

PERFORMANCE ANALYSIS OF VGGNET FOR DOS AND DDOS DETECTION IN WIRELESS SENSOR NETWORKS

Hajar Fares¹
Zahra Oughannou
Oussama Hamal
Zakaria Elrhadiouini
Abderrahmane Hajraoui

Received 09.08.2024.
Revised 04.02.2025.
Accepted 20.02.2025.

Keywords:

Wireless Sensor Networks, Intrusion
Detection, Machine Learning,
Deep Learning, DoS Attack,
DDoS Attack

ABSTRACT

Intrusion detection have become absolutely essential in today's IT infrastructure, primarily, because they play a critical role in maintaining network security, these systems offers efficient and high-performance solutions for spotting and mitigating a broad spectrum of network attacks. As communication technologies advance rapidly and become more widespread, the risk of malicious users exploiting network vulnerabilities has grown substantially. This surge in potential threats has paved the way for highly sophisticated, automated, and distributed attacks, which traditional IDS frameworks find challenging to counter effectively. Given these advanced threats, there is an urgent need to explore and implement more robust and adaptive IDS methodologies. This contribution examines and assesses the VGGNet deep learning model in detail, with a focus on intrusion detection tasks. We concentrate on strengthening the security of wireless sensor networks (WSNs), which are vulnerable to denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks because of their low processing power and frequent deployment in hostile situations. We use our suggested approach to two well-known datasets, CICDDoS-2019 and WSN-DS, to assess its performance. The WSN-DS dataset, which captures a range of legitimate and malicious traffic patterns, was created especially for WSN situations. Meanwhile, a thorough collection of DDoS attack scenarios is offered by the CICDDoS-2019 dataset. We use these datasets to undertake a thorough performance assessment of our VGGNet-based model, including common measures like recall, precision, accuracy, F1-score, and confusion matrix. The results of our tests demonstrate that the VGGNet model performs remarkably well in identifying intrusions, obtaining an accuracy rate of 0.979. This high degree of accuracy demonstrates how deep learning models, such as VGGNet, have the potential to significantly improve the resilience and dependability of IDS in defending contemporary network infrastructures against changing cyberthreats.



¹ Corresponding author: Hajar Fares
Email: professeurhajar@gmail.com

1. INTRODUCTION

A wireless sensor network (WSN) is a technology that uses spatially dispersed, decentralized, self-organizing sensor nodes to monitor physical parameters like motion, pressure, sound, vibration, temperature, and pollutants. The data collected by these nodes is sent over the network to the base station, which is the main location.

WSNs are used in various applications, including health-care, military, smart city and other applications (Baraneetharan, 2020).

Despite their versatility, these sensors face significant challenges due to their limited computational and communication power, small memory, and constrained energy resources. They become especially vulnerable to several kinds of attacks, such as Distributed Denial of Service (DDoS) and Denial of Service (DoS) attacks, when they are deployed in hostile or remote places. Because sensor nodes have limited resources, detecting DoS attacks in WSNs is particularly difficult. In these attacks, an intruder can perform unauthorized actions such as illegal computations or sends a huge amount of packets continuously to saturate the user's buffer, effectively rendering the system unable to respond to legitimate requests (Psychogyios et al., 2024).

To safeguard WSNs, several security requirements must be met:

- **Confidentiality:** This ensures that data remains hidden from unauthorized users, protecting it from eavesdroppers.
- **Integrity:** It guarantees the reliability of data packets, safeguarding them from being altered by malicious nodes.
- **Authentication:** This process verifies the origin of messages and the identity of communication hosts to prevent packet injection or spoofing (Ayoub, 2020) (Ayoub, 2019).
- **Availability:** It ensures that nodes can access resources when needed, and that data and services remain available on demand, even during malicious attacks

Given the increasing complexity, automation, and distribution of attacks, traditional IDSs struggle to address current network security challenges. IDSs are often divided into two categories: Signature-Based and Anomaly-Based. They can be used in both hardware and software to automate the intrusion detection process. The Signature-Based approach uses a database of known attack patterns to scan in-bound traffic, whereas the Anomaly-Based approach detects deviations from normal traffic patterns.

By maximizing resource consumption in the network, machine learning (ML) algorithms provide real-time solutions that can prolong the network's operational

lifetime. The following are this paper's primary contributions:

- Providing comprehensive details of WSNs, their limitations, and vulnerabilities to attacks.
- Analyzing the performance of VGGNet, a deep learning model, for detecting DoS and DDoS attacks.
- Offering a thorough discussion of experimental results and the limitations of the proposed model.

This paper is structured as follows: Section II presents a recent literature review. Section III provides an overview of the deep learning approach, Section IV describes our model and evaluation techniques, Section V presents evaluation results and a detailed discussion, as well as a proposition of future works. Section VI is a global conclusion of our paper.

