e-ISSN: 2582-5208

International Research Journal of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

WIFI GLOBIN

Akash Shamrao Doltade*1, Krishnendhu PG*2, Lakshmika Unnikrishnan*3, Maneesh KM*4, Linny Sunny*5

*1,2,3,4Student, Department Of Computer Science And Engineering, IES College Of Engineering, Thrissur, Kerala, India.

*5Asst. Prof.. At Department Of Computer Science And Engineering, IES College Of Engineering, Thrissur, Kerala, India.

ABSTRACT

An intrusion detection system (IDS) tailored for Wireless Sensor Networks (WSNs) by leveraging Convolutional Neural Networks (CNNs) combined with ANOVA-based feature selection. WSNs are particularly susceptible to various security threats that can disrupt their operation, making efficient intrusion detection essential for maintaining network integrity. The system begins by collecting network traffic data, including packet details and routing information, and employs ANOVA to select the most relevant features that distinguish between normal and attack traffic. This feature selection process reduces data complexity and improves the model's processing efficiency.

Subsequently, the CNN is trained to recognize patterns indicative of attacks, utilizing layers that include convolutions for feature extraction, activation functions for non-linear transformations, and pooling layers for dimensionality reduction. The output is processed through fully connected layers for the final classification of network traffic as either normal or malicious. The model is evaluated using performance metrics such as accuracy, precision, recall, and F1-score to ensure reliable detection capabilities. Once deployed, the IDS monitors traffic in real-time, issuing alerts for potential intrusions and enabling timely response. The system's periodic retraining feature allows it to adapt to new types of attacks and evolving network behaviors, ensuring continued effectiveness. This project aims to create a scalable, accurate, and resource-efficient IDS for WSNs, enhancing network security through advanced pattern recognition and feature selection techniques.

I. INTRODUCTION

In wireless sensor networks (WSNs), Intrusion Detection Systems (IDS) play a crucial role in identifying and mitigating unknown or unidentified attacks that aim to disrupt or compromise the network's functionality. These attacks may target the network's ability to collect, process, and transmit data, thereby preventing it from performing its intended tasks. The proposed system leverages Convolutional Neural Networks (CNNs), a powerful deep learning technique, combined with ANOVA (Analysis of Variance) feature selection to detect such attacks. CNNs are utilized to automatically learn complex patterns in the network traffic data, making it highly effective in identifying both known and unknown attacks. Meanwhile, ANOVA feature selection is employed to identify the most significant features from the sensor data that contribute to accurate attack detection, improving the system's efficiency by reducing computational overhead and focusing on the most relevant data points. This integrated approach aims to enhance the intrusion detection accuracy and network security by effectively distinguishing between normal network behaviors and malicious activities.

II. LITERATURE SURVEY

The work of P. Sinha, V.K. Jha, A.K. Rai, and B. Bhushan in this paper offers a systematic review of security threats and defenses in wireless sensor networks, structured around the OSI model. It is a valuable resource for those researching WSN security and looking for an overview of the vulnerabilities and countermeasures at each OSI layer.[1]

L. Fernandez Miamo et al. present a novel approach for anomaly detection in 5G networks using a self-adaptive deep learning-based system. Their method enhances the detection of various network anomalies in real-time, offering significant improvements over traditional methods. The system's self-adaptivity makes it suitable for the dynamic nature of 5G, positioning it as an essential tool for maintaining the performance, security, and reliability of next-generation networks. [2]

S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo provide a significant contribution to IoT security with their proposed lightweight IDS. This system effectively balances the need for intrusion detection with the constraints of IoT devices, offering a scalable and efficient solution to enhance the security of resource-constrained networks. Their work is particularly relevant in the context of the growing number of connected IoT devices, where maintaining security without compromising performance is critical. [3]

A. N. Iman and T. Ahmad present a method to improve Intrusion Detection Systems (IDS) by leveraging Boruta for feature selection and optimizing Random Forest parameters. Their approach leads to a more accurate and efficient IDS, better equipped to detect a wide range of intrusions. This work contributes to the field of cybersecurity by providing a more robust solution for protecting networks from malicious activities while addressing the challenges of data complexity and model performance. [4].

