SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V11I6P109

Volume 11 Issue 6, 107-113, June 2024
© 2024 Seventh Sense Research Group®

Original Article

Advancing Intrusion Detection: Application of Distributed Deep Learning on the KDD Cup 99 Dataset

Agalit Mohamed Amine[1], El Youness Idrissi Khamlichi[2]

[1,2]*SIGER Laboratory, Faculty of Science and Technology, Sidi Mohamed Ben Abdellah University, Fez, Morocco.*

[1]*Corresponding Author : mohamedamine.agalit@usmba.ac.ma*

Received: 16 April 2024 Revised: 26 May 2024 Accepted: 11 June 2024 Published: 29 June 2024

Abstract - *Intrusion Detection Systems (IDS) are crucial for protecting IT infrastructures against increasingly sophisticated and evolving threats. Faced with complex attacks such as stealthy or polymorphic threats, conventional methods based on rules or signatures show their limitations. An innovative IDS approach utilizing a deep neural network integrated into a distributed architecture for dynamic and precise network traffic analysis is introduced. Tested on the KDD Cup 99 dataset, this method demonstrated an accuracy of 99.90%, a recall of 99.89%, and a specificity of 100%, marking a significant improvement over traditional IDS systems. The exceptional performance obtained encourages the broader adoption of this system and suggests significant potential for revolutionizing IT security practices. The implications of the findings for current security strategies are also discussed, and directions for future research are proposed.*

Keywords - *Intrusion detection, Deep learning, Distributed IDS architecture, KDD Cup 99, Cybersecurity.*

1. Introduction

Computer networks play a vital role in modern society, facilitating essential activities such as communication, commerce, and the management of critical infrastructures. With this growing dependence comes an increase in the associated risks of cyberattacks, which are becoming increasingly sophisticated and diverse [1]. Intrusion Detection Systems (IDS) are therefore crucial for protecting these infrastructures, enabling the identification of unauthorized access attempts and defending networks against a variety of threats [2]. Traditional IDS based on rules or signatures face increasing difficulties when dealing with innovative attacks, particularly zero-day or polymorphic attacks, which can evade detection based on predefined models [3]. Furthermore, the emergence of the Internet of Things (IoT) exponentially increases the number of connected devices, diversifying attack vectors and thereby complicating network security tasks. These developments call for more adaptive IDS approaches capable of dynamically responding to new threats [4].

Deep learning has revolutionized intrusion detection by enabling models to learn and infer from vast volumes of network traffic data. This learning capability offers improved recognition of complex malicious behaviors, often undetectable by traditional methods. Deep learning architectures such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, and Gated Recurrent Units (GRU) have proven effective, particularly in IoT environments where interactions between devices increase vulnerability risks [5, 6]. However, existing research often lacks flexibility in dynamic network environments.

Although effective, current methods are not always suitable for responding to new threats in real-time. An innovative distributed IDS system leveraging these advanced technologies for more effective network traffic analysis is proposed. Tested on the KDD Cup 99 dataset, this model achieved an accuracy of 99.90%, a recall of 99.89%, and a specificity of 100%. These exceptional performances illustrate the significant potential for improving intrusion detection in the face of constantly evolving cyber threats [7].

2. Background of the KDD 99 Dataset

The KDD Cup 99 dataset is one of the most widely used datasets for evaluating Intrusion Detection Systems (IDS). It was created from data collected during the KDD Cup 1999 competition, organized by the International Knowledge Discovery and Data Mining Tools Competition. This dataset contains a wide variety of simulated attacks on a fictitious military network, providing a rich environment for testing the capabilities of intrusion detection models.

The dataset comprises 41 features and five main classes: normal, DoS (Denial of Service), R2L (Remote to Local), U2R (User to Root), and probe (probes). Its availability and popularity have led to its adoption as a standard benchmark for IDS systems [8].

3. Literature Review

The evolution of Intrusion Detection Systems (IDS) has significantly benefited from the integration of deep learning technologies, making them more effective in various network environments. This section examines how these technologies have been applied to different sectors and the progress they have engendered in the field of cybersecurity.

