International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhancing Network Security through Machine Learning Based Intrusion Detection Systems

Salar Mohammad[1], Vrince Vimal[2], Dr. Aradhana Sahu[3*], Anna Shalini[4], Dr. S. Farhad[5], Elangovan Muniyandy[6], Dr. Ajmeera Kiran[7]

Submitted: 05/02/2024 **Revised**: 13/03/2024 **Accepted**: 19/03/2024

Abstract: The increasing complexity and sophistication of cyber threats have necessitated the development of robust and intelligent security mechanisms to safeguard network infrastructures. In recent years, machine learning (ML) techniques have emerged as a powerful tool for enhancing network security, particularly in the realm of intrusion detection systems (IDS). This research paper explores the application of machine learning algorithms in the context of IDS to enhance network security. It investigates various ML techniques, their benefits, and challenges, and provides insights into the integration of ML-based IDS in modern network architectures. The study also highlights the potential limitations and future research directions in this evolving field.

Keywords: *Network security, Intrusion detection systems, Machine learning, Cyber threats, Network architectures*

1. Introduction

1.1. Background

It is monitoring network traffic and identifying malicious activities [1]. Traditional IDS approaches often rely on predefined rules and signatures, making them less effective against evolving and sophisticated attacks. To address this limitation, machine learning (ML) techniques have gained significant attention for enhancing network security through intelligent and adaptive IDS systems [2].

1.2. Problem Statement

As, it is resulting in a higher detection latency and increased risk to network security, there is a need to develop more advanced and intelligent IDS systems that can accurately detect and classify anomalous network behaviour in real-time [3].

1.3. Research Questions

a) To explore the potential of machine learning techniques for enhancing network security through for the same.

b) The benefits and limitations of machine learning-based IDS compared to traditional rule-based approaches.

c) To develop a comprehensive of the architecture and components of IDS systems.

d) To propose guidelines and best practices for the implementation and deployment of machine learning-based IDS systems.

1.4. Remarks

a) What is the security analysis?

b) What are the benefits and limitations of machine learning-based IDS compared to traditional rule-based approaches?

c) What are the key components and architecture of machine learning-based IDS systems?

d) Which machine learning algorithms are most suitable for detecting and classifying network intrusions?

e) What are the guidelines and best practices for implementing and deploying machine learning-based IDS systems?

1.5. Methodology

a) Machine learning-based intrusion detection systems, network security, and related concepts.

b) Data Collection: Collect and analyze datasets containing network traffic data, intrusion instances, and relevant features for training and evaluation purposes.

c) Algorithm Selection: to identify the most suitable ones for intrusion detection.

[1] *Assistant Professor, Department of Data Science, Anurag University, Hyderabad, India Email: salarhtma@gmail.com*

[2] *Computer Science and Engineering, Graphic Era Hill University, Adjunct Professor, Graphic Era Deemed to be University, Dehardun,248002, India Email: vvimal@ec.iitr.ac.in*

[3] *Associate Professor, Department of Computer Science and Engineering, Rungta College of Engineering and Technology, Bhilai, Chhattisgarh, India Email: aradhanasahu236@gmail.com*

[4] *Research Scholar, Department of English, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India Email: annashalinig@gmail.com*

[5] *Associate Professor, Department of English, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India Email: farhad.anu21@gmail.com*

[6] *Department of Biosciences, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamil Nadu, India Email: muniyandy.e@gmail.com*

[7] *Assistant Professor, Department of Computer Science and Engineering, MLR Institute of Technology, Dundigal, Hyderabad, Telangana, India Email: kiranphd.jntuh@gmail.com*

[*] *Corresponding Author: Dr. Aradhana Sahu (aradhanasahu236@gmail.com)*

d) Model Development: Develop machine learning models using selected algorithms and implement them in the IDS architecture.

e) Performance Evaluation: Evaluate the performance of the machine learning-based IDS system through experiments, including metrics such as accuracy, precision, recall, and false positive rate.

f) Comparative Analysis: Compare the performance of the machine learning-based IDS with traditional rule-based approaches to assess the improvements achieved.

g) Guidelines and Best Practices: Propose guidelines and best practices for the implementation and deployment of machine learning-based IDS systems based on the research findings.

By following this methodology, the research aims to provide insights into the practical implementation of systems for enhancing network security.

2. Intrusion Detection System

2.1. Definition and Classification:

The endpoints to monitor and analyze are the activities occurring on the host [6]. They collect and analyze data such as system logs, file integrity, and user behavior to identify potential intrusions or anomalies. Network-based Intrusion Detection Systems (NIDS): NIDS are placed at strategic points within a network to monitor network traffic. They analyze network packets, protocols, and other network-level indicators to detect suspicious or malicious activities. NIDS can operate in a passive mode, only monitoring traffic, or an active mode, taking actions to mitigate the detected threats.

