International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307

OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/CSEIT24104128

Review of Intrusion Detection System for Prediction of Cyber Attacks using AI Techniques

Divya Yadav[1], Prof. Chetan Gupta[2], Dr. Ritu Shrivastava[3]

M. Tech. Research Scholar[1], Assistant Professor[2], Professor[3]

Department of CSE, SIRTS, Bhopal, India[1], Department of CSE, SIRT, Bhopal, India

ARTICLEINFO

Article History:

Accepted : 05 Aug 2024

Published: 16 Aug 2024

Publication Issue

Volume 10, Issue 4

July-August-2024

Page Number

275-281

ABSTRACT

The ever-evolving threat landscape of cyber-attacks necessitates continuous advancements in intrusion detection systems (IDS). This paper delves into the application of Artificial Intelligence (AI) techniques to enhance the predictive capabilities of IDS. We explore the limitations of traditional signature-based and anomaly-based IDS approaches and highlight the potential of AI methods like machine learning (ML) and deep learning (DL) for identifying and predicting novel and sophisticated cyber-attacks. By integrating AI into IDS, organizations can bolster their cyber security posture, proactively mitigate threats, and safeguard their critical infrastructure.

Keywords : IDS, Cyber, AI, NIDS, HIDS, Security.

I. INTRODUCTION

In today's interconnected world, cyber-attacks pose a constant threat to organizations of all sizes. Malicious actors relentlessly develop novel attack vectors, targeting networks and systems to steal data, disrupt operations, or cause financial damage. To combat this evolving threat landscape, intrusion detection systems (IDS) serve as a critical line of defense. These systems continuously monitor network traffic and system activity, seeking patterns indicative of unauthorized access or malicious activity.

Traditional IDS approaches primarily rely on signature-based detection, which compares network traffic patterns to a predefined database of known attack signatures. While effective against known threats, this approach struggles to identify novel attacks that lack a pre-defined signature. Anomaly-based IDS, on the other hand, attempts to detect deviations from normal network behavior. However, these systems can generate a high number of false positives, making it difficult to distinguish between legitimate activity and actual attacks.

The limitations of traditional IDS methods necessitate a paradigm shift towards more sophisticated and adaptive detection mechanisms. Here, Artificial Intelligence (AI) emerges as a game-changer. By leveraging AI techniques like machine learning (ML) and deep learning (DL), IDS can evolve beyond static signatures and learn to recognize complex attack patterns in real-time. Machine learning algorithms can be trained on vast datasets of network traffic and attack

simulations, enabling them to identify subtle anomalies and predict potential cyber-attacks with greater accuracy.

Deep learning, a subset of ML, utilizes artificial neural networks with multiple layers to process and analyze complex data. Deep learning models can be trained to discover hidden patterns within network traffic data, allowing them to identify even the most sophisticated and obfuscated cyberattacks. This advanced predictive capability empowers organizations to proactively mitigate threats before they can inflict significant damage.

Figure 1: Cyber security

The integration of AI into IDS offers several advantages beyond improved threat detection. AI-powered IDS can automate the analysis of vast quantities of network data, freeing up IT security personnel to focus on more strategic tasks. Additionally, AI models can continuously learn and adapt to new attack vectors, ensuring that detection capabilities remain relevant in the face of ever-evolving threats.

However, the implementation of AI-powered IDS comes with its own set of challenges. The effectiveness of AI models hinges on the quality and quantity of data available for training. Additionally, ensuring the interpretability and explainability of AI-based decisions is crucial for building trust within security teams. These challenges and potential solutions will be explored in a later section of this paper.

In conclusion, AI represents a powerful tool for enhancing the predictive capabilities of Intrusion Detection Systems. By leveraging AI techniques, organizations can develop more robust cyber security defenses, proactively identify and mitigate cyber-attacks, and safeguard their critical infrastructure in an increasingly perilous digital landscape. As AI technology continues to evolve and adapt, its role in shaping the future of intrusion detection is certain to become even more pivotal.

II. LITERATURE SURVEY

S. Ho et al.,[1] IDS model has been created with the purpose of identifying network intrusions by categorizing all of the packet traffic in the network as either benign or malicious. Training and validation of the suggested model were carried out with the use of the dataset that was provided by the Canadian Institute for Cyber security Intrusion Detection System (CICIDS2017). A number of metrics, including the overall accuracy, attack detection rate, false alarm rate, and training overhead, have been analyzed and evaluated for the model. A comparative analysis of the performance of the suggested model in comparison to nine other well-known classifiers has been published.