Vishal Choudhary proposes an innovative intrusion detection technique for Wireless Sensor Networks that leverages frequency analysis to identify anomalies and potential attacks. The approach is designed to be efficient, addressing the resource constraints inherent in WSNs while providing effective intrusion detection. This paper contributes to the field of WSN security by offering a lightweight, scalable, and adaptive solution that can improve the protection of these networks against a wide range of malicious activities. [5]

Jayasree Agarkhed introduces an innovative machine learning-based technique for intrusion detection in Wireless Sensor Networks. By applying both supervised and unsupervised learning methods, the paper offers a flexible and adaptive solution that improves the detection of network intrusions while being mindful of the limited resources in WSNs. This work contributes to the growing body of research aimed at enhancing the security and resilience of WSNs through intelligent, data-driven approaches.. [6]

M.P. Singh presents an anomaly-based Intrusion Detection System (IDS) for Wireless Sensor Networks (WSNs**)** that effectively detects abnormal network behaviors and potential intrusions. The paper provides a practical solution to the security challenges faced by WSNs, particularly in detecting novel attacks without significant computational overhead. The proposed system is lightweight and adaptive, making it a suitable solution for the resource-constrained and dynamic nature of WSNs.. [7]

Rabah Attia presents a novel hierarchical anomaly-based intrusion detection and localization system designed for IoT networks. The proposed system improves both intrusion detection accuracy and resource efficiency by using a multi-layered detection approach, where local devices handle basic anomaly detection and higher-level aggregators process more complex patterns. The addition of localization techniques allows the system to pinpoint the source of the intrusion, enhancing the overall security and responsiveness of IoT networks. This work provides a scalable and efficient solution to the growing security challenges in IoT environments, making it highly relevant for a wide range of IoT applications..[8]

Patrick Vanin, Thomas Newe, Lubna Luxmi Dhirani, Eoin O'Connell, Donna O'Shea, Brian Lee, and Muzaffar Rao explore the application of Artificial Intelligence (AI) and Machine Learning (ML) techniques in the design and implementation of Network Intrusion Detection Systems (NIDS). The authors provide a comprehensive study of how AI/ML methods are being integrated into NIDS to enhance the detection and prevention of cyberattacks, particularly in the context of evolving network threats. [9]

J. Jabez and B. Muthukumar propose an Intrusion Detection System (IDS) that uses outlier detection for anomaly detection. Their approach identifies abnormal network behaviors that could indicate intrusions, offering a way to detect unknown attacks. The paper emphasizes the advantages of anomaly-based detection over signature-based methods, particularly in detecting new threats. The authors discuss the effectiveness of their proposed method, highlighting its ability to reduce false positives and maintain high accuracy in detecting intrusions. [10]

Mohit Tiwari, Raj Kumar, Akash Bharti, and Jai Kisha discuss the development and implementation of an Intrusion Detection System (IDS). The authors focus on how IDS can be used to monitor and detect unauthorized access or malicious activities in computer networks. They review various IDS techniques, including signature-based and anomaly-based methods, and highlight the importance of IDS in enhancing network security by identifying potential threats in real-time. The paper also examines the challenges and solutions in designing effective IDS for modern network environments. [11].

Ansam Khraisat and Ammar Alazab provide a critical review of Intrusion Detection Systems (IDS) in the context of the Internet of Things (IoT). They analyze various IDS techniques, deployment strategies, and validation approaches used in IoT environments. The authors discuss the types of cyberattacks targeting IoT devices and networks, along with the public datasets commonly used for IDS evaluation. They also highlight key challenges in implementing IDS for IoT, such as resource constraints, scalability, and the evolving nature of threats. The paper offers valuable insights into the state-of-the-art in IoT security and the gaps that need to be addressed for more effective intrusion detection in IoT networks.. [12]

Zeeshan Ahmad, Adnan Shahid Khan, Cheah Wai Shiang, and Johari Abdullah conduct a systematic study of Machine Learning (ML) and Deep Learning (DL) approaches used in Network Intrusion Detection Systems (NIDS). The authors review various ML and DL techniques applied to detect network intrusions, comparing their effectiveness in identifying threats such as cyberattacks and unauthorized access. They focus on how these advanced methods can improve the accuracy and efficiency of intrusion detection systems over traditional methods. The paper also discusses challenges, datasets, and the future direction of applying AI-based approaches to enhance NIDS for modern network security.[13]

Melad Mohammed Issa, Mohammad Aljanabi, and Hassan M. Muhialdeen provide a systematic literature review on Intrusion Detection Systems (IDS). They examine the latest research trends, algorithms, and methods used in IDS, focusing on the various approaches applied to detect network intrusions. The paper highlights the most commonly used datasets for evaluating IDS performance and discusses the limitations of current IDS technologies, such as high false positive rates, scalability issues, and the challenge of detecting new and sophisticated attacks. The authors also offer insights into future directions for IDS research, aiming to improve accuracy, efficiency, and adaptability in the face of evolving cybersecurity threats. [14]