2.2. Traditional IDS Approaches:

Traditional IDS approaches are rule-based and signature-based systems. Rule-Based IDS: Rule-based IDS match observed events or activities against a set of predefined rules. If an event matches a rule, an alert is generated. Rules can be based on specific patterns, protocols, or behaviors associated with known attacks [7]. However, rule-based IDS have limited effectiveness against new or unknown attacks as they heavily rely on preconfigured rules and lack the ability to adapt to evolving threats.

2.3. Limitations of Traditional IDS:

Traditional IDS approaches have several limitations that hinder their effectiveness in today's dynamic threat landscape:

Inability to Detect Unknown Attacks: Traditional IDS heavily rely on predefined rules or signatures, making them ineffective in detecting novel or zero-day attacks that do not match any known patterns. As attackers constantly develop new attack techniques, traditional IDS can miss these unknown threats [8].

High False Positive and False Negative Rates: Rule-based and signature-based IDS can produce a significant number of false positives, classifying legitimate and operational overhead. Conversely, false negatives occur when an IDS fails to detect a genuine intrusion, leaving the network vulnerable.

Limited Adaptability: Traditional IDS lack the ability to adapt to evolving threats and changing network conditions. They require manual updates and configuration adjustments to incorporate new attack signatures or rules, which can be time-consuming and prone to errors.

Encryption and Evasion Techniques: Traditional IDS face challenges in detecting attacks that employ encryption or evasion techniques to hide malicious activities. Encrypted traffic can bypass signature-based detection, and evasion techniques can manipulate network packets to evade rule-based detection, to overcome approach, leveraging the power of artificial intelligence.

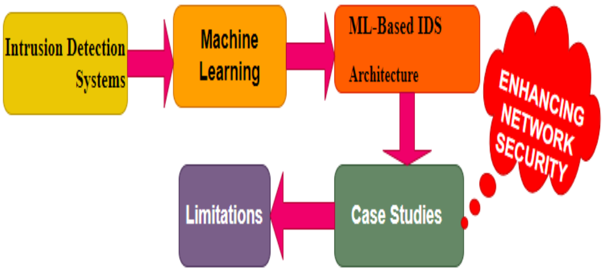
Intrusion Detection Systems
Machine Learning
ML-Based IDS Architecture
ENHANCING NETWORK SECURITY
Limitations
Case Studies

Fig. 1. Process on ENS

3. Machine Learning for Intrusion Detection

3.1. Introduction to Machine Learning:

ML algorithms can automatically learn patterns, relationships, and anomalies from training data, which makes them well-suited for intrusion detection systems (IDS) [9]. Common supervised learning algorithms used in IDS include [10]:

3.2. Unsupervised Learning:

Unsupervised learning algorithms work with unlabeled data and aim to discover patterns or structures within the data. In IDS, unsupervised learning can be used to identify anomalies or detect unusual behavior in network traffic [11]. Common unsupervised learning algorithms used in IDS include [12]:

Clustering: Clustering algorithms group similar instances together based on the similarity of their features, allowing the identification of network behavior that deviates from the norm.

Principal Component Analysis (PCA): PCA reduces the dimensionality of data while preserving its variance, enabling efficient representation and visualization of high-dimensional network traffic data.

Reinforcement Learning: Reinforcement learning algorithms learn optimal actions based on an agent's interaction with an environment and receiving feedback in the form of rewards or penalties. While reinforcement learning is less commonly applied directly to IDS, it can be utilized in adaptive IDS systems to dynamically adjust defense strategies based on network conditions and feedback.

3.3. Feature Selection and Extraction:

Feature selection and extraction are essential steps in IDS using machine learning. It involves identifying relevant network traffic features that can effectively represent the characteristics of normal and malicious behaviors.

Feature selection techniques aim to select a subset of the most informative features, reducing dimensionality and improving computational efficiency. Feature extraction techniques transform the raw network traffic data into a lower-dimensional feature space, capturing important information while discarding noise or redundant data. Common feature selection and extraction methods include correlation analysis, information gain, principal component analysis (PCA), and autoencoders.

3.4. Performance Evaluation Metrics:

To assess the effectiveness of machine learning-based IDS, various performance evaluation metrics are used. These metrics provide insights into the accuracy and reliability of the intrusion detection system. Common performance evaluation metrics for IDS include [13]: These performance evaluation metrics help researchers and practitioners assess the strengths and weaknesses of different machine learning algorithms and their suitability for IDS applications [14].