3.1. IDS in Wireless Sensor Networks

H. M. Saleh et al. explored the application of deep neural networks to enhance the security of wireless sensor networks, focusing on cross-correlation techniques for feature extraction, highlighting their effectiveness in detecting complex threats [9].

3.2. IDS for Web Applications

R. Branco et al. discussed the implementation of IDS based on network traffic and log analysis for web applications. They utilized natural language processing and machine learning, demonstrating significant improvement in detecting attacks targeting web applications [10].

3.3. Cross-Disciplinary Applications of Deep Learning

T. Lei et al. showed that deep learning techniques could be applied beyond cybersecurity, such as in the simulation of plant phenological phenomena, illustrating the versatility and capability of these techniques to handle complex data sets analogous to those of network traffic [11].

3.4. Enhancement of IDS in IoT Networks

K. Harahsheh et al. improved feature selection for IDS in the IoT environment, thereby optimizing the performance of machine learning models to address the challenges posed by the diversity and decentralization of IoT devices [12]. H. Im et al. proposed an innovative IDS architecture using cross-check filters for in-vehicle networks, adapting IDS to very specific applications with stringent performance and reliability requirements [13].

3.5. Emerging Technologies in IDS

M. A. Bouke et al. explored the use of the BukaGini algorithm to enhance feature interaction analysis in IDS, reducing false positives and adapting to dynamic network behaviors [14]. M. Fang et al. discussed the application of cycle-consistent generative adversarial networks to improve web security, an innovative approach to addressing constantly evolving cyber threats [15].

3.6. Lightweight IDS for IoT and Phishing Detection

U. Otokwala et al. focused their research on lightweight IDS for IoT, using optimized feature selection and deep autoencoders, which are essential for effective solutions in resource-limited environments [16]. UG scholars utilized convolutional neural networks for phishing detection, demonstrating the effectiveness of these networks in recognizing phishing attempts [17].

Each study contributes to an aspect of intrusion detection, showcasing the breadth and depth of possibilities offered by deep learning. This variety of applications underscores the importance of continuing to develop and integrate advanced techniques into IDS to meet the challenges of modern cybersecurity.

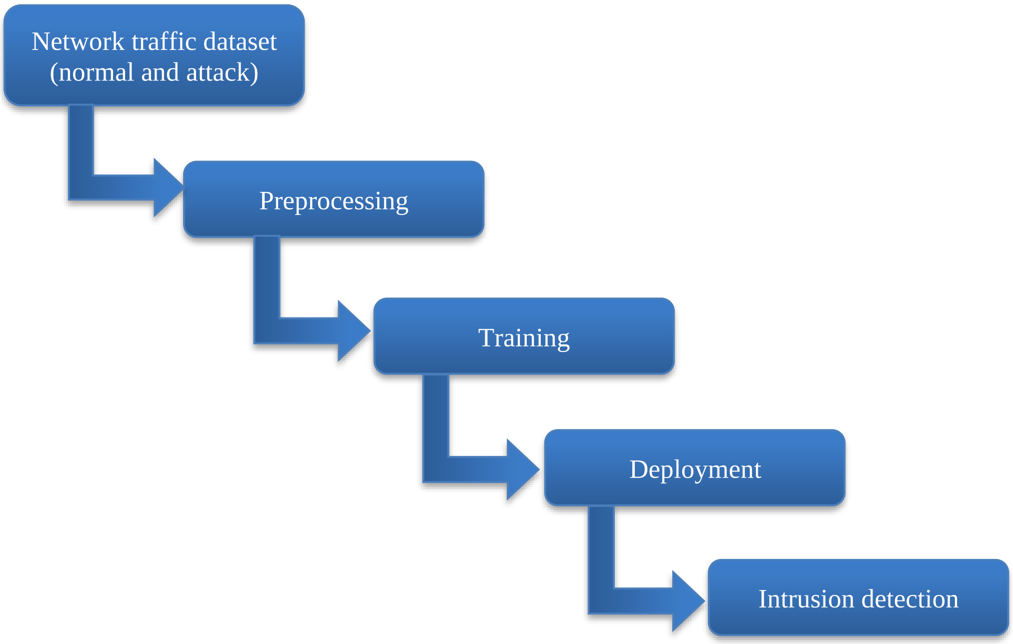

Fig. 1 Deep learning-based intrusion detection model

4. Methodology

4.1. Deep Learning-Based Intrusion Detection Model

4.1.1. Data Pre-Processing

Before any training, network traffic data undergoes rigorous preprocessing to ensure their quality and relevance. This includes normalization, anomaly removal, and transformation into a format that can be utilized by the deep learning model [11]. This precise treatment is essential so that both training and testing data accurately reflect normal traffic and attack patterns, allowing the model to distinguish precisely between the two.