2. RELATED WORKS

Deep learning methodologies have reached near-human level accuracy in various tasks such as image classification (Amato, Falchi, et al., 2018), (M.Tech Scholar et al., 2020), (Tsimenidis et al., 2021), object detection (Vadicamo et al., 2017), object recognition (Girshick et al., 2016). These advancements are largely due to the development of sophisticated neural network architectures and the availability of large datasets for training. Recently, researchers have been exploring the potential of deep learning methods for intrusion detection in network security. While deep learning shines in fields like natural language processing and image recognition (Krizhevsky et al., 2012), its application to breach detection presents unique challenges. Traditionally, rule-based and signature-based systems have performed well in intrusion detection by precisely matching known attack patterns. However, these systems often struggle with new or evolving threats that do not match predefined signatures.

Many researchers have studied deep learning methods for intrusion detection, in recent years.

This review looks at the latest developments in deep learning (DL) and how they can be used in machine learning, especially in intrusion detection methods, as mentioned in the literature. The pros and cons of DL in defence are looked at in conferences, magazines, books, and theses (Jin et al., 2012). While DL is great at understanding natural language and recognising images, it struggles when it comes to breach detection, where rule-based and signature-based systems have traditionally done better (Kutilla et al., 2007).

Amato et al. (2017) have put forth a face-recognition-based intrusion detection solution that works with embedded devices. They have combined between machine and deep learning and they trained their approach on the VGG dataset.

Simonyan and Zisserman's 2014, uses convolutional neural networks (CNNs), which have become common owing to their efficient image data processing via several layers and decreased pooling (Maseer et al., 2021; Bay et al., 2000). The synthesis highlights the need for novel fusion methods that integrate domain-specific information with DL to improve intrusion detection system reliability and resilience, highlighting a major subject for future study.

Conversely, traditional machine learning approaches have also evolved, utilizing techniques such as Support Vector Machines (SVM) and Random Forests. These methods have been effective in various IDS applications, achieving commendable results in real-time attack prediction and system security (Ravindaran et al., 2023; Feng et al., 2023; Shah et al., 2023). However, they often require extensive feature engineering and may not scale as efficiently with the increasing data volume and complexity associated with modern network environments.

It has been suggested that deep learning techniques be combined with conventional techniques in order to capitalize on the advantages of each approach. For instance, combining CNN features with SVM classifiers has been suggested to enhance accuracy and provide robust real-time applications in intrusion detection systems (Azam et al., 2023). This hybrid approach aims to maximize the deep learning capability for feature extraction and the efficiency of traditional classifiers for quick decision-making. Deep learning architectures, such as VGGNet, have shown promise in complex image recognition tasks that parallel the intricacies of network intrusion detection. The modified VGG19 architecture, which includes additional dense layers and dropout to mitigate overfitting, has shown superior performance in classifying complex patterns with an accuracy improvement of 8% over the standard CNN models (Du et al., 2023). This indicates the potential of deep learning architectures to handle high-dimensional data in intrusion detection with a similar level of efficacy.

Furthermore, the application of deep learning for intrusion detection has expanded into real-time systems, where models like the 1D_VGGNet have been tailored for one-dimensional MCDM applications, showing substantial improvements in accuracy and resilience compared to 1D CNNs (Li et al., 2020). This adaptation demonstrates the flexibility of deep learning models to conform to the specific demands of intrusion detection, offering both high performance and adaptability.

While deep learning models like VGGNet provide powerful tools for pattern recognition and data classification, their integration with traditional machine learning methods presents a promising avenue for developing robust, efficient, and scalable intrusion detection systems. Future research should focus on optimizing these integrations and exploring new

architectures that can provide even greater accuracy and faster processing times, essential for keeping pace with the evolving landscape of network security threats.

The research uses deep learning models like Inception V3, VGG16, VGG19, and a tweaked ResNet 50 to automate rice blast disease diagnosis. With a 2,000-image dataset, the system achieved an accuracy of 99.75%. A Gradio-based web app was created for farmers. However, the system faces limitations due to high computing needs and extensive data requirements for model training. Future plans include developing a mobile app for field use and optimizing models for less computing resources (Feng et al., 2023).

This research examines network intrusion detection systems (NIDS) using ML, DL, and DT approaches. It discusses strategies for reducing false positives, adapting to threats, and improving accuracy. While DL has advantages, it also burdens system resources. Future research should optimize these techniques for real-time mobile device use (Almomani et al., 2016).

The study evaluates the effectiveness of convolutional neural network (CNN) models in recognizing underwater objects using side-scan sonar images, focusing on transfer learning for improved prediction accuracy and computational performance. GoogleNet showed the highest accuracy, while custom and pre-trained models were effective in concrete crack detection. Future research should focus on real-world applications and sophisticated models (Sharafaldin et al., 2019).

Batch Normalisation (VGG-M-BN) and a modified VGG network model are introduced in Caffe deep learning for vegetable photo identification and classification. Merging outputs from the first two fully linked layers and applying Batch Normalisation increased model accuracy to 96.5%. Batch Normalisation doubled convergence speed, demonstrating processing efficiency. The study also showed that big training datasets improve model accuracy and generalisation. The ReLU activation function surpasses Sigmoid and Tanh

For the purpose of classifying high-dimensional data, the study provides a one-dimensional visual geometry group network (1D_VGGNet). The classifier makes multicriteria decisions efficiently using one-dimensional convolution operations instead of two-dimensional ones. The network's customisable maxpooling kernel size reduces feature maps, speeding training and prediction. Performance measurement is more accurate with a new objective function. Testing on the MIT-BIH Arrhythmia database and Shaoxing University student accomplishment shows that 1D VGGNet beats 1D CNNs in evaluation metrics (Sharafaldin et al., 2019).