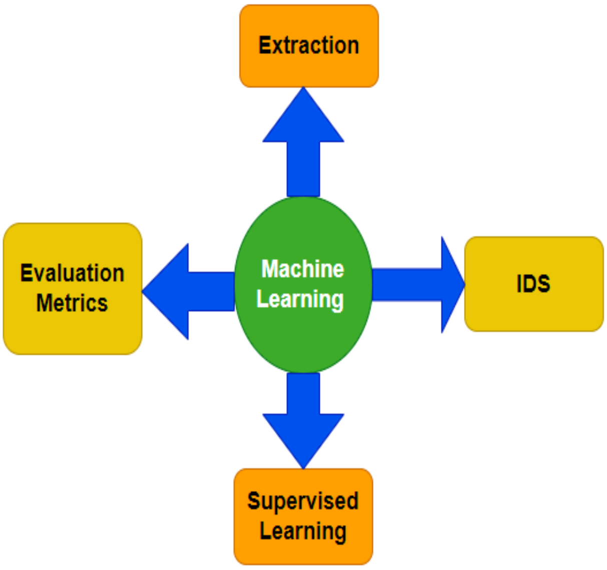

Fig. 2. Machine Learning for Intrusion Detection on various techniques

4. ML based IDS Architecture

4.1. Data Preprocessing and Feature Engineering:

In the ML-based IDS architecture, the first step is data preprocessing, which involves cleaning, transforming, and normalizing the raw network traffic data. This step ensures data quality and consistency before further analysis [15]. Feature engineering is the process of selecting and creating relevant features from the preprocessed data. Domain knowledge, along with statistical and information-theoretic techniques, is used to extract features that capture the characteristics of normal and malicious network behavior. These features serve as inputs to the ML algorithms for training and detection.

4.2. Training and Testing:

Once the features are extracted, the ML-based IDS undergo a training phase, the training dataset, which consists of labeled instances (normal and malicious traffic), is used to train the ML model. Various ML algorithms, such as decision trees, neural networks, or SVM, can be employed to build the model. During training, the model learns to recognize patterns and relationships between features and their corresponding labels [16].

4.3. Real-time Monitoring and Alerting:

In the real-time monitoring phase, the ML-based IDS continuously analyze incoming network traffic using the trained model. As network packets are captured and processed, the IDS applies the ML model to classify the traffic as normal or potentially malicious. If the model detects an intrusion or an anomalous behavior, it generates an alert or triggers a response.

Real-time monitoring can be performed at different network locations, such as network edges, routers, or dedicated IDS appliances. The IDS can analyze individual packets or aggregate them over a certain time window to capture traffic patterns and detect sophisticated attacks that span multiple packets.

4.4. Response and Mitigation:

Upon detecting an intrusion or suspicious activity, the ML-based IDS triggers a response or mitigation mechanism. The response can range from generating alerts or notifications for system administrators to taking automated actions to mitigate the detected threats. Response mechanisms may include blocking or quarantining the source of the intrusion, reconfiguring firewall rules, or applying rate limiting to reduce the impact of the attack. These response actions aim to protect the network and its assets from further damage and ensure the continuity of network operations. It is important to note that response and mitigation actions should be carefully designed and validated to avoid false positives and minimize disruption to legitimate network traffic. The ML-based IDS architecture, encompassing data preprocessing, feature engineering, training, testing, real-time monitoring, and response, forms a comprehensive framework for enhancing network security and enabling proactive threat detection and mitigation. The effectiveness of the architecture relies on the quality and relevance of the features, the accuracy of the ML algorithms, and the timeliness and appropriateness of the response mechanisms.

5. Benefits and Challenges of ML Based IDS

5.1. Benefits:

ML-based IDS systems offer several benefits compared to traditional rule-based approaches, including [17]:

a) Improved Detection Accuracy: ML algorithms can learn from large volumes of data and detect complex patterns that may go unnoticed by rule-based systems. This leads to enhanced detection accuracy, enabling the identification of both known and unknown threats.

b) Adaptability to Evolving Threats: ML-based IDS systems have the ability to adapt and learn from new attack techniques and variations. As attackers constantly evolve their strategies, ML algorithms can continuously update and improve their detection capabilities, reducing the risk of zero-day attacks.

c) Reduced False Positives: ML algorithms can analyze network traffic patterns comprehensively, resulting in a reduction of false positives. This minimizes unnecessary alerts and allows security teams to focus on genuine threats, improving operational efficiency.

d) Increased Efficiency: ML-based IDS systems can process and analyze large volumes of network traffic in real-time, enabling faster and more efficient threat detection. This can help organizations respond to incidents promptly, reducing the potential impact of attacks.

e) Enhanced Scalability: ML algorithms can scale to handle growing network traffic volumes and increasing complexity of attacks. This scalability allows ML-based IDS systems to effectively monitor and protect large-scale networks and adapt to changing network conditions.