Figure 1 illustrates the different steps involved in implementing a deep learning-based intrusion detection model, from preprocessing to intrusion detection.

4.1.2. Model Architecture

A Convolutional Neural Network (CNN) is adopted to characterize and identify attack signatures within network traffic. The CNN, effective in image processing, also proves efficient in identifying complex patterns in network traffic data, thanks to its multiple processing layers [15].

4.1.3. Deployment and Detection

Once trained, the model is deployed on an intrusion detection system that continuously analyzes network traffic and generates an alert if an intrusion is detected.

4.2. Distributed IDS Model Architecture

Figure 2 shows the different components of the distributed IDS system, which includes several IDS sensors distributed across the network that collect and transmit data to a central server.

4.3. IDS System Operation

Data collected by the IDS sensors is analyzed by the deep learning model hosted on the central server, which generates alerts in case an intrusion is detected. These alerts are then transmitted to network administrators for necessary corrective actions [16].

4.4. Model Compilation

The model compilation phase defines the optimizer ('adam'), the loss function ('categorical_crossentropy'), and performance metrics such as precision, recall, and specificity [18]. This configuration is crucial to ensure the efficiency and reliability of the model under real-world conditions.

4.5. Training and Testing Dataset Distribution

To ensure a robust evaluation of the model, the KDD 99 dataset was divided into training and test sets using an 80/20 distribution. This division maintains sufficient variety in the training data while preserving a representative test set. A 10-fold cross-validation was also performed to ensure that the model generalizes well on unseen data sets [19].

