ID model classified network traffic into standard or attack categories. A web-based dashboard was built using Flask and Plotly to visualize classification results and monitor attack trends. The detailed steps, hyperparameter settings, and source code provide a clear framework for reproducibility by other researchers in the field.

Table 2 is performance of each DL model and the proposed optimized ensemble learning-based intrusion detection (OEL-ID). Comparison of model results: Accuracy, Precision, Recall, and F1-score for each model showcases better ensemble performance. Compared to the separate models of VGG16 (96.54%) and Inception (94.08%), this model achieves an accuracy of 98.89%, which is significantly higher. We also achieve 98.74% and 97.81% for recall and F1-score, demonstrating adequate labeling of cyber threats in the OEL-ID framework. The improvement is achieved using the strengths of several pre-trained models through Particle Swarm Optimization (PSO) for IoT intrusion detection. The efficiency of the different deep learning models for intrusion detection using the UNSW-NB15 is

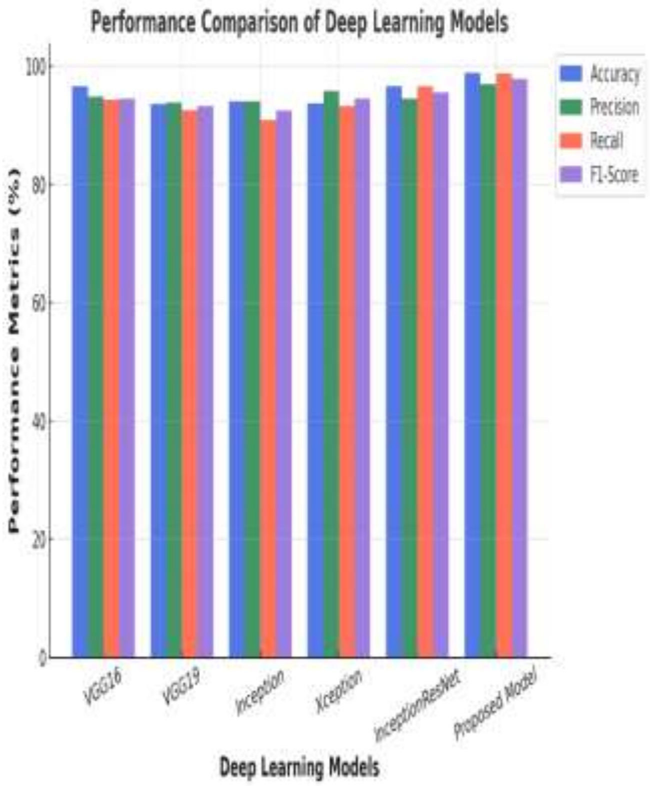


Figure 3. *Performance Comparison of Deep Learning Models.*

shown in Figure 3. The models assessed are VGG16, VGG19, Inception, Xception, InceptionResNet, and the proposed Optimized Ensemble Learning-Based Intrusion Detection (OEL-ID) Framework. The following bar chart shows accuracy, precision, recall, and F1-score for each model, showing the superiority of the ensemble-based approach in this case. Although good performances are achieved for all models, the OEL-ID model demonstrates the best performance accuracy of 98.89 percent, outdoing each deep learning model used individually. The results show that combining different models can improve ID and decrease classification crises.

The OEL-ID model performs better than individual deep learning models for the following three reasons. It leverages transfer learning firstly with trained architectures and pre-trained architectures fine-tuned to cybersecurity use cases. Instead, this utilizes features obtained from large-scale datasets to help in detection. Second, ensemble learning enhances decision-making by aggregating predictions from several outperforming models. These weaknesses are collectively alleviated, allowing for higher recall rates while lowering the amount of false positives reported. Thirdly, particle swarm optimization (PSO) is adapted for hyperparameter searching, allowing dynamic refinement of learning and dropout rates, which is necessary to generalize the model optimally.

