ISSN: 2278-4632
Vol-11 Issue-09, September 2021

OPTIMIZING NETWORK SECURITY VIA MACHINE LEARNING DRIVEN INTRUSION DETECTION SYSTEMS

[#1]KANDUKURI CHANDRASENA CHARY, *Research Scholar,*
[#2]Dr. SATISH NARAYAN GUJAR, *Supervisor*
Department of Computer Science and Engineering,
School of Engineering and Technology,
UNIVERSITY OF TECHNOLOGY, JAIPUR, RAJASTHAN.

ABSTRACT: In order to safeguard network platforms, it is imperative to establish robust and intelligent security systems, as cyber threats are becoming increasingly sophisticated and cunning. In recent years, machine learning (ML) techniques have emerged as a potent instrument for enhancing network security, particularly when employed in conjunction with intrusion detection systems (IDS). This study examines the integration of machine learning algorithms with intrusion detection systems (IDS) to enhance network security. It examines various machine learning methodologies, their advantages and disadvantages, and the methods by which they can be implemented in existing network topologies to enhance security.
KEYWORDS: Network security, Intrusion detection systems, Machine learning, Cyber threats, Network architectures.

1. INTRODUCTION

The advent of the digital age has revolutionized how we communicate, conduct business, and manage our personal lives. This digital transformation, however, has also opened the door to an array of cyber threats, from malware and ransomware to sophisticated, targeted attacks by state actors and organized cybercrime groups. The traditional perimeter-based defense mechanisms, primarily focused on firewalls and signature-based detection systems, are no longer adequate in this rapidly evolving threat landscape. These conventional methods often fall short in detecting zero-day exploits and sophisticated attacks that bypass static security measures. The frequency, complexity, and scale of cyber-attacks have necessitated the exploration of more advanced, intelligent, and adaptive security solutions.

Machine Learning (ML) introduces a paradigm shift in network security by offering adaptive, intelligent, and scalable solutions capable of addressing the limitations of traditional Intrusion Detection Systems (IDS). ML-based IDS leverage algorithms capable of learning from vast amounts of data, identifying patterns, and detecting anomalies that may indicate malicious activity. These systems can continuously improve their detection capabilities by learning from both previous attacks and benign behaviors, thus staying ahead of emerging threats. By employing techniques such as deep learning, neural networks, and ensemble methods, ML-based IDS can analyze complex datasets at unprecedented speeds, offering a significant advantage over manual and heuristic-based approaches.

The application of ML in intrusion detection is diverse, encompassing techniques such as supervised learning, unsupervised learning, and reinforcement learning. Supervised learning models are trained on labeled datasets containing both normal and malicious behaviors, allowing them to classify future network activities accurately. These models benefit from extensive training data, which enhances their ability to recognize known threats and predict new variations. Unsupervised learning, on the other hand, does not require labeled data and is adept at identifying novel threats through anomaly detection. This approach is particularly valuable for discovering previously unknown attack vectors, as it relies on identifying deviations from established normal behavior rather than pre-defined signatures. Reinforcement learning, although less common, offers potential for adaptive response strategies by learning optimal actions through interactions with the network

ISSN: 2278-4632
Vol-11 Issue-09, September 2021

environment. This technique enables IDS to dynamically adjust their detection and response strategies based on the evolving threat landscape and the effectiveness of past actions.

Furthermore, the integration of ML-based IDS with existing security infrastructure can enhance the overall resilience of network defenses. These systems can work in tandem with other security tools, providing a layered security approach that combines the strengths of various technologies. For instance, ML-based IDS can complement traditional signature-based systems by providing early warnings about suspicious activities that may not yet be recognized as threats. By incorporating real-time data analysis, ML-based IDS can also offer predictive insights, enabling proactive threat mitigation and reducing the time between detection and response. This synergy between traditional and advanced security measures creates a more robust and comprehensive defense mechanism, capable of addressing both known and unknown threats.