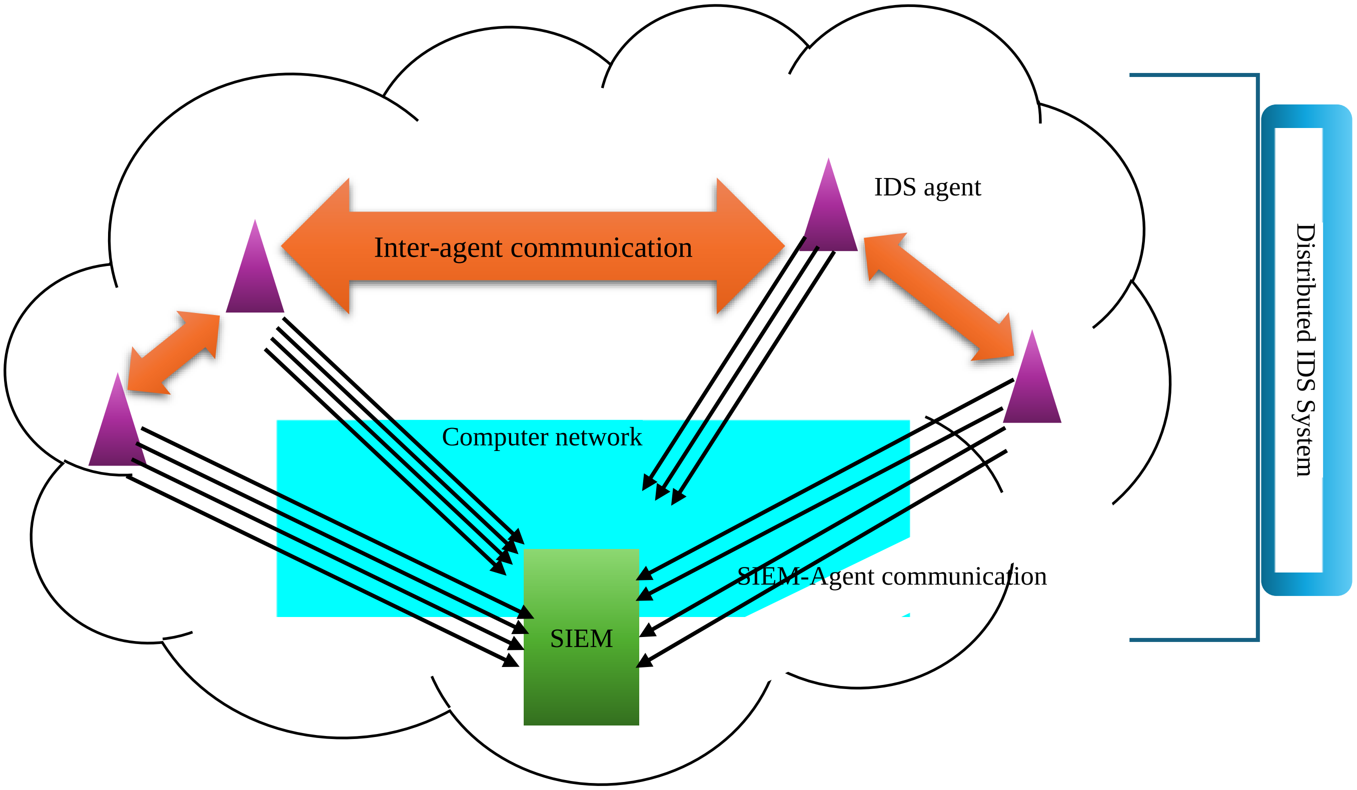

Fig. 2 Distributed IDS architecture diagram

4.6. Evaluation Metrics

In addition to precision, recall, and specificity, standard performance metrics were calculated to evaluate the model's performance [20] finely.

5. Results

5.1. Interpretation of Results

The model achieved an exceptional accuracy of 99.90%, indicating that almost all the model's predictions were correct. This metric illustrates the overall effectiveness of the model in discriminating between malicious activities and legitimate network traffic [21]. The recall (or sensitivity) was measured at 99.89%, meaning that the model successfully identified almost all actual attacks present in the test dataset. This high sensitivity is crucial for an operational security system, minimizing the risk of undetected attacks [22]. The specificity reached 100%, demonstrating that the model perfectly recognised and excluded every instance of normal traffic, thus avoiding any service interruption due to false alerts, which is vital for maintaining operational efficiency without compromising security [23]. Table 1 presents the performance metrics of the proposed model, illustrating its exceptional performance in terms of precision, recall, specificity, and accuracy.

Table 1. Performance metrics

Metrics	Value
Precision	99.90%
Recall	99.89%
Specificity	100.00%
Accuracy	99.90%

5.2. Confusion Matrix

The confusion matrix (see Figure 3) provides a visual representation of the model's performance, where True Positives (TP) and True Negatives (TN) show the correct classifications made by the system. The 100% specificity confirms that there were no False Positives (FP), which is ideal for the reliability of the IDS. False Negatives (FN) were extremely rare, demonstrating the model's effectiveness in detecting actual attacks [22][24].