We demonstrate through experiments that the OEL-ID framework achieves a record-high recall of 98.74 percent which ensures low false negatives leading to no cyber threats getting through undetected. It also features a higher precision of 96.89 percent, reducing false positives, thus making it a more reliable option for real-life IoT security applications. The F1-score, which is a weighted average of precision and recall, is 97.81 percent, proving that the model is competent in tackling cybersecurity threats. The performance improvements indicatethe benefit of combining transfer learning, ensemble learning, and PSO optimization which make the OELID framework a very attractive solution for the security of the IoT environment. In Table 3, we provide an ablation study of the OEL-ID model, showing the effect of different components on performance. The final baseline model (using a single CNN) reached an accuracy of 91.34%, a mean accuracy of 94.21% with transfer learning. Using PSO optimization raises the accuracy even more to 96.12%, optimizing hyperparameters for better generalization. Finally, the ensemble learning mechanism that assembles multiple models improves its accuracy up to 97.45%. With all the improvements fed into the OEL-ID model, the complete OEL-ID model achieves maximum accuracy of 98.89% with top precision, recall and F1-score. These results confirm the importance of combining multiple deep learning sub-techniques to detect any intrusion.

***Table 3.** Ablation Study of OEL-ID Model*

Model Configura-tion	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**
Baseline Model (Single CNN)	91.34	89.87	90.12	90.99
With Transfer Learning	94.21	92.45	93.15	92.79
With PSO Optimization	96.12	94.98	95.78	95.37
With Ensemble Learning	97.45	96.32	97.12	96.71
Full OEL-ID Model	**98.89**	**96.89**	**98.74**	**97.81**

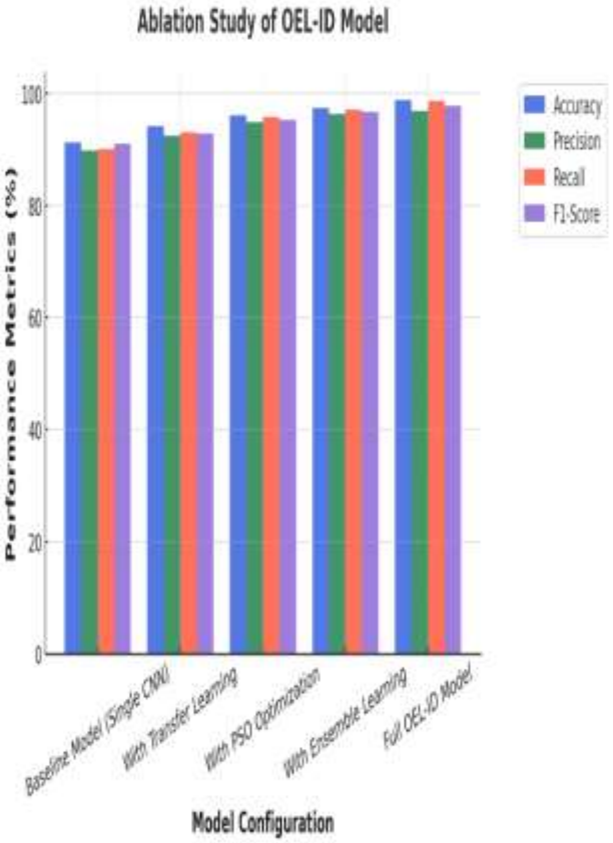


***Figure 4.** Ablation Study of OEL-ID Model*

The ablation study of OEL-ID model, which shows the effect of different enhancements on performance, shown in figure 4. The accuracy rate of the baseline model (CNN) is 91.34 percent. With transfer learning, the accuracy of the model increases to 94.21 percent, an apparent benefit of easy transfer to extract features. This improvement enables the model to capture stronger signals leading to a reduction of false positives and an increase in precision.

This is extremely effective but dynamic tuning of hyper parameters can increase the accuracy by removing the limit thus the PSO optimization increases the performance of the model by optimizing hyper parameters making it 96.12 percent accuracy. This modification close the loop be far more efficient, learning to generalize well across a variety of cyber threat types. This combination of several deep learning models is ensemble learning, and when applying it, the final accuracy is 97.45 percent. Combining models saves the weaknesses of each model and increases the recall, so the overall system becomes more accurate in detecting an attack.