3. DEEP LEARNING FOR INTRUSION DETECTION

Deep learning, a specialized branch of artificial neural networks (ANN), excels in representing data through hierarchical, multi-layered structures as illustrated in Figure 1. This approach enables the transformation of

raw data into more abstract and useful representations as it progresses through successive layers. Because such a hierarchical approach is so good at identifying intricate patterns and relationships in data, deep learning models are well suited for a variety of uses, such as intrusion detection in network security (Amato, Carrara, et al., 2018).

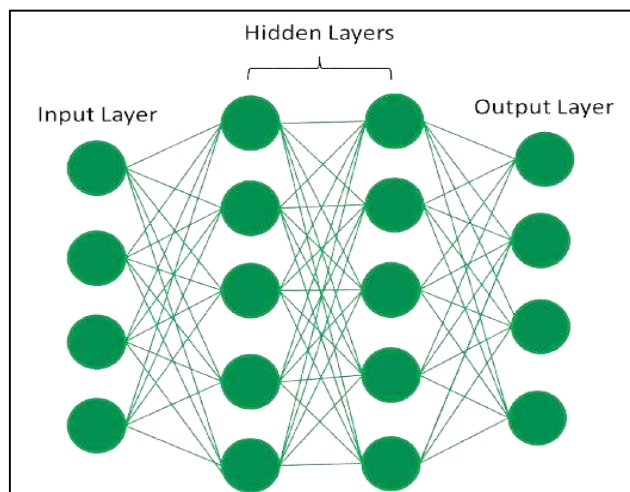


Figure 1. Deep learning architecture.

Deep learning's ability to handle both labeled and unlabeled data is one of its main advantages. Because of their flexibility, models that can be trained on massive volumes of totally, partially, or completely unlabeled data can be created. This capability is especially beneficial in intrusion detection, where labeled attack data may be scarce or incomplete. The following algorithms are commonly used in deep learning, each offering unique strengths for different types of data and tasks.

- **Recurrent Neural Networks (RNNs):** RNNs specialize in processing sequential data, where the current output depends not only on the present input but also on previous inputs. Because of this, RNNs can be used for applications like natural language processing and time series analysis. In intrusion detection, RNNs can model the temporal dynamics of network traffic, capturing patterns over time that may indicate an attack.
- **Convolutional Neural Networks (CNNs):** CNNs are made to handle input, like images, that has a structure resembling a grid. They are highly effective at feature extraction through a series of convolutional layers that detect patterns like edges and textures, followed by pooling layers that reduce dimensionality. In the context of intrusion detection, CNNs can be applied to analyse network traffic data, identifying patterns indicative of malicious activity.
- **Long Short-Term Memory (LSTM):** this deep learning model is a type of RNN designed to address long-term dependencies. They can learn and remember over longer sequences, making

them advantageous for tasks where context over extended periods is crucial. For intrusion detection, LSTMs can track the evolution of network traffic over time, identifying subtle anomalies that develop gradually.

- **The Multi-Layer Perceptron (MLP)** is a feed-forward artificial neural network that uses multiple layers to represent data. MLPs use backpropagation for training and are well-suited for tasks where data can be represented in a tabular format. In intrusion detection, MLPs can classify network traffic data based on predefined features.

Recent advancements in CNNs have significantly enhanced their performance, especially in tasks involving image and spatial data. But in order for these models to train well, they frequently need a significant amount of computing power and specialized hardware, including graphics processing units (GPUs). This requirement poses a challenge in resource-constrained environments like WSNs, where computational and energy resources are limited. Despite these challenges, the ability of CNNs to extract high-level features and patterns from raw data makes them a powerful tool in developing robust IDS.

In summary, the versatility and power of deep learning algorithms, including CNNs, RNNs, LSTMs, and MLPs, offer promising avenues for enhancing intrusion detection systems. By leveraging these advanced models, it is possible to develop IDS that are more accurate, resilient, and capable of adapting to the evolving landscape of network security threats.

4. MODEL DESCRIPTION AND METHODOLOGY

The proposed classifier model is structured through a series of essential steps as illustrated in Figure 2, each critical to the development and evaluation of the intrusion detection system. These steps include dataset selection, data preprocessing, model training, classification of the test set, and comprehensive performance evaluation. This methodology ensures a rigorous and systematic approach to leveraging deep learning for intrusion detection.