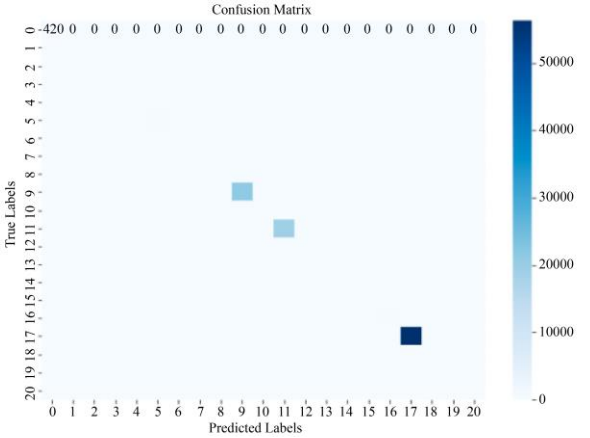

Fig. 3 Confusion matrix of the proposed model

5.3. Graphical Representation of Results

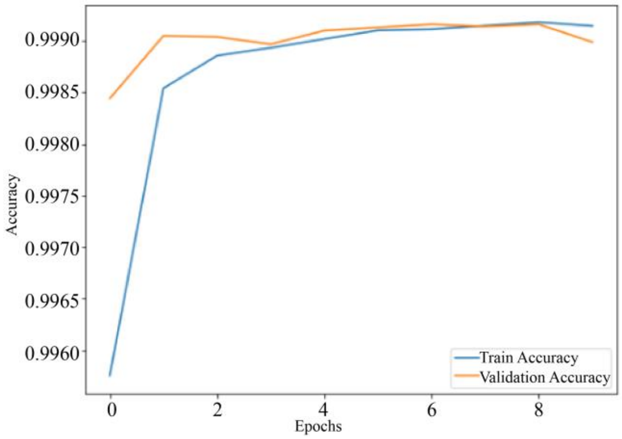

Fig. 4 Training and validation accuracy over epochs

Figure 4 illustrates the evolution of training and validation accuracy over epochs. This representation shows how the model improved over time and indicates a stable convergence of performance.

6. Discussion

6.1. Comparison with State-of-the-Art Techniques

6.1.1. Advantages of CNN Over Traditional Approaches

The model based on Convolutional Neural Networks (CNN) has shown superior performance compared to traditional approaches based on rules and signatures, which have proven ineffective against zero-day and polymorphic attacks. Unlike traditional methods, CNNs can automatically extract and learn complex features from network traffic data, making them more adaptive and robust against new threats.

6.1.2. Comparison with Other Deep Learning Models

When comparing this model with other deep learning techniques, such as Long Short-Term Memory networks (LSTM) and Gated Recurrent Units (GRU), the CNN approach demonstrated a better ability to capture complex spatial data patterns thanks to its multiple convolutional layers. For instance, Hussein (2024) reported an accuracy of 94.3% using an LSTM model for intrusion detection, whereas this CNN model achieved an accuracy of 99.90% [21].

6.1.3. Robustness Against Various Attacks

This study also highlighted the robustness of the CNN model against different types of attacks, including Denial of Service (DoS) attacks, Remote to Local (R2L) attacks, and User to Root (U2R) attacks. The model's perfect specificity of 100% demonstrates its ability to minimize false positives, which is crucial for operational environments where false alerts can lead to significant costs.

6.2. Reasons for Superior Performance

6.2.1. Data Preprocessing and Normalization

A significant part of the success lies in rigorous data preprocessing and normalization. By cleaning and transforming the data appropriately, it was possible to reduce noise and anomalies, allowing the model to learn more relevant patterns and make more accurate predictions.

6.2.2. Model Architecture

The model architecture, with its multiple convolutional layers and dropout layers, to prevent overfitting, played a crucial role in improving detection accuracy and robustness. This configuration allows the model to capture complex hierarchical features and generalize better on unseen datasets.

6.2.3. Hyperparameter Optimization

Key hyperparameters such as the learning rate, batch size, and activation functions were also optimized, contributing to improved convergence and overall model performance. The use of the Adam optimizer helped accelerate convergence and find an optimal local minimum more efficiently.

6.3. Implications for Cybersecurity

6.3.1. Reduction of False Alerts

The model's 100% specificity indicates that it perfectly recognized and excluded every instance of normal traffic, thus avoiding any service interruption due to false alerts. This is particularly important in production environments where interruptions can have severe consequences.

6.3.2. Real-Time Detection

The model's ability to detect intrusions in real-time through a distributed architecture enhances proactive security strategies. This approach allows for rapid response to emerging threats, minimizing potential damage caused by successful attacks.

6.4. Limitations and Future Directions

6.4.1. Real-Time Adaptive Learning

Despite high performance, the model could benefit from integrating real-time adaptive learning mechanisms to better adapt to new emerging attack vectors. As suggested by Anusha et al. (2024), this approach could improve the responsiveness and effectiveness of IDS in dynamic environments [22].

6.4.2. Federated Learning

The integration of federated learning techniques, as explored by Nuhu et al. (2024), could enhance the robustness of the IDS against distributed attacks and improve the model's generalizability across different network domains. This approach would allow collaboration between multiple decentralized devices or servers without compromising data privacy [25].

7. Conclusion

This study has validated the effectiveness of a Convolutional Neural Network (CNN) model for network intrusion detection. The results demonstrate that the model offers exceptional accuracy (99.90%), sensitivity (99.89%), and specificity (100%). These performances illustrate the model's ability to reliably and accurately identify real security threats while minimizing false alerts.