Using transfer learning, PSO optimization, and ensemble learning, the developed full OEL-ID model obtains the highest accuracy of 98.89 percent. The precision, recall and F1-score achieves their maximum values, which shows a balanced performance. These findings validate that integrating several deep learning strategies powerfully augments the performance of the IoT IDS, which serves as a resilient approach to addressing the issue of cybersecurity.

5. Discussion

IoT environments exhibit many features that reflect the complexity of the cyber threat, which means that self-learning systems offer much more robust security solutions than traditional rule-based intrusion detection systems. Traditional techniques cannot cope with the changing patterns of attacks which yields a high rate of undetected threat and false positives. Although existing deep learning-based intrusion detection models have shown potential, most of them fall short in terms of generalization, typical feature extraction, and hyperparameter tuning, which makes them unfeasible for practical applications. In this research, we tackle these challenges with an optimally tuned ensemble learning-based intrusion detection framework, utilizing transfer learning and PSO for signal intensity amplitude ratio for enhanced detection accuracy and model robustness.

One fundamental weakness pointed out by the state of the art is that existing models lack the ability to easily combine heterogeneous feature representations from multiple sources. Most of the intrusion detection frameworks are based on single deep learning models which are prone to overfitting and biased for individual attacks. In addition, systematic hyperparameter search would have increased the models flexibility to perform well in real cases, a fact that is usually lost]} To address these concerns, the presented methodology combines diverse pre-trained CNNs for a strong generalization of discriminative features, utilizes PSO for parameter optimization of every base learner, and applies an ensemble strategy to strengthen the classification performance.

Compared with the state-of-the-art approaches, the experimental results validate the proposed model which has an accuracy of 98.89%. By leveraging both transfer learning and ensemble learning, it can improve attack category-wise generalization, providing reduced false alarm and higher confidence in detecting attacks. These hyperparameters lead to a faster convergence and more stability of the model making the system more applicable to real-time usage in Cybersecurity. This research adds value to state-of-the-art by overcoming the current set of limitations, paving the way for reliability adaptation to real-time IoT environments for deep learning models targeting intrusion detection. Availability of transfer learning, PSO optimization, and ensemble learning portfolio provides a new practical direction to enhance detection accuracy. The limitations of this study and avenues for future research are discussed in section 5.1.

5.1 Limitations of the Study

Limitations and Future Directions Still, this study is not without limitations. First, the computational complexity of the ensemble model based on PSO optimization exacerbates training time and demands heavy hardware usages which restricts its utilization from real-time IoT scenarios. Over the last few years, transfer learning has been popular in improving feature extraction, however, relying on pre-trained CNN architectures, which were designed on other types of data (e.g., image) may not represent the characteristics of network traffic very well. Third, the model performance is heavily dependent on the training dataset, and updating the model may be a mandatory as the IoT networks are dynamically changing and it is necessary in practice that unseen attack patterns are applied.

6. Conclusion and Future Work

In this work, we present a deep learning based framework using transfer learning approach and apply it on pre-trained models to mitigate cybersecurity in IoT scenarios. We further use Particle Swarm Optimization (PSO) for hyperparameter tuning to ensure that deep learning models perform their best in our system. Our system can potentially beat isolated models by taking the combination of best-performing models in an ensemble way. Based on this framework and the optimization mechanisms, we develop our algorithm, called Optimized Ensemble Learning Based Intrusion Detection (OEL-ID), to improve intrusion detection and cybersecurity in IoT scenarios. We conducted an empirical study on the UNSW-NB15 benchmark dataset for our method, resulting in an accuracy of 98.89% which has surpassed current deep learning models. This shows that our system holds a high potential towards its integration into IoT scenarios, enhancing security of underlying applications. If any of the activities are classified as attacks, this indicates the presence of an attack type According to the training data, our framework is also supervised and it should be noted here. However, we might not be able to identify any future unknown/index attacks types with our system. Such limitation has to be solved with further research. In the future, we will contribute to either building or improving the system based around the unsupervised learning approaches to identify unseen attacks.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Ibitoye, O., Shafiq, O., & Matrawy, A. (2019). Analyzing Adversarial Attacks against Deep Learning for Intrusion Detection in IoT Networks. *2019 IEEE Global Communications Conference (GLOBECOM).* 1-6. https://doi.org/10.1109/globecom38437.2019.9014337

