ISSN: 2945-4565 VOL 05, ISSUE 02, 2026

Ai-Driven Intrusion Detection System for Enhancing Real-Time Cybersecurity

Chibubi Christopher*
Dmi St. Eugene University.

Abstract

This study explored the use of Artificial Intelligence and Machine Learning techniques for intrusion detection in network security. Four benchmark datasets — NSL-KDD, UNSW-NB15, CICIDS2017, and ToN_IoT — were used to analyze and compare the performance of different machine learning and deep learning models. Models such as Random Forest, Logistic Regression, SVM, k-NN, Decision Tree, MLP, and LSTM were trained for both binary and multiclass classification tasks. Results showed high accuracy in binary attack detection, especially with Random Forest and LSTM models, while multiclass classification faced challenges due to class imbalance and rare attack types. The study concluded that AI-based IDS systems are effective for network security, and that feature engineering, dimensionality reduction, and hybrid learning methods can further improve detection performance and efficiency.

Keywords: Artificial Intelligence, Intrusion Detection System, Machine Learning, Network Security, Deep Learning, Cybersecurity, Anomaly Detection, Random Forest, LSTM, Multiclass Classification.

1. INTRODUCTION

Background of the study

The rapid expansion of digital networks has led to an unprecedented rise in cyber threats, making network security a critical area of concern for organizations worldwide. Cybersecurity threats are becoming increasingly sophisticated, with attackers leveraging advanced techniques to infiltrate systems, disrupt operations, and exfiltrate sensitive data. With the proliferation of cloud computing, the Internet of Things (IoT), and distributed architectures, the attack surface has widened, exposing organizations to new vulnerabilities and risks (Drewek-Ossowicka et al., 2020). Consequently, traditional security mechanisms such as firewalls, antivirus software, and intrusion prevention systems are no longer sufficient to detect and mitigate emerging threats effectively.

Intrusion Detection Systems (IDS) have been developed as a crucial component of cybersecurity to monitor network activity and detect malicious behavior in real time. IDS solutions are broadly classified into signature-based and anomaly-based detection systems (Manori, 2024). Signature-based IDS rely on known attack signatures and patterns to identify intrusions, making them highly effective against previously documented threats but ineffective against zero-day attacks (Naveed et al., 2022). In contrast, anomaly-based IDS focus on identifying deviations from established network behavior, allowing them to detect novel threats. However, traditional anomaly detection methods of ten suffer from high false positive rates, leading to inefficiencies and increased workload for cyber security analysts (Sandosh and Kodipyaka, 2023).

Artificial Intelligence (AI) techniques have emerged as transformative solutions to enhance

ISSN: 2945-4565 VOL 05, ISSUE 02, 2026

the effectiveness of IDS. AI-powered IDS leverage machine learning algorithms to analyze vast amounts of network traffic data, detect anomalies, and identify malicious activity with higher accuracy than conventional methods (Vinayakumar et al., 2019). By using historical attack data to train models, AI- based IDS can learn from previous incidents, enabling them to predict and detect emerging threats proactively. The integration of AI into IDS presents significant opportunities for improving cybersecurity, reducing false positives, and automating threat detection and response mechanisms.

Problem Statement

Despite advancements in cybersecurity, organizations continue to struggle with detecting and responding to sophisticated cyber threats in real-time. Traditional IDS face several limitations, including high false positive rates, limited adaptability to evolving attack strategies, and reliance on pre- defined signatures that do not account for unknown threats. These challenges have led to increased interest in AI-driven solutions that leverage machine learning to enhance IDS effectiveness. How- ever, AI-based IDS are not without challenges.