It is possible to identify such incursions with the use of datasets and by continuously updating them, as stated by V. K. Navya et al. [2]. One technique that stands out is the Deep Neural Network (DNN), which is a sort of deep learning model. This algorithm contributes to the development of an Intrusion Detection System (IDS) that is both flexible and effective, allowing it to detect and categorize cyberattacks that are unexpected and unpredictable.

In order to enhance the detection of cyberattacks, Y. A. Farrukh et al., [3] offer a two-layer hierarchical machine learning model that has an accuracy of 95.44%. The initial layer of the model is used to differentiate between the two modes of operation, which are classified as either the normal state or the cyberattack. The second layer is that which is utilized for the purpose of categorizing the state into various kinds of cyberattacks. With the layered method, the model is given the option to concentrate its training on

the specific task that is being performed by the layer, which ultimately leads to an improvement in the accuracy of the model.

According to S. Thirimanne [4], the primary objective of this research is to identify the most effective machine learning algorithm for intrusion detection. This algorithm will be trained using the NSL-KDD and the UNSW-NB15 datasets. Additionally, a comparative analysis will be carried out between six different machine learning algorithms that are classified as supervised, semi-supervised, and unsupervised learning. Support Vector Machines (SVM) and Deep Neural Networks (DNN) perform better for NSL-KDD and UNSW-NB15, respectively, according to the findings of this study, which showed that the performance of supervised and semi-supervised machine learning algorithms outperformed the performance of unsupervised machine learning algorithms for both datasets.

An overview of DRL strategies that have been developed for cyber security was presented by T. T. Nguyen [5]. We concentrate on many critical topics, including DRL-based security methods for cyber-physical systems, autonomous intrusion detection techniques, and multiagent DRL-based game theory simulations for defense strategies against cyberattacks. Extensive discussions and future research ideas on DRL-based cyber security are also included in this article. We anticipate that this exhaustive evaluation will lay the groundwork for future research on examining the potential of emerging DRL to deal with more complex cyber security issues and will also make it easier for such research to be conducted.

The model that was provided by W. Xu et al. [6] makes use of the most efficient reconstruction error function, which is a crucial component in the model's ability to determine whether a network traffic sample is normal or abnormal. Because of these sets of unique methodologies and the ideal model architecture, our model is able to be better equipped for feature learning and dimension reduction, which ultimately results in improved detection accuracy as well as f1-score. We assessed our suggested model on the NSL-KDD dataset, which outperformed other approaches that were comparable by achieving the greatest accuracy and f1-score in detection, which were respectively 90.61% and 92.26%.

The attention mechanism developed by K. Cao et al. [7] is applied in order to accurately collect essential qualities that are representative of the structural properties of traffic data. In addition, a CuDNN-based long short-term memory network is utilized in order to swiftly accelerate the convergence of the model while simultaneously learning time-related information regarding the traffic. Finally, global maxpooling is implemented in order to improve the generalization capabilities of the proposed model and to reduce the amount of data that is included inside it. The results of the experiments conducted on the UNSW-NB15 dataset demonstrate that the suggested model has an accuracy of binary classification that can reach up to 92.65%. In addition to that, it has an accuracy of 81.28% when it comes to identifying different types of attacks.

In the study by I. Ullah [8], a multiclass classification model is developed with the help of a convolutional neural network model. After that, the proposed model is put into action by employing convolutional neural networks in one-dimensional, two-dimensional, and three-dimensional space. The BoT-IoT, IoT Network Intrusion, MQTT-IoT-IDS2020, and IoT-23 intrusion detection datasets are utilized in order to evaluate the convolutional neural network model that has been presented. Through the utilization of a convolutional neural network multiclass pre-trained model, transfer learning is utilized to achieve binary and multiclass classification.

According to D. Park et al. [9], a model for an intrusion detection system that is based on deep learning has been developed. This model examines sophisticated attack patterns by performing data learning. Deep learning models, on the other hand, have the drawback of having to teach themselves new information every time a new cyberattack strategy is discovered. The

amount of time that is necessary to learn a substantial amount of data is not beneficial. Using the Leipzig Intrusion Detection Data Set (LID-DS), which is a host-based intrusion detection data set that was released in 2018, an experiment was carried out for the purpose of this study.