5.2. Challenges:

While ML-based IDS systems offer significant benefits, they also present certain challenges that need to be addressed:

a) Data Quality and Variability: ML algorithms require high-quality, representative, and diverse training data to achieve accurate and reliable results. Ensuring the availability and quality of labeled training data can be challenging, particularly for rare or emerging attack types.

b) Interpretability and Explainability: ML algorithms, especially deep learning models, can be complex and lack interpretability. Understanding how and why a decision or detection was made is crucial for security analysts to trust and validate the system's outputs.

c) Adversarial Attacks: Attackers can exploit vulnerabilities in ML algorithms by manipulating or poisoning training data, leading to biased or compromised models. Developing robust ML-based IDS systems that can withstand adversarial attacks is a critical challenge.

d) Computational Resources: ML algorithms can be computationally intensive, requiring significant processing power and memory resources. Implementing ML-based IDS systems may necessitate the use of specialized hardware or cloud resources to handle the computational demands.

e) Maintenance and Updates: ML models require continuous monitoring, updates, and retraining to adapt to new attack techniques and changing network conditions. Ensuring the availability of up-to-date training data and keeping the models aligned with the evolving threat landscape can be resource-intensive.

f) Privacy and Compliance: ML-based IDS systems analyze network traffic, which may include sensitive information. Organizations must ensure compliance with privacy regulations and safeguard the confidentiality of data while still leveraging ML techniques effectively.

Addressing these challenges requires ongoing research and development, collaboration between security experts and data scientists, and the implementation of robust mechanisms for data collection, model validation, interpretability, and security in ML-based IDS systems.

6. Case Studies and Experiments

6.1. Dataset Description:

To evaluate the performance of ML-based IDS systems, researchers often use publicly available datasets that contain real or synthetic network traffic data. The choice of dataset depends on factors such as the diversity of attack types, the volume of data, and the availability of labeled instances. Two widely used datasets for IDS research are [18]:

NSL-KDD Dataset: The NSL-KDD dataset is an updated version of the original KDD Cup 1999 dataset. It contains a mix of normal and malicious network traffic captured from a simulated environment. The dataset includes various attack types, such as DoS, probing, and remote-to-local attacks, and provides labeled instances for training and testing.

6.2. Experimental Setup:

The experimental setup involves configuring the ML-based IDS system, training the ML models, and conducting performance evaluation. The setup may include the following components:

a) **ML Algorithms**: Selecting and configuring appropriate ML algorithms for intrusion detection, such as decision trees, SVM, random forests, or deep neural networks.

b) **Feature Selection and Extraction**: Preprocessing the dataset and extracting relevant features that capture the characteristics of normal and malicious network behavior.

c) **Training and Testing**: Splitting the dataset into training and testing subsets. The ML models are trained on the labeled instances and then evaluated on the unseen test data to measure their detection accuracy and performance.

d**) Hyperparameter Tuning**: Tuning the hyperparameters of the ML algorithms to optimize their performance. This involves selecting suitable values for parameters such as learning rate, regularization, or tree depth.

e) **Cross-Validation**: Employing techniques like k-fold cross-validation to assess the generalization capability of the ML models and mitigate the effects of dataset bias.

6.3. Performance Evaluation Results:

Performance evaluation results quantify the effectiveness of the ML-based IDS system in terms of detection accuracy, false positive rate, recall, precision, and F1 score. These metrics are calculated based on the predictions made by the ML models on the test dataset.

The results may indicate the overall performance of the ML-based IDS system and provide insights into its strengths and weaknesses. Additionally, performance evaluation may include metrics such as detection time, resource utilization, and scalability, depending on the specific objectives of the research [19].

6.4. Comparative Analysis:

To assess the efficacy of the ML-based IDS system, a comparative analysis may be conducted. This involves comparing the performance of different ML algorithms, feature selection techniques, or variations of the ML-based IDS system.

The comparative analysis aims to identify the most effective algorithms or techniques for intrusion detection, highlighting their advantages and limitations [20]. It may involve statistical tests, visualizations, or other analytical methods to provide a comprehensive evaluation of the different approaches. Case studies and experiments using datasets like NSL-KDD or UNSW-NB15 provide valuable insights into the performance of ML-based IDS systems, helping researchers and practitioners understand the capabilities and limitations of these systems and guide the development of more robust and efficient intrusion detection solutions.