Amir Andalib and Vahid Tabataba Vakili propose an autonomous intrusion detection system (IDS) that leverages an ensemble of advanced machine learning models to detect network intrusions. The authors focus on improving detection accuracy and minimizing false positives by combining the strengths of multiple learning algorithms. The proposed system uses an ensemble approach to enhance the IDS's ability to adapt to new and evolving threats, ensuring robust performance in real-time network environments. The paper demonstrates how this ensemble method outperforms individual models, offering a promising solution for more effective network security. [15]

III. METHODOLOGY

3.1 Methodological Review

The methodology for developing an Intrusion Detection System (IDS) using Convolutional Neural Networks (CNN) with ANOVA feature selection for Wireless Sensor Networks (WSNs) involves the following detailed steps:

3.1.1. Data Collection and Preprocessing

Dataset Selection: Gather or create a dataset that reflects both normal network traffic and various types of intrusions in WSNs.

Data Preprocessing: Clean the dataset by handling missing values, normalizing the data for uniformity, and converting any categorical variables into numerical formats.

Data Splitting: Divide the dataset into training, validation, and test sets for training the model, tuning hyperparameters, and evaluating performance.

3.1.2. Feature Selection using ANOVA

ANOVA (Analysis of Variance): This statistical technique is used to select the most significant features from the dataset, which helps reduce dimensionality and focuses on features that impact the detection outcome.

Feature Scoring: Score each feature based on its statistical relevance to the target variable (i.e., intrusion detection), and retain the most significant ones.

Feature Extraction: Extract and prepare the selected features for input into the CNN model.

3.1.3. CNN Model Design and Training

Architecture Design: Create a CNN architecture with multiple convolutional layers followed by pooling layers to learn spatial hierarchies of features.

Convolutional Layers: Apply filters to the input data to extract features and patterns.

Activation Function: Use non-linear activation functions like ReLU (Rectified Linear Unit) to introduce non-linearity.

Pooling Layers: Use max pooling or average pooling to reduce the dimensions of the data, improving computational efficiency and generalization.

Fully Connected Layers: Connect the learned features to dense layers that classify them into normal or attack categories.

Output Layer: Use a softmax or sigmoid activation function for the final classification output.

Training Process: Train the model using the training dataset and monitor its performance with the validation set. Adjust hyperparameters such as learning rate and batch size as needed.

Loss Function and Optimization: Employ cross-entropy loss for classification and use optimizers like Adam or stochastic gradient descent (SGD) to minimize loss.

3.1.4. Model Evaluation

Testing: Evaluate the trained CNN on the test set to measure its performance using metrics like accuracy, precision, recall, F1-score, and confusion matrix.

Result Analysis: Analyze the results to ensure the model meets desired benchmarks for detecting intrusions. Make iterative improvements as necessary by adjusting model parameters or re-examining feature selection.

3.1.5. Deployment and Monitoring

Deployment: Implement the IDS within the WSN infrastructure for real-time traffic monitoring.

Continuous Monitoring: Continuously monitor network activity and flag suspicious patterns for potential intrusions. Periodically retrain the model with new data to improve its adaptability.

Performance Assessment: Regularly check the system’s detection performance to maintain a high detection rate and low false positive rate.

IV. RESULT AND DISCUSSION

The model's effectiveness is demonstrated through metrics such as accuracy, precision, recall, and F1-score, which collectively provide a comprehensive view of its classification capabilities. The use of ANOVA-based feature selection significantly enhances the model's efficiency by ensuring that only the most relevant features are processed, thereby reducing computational overhead and improving processing speed. This is particularly important for WSNs, where resource constraints such as limited processing power and energy consumption must be managed carefully.

The CNN-based model shows high accuracy in detecting various types of attacks, indicating its strong capability in recognizing complex patterns in network traffic. Precision and recall values highlight the model's ability to not only detect attacks with minimal false positives but also ensure that actual threats are identified with low false-negative rates. The F1-score, which balances precision and recall, reflects the model's reliability in maintaining this trade-off. These results underscore the model's robustness in distinguishing between normal and malicious network behavior.

During testing, the proposed IDS effectively handled real-time data, demonstrating its applicability for continuous network monitoring. The system's ability to alert administrators in the event of suspicious activity adds an extra layer of security, enabling rapid response to potential intrusions. Additionally, discussions may touch on the adaptability of the model; its architecture supports periodic retraining, allowing it to incorporate new attack patterns and evolving network behaviors, which is critical for maintaining its relevance over time.