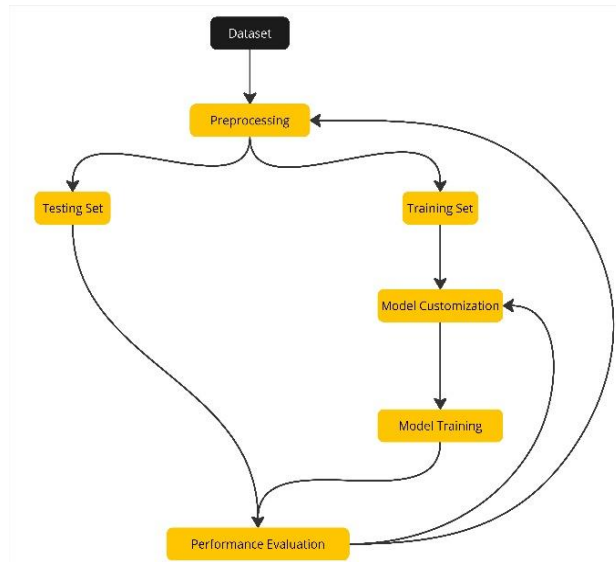


Figure 2. Proposed classifier Model

4.1 Dataset selection

The comprehensiveness and quality of the datasets utilized for training and assessment have a significant impact on the efficacy of an intrusion detection system. WSN-DS and CICDDoS-2019 are two well-known datasets that we chose for this investigation.

WSN-DS (Almomani et al., 2016): This dataset is tailored for intrusion detection within wireless sensor networks. Compiled by Iman Almomani et al., WSN-DS contains 23 attributes and 374,661 records, representing various types of network traffic. These include normal traffic as well as four distinct types of DoS attacks: Blackhole, Grayhole, Flooding, and Scheduling. The diversity and specificity of the data make it an ideal choice for evaluating the performance of IDS in WSN environments.

CICDDoS-2019 (Sharafaldin et al., 2019): Developed by the Canadian Institute for Cybersecurity, the CICDDoS-2019 dataset is comprehensive in scope, encompassing 80 features related to network traffic. This dataset is designed to detect a wide range of DDoS attacks, including reflective DDoS, UDP, UDP-Lag, and SYN attacks. The deep learning model can be trained and

tested on a strong basis thanks to the large feature set and range of attack kinds.

4.2 PREPROCESSING

One of the most important steps in getting the datasets ready for model training is effective data preprocessing. The preprocessing workflow involves several key tasks:

- **Column Name Cleaning:** Removing spaces from column names to ensure consistency and prevent errors during data manipulation.
- **Irrelevant Data Removal:** Eliminating columns and rows that do not contribute to the model's predictive capability. This step is essential to reduce noise in the data and improve model performance.
- **Handling Missing Values:** Addressing rows with missing values by either imputing missing data or removing incomplete rows to prevent biases and inaccuracies in the model.
- **Duplicate Removal:** Ensuring data integrity by removing duplicate records. Duplicate entries can distort the training process and lead to overfitting.
- **Label Mapping:** Standardizing label names to maintain consistency in the output categories. This step includes converting categorical labels into numerical values suitable for machine learning algorithms.
- **Data Balancing:** Adjusting the dataset to prevent model bias towards any particular class. To guarantee a balanced representation of each class, this is usually accomplished by methods like undersampling the dominant class or oversampling the minority class.
- **Figures 3** illustrates WSN-DS after oversampling and **Figure 4** shown CICDDoS-2019 dataset after oversampling
- **Feature Scaling and Transformation:** Normalizing the data make sure that every feature adds the same amount to the model's learning. This often involves scaling features to a standard range, such as [0, 1], and applying transformations to stabilize variance and enhance model performance.
- **Data Splitting:** Dividing the dataset into training and testing sets to evaluate the model's performance on un- seen data. Typically, a split of 70-80.

The preprocessing steps significantly impact the quality of the model's input data, thereby influencing its performance. The following figures illustrate the datasets after preprocessing, showing the distribution of classes and the feature scaling applied.

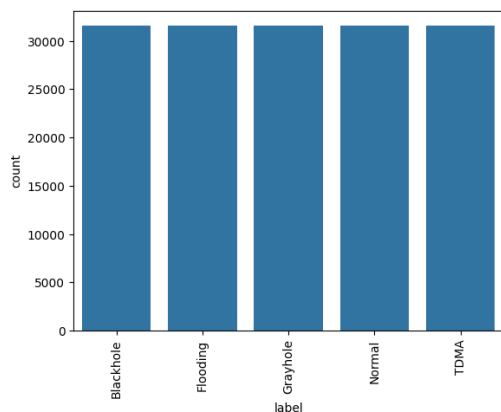


Figure 3. WSN-DS Dataset after Oversampling

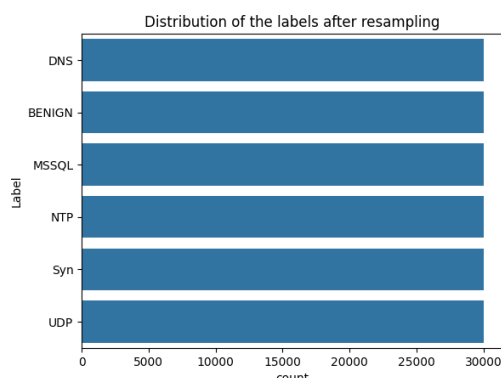


Figure 4. CICDDoS-2019 Dataset after Oversampling

4.3 MODEL BUILDING

The core of our methodology involves the application of VGGNet, a deep learning architecture developed by the Visual Graphics Group (VGG) at Oxford University. Originally designed for image classification, VGGNet can be adapted for other complex tasks, including intrusion detection. The architecture explores the relationship between network depth and performance, utilizing small convolution kernels and maximum pooling layers to build deep networks comprising 11 to 19 layers (as shown in Figure 5).