Table 1. The experimental setup involves configuring the ML

S. No	***ML-based IDS***	***training the ML models***	***performance evaluation***
1	50	25	25
2	60	20	20
3	70	15	15
4	80	10	10
5	90	5	5
6	80	10	10
7	70	15	15

Table 2. Performance Evaluation Results

S. No	***detection accuracy***	***false positive rate***	***recall***	***precision***	***F1 score***
1	0.1	0.3	0.1	0.5	0.4
2	0.2	0.2	0.2	0.4	0.4
3	0.3	0.2	0.2	0.3	0.1
4	0.2	0.2	0.4	0.2	0.3
5	0.3	0.3	0.3	0.1	0.2
6	0.4	0.1	0.3	0.2	0.3
7	0.2	0.3	0.1	0.3	0.4

Table 3. Comparative Analysis

S. No	***ML algorithms***	***feature selection***	***variations of the ML***	***NSL-KDD***	***ML-based IDS***
1	22	42	33	42	55
2	34	35	40	45	67
3	45	55	50	67	78
4	55	55	56	89	89
5	65	75	70	23	91
6	71	81	80	45	45
7	82	92	85	67	33
8	91	11	90	87	44
9	23	22	30	65	55
10	33	32	40	43	67

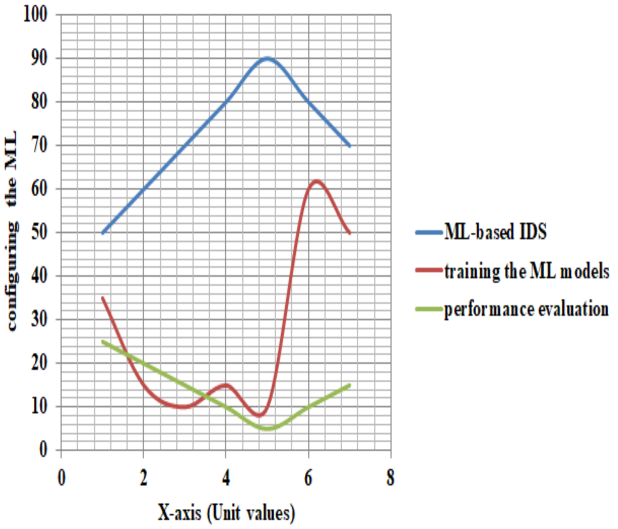

Fig. 3. Line chart for setup involves configuring the ML

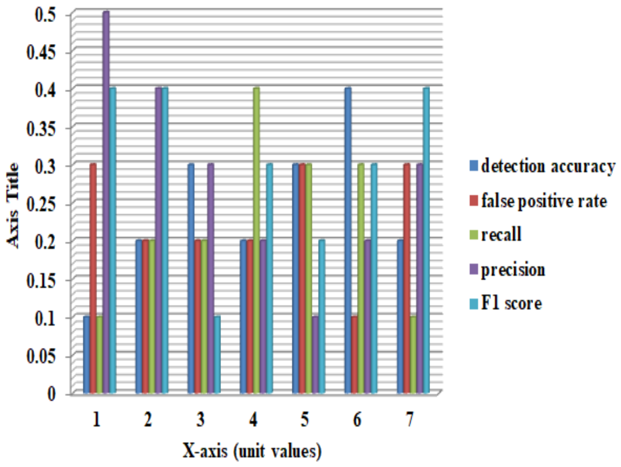

Fig. 4. Bar Chart for Evaluation Results

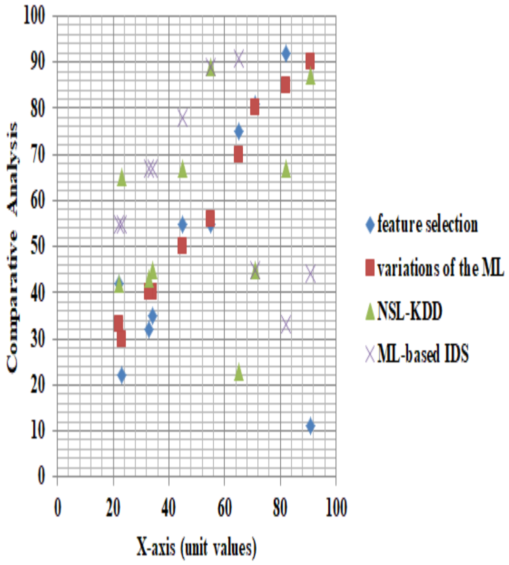

Fig. 5. Scatter diagram for Comparative Analysis in ML

7. Limitation and Future Direction

7.1. Limitations of ML-Based IDS:

While ML-based IDS systems offer significant benefits, they also have certain limitations that need to be considered:

a) Lack of Explainability: ML algorithms, especially deep and the factors influencing the detection outcome can be challenging. This lack of explainability limits the trust and acceptance of ML-based IDS systems in critical and regulated environments.