An outlier detection (also known as anomaly detection) problem and a challenging multiclass classification problem consisting of 14 classes (13 Modbus/TCP cyberattacks and normal instances) were successfully solved by the proposed intrusion detection system (IDS) that was developed by I. Siniosoglou et al. [10]. This IDS was validated in four real-world SG evaluation environments, which are as follows: (a) SG lab, (b) substation, (c) hydropower plant, and (d) power plant. Also, MENSA is able to differentiate between five different cyberattacks directed on DNP3.

For the purpose of providing distributed intrusion detection engines with privacy, c. Gupta et al. [11] have created Peer privacy-preserving intrusion detection techniques are compared with the Previous framework, and the results of the experiments show that the DBF framework performs better than the other competing models. The framework has the potential to be utilized as a decision support system that can provide users and cloud providers with assistance in the process of securely moving their data in a timely and dependable manner.

C. Gupta [12] introduced a new feature selection method, which was validated using the NSL-KDD dataset. Through the use of this method, the dimensionality of the dataset is decreased, and the efficiency of the calculations is considerably improved. In order to determine whether or whether the new feature selection method is more effective in terms of calculation efficiency, the KNN algorithm is utilized.

III.PROBLEM IDENTIFICATION

The problem domain of Intrusion Detection Systems (IDS) for the prediction of cyber attacks encompasses the need to safeguard information systems from unauthorized access, malicious activities, and security breaches. As cyber threats become increasingly sophisticated and frequent, traditional IDS methods, which often rely on signature-based detection, are insufficient. These methods struggle with:

- **Detecting Zero-day Attacks:** New and previously unknown threats that have no existing signatures.
- **High False Positives/Negatives:** Misidentifying benign activities as malicious or failing to detect actual threats.
- **Scalability Issues:** Difficulty in handling large-scale networks and the vast amount of data generated.
- **Evasion Tactics:** Attackers using sophisticated techniques to bypass traditional IDS mechanisms.

IV.PROPOSED WORK

The objective is to enhance IDS by leveraging Artificial Intelligence (AI) techniques, particularly Machine Learning (ML) and Deep Learning (DL), to predict and detect cyber attacks more accurately and efficiently. The specific goals include:

1. **Improving Detection Accuracy:**
   - Develop AI models that can recognize complex patterns and anomalies in network traffic to detect a wide range of cyber threats.
   - Reduce the rate of false positives and negatives to minimize unnecessary alerts and ensure genuine threats are identified.
2. **Enhancing Adaptability:**
   - Create adaptable AI-driven IDS that can learn and evolve with emerging threats, ensuring continuous protection against new and sophisticated attack vectors.
3. **Scalability:**
   - Ensure the AI-driven IDS can handle large volumes of data and high-traffic network environments without compromising performance.

4. **Operational Efficiency:**
    - Reduce the computational resources required for effective intrusion detection, making the system feasible for deployment in various organizational environments.

By achieving these objectives, AI-enhanced IDS aim to provide a robust, scalable, and efficient solution for protecting information systems from an ever-evolving landscape of cyber threats.

IOT Intrusion Detection Systems Techniques

IoT Interruption is characterized as an unapproved activity or movement that hurts the IoT biological system. For instance, an assault that will make the PC administrations inaccessible to its real clients is viewed as an interruption. An IDS is characterized as a product or equipment framework that keeps up with the security of the framework by recognizing vindictive exercises on the PC frameworks. The primary point of IDS is to distinguish unapproved PC utilization and vindictive organization traffic which is preposterous while utilizing a customary firewall. This outcomes in making the PC frameworks exceptionally defensive against the noxious activities that compromise the accessibility, respectability, or secrecy of PC frameworks.