This paper aims to explore the potential of Machine Learning in enhancing network security through the development and implementation of advanced Intrusion Detection Systems. By examining current methodologies, challenges, and case studies, we seek to provide a comprehensive overview of how ML can transform network security. We will delve into the specific ML techniques that have shown promise in IDS applications, such as decision trees, support vector machines, and clustering algorithms. Additionally, we will address the challenges associated with ML-based IDS, including the need for high-quality training data, the risk of adversarial attacks, and the complexity of integrating these systems into existing security frameworks. Through this exploration, we hope to highlight the critical role that ML-based IDS can play in creating a more secure and resilient digital environment. By understanding the capabilities and limitations of these systems, we can better prepare for the future of network security and ensure that our digital infrastructures are protected against an ever-evolving array of cyber threats.

2. INTRUSION DETECTION SYSTEM

Definition and Classification

NIDS are strategically placed throughout a network to monitor its activity. They examine network packets, protocols, and other network-level indicators to identify behavior that appears unusual or detrimental.

Network-based Intrusion Detection Systems (NIDS): There are two modes of operation for NIDS: active and inactive. Inactive mode entails the monitoring of traffic, while active mode involves the mitigation of identified hazards.

Traditional IDS Approaches:

The most prevalent methods for constructing intrusion monitoring systems are rule-based and signature-based systems. The IDS that adheres to the regulations: Intrusion detection systems (IDS) that employ rules compare the detected activity to a predetermined set of rules. An alert is generated when an event satisfies a condition. By examining specific actions, processes, or patterns that are associated with recognized assaults, rules can be established. On the other hand, rule-based IDS are only partially effective against new or unknown assaults because they are reliant on pre-established rules and are unable to adapt to new threats. Activities that conventional IDS are incapable of performing

Limitations of Traditional IDS

The following are the reasons why traditional intrusion detection systems (IDS) are ineffective in the face of the evolving hazards of today:

Inability to Detect Unknown Attacks:

Standard intrusion detection systems are inadequate at identifying novel assaults that do not conform to any established patterns, as they depend on predefined criteria or signatures. Standard IDS may fail to detect these emerging threats, as attackers are consistently devising novel methods of entry.

High False Positive and False Negative Rates:

When rule-based and signature-based intrusion detection systems are employed to differentiate between genuine threats and operational overhead, numerous false positives may occur. A false negative occurs when an intrusion detection system (IDS) fails to detect a genuine

ISSN: 2278-4632
Vol-11 Issue-09, September 2021

compromise, thereby exposing the network to attack.

Limited Adaptability:

Standard intrusion detection systems are incapable of adapting to the constantly evolving network conditions and hazards.

Introducing new attack signatures or rules necessitates manually updating and altering the configuration, which can be time-consuming and result in errors.

Encryption and Evasion Techniques:

The detection of attacks that conceal detrimental behavior through evasion or encryption is a challenging task for conventional intrusion detection systems. The strategy can be circumvented by employing evasion techniques. These methods encrypt data to prevent it from being detected by signature-based detection and modify network packets to prevent their detection by rule-based detection. This leverages the capabilities of artificial intelligence.

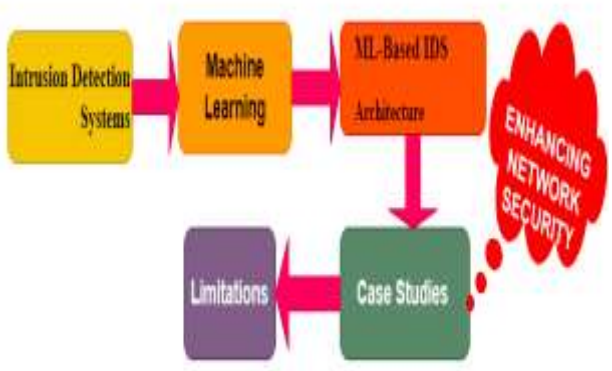

Fig. 1. Process on ENS

3. MACHINE LEARNING FOR INTRUSION DETECTION

Introduction to Machine Learning:

Machine learning algorithms are perfect for intrusion detection systems (IDS) because of their ability to automatically identify patterns, correlations, and irregularities in training data. Typical supervised learning methods in IDS are as follows.