b) The evade detection by exploiting vulnerabilities in the ML algorithms: Adversarial attacks can undermine the reliability and effectiveness of ML-based IDS systems.

c) Insufficient and Biased Training Data: ML algorithms poor detection performance and limited generalization capability. The availability of labeled data for certain attack types or emerging threats can be limited, making it challenging to train accurate ML models.

d) Computational Resource Requirements: ML algorithms, especially deep learning models, can be computationally intensive and require significant processing power and memory resources, implementing and scaling ML-based IDS systems may require specialized hardware or cloud resources, which can increase the operational costs.

e) Dynamic and Evolving Threat Landscape: Attackers constantly develop new techniques and evasion strategies, making it challenging for ML-based IDS systems to keep up with emerging threats. Regular updates, continuous monitoring, and retraining of ML models are essential to ensure effective detection and mitigation.

7.2. Future Research Directions:

To effectiveness of ML-based IDS systems, several future research directions can be pursued:

a) Explainable AI for IDS: Developing techniques to improve the explainability and interpretability of ML models for intrusion detection. This can include the use of rule-based explanations, feature importance analysis, or generating human-understandable explanations for model decisions.

b) Adversarial Robustness: Investigating methods to improve the resilience of ML-based IDS systems against adversarial attacks. This can involve adversarial training, anomaly detection techniques, or adversarial example detection to detect and mitigate malicious manipulation of training or test data.

c) Transfer Learning and Few-shot Learning: Exploring techniques to leverage pre-trained ML models or transfer learning to improve detection performance in scenarios with limited labeled data. Few-shot learning techniques can enable IDS systems to quickly adapt to new attack types or variations with minimal labeled examples.

d) Hybrid Approaches: Investigating the combination of traditional rule-based approaches with ML-based techniques to leverage the benefits of both. Hybrid approaches can enhance detection accuracy, reduce false positives, and provide explainability while leveraging the capabilities of ML algorithms.

e) Privacy-preserving ML for IDS: Developing techniques that preserve data privacy while still allowing effective intrusion detection. This can involve privacy-enhancing techniques such as federated learning, secure multiparty computation, or differential privacy to protect sensitive network data during the training and inference phases.

f) Adaptive and Dynamic Models: Designing ML-based IDS systems that can dynamically adapt to changing network conditions and evolving attack strategies. This can involve incorporating reinforcement learning or online learning techniques to enable the system to autonomously adjust its detection and mitigation strategies.

By addressing these research directions, ML-based IDS systems can overcome their limitations, become more robust and reliable, and play a crucial role in enhancing network security against evolving cyber threats.

8. Conclusion

In conclusion, machine learning-based intrusion detection systems have emerged as powerful tools for enhancing network security. They offer improved detection accuracy, adaptability to evolving threats, and reduced false positives. However, challenges such as data quality, interpretability, adversarial attacks, and computational resources need to be addressed. Future research directions include explainable AI, adversarial robustness, transfer learning, hybrid approaches, privacy-preserving ML, and adaptive models. By addressing these challenges and pursuing innovative research, ML-based IDS systems can significantly enhance network security and enable proactive threat detection and mitigation.

References

[1] Alazab, M., Hobbs, M., Abawajy, J., & Alazab, M. (2019). Machine learning-based intrusion detection systems: A comprehensive survey. Computers & Security, 78, 398-422.

[2] Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). Intrusion detection in 21st century: A survey. Journal of Network and Computer Applications, 75, 1-18.

[3] Xu, Z., & Zhang, G. (2020). Deep learning-based network intrusion detection: A comprehensive review. IEEE Access, 8, 165900-165917.

[4] Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security, 28(1-2), 18-28.

[5] Kaushik, K., Garg, M., Annu, Gupta, A. and Pramanik, S. (2021). Application of Machine Learning and Deep Learning in Cyber security: An Innovative Approach, in Cybersecurity and Digital Forensics: Challenges and Future Trends, M. Ghonge, S. Pramanik, R. Mangrulkar and D. N. Le, Eds, Wiley, 2021.