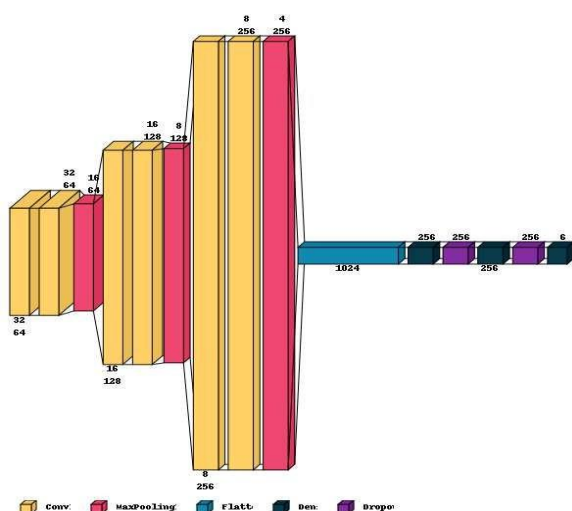


Figure 5. VGGNet Architecture.

4.4 EVALUATION METRICS

To deeply assess the robustness of the intrusion detection models, we employ a range of standard evaluation metrics.

- **Accuracy:** is a broad indicator of the model's effectiveness that provides an overall prediction of the right classes.
- **F1-Score:** The F1-Score, which provides a balanced assessment of a model's accuracy, particularly in situations when there is a class imbalance, is the harmonic mean of precision and recall.
- **Precision:** To determine how accurate the model is at identifying positive instances, precision computes the ratio of true positive predictions to all positive predictions.
- **Recall:** Also referred to as sensitivity, this metric expresses the percentage of genuine positives that the model accurately recognized from all real positive instances, demonstrating its capacity to identify positive cases.
- **Confusion Matrix:** This table displays the true positives, true negatives, false positives, and false negatives to give a thorough analysis of the model's performance. It provides information about the kinds and frequencies of errors that the model makes.

Together, these metrics offer a broad framework for evaluation, guaranteeing that the model's performance is evaluated from several angles and producing more robust and dependable intrusion detection systems.

5. EXPERIMENTATION AND RESULTS

We evaluated VGGNet's performance in detecting DoS and DDoS attacks using the WSN-DS and CICDDoS-2019 datasets. The results are presented in Figures 6, 7, and tables 1 and 2, showing metrics and confusion matrices.

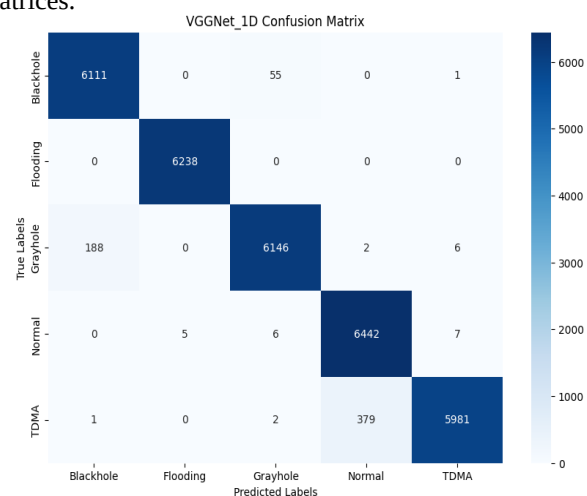


Figure 6. Confusion Matrix of VGGNet on WSN-DS

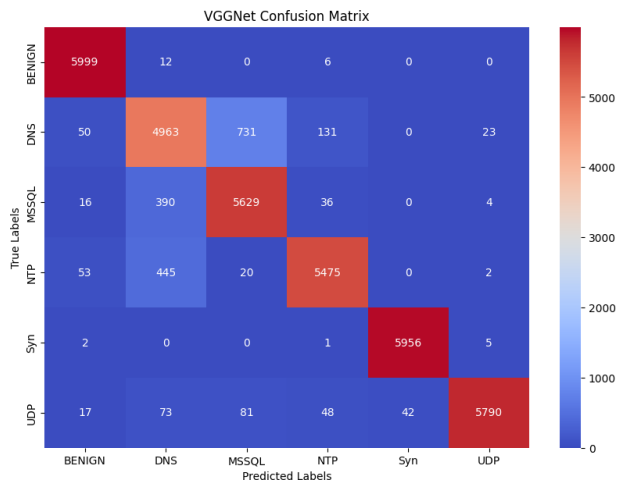


Figure 7. Confusion Matrix of VGGNet on CICDDoS-2019

Table 1. VGGNet on WSN-DS Classification Report

	precision	recall	f1-score	support
Blackhole	0.97	0.99	0.98	6167
Flooding	1.00	1.00	1.00	6238
Grayhole	0.99	0.97	0.98	6342
Normal	0.94	1.00	0.97	6460
TDMA	1.00	0.94	0.97	6363
accuracy	0.98 (31570 instances)			
macro avg	0.98	0.98	0.98	31570
weighted avg	0.98	0.98	0.98	31570