[2] Madhu, B., Chari, M.V.G., Vankdothu, R., Silivery, A.K. and Aerranagula, V. (2023). Intrusion detection models for IOT networks via deep learning approaches. *Measurement: Sensors*. 25, 1-14. https://doi.org/10.1016/j.measen.2022.100641

[3] Keshk, M., Koroniotis, N., Pham, N., Moustafa, N., Turnbull, B. and Zomaya, A.Y. (2023). An explainable deep learning-enabled intrusion detection framework in IoT networks. *Information Sciences*. 639;1-20. https://doi.org/10.1016/j.ins.2023.119000

[4] Bassey, J., Adesina, D., Li, X., Qian, L., Aved, A., & Kroecker, T. (2019). Intrusion Detection for IoT Devices based on RF Fingerprinting using Deep Learning. *2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC).* 98-104. https://doi.org/10.1109/fmec.2019.8795319

[5] Fatani, A., Abd Elaziz, M., Dahou, A., Al-Qaness, M.A. and Lu, S. (2021). IoT intrusion detection system using deep learning and enhanced transient search optimization. *IEEE Access*. 9;123448-123464. https://doi.org/10.1109/ACCESS.2021.3109081

[6] Lazzarini, R., Tianfield, H. and Charissis, V. (2023). A stacking ensemble of deep learning models for IoT intrusion detection. *Knowledge-Based Systems.* 279;1-13. https://doi.org/10.1016/j.knosys.2023.110941.

[7] Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications.* 50;1-19. https://doi.org/ 10.1016/j.jisa.2019.102419.

[8] Bakhsh, S.A., Khan, M.A., Ahmed, F., Alshehri, M.S., Ali, H. and Ahmad, J. (2023). Enhancing IoT network security through deep learning-powered Intrusion Detection System. *Internet of Things.* 24;1-36. https://doi.org/10.1016/j.iot.2023.100936

[9] Jayalaxmi, P.L.S., Saha, R., Kumar, G., Conti, M. and Kim, T.H. (2022). Machine and deep learning solutions for intrusion detection and prevention in IoTs: A survey. *IEEE Access*, 10;121173-121192. https://doi.org/10.1109/ACCESS.2022.3220622

[10] Bovenzi, G., Aceto, G., Ciuonzo, D., Persico, V., & Pescape, A. (2020). A Hierarchical Hybrid Intrusion Detection Approach in IoT Scenarios. *GLOBECOM 2020 - 2020 IEEE Global Communications Conference.* 1-7. https://doi.org/10.1109/globecom42002.2020.9348167.

[11] Vishwakarma, M. and Kesswani, N. (2022). DIDS: A Deep Neural Network based real-time Intrusion detection system for IoT. *Decision Analytics Journal.* 5;1-9. https://doi.org/10.1016/j.dajour.2022.100142

[12] Soliman, S., Oudah, W. and Aljuhani, A.,(2023). Deep learning-based intrusion detection approach for securing industrial Internet of Things. *Alexandria Engineering Journal* 81;371-383. https://doi.org/10.1016/j.aej.2023.09.023.

[13] Rezvy, S., Luo, Y., Petridis, M., Lasebae, A., & Zebin, T. (2019). An efficient deep learning model for intrusion classification and prediction in 5G and IoT networks. *2019 53rd Annual Conference on Information Sciences and Systems (CISS).* 1-6. https://doi.org/10.1109/ciss.2019.8693059

[14] Saleem, T. J., & Chishti, M. A. (2020). Deep learning for the internet of things: potential benefits and use-cases. *Digital Communications and Networks.* 1-24. https://doi.org/10.1016/j.dcan.2020.12.002

[15] Akgun, D., Hizal, S. and Cavusoglu, U. (2022). A new DDoS attacks intrusion detection model based on deep learning for cybersecurity. *Computers & Security.* 118;1-13. https://doi.org/10.1016/j.cose.2022.102748