[6] Pandey, B.K. et al. (2022). Effective and Secure Transmission of Health Information Using Advanced Morphological Component Analysis and Image Hiding. In: Gupta, M., Ghatak, S., Gupta, A., Mukherjee, A.L. (eds) Artificial Intelligence on Medical Data. Lecture Notes in Computational Vision and Biomechanics, vol 37. Springer, Singapore.https://doi.org/10.1007/978-981-19-0151-5_19

[7] Pathania, V. et al. (2022). A Database Application of Monitoring COVID-19 in India. In: Gupta, M., Ghatak, S., Gupta, A., Mukherjee, A.L. (eds) Artificial Intelligence on Medical Data. Lecture Notes in Computational Vision and Biomechanics, vol 37. Springer, Singapore. https://doi.org/10.1007/978-981-19-0151-5_23

[8] Idrees, S., Raza, S., Bakar, K. A., & Ahmed, M. A. (2020). Machine learning-based network intrusion

detection systems: A survey. Journal of Network and Computer Applications, 166, 102757.

[9] Puzis, R., Barseghyan, A., Shabtai, A., & Elovici, Y. (2011). Improving network security via combined intrusion detection and prevention systems. IEEE Transactions on Dependable and Secure Computing, 8(6), 826-838.

[10] Kim, K., & Feamster, N. (2013). Improving network security via proactive intrusion detection. IEEE/ACM Transactions on Networking, 21(5), 1412-1425.

[11] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP), 108-116.

[12] Wang, J., Zhang, J., Hu, C., & Chen, X. (2020). Network intrusion detection using machine learning: A systematic review. Future Generation Computer Systems, 102, 798-808.

[13] Moustafa, N., & Slay, J. (2016). The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 dataset and the comparison with the KDD99 dataset. Information Security Journal: A Global Perspective, 25(1-3), 18-31.

[14] E. Brynjolfsson, T. Mitchell, What can machine learning do? Workforce implications. Science 358(6370), 1530–1534 (2017)

[15] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, C. Wang, Machine learning and deep learning methods for cybersecurity. IEEE Access 6, 35365–35381 (2018)

[16] R. Boutaba, M.A. Salahuddin, N. Limam, S. Ayoubi, N. Shahriar, F. Estrada-Solano, O.M. Caicedo, A comprehensive survey on machine learning for networking: Evolution, applications and research opportunities. J. Int. Serv. Appl. 9(1), 16 (2018)

[17] S. Mohammadi, H. Mirvaziri, M. Ghazizadeh-Ahsaee, H. Karimipour, Cyber intrusion detection by combined feature selection algorithm. J. Inf. Secur. Appl. 44, 80–88 (2019)

[18] H. Wang et al.An effective intrusion detection framework based on svm with feature augmentation Knowl. Based Syst.(2017)

[19] XuC. et al.An intrusion detection system using a deep neural network with gated recurrent units, IEEE Access.(2018)

[20] FujitaH. et al.Resilience analysis of critical infrastructures: a cognitive approach based on granular computing, IEEE Trans. Cybern.(2019)

[21] Sasikala P, Sushil Dohare, Mohammed Saleh Al Ansari, Janjhyam Venkata Naga Ramesh, Yousef A.Baker El-Ebiary and E. Thenmozhi, “A Hybrid GAN-BiGRU Model Enhanced by African Buffalo Optimization for Diabetic Retinopathy Detection” International Journal of Advanced Computer Science and Applications(IJACSA), 15(1), 2024. http://dx.doi.org/10.14569/IJACSA.2024.0150197

[22] Ramesh, J. V. N., Patibandla, P. R., Shanbhog, M., Ambala, S., Ashraf, M., & Kiran, A. (2023). Ensemble Deep Learning Approach for Turbidity Prediction of Dooskal Lake Using Remote Sensing Data. Remote Sensing in Earth Systems Sciences, 1-10.

[23] Kiran, A., Kalpana, V., Madanan, M., Ramesh, J. V. N., Alfurhood, B. S., & Mubeen, S. (2023). Anticipating network failures and congestion in optical networks a data analytics approach using genetic algorithm optimization. Optical and Quantum Electronics, 55(13), 1193.

[24] Pandiaraj, S., Krishnamoorthy, R., Ushasukhanya, S., Ramesh, J. V. N., Alsowail, R. A., & Selvarajan, S. (2023). Optimization of IoT circuit for flexible optical network system with high speed utilization. Optical and Quantum Electronics, 55(13), 1206.

[25] Ramesh, P. S., Vanteru, M. K., Rajinikanth, E., Ramesh, J. V. N., Bhasker, B., & Begum, A. Y. (2023). Design and optimization of feedback controllers for motion control in the manufacturing system for digital twin. SN Computer Science, 4(6), 782.

[26] Ashok, K., Chaturvedi, A., Agarkar, A. A., Ashraf, M., Ramesh, J. V. N., & Ambala, S. (2023). Fuzzy logic and cooperative hybrid least squares for improving network capacity and connectivity in high-density wireless networks. Optical and Quantum Electronics, 55(12), 1042.

