ISSN: 2366-1313

Enhancing Network Security through Machine Learning Based Intrusion Detection Systems

Gujju Bhaskar Rao, Research Scholar and Dr. Suribabu Potnuri, Professor, Supervisor, Department of Computer Science and Engineering, J.S. University, Shikohabad, U.P; B.Laxmikantha, Co-Supervisor, Malla Reddy Institute of Engineering and Technology,Hyderabad,India email: bhaskarrao.g@gmail.com

ABSTRACT

For the purpose of protecting network infrastructures, the development of security systems that are both robust and intelligent has become necessary as the complexity and sophistication of cyber-attacks continues to grow. Specifically in the realm of intrusion detection systems (IDS), machine learning (ML) technologies have become more significant in terms of their contribution to the enhancement of network security. In order to enhance the safety of computer networks, the purpose of this research project is to evaluate the use of machine learning techniques within the context of intrusion detection systems (IDS). The paper examines a number of different machine learning methodologies, as well as their benefits and challenges. Additionally, it provides insightful thoughts on the incorporation of machine learning-based intrusion detection systems into modern network topologies. The report also places an emphasis on the potential limitations and areas that need additional exploration in relation to this evolving topic.

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

1. INTRODUCTION

The system is continuously monitoring the flow of data across the network and precisely recognizing any behaviors that may be damaging or suspicious [1]. Conventional intrusion detection systems (IDS) often rely on pre-established rules and signatures, which makes them less effective in defending against attacks that are both dynamic and complicated. Machine learning (ML) techniques have received a significant amount of attention for the purpose of enhancing network security via the use of intelligent and adaptive intrusion detection systems (IDS) in order to circumvent this limitation.

2. Problem Statement

Because of the negative effects of rising detection latency and the increased dangers to network security, there is a need to develop Intrusion Detection Systems (IDS)

ISSN: 2366-1313

that are more advanced and intelligent. These IDS should be able to accurately recognize and classify aberrant network activity in real time.

3. Methodology

The subjects that are discussed include network security, machine learning-based intrusion detection systems, and other issues linked with these areas.

Collecting Data: For the aim of training and assessing, it is necessary to collect and analyze datasets that include information about network traffic, events of intrusion, and essential features.

The process of selecting the most effective algorithms for intrusion detection is referred to as "algorithm selection."

Model Development: Using certain methods, develop machine learning models, and then incorporate those mols into the architecture of the intrusion detection system.

Performance Evaluation: It is necessary to evaluate the performance of the Intrusion Detection System (IDS) that is based on machine learning by carrying out experiments and assessing metrics such as accuracy, precision, recall, and false positive rate.

Evaluating the efficacy of the machine learning-based Intrusion Detection System (IDS) in contrast to traditional rule-based methodologies in order to evaluate the amount of improvements gained is the objective of the comparative analysis.

guidelines: Based on the findings of the research, provide suggestions for guidelines and best practices for the implementation and deployment of intrusion detection systems (IDS) that make use of machine learning.

In order to achieve its goal, the research will adhere to this methodology in order to gather insights into the real implementation of technologies that significantly improve network security.

4. INTRUSION DETECTION SYSTEM

Definition and Classification:

It is necessary to monitor and assess the endpoints, which are the activities that are taking place on the host [6]. They are tasked with the responsibility of collecting and analyzing data, which includes system logs, file integrity, and user activity, with the goal of identifying any intrusions or anomalies that may have occurred. In order to keep track of the traffic that is moving across a network, network-based intrusion detection systems (NIDS) are strategically placed within the network. An examination of network packets, protocols, and other signs at the network level is carried out by the analysts in order to discover any potentially malicious or suspicious transactions. National Intrusion

ISSN: 2366-1313

Detection System (NIDS) has the flexibility to operate in either a passive mode, in which it only monitors network traffic, or an active mode, in which it takes preventative actions to safeguard against threats that have been recognized.

5. Traditional IDS Approaches:

Signatures are used in conventional intrusion detection systems, which are rule-based. Rule-Based Intrusion Detection System (IDS): Intrusion Detection Systems (IDS) that function according to rules compare the events or activities that have been seen with a set of rules that have been specified. When a rule can be found to connect with an occurrence, an alert is generated. It is possible to define rules based on specific patterns, methods, or behaviors that are associated with attacks that have been identified [7]. However, rule-based intrusion detection systems (IDS) have limited effectiveness when faced with fresh or unexpected attacks. This is due to the fact that these systems primarily rely on pre-established rules and do not have the potential to adapt to new threats as they emerge.