Sl.no	Title	Methods	Description
1.	A Systematic Review of Security Threats and Defenses in Wireless Sensor Networks	OSI Model Framework, Security Threats & Defenses	Review of security threats and defenses in WSN, structured around the OSI model, highlighting vulnerabilities and countermeasures at each layer.
2.	Anomaly Detection in 5G Networks Using Self-Adaptive Deep Learning-Based System	Deep Learning, Self-Adaptive Systems	Proposes a self-adaptive deep learning-based system for real-time anomaly detection in 5G networks, improving detection capabilities over traditional methods.
3.	Lightweight IDS for IoT Security	Lightweight IDS, Resource-Constrained Devices	Introduces a lightweight IDS tailored for IoT, balancing security with the constraints of IoT devices, offering scalability and efficiency for large networks of connected devices.
4.	Improvement of IDS Using Boruta and Random Forest Optimization	Feature Selection (Boruta), Random Forest	Enhances IDS performance by using Boruta for feature selection and optimizing Random Forest parameters, improving intrusion detection accuracy and efficiency.
5.	Frequency Analysis-Based IDS for Wireless Sensor Networks	Frequency Analysis	Proposes an IDS for WSNs based on frequency analysis, efficiently identifying anomalies and potential attacks while addressing WSN resource constraints.
6.	Machine Learning-Based IDS for Wireless Sensor Networks	Supervised & Unsupervised Learning	Introduces a hybrid machine learning technique for intrusion detection in WSN, using both supervised and unsupervised methods to adapt and detect network intrusions efficiently.
7.	Anomaly-Based IDS for Wireless Sensor Networks	Anomaly Detection	Proposes an anomaly-based IDS for WSNs, effectively detecting abnormal network behaviors and intrusions with minimal computational overhead.
8.	Hierarchical Anomaly-Based IDS for IoT Networks	Hierarchical Anomaly Detection, Localization	Proposes a hierarchical IDS for IoT networks, improving detection accuracy and resource efficiency, with added localization to pinpoint the source of intrusions.
9.	AI/ML for Network Intrusion Detection Systems	Artificial Intelligence, Machine Learning	Reviews the use of AI/ML techniques in NIDS to enhance the detection and prevention of

			cyberattacks, focusing on evolving network threats.
10.	Outlier Detection for Anomaly Detection in IDS	Outlier Detection, Anomaly Detection	Proposes an IDS based on outlier detection for identifying abnormal behaviors and detecting unknown attacks, emphasizing reduced false positives.

V. REFERENCES

[1] P. Sinha, V.K. Jha, A.K. Rai, B. Bhushan. A Systematic Review of Security Threats and Defenses in Wireless Sensor Networks.

[2] L. Fernandez Miamo et al. Anomaly Detection in 5G Networks Using Self-Adaptive Deep Learning-Based System.

[3] S. U. Jan, S. Ahmed, V. Shakhov, I. Koo. Lightweight IDS for IoT Security.

[4] A. N. Iman, T. Ahmad. Improvement of IDS Using Boruta and Random Forest Optimization.

[5] Vishal Choudhary. Frequency Analysis-Based IDS for Wireless Sensor Networks.

[6] Jayasree Agarkhed. Machine Learning-Based IDS for Wireless Sensor Networks.

[7] M.P. Singh. Anomaly-Based IDS for Wireless Sensor Networks.

[8] Rabah Attia. Hierarchical Anomaly-Based IDS for IoT Networks.

[9] Patrick Vanin, Thomas Newe, Lubna Luxmi Dhirani, Eoin O'Connell, Donna O'Shea, Brian Lee, Muzaffar Rao. AI/ML for Network Intrusion Detection Systems.

[10] J. Jabez, B. Muthukumar. Outlier Detection for Anomaly Detection in IDS.

[11] Mohit Tiwari, Raj Kumar, Akash Bharti, Jai Kisha. Development and Implementation of IDS for Network Security.

[12] Ansam Khraisat, Ammar Alazab. Critical Review of IDS for IoT Networks.

[13] Zeeshan Ahmad, Adnan Shahid Khan, Cheah Wai Shiang, Johari Abdullah. Systematic Study of ML/DL in Network Intrusion Detection Systems.

[14] Melad Mohammed Issa, Mohammad Aljanabi, Hassan M. Muhialdeen. Literature Review on IDS Trends and Challenges.

[15] Amir Andalib, Vahid Tabataba Vakili. Autonomous IDS Using Ensemble of Advanced Learners.