[16] Ullah, I. and Mahmoud, Q.H. (2021). Design and development of a deep learning-based model for anomaly detection in IoT networks. *IEEE Access* 9;103906-103926. https://doi.org/10.1109/ACCESS.2021.3094024

[17] Qiu, H., Dong, T., Zhang, T., Lu, J., Memmi, G., & Qiu, M. (2021). Adversarial Attacks Against Network Intrusion Detection in IoT Systems. *IEEE Internet of Things Journal.* 8(13);10327–10335. https://doi.org/10.1109/jiot.2020.3048038

[18] Kasongo, S.M. (2023). A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework. *Computer Communications,* 199;113-125. https://doi.org/10.1016/j.comcom.2022.12.010.

[19] Rahman, S. A., Tout, H., Talhi, C., & Mourad, A. (2020). Internet of Things Intrusion Detection: Centralized, On-Device, or Federated Learning? *IEEE Network.* 34(6);310–317. https://doi.org/10.1109/mnet.011.2000286

[20] Hnamte, V. and Hussain, J. (2023). DCNNBiLSTM: An efficient hybrid deep learning-based intrusion detection system. *Telematics and Informatics Reports.* 10;1-13. https://doi.org/10.1016/j.teler.2023.100053.

[21] Cassales, G. W., Senger, H., de Faria, E. R., & Bifet, A. (2019). IDSA-IoT: An Intrusion Detection System Architecture for IoT Networks. *2019 IEEE Symposium on Computers and Communications (ISCC).* 1-7. https://doi.org/10.1109/iscc47284.2019.8969609

[22] Anushiya, R. and Lavanya, V.S. (2023). A new deep-learning with swarm based feature selection for intelligent intrusion detection for the Internet of things. *Measurement: Sensors*, 26, pp.1-9.. https://doi.org/10.1016/j.measen.2023.100700.

[23] Yahyaoui, A., Abdellatif, T., & Attia, R. (2019). Hierarchical anomaly based intrusion detection and localization in IoT. *2019 15th International Wireless Communications & Mobile Computing Conference*. 108-113. https://doi.org/10.1109/iwcmc.2019.8766574

[24] Li, B., Wu, Y., Song, J., Lu, R., Li, T., & Zhao, L. (2020). DeepFed: Federated Deep Learning for Intrusion Detection in Industrial Cyber-Physical Systems. *IEEE Transactions on Industrial Informatics.* 1–10. https://doi.org/10.1109/tii.2020.3023430

[25] Hazman, C., Guezzaz, A., Benkirane, S. and Azrour, M. (2023). lIDS-SIoEL: intrusion detection framework for IoT-based smart environments security using ensemble learning. Cluster Computing, 26(6);4069-4083. https://doi.org/10.1007/s10586-022-03810-0.

[26] Singh, P., P, J. J., Pankaj, A., & Mitra, R. (2021). Edge-Detect: Edge-Centric Network Intrusion Detection using Deep Neural Network. *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC).* 1-6. https://doi.org/10.1109/ccnc49032.2021.9369469

[27] Hasan, M., Milon Islam, M., Islam, I., & Hashem, M. M. A. (2019). Attack and Anomaly Detection in IoT Sensors in IoT Sites Using Machine Learning Approaches. *Internet of Things*, 100059. 7;1-14. *https://doi.org/*10.1016/j.iot.2019.100059

[28] Campos, E.M., Saura, P.F., González-Vidal, A., Hernández-Ramos, J.L., Bernabe, J.B., Baldini, G. and Skarmeta, A. (2022). Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges. *Computer Networks.* 203;1-16. https://doi.org/10.1016/j.comnet.2021.108661.

[29] Pecori, R., Tayebi, A., Vannucci, A., & Veltri, L. (2020). IoT Attack Detection with Deep Learning Analysis. *2020 International Joint Conference on Neural Networks (IJCNN).* 1-8. https://doi.org/10.1109/ijcnn48605.2020.9207171

[30] [30] Catillo, M., Pecchia, A. and Villano, U. (2023). CPS-GUARD: Intrusion detection for cyber-physical systems and IoT devices using outlier-aware deep autoencoders. *Computers & Security.* 129;1-15. https://doi.org/10.1016/j.cose.2023.103210.