A. 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.

ISSN: 2366-1313

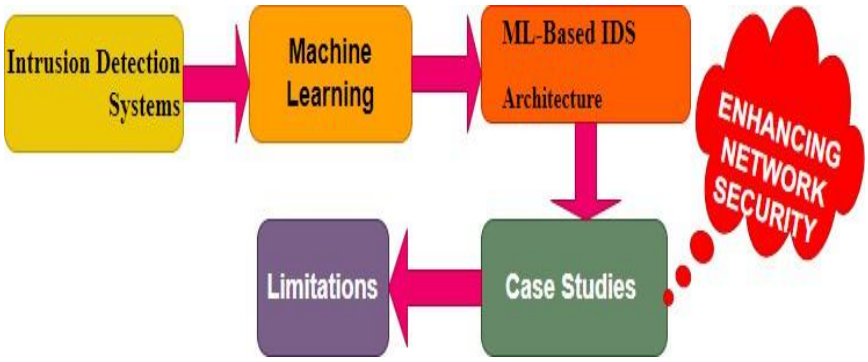

Fig. 1. Process on ENS

6. MACHINE LEARNING FOR INTRUSION DETECTION

Machine learning algorithms have the capacity to independently gain information about patterns, correlations, and anomalies from a collection of data that is utilized for training purposes. The fact that they possess this quality makes them exceptionally well-suited for the function of intrusion detection systems (IDS) [9]. Some examples of supervised learning techniques that are often used in intrusion detection systems (IDS) include [10].

Unsupervised Learning:

When applied to data that does not include any labels, unsupervised learning algorithms seek to discover patterns or structures that are already present in the data. Their goal is to discover these patterns or structures. It is possible to apply unsupervised learning in Intrusion Detection Systems (IDS) to find irregularities or identify behavior that is not usual in network traffic [11]. The following are examples of unsupervised learning approaches that are often used in Intrusion Detection Systems (IDS): [12].

Clustering:

Clustering methods are used to classify occurrences that are comparable by analyzing the degree to which their characteristics are identical to one another. Because of this, it is possible to identify irregularities in the pattern of network activity that are not typical. Principal Component Analysis, often known as PCA, is a statistical method that is used to minimize the dimensionality of a dataset while simultaneously preserving the maximum amount of information that can be obtained. Principal Component Analysis, often known as PCA, is a method that may be used to reduce the dimensionality of data while maintaining its variability. For the purpose of determining the most significant features or factors that have the largest influence on the total variability in the data, it is often

ISSN: 2366-1313

used in the fields of data analysis and machine learning. Because of this, it is possible to acquire a representation and presentation of data connected to network traffic that contains a significant number of dimensions that is more efficient

Reinforcement Learning:

Through the process of having an agent interact with an environment and receiving feedback in the form of incentives or penalties, reinforcement learning systems are able to acquire optimal behaviors. Even though reinforcement learning is not often used directly in Intrusion Detection Systems (IDS), it has the potential to be utilized in adaptive IDS systems in order to dynamically adjust security tactics in accordance with the conditions of the network and feedback.

7. Feature Selection and Extraction:

When it comes to Intrusion Detection Systems (IDS) that make use of machine learning methods, the steps of feature selection and extraction are quite important. The technique comprises locating relevant network traffic properties that are capable of correctly depicting the characteristics of both legitimate and malicious activities.

The purpose of feature selection techniques is to pick a smaller collection of features that provide the most valuable information. This, in turn, helps to minimize the complexity of the data and enhances the speed at which computation can be performed. Feature extraction techniques transform the initial data on network traffic into a feature space that has fewer dimensions. This facilitates the preservation of critical information while simultaneously removing material that is either unnecessary or duplicated. The methods of correlation analysis, information gain, principal component analysis (PCA), and autoencoders are examples of typical procedures that are used in the process of choosing and extracting features.

8. Performance Evaluation Metrics:

There are several different performance evaluation criteria that are used in order to evaluate the effectiveness of Intrusion Detection Systems (IDS) that are based on machine learning. Through the use of these indicators, significant information on the accuracy and reliability of the intrusion detection system may be obtained. The following [13] are examples of typical criteria that are used to evaluate the performance of intrusion detection systems (IDS): Academics and practitioners alike may benefit from these performance evaluation criteria when it comes to analyzing the advantages and disadvantages of different machine learning algorithms and determining whether or not they are suitable for use in intrusion detection systems [14].