A. Signature-based intrusion detection systems (SIDS)

Signature interruption location frameworks (SIDS) use design matching procedures to track down a referred to assault; these are otherwise called Information based Recognition. In SIDS, matching techniques are utilized to track down a past interruption [13]. As such, when an interruption signature matches the mark of a past interruption that as of now exists in the mark data set, an alert sign is set off. For SIDS, the host's logs are reviewed to observe arrangements of orders or activities which have recently been distinguished as malware. SIDS has likewise been named in the writing as Information Based Discovery or Abuse Recognition. Customary strategies for SIDS experience issues in distinguishing assaults that length different parcels as they inspect network bundles and perform matching against an information base of marks. With the expanded refinement of current malware, separating mark data from different bundles might be required. With this, IDS needs to bring the substance of prior parcels also. For making a mark for SIDS, by and large, there have been a few strategies where marks are made as state machines, formal language string designs or semantic circumstances [14][15].

B. Anomaly-based intrusion detection system (AIDS)

Helps has drawn in a great deal of researchers due to its element to beat the constraint of SIDS. In Helps, a typical model of the conduct of a PC framework is made utilizing AI, measurable based or information based techniques. Any huge deviation between the noticed conduct and the model is viewed as an irregularity, which can be deciphered as an interruption P16][17].

The primary benefit of Helps is the capacity to distinguish zero-day assaults on the grounds that perceiving the strange client movement doesn't depend on a mark information base. Helps sets off a risk signal when the inspected conduct goes amiss from ordinary conduct. Moreover, Helps has various advantages [18]. To begin with, they can find inside malignant exercises. Assuming an interloper begins making exchanges in a taken record that are unidentified in the average client movement, it makes a caution. Second, it is trying for a cybercriminal to perceive what a typical client conduct is without delivering a ready as the framework is developed from redid profiles [19].

C. Machine Learning based Technique

AI is the most common way of separating information from huge amounts of information. AI models include a bunch of rules, techniques, or complex "move works" that can be applied to observe intriguing information designs or to perceive or anticipate conduct. AI procedures have been applied broadly in the space of Helps. To extricate the information from interruption datasets, various calculations and strategies, for example, grouping, brain organizations, affiliation

rules, choice trees, hereditary calculations, and closest neighbor techniques are used.

V. CONCLUSION

The network intrusion system prevent the cyber world form the various attack. There are various techniques based on the artificial intelligence, machine learning and deep learning, which can able to handle the attack prediction. This paper present the review of the cyber security using machine and deep learning techniques. In the future take some suitable dataset based on the KDD from the machine learning repository and apply the classification algorithm.

VI. REFERENCES

1. S. Ho, S. A. Jufout, K. Dajani and M. Mozumdar, "A Novel Intrusion Detection Model for Detecting Known and Innovative Cyberattacks Using Convolutional Neural Network," in IEEE Open Journal of the Computer Society, vol. 2, pp. 14-25, 2022, doi: 10.1109/OJCS.2021.3050917.
2. V. K. Navya, J. Adithi, D. Rudrawal, H. Tailor and N. James, "Intrusion Detection System using Deep Neural Networks (DNN)," 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), 2021, pp. 1-6, doi: 10.1109/ICAECA52838.2021.9675513.
3. Y. A. Farrukh, Z. Ahmad, I. Khan and R. M. Elavarasan, "A Sequential Supervised Machine Learning Approach for Cyber Attack Detection in a Smart Grid System," 2021 North American Power Symposium (NAPS), 2021, pp. 1-6, doi: 10.1109/NAPS52732.2021.9654767.
4. S. Thirimanne, L. Jayawardana, P. Liyanaarachchi and L. Yasakethu, "Comparative Algorithm Analysis for Machine Learning Based Intrusion Detection System," 2021 10th International Conference on Information and Automation for Sustainability (ICIAfS), 2021, pp. 191-196, doi: 10.1109/ICIAfS52090.2021.9605814.
5. T. T. Nguyen and V. J. Reddi, "Deep Reinforcement Learning for Cyber Security," in IEEE Transactions on Neural Networks and Learning Systems, doi: 10.1109/TNNLS.2021.3121870.
6. W. Xu, J. Jang-Jaccard, A. Singh, Y. Wei and F. Sabrina, "Improving Performance of Autoencoder-Based Network Anomaly Detection on NSL-KDD Dataset," in IEEE Access, vol. 9, pp. 140136-140146, 2021, doi: 10.1109/ACCESS.2021.3116612.
7. K. Cao, J. Zhu, W. Feng, C. Ma, M. Liu and T. Du, "Network Intrusion Detection based on Dense Dilated Convolutions and Attention Mechanism," 2021 International Wireless Communications and Mobile Computing (IWCMC), 2021, pp. 463-468, doi: 10.1109/IWCMC51323.2021.9498652.
8. I. Ullah and Q. H. Mahmoud, "Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks," in IEEE Access, vol. 9, pp. 103906-103926, 2021, doi: 10.1109/ACCESS.2021.3094024.
9. D. Park, S. Kim, H. Kwon, D. Shin and D. Shin, "Host-Based Intrusion Detection Model Using Siamese Network," in IEEE Access, vol. 9, pp. 76614-76623, 2021, doi: 10.1109/ACCESS.2021.3082160.
10. I. Siniosoglou, P. Radoglou-Grammatikis, G. Efstathopoulos, P. Fouliras and P. Sarigiannidis, "A Unified Deep Learning Anomaly Detection and Classification Approach for Smart Grid Environments," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1137-1151, June 2021, doi: 10.1109/TNSM.2021.3078381.
11. Solanki, S., Gupta, C., & Rai, K. (2020). A survey on machine learning based Intrusion Detection