Table 2. VGGNet on CICDDoS classification Report

	precision	recall	f1-score	support
BENIGN	0.98	1.00	0.99	6017
DNS	0.84	0.84	0.84	5898
MSSQL	0.87	0.93	0.90	6075
NTP	0.96	0.91	0.94	5995
Syn	0.99	1.00	1.00	5964
UDP	0.99	0.96	0.98	6051
accuracy	0.94 (36000 instances)			
macro avg	0.94	0.94	0.94	36000
weighted avg	0.94	0.94	0.94	36000

6. DISCUSSION

6.1 Comparison with related works

Our work demonstrates a significant improvement over existing methodologies in several key areas. Traditional machine learning approaches, such as those discussed by E. Baraneetharan (Baraneetharan, 2020), primarily rely on feature engineering and manual intervention, which can be time-consuming and may not scale well with large datasets. In contrast, our deep learning approach using VGGNet automates feature extraction, leveraging convolutional layers to capture intricate patterns in the data, which significantly enhances

detection accuracy. (Amato, Carrara, et al., 2018) utilized deep learning in conjunction with a KNN classifier and ResNet-50 for intrusion detection. While their approach achieved commendable results, our use of VGGNet, specifically adapted for WSN environments, demonstrated superior performance with an accuracy rate of 0.979. This high level of accuracy underscores the potential of deep learning models like VGGNet to significantly enhance the robustness and reliability of IDS in protecting modern network infrastructures against evolving cyber threats.

The work by Kaur and Kumar (M.Tech Scholar et al., 2020) explored the use of Artificial Neural Networks (ANN) with the Grey Wolf Optimizer (GWO) for intrusion detection. While their model showed improved classification performance, it still required significant manual feature engineering and optimization efforts. Our approach, leveraging the VGGNet model, reduces the dependency on manual feature selection through its ability to automatically learn hierarchical feature representations from raw input data, thus offering a more scalable and efficient solution.

In a study by Tsimenidis et al. (2021), Recurrent Neural Networks (RNNs) were the main tool used in deep learning techniques for IoT intrusion detection, as they allow for the capturing of temporal patterns in network traffic. Although RNNs are effective for sequential data, they often face challenges with long-term dependencies and computational efficiency. Our use of VGGNet, which is particularly adept at handling spatial data, provides a complementary approach by efficiently processing and learning from static snapshots of network traffic data, leading to high accuracy in detecting both DoS and DDoS attacks.

Psychogyios et al. (2024) used deep learning for time series data intrusion detection, demonstrating how well Long Short-Term Memory (LSTM) networks capture temporal dependencies. However, LSTMs can be computationally intensive and may not be ideal for real-time applications in resource-constrained environments. In contrast, VGGNet's convolutional architecture is more suitable for parallel processing and can be optimized for deployment on hardware with limited computational resources, such as those found in WSNs.

Additionally, Jin et al., (2012) investigated the use of driver distraction detection using performance measures, illustrating the potential of machine learning in real-time applications. While their approach was tailored for a different domain, the principles of real-time data processing and the need for efficient model architectures are equally relevant to our work. Our VGGNet-based model, with its high accuracy and robustness, demonstrates its capability to handle real-time intrusion detection tasks effectively.

Maseer et al. (2021) explored hybrid deep learning models for enhancing IoT network intrusion detection.

Their approach combined multiple models to leverage the strengths of each. While hybrid models can offer performance gains, they also introduce complexity and require more computational resources. Our approach focuses on optimizing a single, powerful model (VGGNet), simplifying deployment and maintenance while still achieving high performance.

In summary, our work builds on and extends the capabilities of previous studies by leveraging the VGGNet architecture, which provides several advantages:

- **Automated Feature Extraction:** Reduces the need for manual feature engineering, enabling the model to learn directly from raw data.
- **High Accuracy:** Achieves superior performance in detecting a wide range of network intrusions, including DoS and DDoS attacks.
- **Scalability:** The model's architecture allows it to scale effectively with increasing data volumes, making it suitable for real-time intrusion detection.
- **Resource Efficiency:** Optimized for deployment in resource-constrained environments such as WSNs, where computational and energy resources are limited.
- These advancements highlight the potential of deep learning models like VGGNet to significantly enhance the robustness and reliability of IDS in protecting modern network infrastructures against evolving cyber threats.

6.2 Implications of findings

The high accuracy and robustness of the VGGNet model in detecting DoS and DDoS attacks indicate its potential for deployment in real-world wireless sensor networks (WSNs). The ability to accurately classify various types of network traffic and distinguish between normal and malicious activities can significantly enhance the security posture of WSNs, which are often deployed in critical and resource-constrained environments. Furthermore, the application of such advanced deep learning models can automate and streamline the intrusion detection process, reducing the reliance on manual monitoring and intervention.

6.3 Limitations of the study

Although the results are encouraging, there are several limitations to our study. The computational complexity of deep learning models, such as VGGNet, which demands a lot of memory and processing power, is one of the main obstacles. This can be a constraint in the context of WSNs, where resources are typically limited. Additionally, while the datasets used in this study are comprehensive, they may not cover all possible types of attacks, particularly new and emerging threats. Thus, the model's ability to generalize to entirely new attack patterns remains to be thoroughly evaluated.