ISSN: 2366-1313

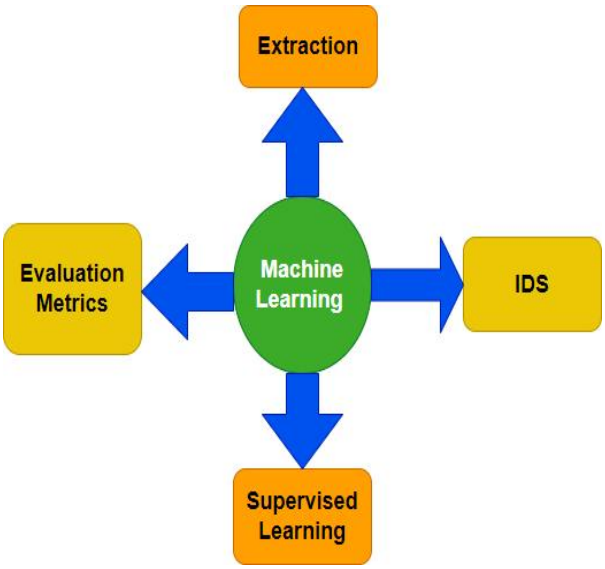

Fig. 2. Machine Learning for Intrusion Detection on various techniques

9. ML based IDS Architecture

The first step in the process of designing an intrusion detection system (IDS) that is based on machine learning (ML) is the completion of the data preparation stage. The duties of cleaning, transforming, and normalizing the raw data that pertains to network traffic are included in this. The importance of this step cannot be overstated when it comes to assuring the quality and consistency of the data before moving on to any further investigation [15]. When it comes to feature engineering, the process entails the meticulous selection and construction of pertinent features from the data that has been preprocessed. For the purpose of extracting features that properly describe the characteristics of both normal and malicious network activity, domain knowledge, in combination with statistical and information-theoretic approaches, is used. These properties serve as inputs to the machine learning algorithms, which are used for the purposes of training and detection respectively.

10. Training and Testing

Following the retrieval of the features, the intrusion detection system (IDS) that is based on machine learning will next proceed to the training phase. A machine learning model is trained during this phase by using the training dataset, which contains labeled instances of both normal and malicious traffic. This phase is also known as the training phase. It is possible to develop the model by using a variety of machine learning strategies, including decision trees, neural networks, and support vector machines (SVM), according to the requirements. During the process of training, the model develops the capacity to recognize and comprehend the patterns and relationships that exist between certain features and the classifications that are associated with them. "[16]" comes from the user's text.

ISSN: 2366-1313

11. Real-time Monitoring and Alerting

During the period of real-time monitoring, the intrusion detection system (IDS) that is based on machine learning continuously analyzes incoming network traffic by making use of the model that it has learnt. During the process of collecting and analyzing network packets, the intrusion detection system (IDS) use the machine learning model to classify them as either normal or perhaps malicious. In the event that the model detects an intrusion or an anomalous behavior, it will either generate an alert or begin a response. It is possible to carry out real-time monitoring at a number of different network locations, such as network edges, routers, or specialist intrusion detection systems (IDS) equipment. Within a certain amount of time, the Intrusion Detection System (IDS) is able to analyze individual packets or combine them in order to recognize traffic patterns and recognize complicated attacks that include a large number of packets.

12. Response and Mitigation

An incursion Detection System (IDS) that is based on machine learning will begin a response or mitigation mechanism if it detects an incursion or activity that is suspicious. It is possible that the response will range from sending alerts or messages to system administrators to using automated procedures in order to combat the threats that have been discovered. applying actions such as blocking or isolating the origin of the illegal access, altering the settings of the firewall, or applying rate limitation are all potential reaction techniques that might be used in order to mitigate the impacts of the attack. These response actions are being carried out with the intention of protecting the network and its assets from any additional damage and ensuring that network operations continue to run without interruption. It is of the utmost importance to underline that the response and mitigation measures must be thoroughly created and validated in order to eliminate false positives and limit interference with the actual operation of the network infrastructure. Data preprocessing, feature engineering, training, testing, real-time monitoring, and reaction are some of the processes that are included in the architecture of the machine learning-based intrusion detection system (IDS). A proactive approach to identifying and mitigating potential risks is the goal of this methodology, which strives to enhance network security. The effectiveness of the architecture is dependent on the quality and relevance of the characteristics, the accuracy of the machine learning algorithms, the promptness and appropriateness of the reaction mechanisms, and the precision of the response mechanisms.