[31] Amanullah, M. A., Habeeb, R. A. A., Nasaruddin, F. H., Gani, A., Ahmed, E., Nainar, A. S. M., … Imran, M. (2020). Deep learning and big data technologies for IoT security. *Computer Communications.* 151;495-517. https://doi.org/10.1016/j.comcom.2020.01.016

[32] Saleem, T. J., & Chishti, M. A. (2019). Deep Learning for Internet of Things Data Analytics. *Procedia Computer Science.* 163;381–390. https://doi.org/10.1016/j.procs.2019.12.120

[33] Verma, A., & Ranga, V. (2019). ELNIDS: Ensemble Learning based Network Intrusion Detection System for RPL based Internet of Things. *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU).* 1-6. https://doi.org/10.1109/iot-siu.2019.8777504

[34] Vishwakarma, M. and Kesswani, N. (2023). A new two-phase intrusion detection system with Naïve Bayes machine learning for data classification and elliptic envelop method for anomaly detection. *Decision Analytics Journal*. 7;1-8. https://doi.org/10.1016/j.dajour.2023.100233.

[35] Elmasry, W., Akbulut, A., & Halim Zaim, A. (2019). Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic. *Computer Networks.* 1-48. https://doi.org/10.1016/j.comnet.2019.107042

[36] Telikani, A., & Gandomi, A. H. (2019). Cost-sensitive stacked auto-encoders for intrusion detection in the Internet of things. *Internet of Things,* 1-25. https://doi.org/10.1016/j.iot.2019.100122

[37] Altunay, H.C. and Albayrak, Z., 2023. A hybrid CNN+ LSTM-based intrusion detection system for industrial IoT networks. *Engineering Science and Technology, an International Journal.* 38;1-13. https://doi.org/10.1016/j.jestch.2022.101322.

[38] Nguyen, T. D., Marchal, S., Miettinen, M., Fereidooni, H., Asokan, N., & Sadeghi, A.-R. (2019). DÏoT: A Federated Self-learning Anomaly Detection System for IoT. *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS).* 1-12. https://doi.org/10.1109/icdcs.2019.00080

[39] Gümüşbaş, D., Yıldırım, T., Genovese, A. and Scotti, F. (2020). A comprehensive survey of databases and deep learning methods for cybersecurity and intrusion detection systems. *IEEE Systems Journal*. 15(2);1717-1731. https://doi.org/10.1109/jsyst.2020.2992966

[40] Amjan Shaik, Bhuvan Unhelkar, & Prasun Chakrabarti. (2025). Exploring Artificial Intelligence and Data Science-Based Security and its Scope in IoT Use Cases. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.869

[41] M. Husain Bathushaw, & S. Nagasundaram. (2024). The Role of Blockchain and AI in Fortifying Cybersecurity for Healthcare Systems. *International Journal of Computational and Experimental Science and Engineering,* 10(4). https://doi.org/10.22399/ijcesen.596

[42] R, U. M., P, R. S., Gokul Chandrasekaran, & K, M. (2024). Assessment of Cybersecurity Risks in Digital Twin Deployments in Smart Cities. *International Journal of Computational and Experimental Science and Engineering,* 10(4). https://doi.org/10.22399/ijcesen.494

[43] Vutukuru, S. R., & Srinivasa Chakravarthi Lade. (2025). CoralMatrix: A Scalable and Robust Secure Framework for Enhancing IoT Cybersecurity. *International Journal of Computational and Experimental Science and Engineering,* 11(1). https://doi.org/10.22399/ijcesen.825

[44] Ahmed, U., Lin, J.C.W. and Srivastava, G. (2022). A resource allocation deep active learning based on load balancer for network intrusion detection in SDN sensors. *Computer Communications.* 184;56-63. https://doi.org/10.1016/j.comcom.2021.12.009.