One major issue is the computational cost associated with training and deploying deep learning models, which can hinder real-time threat detection in resource-constrained environments (Chowdhury et al., 2020). Additionally, machine learning models require large and diverse datasets for effective training, and their accuracy is highly dependent on feature selection and data preprocessing techniques. Another significant concern is adversarial machine learning, where attackers manipulate input data to evade detection, potentially rendering AI-based IDS ineffective (Biggio & Roli, 2018). Furthermore, explainability and interpretability remain critical challenges, as AI-driven security solutions often operate as "black-box" models, making it difficult for analysts to understand their decision-making processes. This research seeks to address these challenges by developing AI-powered IDS models that optimize detection accuracy while minimizing computational overhead and false positive rates. It also aims to explore methods for improving the interpretability of AI-driven security solutions to enhance trust and adoption in practical cybersecurity environments.

Research Objectives

1. The primary objective of this study is to investigate the role of AI in enhancing IDS and to develop machine learning models capable of detecting unusual patterns in network traffic with high accuracy. The specific objectives of the research are:
2. To examine existing AI-based intrusion detection methodologies and assess their effective- ness in cybersecurity.
3. To analyze machine learning models commonly used for intrusion detection, focusing on supervised, unsupervised, and hybrid approaches.
4. To evaluate the impact of feature engineering and selection techniques on IDS performance.
5. To explore the integration of AI-powered IDS with traditional cybersecurity frameworks and assess their compatibility.
6. To investigate key challenges such as adversarial machine learning and propose strategies to enhance model robustness.
7. To critically assess the performance of AI-based IDS using standard evaluation metrics, including accuracy, precision, recall, F1-score, and ROC-AUC.

Significance of the Study

The increasing frequency and sophistication of cyber threats necessitate advanced security

ISSN: 2945-4565 VOL 05, ISSUE 02, 2026

mechanisms that go beyond traditional intrusion detection methods. This study is significant as it provides insights into how AI can be leveraged to enhance IDS, improving their accuracy and adaptability to emerging threats. By analyzing AI-powered IDS models, this research contributes to cybersecurity innovation, offering practical solutions that organizations can implement to strengthen their net- work defenses. The findings of this study will benefit various stakeholders, including cybersecurity professionals, IT security managers, and researchers. For cybersecurity professionals, AI-driven IDS can serve as a powerful tool for threat detection and mitigation, reducing manual workload and response time. IT security managers can use the research findings to implement AI-based security solutions that improve organizational resilience against cyber threats. Additionally, researchers in AI and cybersecurity can build upon this study to explore new methodologies for enhancing IDS performance and addressing emerging challenges in adversarial machine learning and model interpretability.

Scope and Limitations

This research focuses on the analysis and evaluation of AI-based IDS using publicly available network traffic datasets, such as CICIDS2017 and UNSW-NB15. The study involves reviewing and assessing machine learning models for intrusion detection, conducting simulations to analyze their performance, and exploring their effectiveness in detecting cyber threats. The research does not involve developing or deploying a live IDS in a real-world network environment but instead relies on theoretical and experimental evaluations.

While various machine learning approaches will be explored, the study will primarily focus on supervised learning, unsupervised learning, and hybrid methods. The computational efficiency of the analyzed models will be considered; however, due to hardware limitations, extensive deep learning architectures requiring high-performance computing resources may not be fully implemented. Additionally, this research acknowledges the challenges associated with adversarial attacks on AI models and model explainability but does not provide a full implementation of adversarial defenses or interpretability frameworks.

Theoretical and Conceptual Foundations of Ai-Powered Intrusion Detection Systems

Introduction

The increasing sophistication and frequency of cyber threats have rendered traditional cybersecurity measures insufficient in defending modern digital infrastructures (Ahmad et al., 2022). Among these threats, network intrusions stand out for their potential to disrupt systems, compromise sensitive information, and cause significant economic losses. To combat this growing menace (Aldar-wbi et al., 2022), Intrusion Detection Systems (IDS) have become indispensable tools in the cyber- security landscape. However, traditional IDS, particularly signature-based models, have exhibited serious limitations in adapting to new and emerging threats (Ahmad et al., 2020). The integration of Artificial Intelligence (AI)**,** especially Machine Learning (ML)**,** has emerged as a promising approach to enhancing the adaptability, accuracy, and efficiency of IDS (Dina et al., 2021).