Unsupervised Learning:

Algorithms for unsupervised learning look for structures or patterns in unlabeled data. IDS can utilize unsupervised learning to find anomalies or unusual behavior in network traffic. Typically, IDS makes use of unsupervised learning techniques like:

Clustering: Clustering techniques combine similar instances together based on feature similarities in order to identify outliers in network activity. Analyzing principal components (PCA): High-dimensional network traffic data is easier to express and visualize thanks to PCA, which reduces dimensionality while maintaining variance.

Reinforcement Learning: By observing how an agent interacts with its surroundings and receiving feedback in the form of rewards or penalties, reinforcement learning algorithms are able to choose the best course of action. While it is not frequently applied directly to intrusion detection systems (IDS), adaptive IDS systems can make use of reinforcement learning to dynamically modify protection strategies in response to feedback and network conditions.

Feature Selection and Extraction:

The crucial phases of IDS feature extraction and selection involve machine learning. Finding pertinent network traffic features that faithfully capture the traits of both benign and malevolent behavior is necessary. By selecting a subset of the most valuable features, feature selection techniques aim to reduce dimensionality while boosting computational efficiency. Feature extraction techniques take unprocessed network traffic data and turn it into a lower-dimensional feature space by removing noise or redundant data and capturing important information. The most widely used methods for feature selection and extraction are autoencoders, principal component analysis (PCA), correlation analysis, and information gain.

Performance Evaluation Metrics:

A variety of performance evaluation criteria are employed to appraise the efficacy of IDS based on machine learning. The accuracy and dependability of the intrusion detection system are well illustrated by these measurements. Typical metrics for assessing IDS performance are as follows. Researchers and practitioners can evaluate the merits and drawbacks of different machine learning algorithms and their suitability for IDS

ISSN: 2278-4632
Vol-11 Issue-09, September 2021

applications with the use of these performance evaluation criteria.

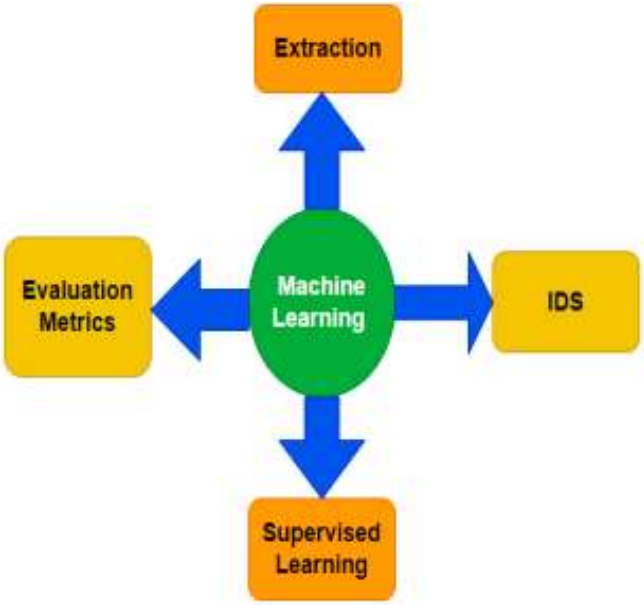

Fig. 2. Machine learning for diverse methodological approaches to intrusion detection.

4. ML BASED IDS ARCHITECTURE

Data Preprocessing and Feature Engineering:

Data Preprocessing and Feature Engineering: Data preprocessing, which comprises cleaning, converting, and normalizing raw network traffic data, is the initial stage in the ML-based IDS architecture. Prior to conducting further analysis, this technique makes sure the data is reliable and consistent. The process of choosing and producing relevant features from preprocessed data is known as feature engineering. Features that characterize both benign and detrimental network behavior are extracted using domain knowledge, statistical and information-theoretic methods, and domain expertise.