7.1. Key Findings and their Importance

- High Accuracy: Confirms that most of the model's predictions were correct, thus validating the reliability of CNNs in the context of cybersecurity.
- High Sensitivity: Ensures that the system can effectively detect real attacks, an indispensable characteristic of any operational security system.
- Perfect Specificity: Indicates that the model correctly identified all instances of normal traffic, which is crucial for reducing service interruptions due to incorrect security alerts.

7.2. Future Implications for Research and Practice

The results of this study encourage further integration of deep learning into intrusion detection systems, especially in dynamic and constantly evolving network environments. The adoption of deep learning models improves the ability of security systems to adapt to new threats without the need for frequent updates to threat signatures, as discussed in the works of Helali [24] and Gudimetla [26].

The extension of this research could explore more complex or hybrid deep learning models, combining different neural network architectures for even more robust and accurate detection. Additionally, the integration of federated learning techniques, as suggested by Younas et al. [27], could enable more distributed and scalable threat detection, well-suited to large enterprise networks and cloud environments. These approaches could lead to more resilient and customizable IDS that better address the challenges of modern security. Moreover, the exploration of machine learning techniques for anomaly detection in network traffic, as mentioned in [28], could provide further perspectives for improving intrusion detection systems.

References

[1] Ayuba John et al., "Cluster-Based Wireless Sensor Network Framework for Denial-of-Service Attack Detection Based on Variable Selection Ensemble Machine Learning Algorithms," *Intelligent Systems with Applications*, vol. 22, pp. 1-12, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[2] Dandy Pramana Hostiadi et al., "A New Approach of Botnet Activity Detection Models Using Combination of Univariate and ANOVA Feature Selection Techniques," *International Journal of Intelligent Engineering and Systems*, vol. 17, no. 3, pp. 485-502, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[3] Rami Sihwail, Mariam Al Ghamri, and Dyala Ibrahim, "An Enhanced Model of Whale Optimization Algorithm and K-Nearest Neighbors for Malware Detection," *International Journal of Intelligent Engineering and Systems*, vol. 17, no. 3, pp. 606-621, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[4] Ammaiyappan Kavitha, and Valavandan Srinivasan Meenakshi, "Collaborative Attackers Detection and Route Optimization by Swarm Intelligentbased Q-learning in MANETs," *International Journal of Intelligent Engineering and Systems*, vol. 17, no. 3, pp. 563-574, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] Young-Woo Hong, and Dong-Young Yoo, "Multiple Attack Detection Using SHAP and Heterogeneous Ensemble Model in UAV's Controller Area Network," *Preprints, Computer Science and Mathematics*, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[6] Widi Santoso, Rahayu Safitri, and Samidi, "Integration of Artificial Intelligence in Facial Recognition Systems for Software Security, *Sinkron : Journal and Research in Informatics Engineering*, vol. 8, no. 2, pp. 1208-1214, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[7] Teoh Chun Hwung, and Yuhanis Yusof, "Enhanced Network Security: A Data Mining Approach to Intrusion Detection," *Journal of Digital System Development*, vol. 2, no. 1, pp. 140–153, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[8] Mahbod Tavallaee et al., "A Detailed Analysis of the KDD CUP 99 Dataset," *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, Ottawa, ON, Canada, pp. 1-6, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[9] Hadeel M. Saleh, Hend Marouane, and Ahmed Fakhfakh, "A Comprehensive Analysis of Security Challenges and Countermeasures in Wireless Sensor Networks Enhanced by Machine Learning and Deep Learning Technologies," *International Journal of Safety and Security Engineering*, vol. 14, no. 2, pp. 373-386, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[10] Rodrigo Branco, Vinicius Cogo, and Iberia Medeiros, "Towards a Web Application Attack Detection System based on Network Traffic and Log Classification," *Proceedings of the 19th International Conference on Evaluation of Novel Approaches to Software Engineering ENASE*, Angers, France, vol. 1, pp. 692-699, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Tong Lei et al., "Simulation of Automatically Annotated Visible and Multi/Hyperspectral Images Using the Helios 3D Plant and Radiative Transfer Modeling Framework," *Plant Phenomics A Science Partner Journal*, vol. 6, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[12] Khawlah Harahsheh, Rami Al-Naimat, and Chung-Hao Chen, "Using Feature Selection Enhancement to Evaluate Attack Detection in the Internet of Things Environment," *Electronics*, vol. 13, no. 9, pp. 1-16, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[13] Hyungchul Im, Donghyeon Lee, and Seongsoo Lee, "A Novel Architecture for an Intrusion Detection System Utilizing Cross-Check Filters for In-Vehicle Networks," *Sensors*, vol. 24, no. 9, pp. 1-20, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] Mohamed Aly Bouke et al., "Application of Bukagini Algorithm for Enhanced Feature Interaction Analysis in Intrusion Detection Systems," *PeerJ Computer Science*, vol. 10, pp. 1-26, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[15] Menghao Fang et al., "Reinventing Web Security: An Enhanced Cycle-Consistent Generative Adversarial Network Approach to Intrusion Detection," *Electronics*, vol. 13, no. 9, pp. 1-21, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[16] Uneneibotejit Otokwala, Andrei Petrovski, and Harsha Kalutarage, "Optimized Common Features Selection and Deep-Autoencoder (OCFSDA) for Lightweight Intrusion Detection in Internet of Things," *International Journal of Information Security*, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[17] J. Jayapradha et al., "Intrusion Detection System for Phishing Detection Using Convolution Neural Network," *International Journal of Computing and Digital Systems*, pp. 1-10, 2024. [Google Scholar] [Publisher Link]