Conceptual Foundations OF AI in Cybersecurity

The convergence of artificial intelligence and cybersecurity has led to a transformative shift in how cyber threats are detected, analyzed, and mitigated. Several authors have contributed theoretical and practical insights that lay the foundation for AI-powered IDS.

One foundational work is *Artificial Intelligence for Cybersecurity: Techniques, Challenges, and Advances* by Mark Stamp (2020), which provides an extensive overview of AI's role in transforming cybersecurity, particularly in intrusion detection. Stamp's book is significant for outlining the evolution from rule-based systems to AI-enabled frameworks, highlighting key

ISSN: 2945-4565 VOL 05, ISSUE 02, 2026

machine learning algorithms such as Support Vector Machines (SVM), Artificial Neural Networks (ANN), and Deep Learning models like Convolutional Neural Networks (CNN). These models form the theoretical core of many modern IDS systems. While the text successfully bridges theoretical AI concepts with cybersecurity needs, it lacks in-depth discussion on real-world deployment strategies, which limits its applicability for practitioners.
In contrast, *Machine Learning for Cybersecurity Cookbook* by Tsukerman (2019) emphasizes hands- on implementation, using real code and practical examples to show how AI techniques are applied to detect anomalies and adversarial behaviors in networks. Tsukerman contributes valuable insight into model evaluation, dataset preparation, and performance tuning. However, his work leans more toward the technical application than conceptual discourse, making it more of a practitioner's guide than a theoretical resource.
Similarly, Alazab and Awad's (2019) *Deep Learning Applications for Cybersecurity* explores advanced architectures such as auto encoders, LSTM networks, and Generative Adversarial Networks (GANs), providing a rich theoretical basis for understanding how deep learning models can enhance anomaly detection. The book also examines feature engineering, a critical aspect of model performance, although it assumes the reader already has significant prior knowledge in deep learning.
Bhushan's *Cybersecurity and Artificial Intelligence* (2021) adds a valuable ethical and philosophical dimension to the discussion. This work covers reinforcement learning, threat intelligence, and the use of Natural Language Processing (NLP) in cybersecurity, offering a broader conceptual under- standing. The inclusion of legal and ethical implications adds depth to the theoretical framework, bridging technical innovation with societal accountability.
Finally, *Artificial Intelligence and Cyber Security: A Hands-On Approach* by Parisi (2020) provides a balanced view by integrating theory with practical deployment. It highlights the use of real-world datasets like CICIDS2017 and UNSW-NB15 and explores explainable AI (XAI) tools such as SHAP and LIME. These tools address a key conceptual challenge in cybersecurity—interpretability—which is crucial for trust and transparency in AI-driven systems.

Theoretical Framework of Intrusion Detection Systems (IDS)

An Intrusion Detection System (IDS) is a crucial cybersecurity mechanism designed to monitor, analyze, and respond to network traffic anomalies that may indicate malicious activities (Smithie, 2023). These systems play a significant role in identifying unauthorized access attempts, insider threats, malware infections, and sophisticated cyberattacks such as Advanced Persistent Threats (APTs). As cyber threats continue to evolve, IDS solutions have become increasingly important in safeguarding network infrastructures and ensuring business continuity. IDS solutions can be broadly categorized into two primary types: signature-based IDS and anomaly-based IDS (Tidjon et al., 2019). Each approach has unique strengths and weaknesses, making them suitable for different security scenarios.

Signature-Based IDS

Rooted in deterministic logic, signature-based IDS operate on the principle of pattern matching, wherein known threat signatures are stored in databases and compared against observed network activity (Sommestad et al., 2021). This method is grounded in formal rule-based systems, which are effective at recognizing predefined patterns but are limited by their dependence on historical data. The theoretical limitation here lies in their static nature; without constant updates, they are unable to detect zero-day attacks or novel variations of existing threats (Masdari, 2020).