6.4 Future works

Future research should focus on addressing the limitations identified in this study. This includes optimizing the VGGNet architecture for deployment in resource-constrained environments by exploring techniques such as model pruning, quantization, and efficient neural network architectures.

Additionally, expanding the dataset to include a wider variety of attack types and continuously updating it with new threat patterns will help in enhancing the model's robustness. Future work could also explore the integration of VGGNet with other machine learning techniques, such as ensemble methods, to further improve detection accuracy and resilience against sophisticated attacks.

7. CONCLUSION

This study demonstrates the effectiveness of VGGNet developing competent intrusion detection systems (IDSs) capable of accurately detecting malicious DoS and DDoS traffic. With an accuracy of 0.979 on the WSN-DS dataset and 0.94 on the CICDDoS-2019 dataset, we achieved higher performance by utilizing the strengths of the VGGNet architecture. This high degree of accuracy highlights how deep learning models, such as VGGNet, may greatly improve the resilience and dependability of IDS in defending contemporary network infrastructures against changing cyberthreats.

Our comprehensive evaluation highlights several key advantages of using VGGNet for IDS in wireless sensor networks (WSNs), including its ability to automate feature extraction, handle large-scale data efficiently, and maintain high detection accuracy even in resource-constrained environments. These characteristics make VGGNet a promising solution for real-world applications where robust and scalable security measures are critical.

The implications of our findings extend beyond the immediate context of WSNs. The principles and techniques demonstrated in this study can be adapted and applied to other types of networks and environments, contributing to the broader field of network security. By adopting advanced deep learning methodologies, organizations can improve their defensive capabilities against a wide range of cyber threats, enhancing overall network resilience.

Despite the promising results, our study also identified several areas for future research. Addressing the computational complexity of deep learning models remains a priority, particularly in optimizing VGGNet for deployment in resource-constrained environments. Exploring techniques such as model pruning, quantization, and efficient neural network architectures will be essential to further enhance the model's applicability and performance.

Additionally, expanding the dataset to include a wider variety of attack types and continuously updating it with new threat patterns will help in enhancing the model's robustness. Future work could also explore the integration of VGGNet with other machine learning techniques, such as ensemble methods, to further improve detection accuracy and resilience against sophisticated attacks.

In conclusion, this study highlights the potential of VGGNet and similar deep learning models to transform

the landscape of intrusion detection. By continuously improving and adapting these models, we can ensure that IDSs remain effective in protecting critical network infrastructures from increasingly sophisticated cyber threats. The advancements presented in this research pave the way for more secure and resilient network systems, capable of withstanding the challenges posed by the ever-evolving cyber threat landscape.

Acknowledgment: I would like to express my deepest gratitude to all the contributors of this paper.

References:

- Almomani, I., Al-Kasasbeh, B., & Al-Akhras, M. (2016). WSN-DS: A dataset for intrusion detection systems in wireless sensor networks. *Journal of Sensors*, 2016, Article 4731953. <https://doi.org/10.1155/2016/4731953>
- Amato, G., Carrara, F., Falchi, F., Gennaro, C., Meghini, C., & Vairo, C. (2017). Deep learning for decentralized parking lot occupancy detection. *Expert Systems with Applications*, 72, 327–334. <https://doi.org/10.1016/j.eswa.2016.10.055>
- Amato, G., Carrara, F., Falchi, F., Gennaro, C., & Vairo, C. (2018). Facial-based intrusion detection system with deep learning in embedded devices. In *Proceedings of the 2018 International Conference on Sensors, Signal and Image Processing* (pp. 64–68). Association for Computing Machinery. <https://doi.org/10.1145/3290589.3290598>
- Amato, G., Falchi, F., Gennaro, C., & Vairo, C. (2018, April 22). A comparison of face verification with facial landmarks and deep features. In *Proceedings of the 2018 International Conference on Computer Vision and Pattern Recognition*. (No publisher specified).
- Ayoub, A. N. (2019). Lightweight secure scheme for IoT-cloud convergence based on elliptic curve. *Journal of Theoretical and Applied Information Technology*, 97(1), 144–155.
- Ayoub, A. N. (2020). A lightweight secure CoAP for IoT-cloud paradigm using elliptic-curve cryptography. *Indonesian Journal of Electrical Engineering and Computer Science*, 17(3), 1460–1470.
- Azam, Z., Islam, M. M., & Huda, M. N. (2023). Comparative analysis of intrusion detection systems and machine learning-based model analysis through decision tree. *IEEE Access*, 11, 80348–80391. <https://doi.org/10.1109/ACCESS.2023.3296444>
- Baraneetharan, E. (2020). Role of machine learning algorithms intrusion detection in WSNs: A survey. *Journal of Information Technology and Digital World*, 2(3), 161–173.
- Bay, S. D., Kibler, D., Pazzani, M. J., & Smyth, P. (2000). The UCI KDD archive of large data sets for data mining research and experimentation. *SIGKDD Explorations Newsletter*, 2(2), 81–85. <https://doi.org/10.1145/380995.381030>
- Du, X., Sun, Y., Song, Y., Sun, H., & Yang, L. (2023). A comparative study of different CNN models and transfer learning effect for underwater object classification in side-scan sonar images. *Remote Sensing*, 15(3), Article 593. <https://doi.org/10.3390/rs15030593>
- Feng, S., Zhao, L., Shi, H., Wang, M., Shen, S., & Wang, W. (2023). One-dimensional VGGNet for high-dimensional data. *Applied Soft Computing*, 135, Article 110035. <https://doi.org/10.1016/j.asoc.2023.110035>
- Girshick, R., Donahue, J., Darrell, T., & Malik, J. (2016). Region-based convolutional networks for accurate object detection and segmentation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 38(1), 142–158. <https://doi.org/10.1109/TPAMI.2015.2437384>
- Jin, L., Niu, Q., Hou, H., Xian, H., Wang, Y., & Shi, D. (2012). Driver cognitive distraction detection using driving performance measures. *Discrete Dynamics in Nature and Society*, 2012, Article 432634. <https://doi.org/10.1155/2012/432634>
- Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). ImageNet classification with deep convolutional neural networks. In *Advances in Neural Information Processing Systems* (Vol. 25). Neural Information Processing Systems Foundation. https://proceedings.neurips.cc/paper_files/paper/2012/hash/c399862d3b9d6b76c8436e924a68c45b-Abstract.html
- Kuttila, M., Jokela, M., Markkula, G., & Rue, M. R. (2007). Driver distraction detection with a camera vision system. In *2007 IEEE International Conference on Image Processing* (Vol. 6, pp. VI-201–VI-204). IEEE. <https://doi.org/10.1109/ICIP.2007.4379556>
- Li, Z., Li, F., Zhu, L., & Yue, J. (2020). Vegetable recognition and classification based on improved VGG deep learning network model. *International Journal of Computational Intelligence Systems*, 13(1), 559–564. <https://doi.org/10.2991/ijcis.d.200425.001>