Training and Testing:

The training stage of the ML-based IDS begins after feature extraction. The ML model is trained using the training dataset, which includes labeled instances of both malicious and legitimate traffic. Numerous machine learning algorithms, including decision trees, neural networks, and support vector machines (SVMs), can be used to build the model. The model gains the ability to identify patterns and connections between features and the labels that correspond to them throughout the training phase.

Real-time Monitoring and Alerting:

During the real-time monitoring stage, the ML-based IDS continuously analyzes incoming network traffic using the trained model. The IDS employs an ML model to classify intercepted and processed network packets as legitimate or possibly malicious. The model sends an alert or initiates a response when it notices abnormal behavior or an incursion.

Numerous network sites, such as routers, network boundaries, and specialized IDS equipment, can be used for real-time monitoring. To identify sophisticated attacks that span several packets and capture traffic patterns, the intrusion detection system (IDS) can either analyze individual packets or aggregate them over a predetermined duration.

Response and Mitigation:

The ML-based IDS initiates a response or mitigation mechanism upon identifying an intrusion or suspicious activity. The response could take many different forms, like sending out alerts or cautions to system administrators or putting in place automated processes to lessen the hazards that have been found. By employing rate limiting, altering firewall rules, or severing or quarantining the intrusion's source, the attack's impact can be reduced. These reaction procedures are designed to keep the network functioning properly while simultaneously safeguarding its assets and preventing additional harm to them. It is imperative to emphasize that in order to prevent false positives and lessen interference with actual network activity, reaction and mitigation methods need to be meticulously established and tested. A thorough framework for enhancing network security and streamlining proactive threat detection and mitigation is offered by the ML-based IDS architecture. Preprocessing data, feature engineering, testing, training, real-time monitoring, and response are all covered. The precision of the machine learning algorithms, the suitability and promptness of the response mechanisms, and the caliber and pertinence of the features all contribute to the architecture's effectiveness.

ISSN: 2278-4632
Vol-11 Issue-09, September 2021

5. BENEFITS AND CHALLENGES OF ML BASED IDS

Benefits:

ML-based intrusion detection systems provide several advantages over conventional rule-based methods. These advantages include:

a) Improved Detection Accuracy: Large data sets can be used by machine learning algorithms to identify subtle patterns that rule-based systems could overlook. Higher detection accuracy as a result makes it possible to identify threats that are both known and unknown.

b) Adaptability to Evolving Threats: Machine learning-based intrusion detection systems have the ability to recognize and adjust to novel attack strategies and variants. ML algorithms have the potential to continuously enhance and upgrade their detection capabilities, reducing the risk of zero-day assaults even as attackers adapt their methods.

c) Reduced False Positives: False positives can be less common when machine learning algorithms thoroughly analyze network traffic patterns. By reducing the number of pointless alerts, this increases operational efficiency and frees up security staff to concentrate on real threats.

d) Increased Efficiency: Massive volumes of network traffic may be processed and analyzed in real time by ML-based IDS systems, which makes threat detection more effective and quick. This might lessen the possible impact of assaults by assisting organizations in responding swiftly to crises.

e) Enhanced Scalability: The volume of network traffic and the growing complexity of threats are both manageable for ML algorithms. Because of its scalability, machine learning-based intrusion detection systems can effectively monitor and safeguard expansive networks while adjusting to dynamic network conditions.

Challenges:

While ML-based intrusion detection systems offer many benefits, they also present unique obstacles that need to be addressed:

a) Data Quality and Variability: To provide consistent and accurate results, machine learning algorithms need training data that is representative, diverse, and of a high caliber. Ensuring the quality and availability of labeled training data might provide a challenge, particularly for novel or uncommon attack kinds.

b) Interpretability and Explain ability: One possible issue with machine learning algorithms, especially deep learning models, is that they can be complicated and challenging to understand. To establish confidence and assess the system's results, security analysts need to comprehend the thought process and logic that go into a decision or detection.

c) Adversarial Attacks: Attackers can use flaws in machine learning algorithms to create biased or corrupted models by tampering with or manipulating training data. One of the main challenges is developing ML-based intrusion detection systems that are resilient to adversarial attempts.