ISSN: 2945-4565 VOL 05, ISSUE 02, 2026

Despite these shortcomings, the signature-based model offers high precision and low false positives, which aligns with formal logic-based detection systems. However, it emphasizes reactive security rather than proactive threat anticipation, making it an incomplete solution in dynamic cyber environments (Agoramoorthy et al., 2023).

Anomaly-Based IDS

Anomaly-based systems are built on statistical modeling and machine learning principles, which classify behaviors based on deviations from a learned norm. Unlike deterministic logic, these sys- tems use probabilistic reasoning to detect deviations from expected behavior patterns . The theoretical advantage here is flexibility by training on "normal" behavior, the model can detect a wide variety of novel threats. However, anomaly-based systems are known to generate high false positive rates due to variability in legitimate user behavior

Modern anomaly-based IDS leverage unsupervised learning and time-series analysis to improve con- textual awareness and behavioral modeling. The theoretical underpinning lies in behavioral heuristics and statistical outlier detection, which make these systems more adaptable but also more com- putationally intensive.

Hybrid IDS

Given the limitations of both signature-based and anomaly-based IDS, researchers have explored that combine elements of both methods to enhance threat detection capabili- ties. Hybrid IDS leverage the strengths of signature-based detection in identifying known threats while also utilizing anomaly detection techniques to detect previously unseen attack patterns (Buczak & Guven, 2016). This combination allows organizations to benefit from the high accuracy of signature-based detection while mitigating the high false positive rates associated with anomaly- based approaches. Hybrid IDS often employ multi-layered architectures where different detection engines work collaboratively to analyze network traffic. For example, a hybrid IDS may use signature-based detection for preliminary filtering of known threats and then apply anomaly-based techniques to inspect suspicious traffic that does not match any known signatures (Sharma et al., 2024). This layered approach enhances the overall security posture by ensuring that even sophisticated cyber threats are detected before they can cause damage.

One of the major benefits of hybrid IDS is their adaptability. By continuously learning from both historical attack data and real-time network behavior, these systems can dynamically adjust their detection parameters to improve accuracy (Javaid et al., 2016). Additionally, hybrid IDS solutions can leverage advanced machine learning techniques, such as deep learning and reinforcement learning, to enhance their detection capabilities and minimize false alarms. Despite these advantages, hybrid IDS implementations also come with challenges. They require higher computational resources compared to standalone IDS solutions, making deployment in re- source-constrained environments more difficult. Moreover, managing and fine-tuning a hybrid IDS requires specialized expertise in cybersecurity and machine learning, adding complexity to the op- erational workload of security teams (Alharbi et al., 2023).

Intrusion Prevention Systems (IPS) vs. Intrusion Detection Systems (IDS)

It is important to distinguish between Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). While both serve the purpose of enhancing network security, they operate differently (Abbas et al., 2023). IDS are primarily designed for passive monitoring and alerting, meaning they do not take direct action against detected threats. Instead, they notify security administrators, who then take appropriate response measures (Bharti et al., 2024). On

ISSN: 2945-4565 VOL 05, ISSUE 02, 2026

the other hand, IPS solutions actively block and mitigate threats in real time by automatically enforcing security policies and pre- venting malicious activities from compromising the network

IPS solutions are often integrated with IDS capabilities to form Intrusion Detection and Prevention Systems (IDPS), which combine real-time monitoring, detection, and automated response mecha- nisms (Coulibaly, 2020). While IPS solutions offer a proactive approach to threat mitigation, they must be carefully configured to avoid blocking legitimate traffic, which could lead to service disrup- tions. IDS solutions, on the other hand, provide valuable forensic insights by logging and analyzing network events without interfering with normal operations (Azam et al., 2023).