13. BENEFITS AND CHALLENGES OF ML BASED IDS

A. Benefits:

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

Improved Detection Accuracy:

ISSN: 2366-1313

Algorithms that are based on machine learning have the capacity to gain knowledge from vast volumes of data and recognize nuanced patterns that would not be recognized by systems that are based on predetermined rules. As a consequence, this leads to an improvement in detection precision, which enables the identification of both known and unknown threats.

Adaptability to Evolving Threats:
The power to modify and gather information from fresh attack tactics and alterations is provided by intrusion detection systems that are based on machine learning. It is possible for machine learning algorithms to modify and improve their detection capabilities in order to combat developing attack strategies, hence lowering the system's susceptibility to zero-day attacks.

Reduced False Positives:
The use of machine learning algorithms allows for a more comprehensive examination of patterns in network data, which ultimately results in a reduction in the frequency of false detections. By reducing the number of unnecessary alerts, security teams are able to focus their attention on actual threats, which ultimately results in an increase in operational efficiency.

Increased Efficiency:
Intrusion Detection Systems (IDS) that are based on machine learning have the capacity to quickly and accurately detect threats. This is accomplished by processing and analyzing huge volumes of network data in real time in a quick and efficient manner. It is conceivable that putting this strategy into action will make it feasible for businesses to quickly fix problems, therefore reducing the potential effects of attacks.

.

Enhanced Scalability:
The ever-increasing volumes of network traffic and the ever-increasing complexity of threats may be effectively managed by machine learning algorithms, which have the capacity to do so efficiently. Intrusion detection systems that are based on machine learning have the ability to extend, which allows them to effectively monitor and protect broad networks while simultaneously adapting to changing network conditions.

.

B. Challenges:

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

ISSN: 2366-1313

Data Quality and Variability:

In order for machine learning algorithms to provide results that are accurate and reliable, they need training data that is of a high quality, is representative of the population, and includes a broad variety of variances. It is possible that securing an appropriate amount of correctly labeled training data will be a challenging undertaking, particularly when dealing with assaults that are either unusual or being developed for the first time.

Interpretability and Explainability:

There is a possibility that machine learning algorithms, and deep learning models in particular, are difficult to comprehend due to their complexity. In order for security analysts to have trust in the outcomes of the system and verify them, it is vital for them to get an understanding of the process and the reasoning that lies behind a decision or detection.

Adversarial Attacks:

Artificial intelligence algorithms may be susceptible to exploitation by malicious actors that corrupt or poison training data, which may lead to models that are prejudiced or compromised. Ensuring that intrusion detection systems that are based on machine learning are robust enough to withstand attacks from adversaries is a challenge that is both essential and difficult to do.

Computational Resources:

It is possible that machine learning approaches are computationally intensive, which means that they need a significant amount of computer capability and memory resources. When deploying intrusion detection systems (IDS) that are based on machine learning, it may be necessary to make use of specialized hardware or cloud resources in order to properly manage the computational needs.

.

Maintenance and Updates:

It is vital for machine learning models to undergo continuous monitoring, updates, and retraining in order for them to properly react to new attack strategies and shifting network conditions. It may be necessary to allocate a large amount of resources in order to guarantee access to the most recent training data and to keep the model consistent with the ever-evolving threat environment.

Privacy and Compliance:

Intrusion Detection Systems (IDS) that are based on machine learning analyze network traffic, which may include sensitive information to some extent. Organizations have a responsibility to

ISSN: 2366-1313

ensure that they comply to privacy requirements and maintain the security of data while also making effective use of machine learning strategies. It is necessary to continuously conduct research and development in order to address these issues. Additionally, it is necessary to encourage collaboration between data scientists and security professionals, as well as to provide robust procedures for the collection of data, validation of models, interpretability, and security in machine learning-based intrusion detection systems.

14. CASE STUDIES AND EXPERIMENTS

For the purpose of evaluating the effectiveness of machine learning-based intrusion detection systems (IDS), researchers often make use of datasets that are available to the public and may include either real or artificially created network traffic data. When choosing a dataset, it is important to take into consideration a number of factors, including the number of different types of attacks, the amount of data, and the availability of labeled instances. The following are two datasets that are often used for research on intrusion detection systems (IDS): [18]

This dataset is the NSL-KDD. The NSL-KDD dataset is an updated version of the first dataset that was awarded at the KDD Cup in 1999. The collection is made up of both benign and malicious network traffic that was found to have been captured from a simulated environment. An assortment of attack techniques, including as denial of service (DoS), probing, and remote-to-local attacks, are included in the dataset. In addition to that, it contains annotated instances that may be used for the purposes of teaching and testing.