d) Computational Resources: Due to their high memory and processing power requirements, machine learning algorithms can be computationally costly. To address the computational needs for designing ML-based IDS systems, you might need to leverage specialized hardware or cloud resources.

e) Maintenance and Updates: For machine learning models to adjust to evolving network conditions and novel attack tactics, they need to be continuously monitored, updated, and retrained. Maintaining the models' alignment with the changing threat landscape and ensuring the availability of current training data may come at a cost.

f) Privacy and Compliance: Intrusion detection systems that use machine learning look at network traffic, which could include private data. Businesses must maintain data confidentiality and privacy standards compliance in order to apply machine learning techniques efficiently. In order to solve these issues, machine learning-based IDS systems must be equipped with robust data collecting, model validation, interpretability, and security safeguards. Security experts and data scientists must also work together and conduct ongoing research and development.

ISSN: 2278-4632
Vol-11 Issue-09, September 2021

6. SYSTEM ANALYSIS

Dataset Description:

Scholars frequently assess machine learning-based intrusion detection systems' efficacy using publicly accessible datasets that contain actual or fake network traffic data. The quantity of data, the variety of attack types, and the availability of labeled examples all affect the dataset selection procedure. In the subject of IDS research, two datasets are frequently used:

NSL-KDD Dataset: An improved version of the original KDD Cup 1999 data is the NSL-KDD dataset. It is made up of both legitimate and malicious network traffic that was taken from a virtualized setting. The dataset contains labeled instances for training and testing purposes along with a variety of attack types like DoS, probing, and remote-to-local assaults.

Experimental Setup:

Select and set up machine learning methods (e.g., decision trees, SVM, random forests, and deep neural networks) that are suitable for intrusion detection.

a) ML Algorithms: Configuring the ML-based IDS system, training the ML models, and assessing performance are all part of the experimental setup. The setup could consist of the following elements:

b) Feature Selection and Extraction: Select and set up machine learning methods (e.g., decision trees, SVM, random forests, and deep neural networks) that are suitable for intrusion detection.

c) Training and Testing: Separate the dataset into training and testing subgroups. To assess the ML models' performance and accuracy in detecting objects, they are first trained on labeled examples and subsequently assessed on unseen test data.

d) Hyperparameter Tuning: Adjusting the hyperparameters of machine learning algorithms to increase their efficiency. Finding the best values for variables like learning rate, regularization, and tree depth is necessary for this.

e) Cross-Validation: Evaluating the capacity of machine learning models for generalization and reducing the impact of dataset bias through techniques such as k-fold cross-validation.

Performance Evaluation Results:

The results of the performance evaluation assess the F1 score, recall, precision, false positive rate, and detection accuracy as metrics used to measure the efficacy of the ML-based IDS system. The ML models' predictions on the test dataset are used to compute these measures. The outcomes could be utilized to evaluate the ML-based IDS system's overall effectiveness and learn more about its advantages and disadvantages. Depending on the goals of the study, measures like resource usage, scalability, and detection time may also be included in performance evaluation.

COMPARATIVE ANALYSIS:

A comparison study is one method of determining the effectiveness of the ML-based IDS system. In order to accomplish this, it is necessary to evaluate the effectiveness of various machine learning methods, feature selection strategies, or variants of the ML-based IDS system. The objective of the comparison study is to identify the most effective intrusion detection methods or strategies by examining the advantages and disadvantages of each. It may employ statistical tests, visualizations, or other analytical techniques to obtain a comprehensive understanding of the various plans. By employing datasets such as UNSW-NB15 and NSL-KDD in case studies and tests, researchers and professionals can gain a more comprehensive understanding of the effectiveness of machine learning-based intrusion detection systems. These findings may also be employed to enhance the reliability and effectiveness of intrusion detection systems.

Table 1. The ML is established during the project's establishment.