Theoretical Role of Artificial Intelligence in IDS

The integration of artificial intelligence (AI) into Intrusion Detection Systems (IDS) has revolutionized cybersecurity by enhancing the accuracy, adaptability, and efficiency of threat detection mechanisms. The traditional methods of intrusion detection, which relied on manually crafted rules and signatures, often fell short in identifying sophisticated and evolving cyber threats. AI, particularly through the use of machine learning (ML) and deep learning techniques, has significantly improved the detection of cyberattacks by enabling systems to learn from past incidents, recognize patterns, and adapt to emerging threats in real-time. The application of AI in IDS is brodly classified into supervised learning, unsupervised learning, and hybrid learning approaches, each of which plays a critical role in advancing the effectiveness of modern cybersecurity solutions.

Supervised Learning in Intrusion Detection

Supervised learning is a widely used approach in AI-powered IDS, leveraging labeled datasets to train models that classify network traffic as either benign or malicious. This learning paradigm relies on historical attack data, allowing the model to learn decision boundaries and make predictions based on previously observed patterns (Kumar & Garg, 2020). Several machine learning algorithms have been extensively applied to IDS, each offering distinct advantages and challenges.

One of the most commonly used algorithms in supervised learning for IDS is the Decision Tree (DT), which is a rule-based model that classifies network traffic by sequentially partitioning data according to selected features. Decision trees are computationally efficient and highly interpretable, making them valuable in cybersecurity applications. However, they tend to overfit training data, leading to poor generalization when exposed to new attack patterns. Random Forest (RF), an ensemble-based extension of decision trees, mitigates overfitting by training multiple decision trees on different sub- sets of the data and aggregating their predictions. This method improves IDS accuracy and resilience to noise while maintaining interpretability. However, its computational complexity increases with the number of trees, making it less suitable for real-time IDS applications.

Support Vector Machines (SVM), another popular supervised learning approach, is effective in high- dimensional spaces where network traffic data exhibits complex relationships. SVM models define hyperplanes that maximize the margin between benign and malicious traffic instances, enhancing classification performance. Despite their robustness, SVMs require significant computational re- sources, particularly when dealing with large-scale network datasets. Artificial Neural Networks (ANNs) have also been widely applied in IDS due to their ability to capture intricate non-linear rela- tionships in network traffic. ANNs, particularly Deep Neural Networks (DNNs), have demonstrated superior performance in detecting sophisticated cyberattacks. However, their black-box nature raises concerns regarding interpret-

ISSN: 2945-4565 VOL 05, ISSUE 02, 2026

ability, making them

Unsupervised Learning

Unsupervised learning techniques have gained traction in IDS due to their ability to detect novel and zero-day attacks without requiring predefined labels. These methods analyze network traffic by identifying deviations from established patterns, flagging anomalies that may indicate potential se- curity threats (Shone et al., 2018). Unlike supervised learning, which relies on historical attack data, unsupervised learning enables IDS to detect emerging threats autonomously.

One of the most widely used unsupervised learning techniques in IDS is clustering, which groups similar data points based on inherent structures in the dataset. k-means clustering, for example, partitions network traffic into clusters, with normal and malicious traffic forming distinct groups. While k-Means is computationally efficient, its reliance on pre-defined cluster numbers can limit its adaptability to evolving network behaviors Another effective clustering technique is Density-Based Spatial Clustering of Applications with Noise (DBSCAN), which groups network traffic based on density patterns. DBSCAN is particularly useful in IDS applications as it can detect anomalies in complex network environments (Zhang et al., 2023). However, its performance is highly dependent on the selection of hyperparameters, making it sensitive to variations in network behavior. Autoencoders, a form of deep learning, have also been explored in unsupervised IDS. These neural networks learn compact representations of normal net- work traffic and identify deviations as potential intrusions. Autoencoders have shown remarkable performance in detecting unknown attacks but require substantial computational resources for training and inference (Luo et al.,2019).

Hybrid Learning Approaches in Intrusion Detection

Hybrid learning approaches combine the strengths of supervised and unsupervised learning to create more robust IDS solutions. By leveraging the high accuracy of supervised models and the adapt-ability of unsupervised techniques, hybrid IDS can improve detection performance while mitigating the limitations of individual learning paradigms.