A. 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:

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

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

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.

Hyperparameter Tuning: Tuning the hyperparameters of the ML algorithms to optimize their performance. This involves

ISSN: 2366-1313

selecting suitable values for parameters such as learning rate, regularization, or tree depth.

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.

15. Performance Evaluation Results:

The outcomes of the performance evaluation provide quantifiable assessments of the effectiveness of the machine learning-based intrusion detection system (IDS) in terms of its detection accuracy, false positive rate, recall, precision, and F1 score and other metrics. The machine learning models that were applied to the test dataset were responsible for producing the predictions that were used to calculate these measures.

The results may serve as an indicator of the overall performance of the intrusion detection system (IDS) that is based on machine learning and give useful insights into the inherent benefits and limits of the system. As an additional point of interest, performance evaluation may include characteristics such as detection time, resource consumption, and scalability, all of which are contingent on the specific objectives of the particular research [19].

16. Comparative Analysis:

A comparative study is something that may be done in order to assess the efficiency of the Intrusion Detection System (IDS) that is based on machine learning. In order to do this, it is necessary to assess the effectiveness of a number of different machine learning algorithms, methods for picking features, or many iterations of the machine learning-based intrusion detection system.

A comparative research is being conducted with the objective of identifying the best effective algorithms or techniques for intrusion detection, with a particular focus on highlighting both their strengths and flaws [20]. The procedure may include the use of statistical tests, visualizations, or other analytical methods in order to carry out a comprehensive evaluation of the many choices that are available. The efficacy of machine learning-based intrusion detection systems may be better understood via the use of case studies and experiments that make use of datasets such as NSL-KDD or UNSW-NB15. These studies provide academics and practitioners with a better understanding of the capabilities and limitations of these systems, which in turn makes it easier to build solutions that are more robust and effective in detecting unwanted access.

.