System on NSL-KDD dataset. Int. J. Comput. Appl, 176, 36-39.

12. Gupta, C., Sinhal, A., Kamble, R. (2015). An "Enhanced Associative Ant Colony Optimization Technique-based Intrusion Detection System". Artificial Intelligence and Evolutionary Algorithms in Engineering Systems. Advances in Intelligent Systems and Computing, vol 325. Springer, New Delhi. https://doi.org/10.1007/978-81-322-2135-7_58
13. C Gupta, A Sinhal, R Kamble, "Intrusion detection based on k-means clustering and ant colony optimization: A survey", International Journal of Computer Applications, 20 Volume 79 – No 6, October 2013.
14. Jain, T., Gupta, C. (2022). Multi-Agent Intrusion Detection System Using Sparse PSO K-Mean Clustering and Deep Learning. In: Mathur, G., Bundele, M., Lalwani, M., Paprzycki, M. (eds) Proceedings of 2nd International Conference on Artificial Intelligence: Advances and Applications. Algorithms for Intelligent Systems. Springer, Singapore. https://doi.org/10.1007/978-981-16-6332-1_10.
15. Gupta, C., Kumar, A. & Jain, N.K. An Enhanced Hybrid Intrusion Detection Based on Crow Search Analysis Optimizations and Artificial Neural Network. Wireless Pers Commun 134, 43–68 (2024). https://doi.org/10.1007/s11277-024-10880-3.
16. Solanki, S., Gupta, C., Rai, K., Saxena, M. (2022). An Efficient HIDS System Using Machine Learning Algorithm and Evidence Theory. In: Mathur, G., Bundele, M., Lalwani, M., Paprzycki, M. (eds) Proceedings of 2nd International Conference on Artificial Intelligence: Advances and Applications. Algorithms for Intelligent Systems. Springer, Singapore. https://doi.org/10.1007/978-981-16-6332-1_3.
17. Dubey, S., Gupta, C. (2024). An Effective Model for Binary and Multi-classification Based on RFE and XGBoost Methods in Intrusion Detection System. In: Roy, N.R., Tanwar, S., Batra, U. (eds) Cyber Security and Digital Forensics. REDCYSEC 2023. Lecture Notes in Networks and Systems, vol 896. Springer, Singapore. https://doi.org/10.1007/978-981-99-9811-1_3.
18. Namdev, P., Gupta, C., Dubey, S. (2023). An Improved Intrusion Detection System Using Data Clustering and Support Vector Machine. In: Buyya, R., Misra, S., Leung, YW., Mondal, A. (eds) Proceedings of International Conference on Advanced Communications and Machine Intelligence. MICA 2022. Studies in Autonomic, Data-driven and Industrial Computing. Springer, Singapore. https://doi.org/10.1007/978-981-99-2768-5_37,
19. Gupta, C., Kumar, A., Jain, N.K. (2023). A Detailed Analysis on Intrusion Detection Systems, Datasets, and Challenges. In: Chakraborty, B., Biswas, A., Chakrabarti, A. (eds) Advances in Data Science and Computing Technologies. ADSC 2022. Lecture Notes in Electrical Engineering, vol 1056. Springer, Singapore. https://doi.org/10.1007/978-981-99-3656-4_26.