A common hybrid approach involves using supervised learning models to classify known threats while employing unsupervised techniques to detect anomalies that do not match predefined attack signatures. For example, an IDS may use a Random Forest classifier to detect well-documented cyber threats while utilizing an Autoencoder-based anomaly detection model to identify novel at- tacks (Javaid et al., 2016). This combination enhances IDS adaptability and reduces the risk of undetected zero-day attacks.

Another effective hybrid approach integrates semi-supervised learning, where a small amount of labeled data is used to guide the learning process of an otherwise unsupervised model. Semi-super- vised techniques have proven effective in improving IDS performance, particularly in scenarios where labeled data is scarce or expensive to obtain. Deep learning-based hybrid approaches have also been explored in IDS (Cai et al., 2023). For instance, Convolutional Neural Networks (CNNs) can be combined with Recurrent Neural Networks (RNNs) to enhance both spatial and temporal analysis of network traffic. CNNs extract spatial features, while RNNs capture sequential patterns, providing a comprehensive intrusion detection framework (Vinayakumar et al., 2019). However, such deep learning models require substantial computational resources, posing challenges in real-time deployment.

Explainable AI and Adaptive Learning

Explainable AI (XAI) tools like SHAP and LIME introduce interpretability into black-box models, ena- bling decision support and trust in AI-driven systems Theoretical models of

ISSN: 2945-4565 VOL 05, ISSUE 02, 2026

XAI are grounded in game theory and local approximation, providing post-hoc explanations for model behavior. Adaptive learning mechanisms, including reinforcement learning, allow models to update in real-time based on network feedback, enhancing long-term detection performance (Zhang et al., 2020).

2. RESEARCH PURPOSE, OBJECTIVES

Purpose of the Study

Cybercrime is also projected to inflict up to $10.5 trillion in damage annually by 2025, making the enhancement of intrusion detection and prevention capabilities more urgent (Shankar et al., 2021). Signature-based IDS use cannot match the traditional approaches as they are unable to detect new or emerging attacks that have no matching known pattern (Oluwakemi et al., 2023). Machine learn- ing algorithms in this context are able to analyze enormous volumes of network traffic data to iden- tify infinitesimal anomalies and improve detection rates continuously. The application of AI on IDS can be utilized for improving threat detection and reducing false alarms. In this regard, there exists an absolute motivation for the research of AI-based intrusion detection models that can detect anomalous patterns in network traffic beyond the capabilities of conventional methods (Park et al., 2023).

Against this backdrop, the objective of the present study is to investigate and demonstrate how machine learning models can be built to detect abnormal network traffic patterns (potential intru- sions) with high accuracy. The research is conceptual and experimental. Conceptually, it proposes an AI-based approach to network intrusion detection based on the theoretical foundations from literature. Experimentally, it involves training, developing, and testing a set of machine learning models from publicly available intrusion detection datasets. Notably, the effort is not constructing a deployed enterprise IDS, but developing and testing models under controlled circumstances with benchmark datasets (like NSL-KDD, UNSW-NB15, CICIDS2017, and ToN_IoT). These data sets pro- vide labeled examples of benign and malicious traffic and collectively span a wide range of attack types and network environments – from standard benchmark attacks to modern and IoT-based at- tacks. Using more than one open data set enables the research to thoroughly test across multiple scenarios. Briefly stated, the purpose of this study is to assist in improving IDS capabilities using a rational examination of how AI-powered models may better and more consistently identify mali- cious network behavior i.e. suspicious traffic patterns.

Research Objectives

1. To accomplish the above aim, the research sets the following specific objectives: Learn machine learning models for intrusion detection using well-known benchmark network traffic datasets (e.g., NSL-KDD, UNSW-NB15, CICIDS2017, ToN_IoT). This entails designing the model structure or selecting appropriate algorithms, and learning the models to learn normal vs. malicious traffic patterns.
2. Test and validate the performance of the built AI-based IDS models in detecting intrusions. The models will be evaluated using typical metrics such as detection accuracy, precision/re- call, and false positive rate, in order to determine their capability in detecting attacks with- out creating too many false alarms.
3. Compare different machine learning approaches and configurations in this intrusion detec- tion context for their efficacy. Through experimenting with different algorithms and using feature selection methods, the study aims to determine which approaches are best suited to detect network anomalies.