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

ISSN: 2278-4632
Vol-11 Issue-09, September 2021

Table 2. Results of Performance Assessment

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	Variationsof 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

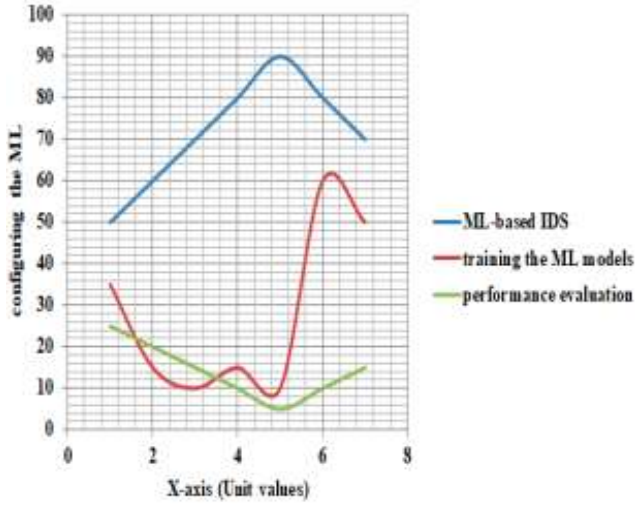

Fig. 3. Machine learning (ML) settings are included in line chart design.

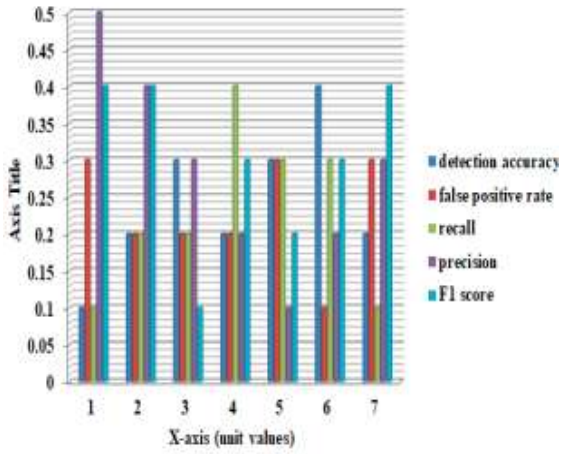

Fig. 4. Bar Chart of Evaluation Results

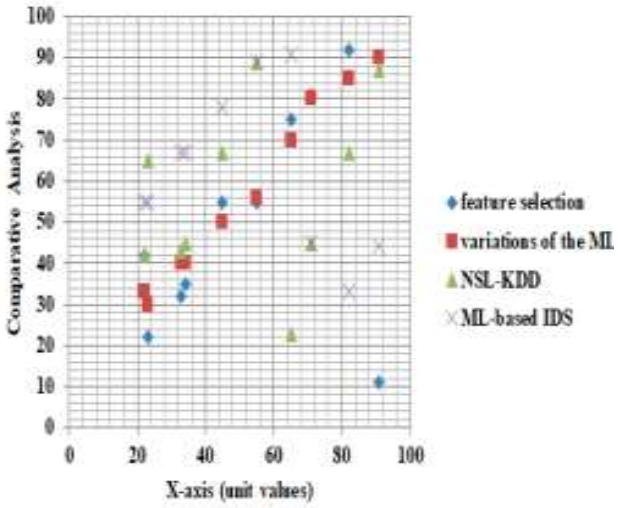

Fig. 5. Scatter diagrams for comparative comparison are used in machine learning.

7. LIMITATION AND FUTURE DIRECTION

Limitations of ML-Based IDS:

Despite the numerous advantages of ML-based intruder detection systems, there are also certain issues that should be considered:

a) Lack of Explain ability: It can be challenging to identify the factors that influence the results of machine learning algorithms and detections, particularly those that are profound. ML-based intrusion detection systems are difficult to trust and employ in critical and controlled scenarios due to their inability to articulate themselves.

b) The evade detection by exploiting vulnerabilities in the ML algorithms: ML-based IDS systems may become less effective and reliable due to threats from external sources.

c) Insufficient and Biased Training Data: Neither are machine learning methods particularly adept at identifying or generalizing objects. It can be challenging to train machine learning models to be accurate when it is difficult to obtain labeled data for specific types of attacks or new threats.