ISSN: 2366-1313

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

ISSN: 2366-1313

9	23	22	30	65	55
10	33	32	40	43	67

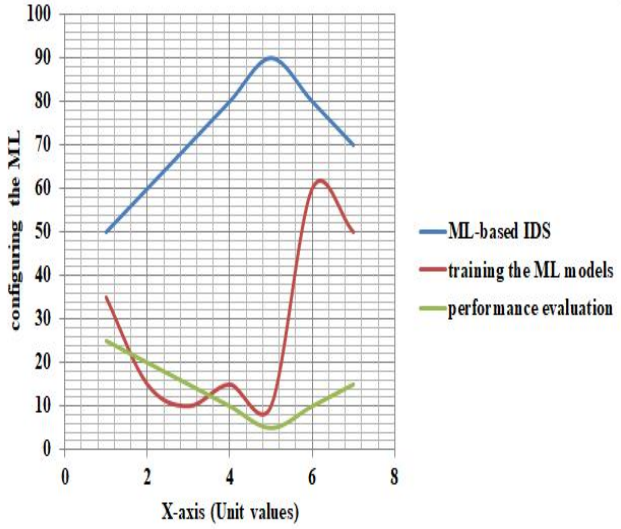

Fig. 3. Line chart for setup involves configuring the ML

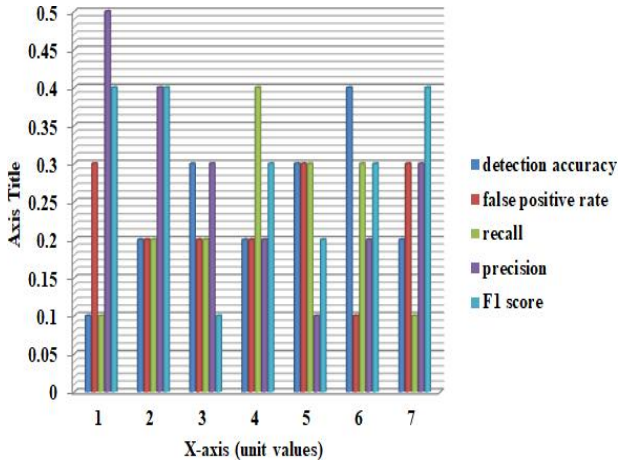

Fig. 4. Bar Chart for Evaluation Results

ISSN: 2366-1313

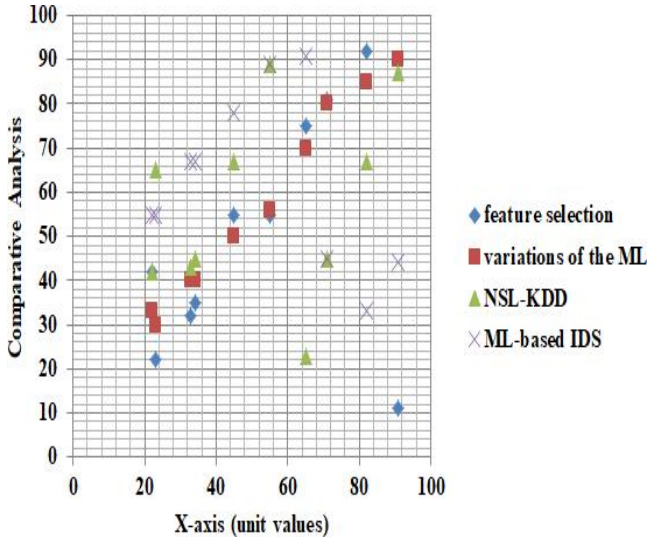

Fig. 5. Scatter diagram for Comparative Analysis in ML

17. LIMITATION AND FUTURE DIRECTION

A. Limitations of ML-Based IDS:

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

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.

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

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.

Computational Resource Requirements: For the sake of implementation and scalability, machine learning techniques, and deep learning models in particular, may be demanding in terms of the computer resources that are available. A significant amount of processing power and memory capacity is required. In order to function properly, machine learning-based intrusion detection systems (IDS) could need specialized hardware or cloud resources, which would result in increased running costs.

.

Dynamic and Evolving Threat Landscape: Attackers constantly develop new techniques and evasion strategies,

ISSN: 2366-1313

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.

B. Future Research Directions:

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

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.

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.

Transfer Learning and Few-shot Learning:

In circumstances when there is a lack of labeled data, it is important to investigate approaches that may improve detection accuracy. These methods include transfer learning and the use of pre-trained machine learning models. By using few-shot learning approaches, intrusion detection systems have the ability to swiftly adapt to new attack types or variations with a low number of labeled cases.

.

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.

Privacy-preserving ML for IDS:

in addition to providing effective intrusion detection, the development of procedures that protect the confidentiality of data. During the training and inference phases, this may involve the use of privacy-enhancing approaches like as federated learning, secure multiparty computing, or differential privacy in order to protect sensitive network data.

Adaptive and Dynamic Models:

The development of intrusion detection systems (IDS) that are based on machine learning and have the capability to adapt in a flexible manner to changing network conditions and evolving attack strategies. One example of this would be the use of

ISSN: 2366-1313

reinforcement learning or online learning techniques, which would enable the system to autonomously adjust its detection and mitigation operations.

By concentrating on these study subjects, machine learning-based intrusion detection systems (IDS) may be able to transcend the constraints that are now in place, improve their resilience and reliability, and play a crucial role in strengthening network security against cyber threats that are always evolving.

18. CONCLUSION

Through the use of machine learning, intrusion detection systems have evolved into powerful instruments for enhancing network security. Their characteristics include increased accuracy in identifying threats, the ability to adapt to shifting threats, and a reduction in the number of false positives that occur. Nevertheless, it is of the utmost importance to address challenges such as the precision of the data, the capability to comprehend and analyze the outcomes, the possibility of malicious attacks, and the availability of computing power. Explainable artificial intelligence, adversarial resilience, transfer learning, hybrid techniques, privacy-preserving machine learning, and adaptable models are some of the potential topics for further research in the future. As a result of addressing these challenges and doing cutting-edge research, machine learning-based intrusion detection systems have the potential to significantly enhance network security and make early detection and prevention of attacks easier.

.

19. 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.

ISSN: 2366-1313

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).

13) Network intrusion detection using machine learning: A systematic review. Future Generation Computer Systems, 102, 798-808.

14) 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.

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

16) Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, C. Wang, Machine

ISSN: 2366-1313

learning and deep learning methods for cybersecurity. IEEE Access 6, 35365–35381 (2018)

17) 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)

18) 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)