ISSN: 2945-4565 VOL 05, ISSUE 02, 2026

4. Analyze the insights for IDS optimization from there. This means examining what type of attack or traffic behavior are hardest to identify and what aspects most affect model performance. The outcomes will be utilized in making recommendations or guidelines for using AI for intrusion detection in the future.

3. CONCLUSIONS

This research proved that AI-based Intrusion Detection Systems (IDS) are highly effective in detecting cyber-attacks through machine learning techniques. By testing various models on four benchmark datasets, the study achieved high detection accuracy, especially for common attacks such as DoS/DDoS, port scanning, and brute-force attacks. The research successfully compared different machine learning and deep learning models and evaluated their performance in binary and multiclass classification tasks.

The study also highlighted challenges such as class imbalance, limited detection of rare attacks, and difficulties in model generalization across different environments. It emphasized that real-world IDS deployment requires continuous learning, proper data handling, and human oversight. Simpler models performed efficiently on structured data, while advanced models like LSTM were more effective for complex attack patterns. The research concluded that AI-powered IDS can provide reliable and accurate cybersecurity solutions when combined with explainability, privacy protection, and balanced model optimization.

4. REFERENCES

[1] Abbas, S., Naser, W., & Kadhim, A. (2023). Subject review: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). *Global Journal of Engineering and Technology Advances*. https://doi.org/10.30574/gjeta.2023.14.2.0031.

[2] Abdiyeva-Aliyeva, G., & Hematyar, M. (2022). Statistic Approached Dynamically Detecting Security Threats and Updating a Signature-Based Intrusion Detection System's Database in NGN. *Journal of Advances in Information Technology*.https://doi.org/10.12720/jait.13.5.524-529.

[3] Abdullah, M., Karim, A., Rahman, M., Hossain, M. I., & Kim, J. M. (2017). A feature selection method for intrusion detection system based on PCA and Recursive Feature Elimination. *Journal of Infor- mation Security and Applications*, 37, 91-102. https://doi.org/10.1016/j.jisa.2017.10.007

[4] Agoramoorthy, M., Ali, A., Sujatha, D., F, M., & Ramesh, G. (2023). An Analysis of Signature-Based Components in Hybrid Intrusion Detection Systems. *2023 Intelligent Computing and Control for Engineering and Business Systems(ICCEBS)*, 1-5. https://doi.org/10.1109/ICCEBS58601.2023.10449209.

[5] Ahmad, I., Haq, Q., Imran, M., Alassafi, M., & Alghamdi, R. (2022). An Efficient Network Intrusion Detection and Classification System. Mathematics. https://doi.org/10.3390/math10030530.

[6] Ahmad, Z., Khan, A., Cheah, W., Abdullah, J., & Ahmad, F. (2020). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies,32. https://doi.org/10.1002/ett.4150.

[7] Ahmed, U., Nazir, M., Sarwar, A. et al. Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering. Sci Rep 15, 1726 (2025). https://doi.org/10.1038/s41598-025-85866-7

ISSN: 2945-4565 VOL 05, ISSUE 02, 2026

[8] Alabbadi, A., & Bajaber, F. (2025). An Intrusion Detection System over the IoT Data Streams Using eXplainable Artificial Intelligence (XAI). Sensors, 25(3), 847. https://doi.org/10.3390/s25030847

[9] Aldarwbi, M., Lashkari, A., & Ghorbani, A. (2022). The sound of intrusion: A novel network intrusion detection system.Comput.Electr.Eng.,104,108455.

[10] Alharbi, S., & Khan, A. (2023). Ensemble Defense System: A Hybrid IDS Approach for Effective Cyber Threat Detection. *2023 33rd International Telecommunication Networks and Applications Confer- ence*, 267-270 https://doi.org/10.1016/j.compeleceng.2022.108455.