- Maseer, Z., Yusof, R., Mostafa, S., Bahaman, N., Musa, O., & Ali, B. (2021). DeepIoT.IDS: Hybrid deep learning for enhancing IoT network intrusion detection. *Computers, Materials & Continua*, 69(3), 3945–3966. <https://doi.org/10.32604/cmc.2021.016074>
- M.Tech Scholar, Kaur, G., Kumar, D., & Professor, Department of Computer Science and Engineering, Guru Jambheshwar University of Science & Technology, Hisar, India. (2020). Classification of intrusion using artificial neural network with GWO. *International Journal of Engineering and Advanced Technology*, 9(4), 599–606. <https://doi.org/10.35940/ijeat.D7597.049420>
- Psychogyios, K., Papadakis, A., Bourou, S., Nikolaou, N., Maniatis, A., & Zahariadis, T. (2024). Deep learning for intrusion detection systems (IDSs) in time series data. *Future Internet*, 16(3), Article 73. <https://doi.org/10.3390/fi16030073>
- Ravindaran, R., N, K., S, P., B, A., Sp, G., K, D., & S, A. (2023). Performance analysis of a VGG based deep learning model for classification of weeds and crops. In *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1–5). IEEE. <https://doi.org/10.1109/ICCCNT56998.2023.10307169>
- Shah, S. R., Qadri, S., Bibi, H., Shah, S. M. W., Sharif, M. I., & Marinello, F. (2023). Comparing Inception V3, VGG 16, VGG 19, CNN, and ResNet 50: A case study on early detection of a rice disease. *Agronomy*, 13(6), Article 1633. <https://doi.org/10.3390/agronomy13061633>
- Sharafaldin, I., Lashkari, A. H., Hakak, S., & Ghorbani, A. A. (2019). Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy. In *2019 International Carnahan Conference on Security Technology (ICCST)* (pp. 1–8). IEEE. <https://doi.org/10.1109/CCST.2019.8888419>
- Tsimenidis, S., Lagkas, T., & Rantos, K. (2021). Deep learning in IoT intrusion detection. *Journal of Network and Systems Management*, 30(1), Article 8. <https://doi.org/10.1007/s10922-021-09621-9>
- Vadicamo, L., Carrara, F., Cimino, A., Cresci, S., Dell'Orletta, F., Falchi, F., & Tesconi, M. (2017). Cross-media learning for image sentiment analysis in the wild. In *2017 IEEE International Conference on Computer Vision Workshops (ICCVW)* (pp. 308–317). IEEE. <https://doi.org/10.1109/ICCVW.2017.45>

Hajar Fares

Equipe of Telecommunication and Detection,
Faculty of Science,
Abdelmalek Essaadi University,
Tetouan,
Morocco
professeurhajar@gmail.com
ORCID 0009-0006-1070-8290

Zahra Oughannou

Ibn Tofail University,
Kenitra,
Morocco
oughannou.zahra@gmail.com
ORCID 0000-0002-6305-2794

Oussama Hamal

SI2M Laboratory, INSEA,
National School of Architecture
ENAM Marrakech,
Morocco
hamal.oussama@gmail.com
ORCID 0000-0002-4384-3927

Zakaria Elrhadiouini

Ibn Tofail University,
Kenitra,
Morocco
elrhadiouini.zakaria@gmail.com

Abderrahmane Hajraoui

Ibn Tofail University,
Kenitra,
Morocco
elrhadiouini.zakaria@gmail.com
ORCID 0000-0002-1647-0117