[18] R Vinayakumar, K.P. Soman, and Prabaharan Poornachandran, "Evaluation of Recurrent Neural Network and its Variants for Intrusion Detection System (IDS)," *International Journal of Information System Modeling and Design*, vol. 8, no. 3, pp. 43-63, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[19] Jiawei Han, Jian Pei, and Hanghang Tong, *Data Mining: Concepts and Techniques*, Elsevier Science, pp. 1-752, 2022. [Google Scholar] [Publisher Link]

[20] David M.W. Powers, "Evaluation: From Precision, Recall and F-Measure to ROC, Informedness, Markedness and Correlation," *Journal of Machine Learning Technologies*, vol. 2, no. 1, pp. 37-63, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[21] Teeb Hussein Hadi, "Deep Learning-Based DDoS Detection in Network Traffic Data," *International Journal of Electrical and Computer Engineering Systems*, vol. 15, no. 5, pp. 404-414, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[22] G. Anusha, Gouse Baigmohammad, and Uma Mageswari, "Detection of Cyber-Attacks on IoT based Cyber-Physical Systems," *MATEC Web of Conferences, International Conference on Multidisciplinary Research and Sustainable Development (ICMED 2024)*, vol. 392, pp. 1-9, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[23] Zhen Wang et al., "An Efficient Intrusion Detection Model Based on Convolutional Spiking Neural Network," *Scientific Reports*, vol. 14, no. 1, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[24] Rasha Gaffer M. Helali, "Phishing Detection Using Hybrid Machine Learning Techniques," *Journal of China University of Mining and Technology*, vol. 29, no. 2, pp. 45-52, 2024. [Publisher Link]

[25] Abdulhafiz Nuhu et al., "Distributed Denial of Service Attack Detection in IoT Networks Using Deep Learning and Feature Fusion: A Review," *Mesopotamian Journal of CyberSecurity*, vol. 4, no. 1, pp. 47-70, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[26] Sandeep Reddy Gudimetla, “Cloud Malware Protection Strategies,” *International Research Journal of Modernization in Engineering Technology and Science*, vol. 6, no. 3, pp. 4325-4326, 2024. [CrossRef] [Publisher Link]

[27] Faizan Younas et al., “An Efficient Artificial Intelligence Approach for Early Detection of Cross-Site Scripting Attacks,” *Decision Analytics Journal*, vol. 11, pp. 1-13, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[28] Richa Singh, Nidhi Srivastava, and Ashwani Kumar, “Machine Learning Techniques for Anomaly Detection in Network Traffic,” *2021 Sixth International Conference on Image Information Processing*, Shimla, India, pp. 261-266, 2021. [CrossRef] [Google Scholar] [Publisher Link]