[11] Alharbi, S., & Khan, A. (2023). Ensemble Defense System: A Hybrid IDS Approach for Effective Cyber Threat Detection. *2023 33rd International Telecommunication Networks and Applications Conference*, 267-270. https://doi.org/10.1109/ITNAC59571.2023.10368510.

[12] Aljanabi1, M. (2023). Safeguarding Connected Health: Leveraging Trustworthy AI Techniques to Harden Intrusion Detection Systems Against Data Poisoning Threats in IoMT Environments. *Babylo- nian Journal of Internet of Things*. https://doi.org/10.58496/bjiot/2023/005.

[13] Al-Riyami, S., Lisitsa, A., & Coenen, F. (2021). Cross-Datasets Evaluation of Machine Learning Models for Intrusion Detection Systems. Proceedings of Sixth International Congress on Information and Communication Technology. https://doi.org/10.1007/978-981-16-2102-4_73.

[14] Arreche, O., Guntur, T., & Abdallah, M. (2024). XAI-IDS: Toward Proposing an Explainable Artificial Intelligence Framework for Enhancing Network Intrusion Detection Systems. *Applied Sciences*. https://doi.org/10.3390/app14104170.

[15] Azam, H., Dulloo, M., Majeed, M., Wan, J., Xin, L., Tajwar, M., & Sindiramutty, S. (2023). Defending the Digital Frontier: IDPS and the Battle Against Cyber Threat. *International Journal of Emerging Multidisciplinaries: Computer Science & Artificial Intelligence*. https://doi.org/10.20944/pre- prints202311.0623.v1.

[16] Azizan, A., Mostafa, S., Mustapha, A., Foozy, C., Wahab, M., Mohammed, M., & Khalaf, B. (2021). A Machine Learning Approach for Improving the Performance of Network Intrusion Detection Systems. Annals of Emerging Technologies in Computing. https://doi.org/10.33166/AETIC.2021.05.025.

[17] Bala, B., & Behal, S. (2024). A Brief Survey of Data Preprocessing in Machine Learning and Deep Learning Techniques. 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 1755-1762. https://doi.org/10.1109/I-SMAC61858.2024.10714767.

[18] Bharti, S. (2024). Intrusion detection and prevention systems (IDS/IPS) for OS protec- tion. *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*. https://doi.org/10.55041/ijsrem31718.

[19] Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning.*Pattern Recognition*, 84, 317-331. https://doi.org/10.1016/j.patcog.2018.07.023.

[20] Bilal, M., Ali, G., Iqbal, M., Anwar, M., Malik, M., & Kadir, R. (2022). Auto-Prep: Efficient and Auto- mated Data Preprocessing Pipeline. IEEE Access, 10, 107764-107784. https://doi.org/10.1109/ACCESS.2022.3198662.

[21] Bovenzi, G., Di Monda, D., Montieri, A., Persico, V., & Pescapé, A. (2024). Classifying attack traffic in IoT environments via few-shot learning. J. Inf. Secur. Appl., 83, 103762. https://doi.org/10.1016/j.jisa.2024.103762.

ISSN: 2945-4565 VOL 05, ISSUE 02, 2026

[22] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153-1176. https://doi.org/10.1109/COMST.2015.2494502

[23] Cai, S., Han, D., & Li, D. (2023). A Feedback Semi-Supervised Learning With Meta-Gradient for Intru- sion Detection. IEEE Systems Journal, 17, 1158-1169. https://doi.org/10.1109/JSYST.2022.3197447.

[24] Cao, J., Lin, L., , R., Guan, H., Tian, M., & Wang, Y. (2022). An Efficient Deep Learning Approach To IoT Intrusion Detection. *Comput. J.*, 65, 2870-2879. https://doi.org/10.1093/comjnl/bxac119.*)*, 1-6. https://doi.org/10.1109/WCNC49053.2021.9417568.