d) Computational Resource Requirements: Machine learning (ML)-based intrusion detection systems may necessitate specialized hardware or cloud resources during the setup and scaling process, which could result in increased operating expenses. The reason for this is that machine learning methods, particularly deep learning

ISSN: 2278-4632
Vol-11 Issue-09, September 2021

models, require a significant amount of memory and processing capacity.

e) Dynamic and Evolving Threat Landscape: Machine learning-based intrusion detection systems struggle to remain current with emerging threats due to the constant development of new methods by attackers to evade detection. In order to ensure that machine learning models are capable of identifying and mitigating risks, it is crucial that they receive consistent updates, undergo retraining, and be closely monitored.

FUTURE RESEARCH DIRECTIONS:

a) Explainable AI for IDS: In order to facilitate intrusion detection, devising methods to simplify and elucidate machine learning models. This could entail the development of comprehensible explanations for model decisions, the utilization of rule-based explanations, or the application of feature importance analysis.

b) Adversarial Robustness: Seeking methods to enhance the resilience of ML-based IDS systems to assaults from malicious actors. This may involve the use of adversarial example detection, anomaly detection methods, or adversarial training to identify and prevent individuals from altering test or training data for malicious purposes.

c) Transfer Learning and Few-shot Learning: Utilizing pre-trained machine learning models or transfer learning to investigate methods for enhancing detection performance in the absence of sufficient labeled data. Few-shot learning can assist IDS systems in promptly responding to new attack types or variations due to the scarcity of labeled examples.

d) Hybrid Approaches: Investigating the potential for machine learning-based and standard rule-based methods to collaborate in order to optimize their respective capabilities. Hybrid methods employ machine learning algorithms to enhance the precision of detection, reduce the incidence of false positives, and provide contextual information.

e) Privacy-preserving ML for IDS: Developing methods that facilitate the detection of intrusions and the protection of data privacy. One potential approach to safeguarding private network data is to implement privacy-enhancing techniques such as secure multiparty computation, differential privacy, or federated learning during the training and inference phases.

f) Adaptive and Dynamic Models: A machine learning-based intrusion detection system that is capable of adapting to new network conditions and attacks in real time. It may be necessary to implement reinforcement learning or online learning techniques in order for the system to modify its own mitigation and detection protocols. These research areas will assist machine learning-based intrusion detection systems in overcoming their current deficiencies, thereby increasing their reliability and safeguarding networks from constantly evolving cyberthreats.

8. CONCLUSION

In summary, intruder detection systems that employ machine learning have been demonstrated to be highly effective in enhancing the security of networks. They provide improved detection accuracy, reduced false positives, and the ability to adjust to new threats. Conversely, it is imperative to promptly address concerns such as interpretability, computational resources, adversarial threats, and data quality. A significant amount of future research will be conducted on adaptive models, adversarial robustness, hybrid techniques, explainable AI, transfer learning, and machine learning that safeguards privacy. By addressing these issues and conducting new research, ML-based intrusion detection and prevention systems can significantly enhance network security and facilitate the identification and prevention of threats prior to their occurrence.

REFERENCES

1. 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.
2. Kaushik, K., Garg, M., Annu, Gupta, A. and Pramanik, S. (2021). Application of Machine Learning and Deep Learning in

ISSN: 2278-4632
Vol-11 Issue-09, September 2021

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.

3. 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
4. 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, vol37. Springer, Singapore. https://doi.org/10.1007/978-981-19-0151-5_23
5. Idrees, S., Raza, S., Bakar, K. A., & Ahmed, M. A. (2020). Machine learning-based network intrusion
6. Alazab, M., Hobbs, M., Abawajy, J., & Alazab, M. (2019). Machine learning-based intrusion detection systems: A comprehensive survey. Computers & Security, 78, 398-422.
7. 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.
8. Xu, Z., & Zhang, G. (2020). Deep learning-based network intrusion detection: A comprehensive review. IEEE Access, 8, 165900-165917.
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)