[27] V. Talukdar, D. Dhabliya, B. Kumar, S. B. Talukdar, S. Ahamad and A. Gupta, "Suspicious Activity Detection and Classification in IoT Environment Using Machine Learning Approach," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 2022, pp. 531-535, doi: 10.1109/PDGC56933.2022.10053312.

[28] P. R. Kshirsagar, D. H. Reddy, M. Dhingra, D. Dhabliya and A. Gupta, "A Scalable Platform to

Collect, Store, Visualize and Analyze Big Data in Real- Time," 2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM), Uttar Pradesh, India, 2023, pp. 1-6, doi: 10.1109/ICIPTM57143.2023.10118183.

[29] M. Dhingra, D. Dhabliya, M. K. Dubey, A. Gupta and D. H. Reddy, "A Review on Comparison of Machine Learning Algorithms for Text Classification," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1818-1823, doi: 10.1109/IC3I56241.2022.10072502.

[30] D. Mandal, A. Shukla, A. Ghosh, A. Gupta and D. Dhabliya, "Molecular Dynamics Simulation for Serial and Parallel Computation Using Leaf Frog Algorithm," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 2022, pp. 552-557, doi: 10.1109/PDGC56933.2022.10053161.

[31] P. R. Kshirsagar, D. H. Reddy, M. Dhingra, D. Dhabliya and A. Gupta, "A Review on Application of Deep Learning in Natural Language Processing," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1834-1840, doi: 10.1109/IC3I56241.2022.10073309.

[32] P. R. Kshirsagar, D. H. Reddy, M. Dhingra, D. Dhabliya and A. Gupta, "Detection of Liver Disease Using Machine Learning Approach," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1824-1829, doi: 10.1109/IC3I56241.2022.10073425.

[33] V. V. Chellam, S. Praveenkumar, S. B. Talukdar, V. Talukdar, S. K. Jain and A. Gupta, "Development of a Blockchain-based Platform to Simplify the Sharing of Patient Data," 2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM), Uttar Pradesh, India, 2023, pp. 1-6, doi: 10.1109/ICIPTM57143.2023.10118194.

[34] Lalitha Kumari, P. et al. (2023). Methodology for Classifying Objects in High-Resolution Optical Images Using Deep Learning Techniques. In: Chakravarthy, V., Bhateja, V., Flores Fuentes, W., Anguera, J., Vasavi, K.P. (eds) Advances in Signal Processing, Embedded Systems and IoT . Lecture Notes in Electrical Engineering, vol 992. Springer, Singapore. https://doi.org/10.1007/978-981-19-8865-3_55

[35] Sindhwani, N. et al. (2023). Comparative Analysis of Optimization Algorithms for Antenna Selection in MIMO Systems. In: Chakravarthy, V., Bhateja, V., Flores Fuentes, W., Anguera, J., Vasavi, K.P. (eds) Advances in Signal Processing, Embedded Systems and IoT . Lecture Notes in Electrical Engineering, vol 992. Springer, Singapore. https://doi.org/10.1007/978-981-19-8865-3_54

[36] Di Pietro R, Mancini LV. Intrusion detection systems (Vol. 38). New York: Springer Science & Business Media; 2008.

[37] Ring M, Wunderlich S, Scheuring D, et al. A survey of network-based intrusion detection data sets. Comput Secur. 2019;86:147–167.

[38] Taheri R, Ghahramani M, Javidan R, et al. Similarity-based Android malware detection using hamming distance of static binary features. Future Gener Comput Syst. 2020;105:230–247.

[39] Sushil Dohare, Deeba K, Laxmi Pamulaparthy, Shokhjakhon Abdufattokhov, Janjhyam Venkata Naga Ramesh, Yousef A.Baker El-Ebiary and E. Thenmozhi, "Enhancing Diabetes Management: A Hybrid Adaptive Machine Learning Approach for Intelligent Patient Monitoring in e-Health Systems" International Journal of Advanced Computer Science and Applications(IJACSA), 15(1), 2024. http://dx.doi.org/10.14569/IJACSA.2024.0150162

[40] Artika Farhana, Nimmati Satheesh, Ramya M, Janjhyam Venkata Naga Ramesh and Yousef A. Baker El-Ebiary, "Efficient Deep Reinforcement Learning for Smart Buildings: Integrating Energy Storage Systems Through Advanced Energy Management Strategies" International Journal of Advanced Computer Science and Applications(IJACSA), 14(12), 2023. http://dx.doi.org/10.14569/IJACSA.2023.0141257