International Conference on Recent Trends in Data Science and its Applications
DOI: rp-9788770040723.094

Machine Learning Techniques in the Defense Sector for Intrusion Detection

Kuldeep G. Pande,
Assistant Professor, Department of Electronics Engineering, Yeshwantrao Chavan College of Engineering,
Wanadongri Hingna Road Nagpur
Maharashtra 441110, India,
ycce.kuldeep@gmail.com

M K. Kirubakaran,
Associate Professor,
Department of IT,
St.Joseph's Institute of Technology,
Chennai-600119, India,
kiruba23@gmail.com

Odnala Srinivas,
Assistant Professor,
Department of CSE, Geethanjali College of Engineering and Technology,
Cheeryal (Vill), Keesara (Md), Medchal (Dist),
Telangana-501301,
shrianiodnala@gmail.com

Jyoti Kharade
Associate Professor, Bharati Vidyapeeth's Institute of Management & Information Technology,
Navi Mumbai 400614, Maharashtra,
India,
kharadejyoti09@gmail.com

P. Anandan,
Assistant Professor,
School of CSE, Vellore Institute of Technology,
Chennai, 600 127, India,
anand.phd.dip@gmail.com

S.Raja,
Assistant Professor,
Department of CSE,
Panimalar Engineering College ,
Poonamallee, Varadarajapuram,
Tamil Nadu 600123,
srbv1986@gmail.com

Abstract- The digital revolution has contributed to the simplification of previously time-consuming tasks. In this research, we are going to study machine learning techniques in the defense sector for intrusion detection. An intrusion prevention system (IPS) is a mechanism for security management that notifies a network managing the system of malicious activity and also attempts to safeguard it. Machine learning is the study of understanding and developing learning methods on its own using the information to optimize performance on a set of tasks. It is classified as a segment of artificial intelligence.

Keywords: Machine learning (ML), defense sector, intrusion detection, intrusion prevention system (IPS)

I. Introduction

In recent years, technological advancements have coincided with a significant rise in hacking and cybersecurity management. Internet connects the entire world, and one of the vulnerable controlling machines can be considered the starting point for the chain of unfortunate events. Some of the motivations for similar events can range from managing financial gain to understanding the political regulations to having fun. However, the main person of the attack may suffer a greater loss than the person intended. A successful hack of a technological company's website, for instance, results in a loss of reputation, which is crucial for any firm. Every day, businesses, governments, and even individuals face this issue without knowing how to address it. The solution is to install a prevention system (IPS). This is a security device that keeps an eye out for and tries to stop hostile activities on a network and system.

An intrusion detection system, often known as an IDS, is a kind of system that monitors the traffic on a network in search of potentially malicious activities and gives warnings when it finds suspicious activity. It is a piece of software that does a search across a network or system to look for potentially dangerous behaviour or violations of rules. Any potentially harmful activity or policy breach is often reported to an administrator or compiled and centralised using a security information and event management (SIEM) system. In order to discriminate between malicious behaviour and false alerts, a SIEM system aggregates outputs from many sources and applies alarm filtering mechanisms.

In spite of the fact that intrusion detection systems keep an eye out for potentially harmful activities on networks, they are also prone to producing false alarms. As a result, businesses have to do additional configuration steps after installing their IDS systems for the very first time. It entails correctly configuring the intrusion detection systems so that they can distinguish between regular traffic on the network and malicious activity based on how the two seem to one other.

Additionally, intrusion prevention systems scan the network packets that are coming into the system to see whether or not they include any harmful code and then immediately send out warning signals.

II. Literature Review

Ahmim, Ahmed, et al. (2020) conducted a comparison of twelve supervised ML methods. This comparative study aims to demonstrate the best ML methods for network traffic classification in specific types of attack or benign traffic, categories of attack or benign traffic. CICIDS'2017 is used as the data set for our experiments, with Random Forest, Jrip, and J48 performing best. Pawlicki et al. (2020) investigated the availability of degrading the performance of the optimized algorithm used here during testing by devising attacks at the time of adversarial using the 4 proposed systems, then proposed a method to identify the attacks. Information is provided under both ANN and the methods of composing attacks as we discussed above. The detection technique is thoroughly understood, and the outcomes of 5 distinct classifiers are differentiated. Detecting adversarial attacks on ANN, to the best of our knowledge, has not been thoroughly researched within the frame for reference of detection of intrusion systems. Nadia Chaabouni et al. (2019) and Sivakumar P (2015) investigated NIDS implementation resources already in existence, including free and open-source network sniffing software and datasets.Then, it analyses, examines, and contrasts government NIDS ideas in the context of the IoT in terms of design, detection methodologies, validation approaches, dangers that have been addressed, and algorithm implementations. The review discusses ML and conventional NIDS methods as well as potential future developments. Because learning algorithms have a high success rate in privacy and security, our emphasis in this study is on IoT NIDS implemented through ML. Maleh, Yassine. (2020), Karnan B et al (2022), and Latchoumi TP et al (2022) deployed the Cooja IoT simulator in IoT 6LoWPAN networks to generate high-fidelity attack data. The most efficient network architecture is chosen for all by evaluating the effectiveness of various network topologies and network scenarios. Test results reveal that ML models for detection of intrusion outperform traditional methods in terms of accuracy, and detection rate by 99 percent. It also necessitates a low rate of energy model overhead and memory, proving that the generated models can be used in confined settings, such as IoT sensors. A denial of service attack-specific DL-based infiltration model was developed by Kim, Jiyeon, et al. (2020), Vemuri et al (2021), and Monica.M et. al. (2022). The most popular dataset for assessing intrusion detection systems is the KDD CUP 1999 dataset, which we utilize for the intrusion dataset (IDS). The four forms of KDD attacks include DoS, user to root, remote to local, and probing. A detailed investigation of rule learning methods and their suitability for IDS in SG was carried out by Liu, Qi, et al. in 2021. It also summarises the most crucial element for understanding and assessing intrusion detection algorithms. This paper not only provides an overview of several important rule learning methods but also the first assessment of their prospective uses in SG security by examining their use in IDS.

Potluri, Sasanka, et al (2018), Sridaran K et. al. (2018), and Buvana M et al (2021) evaluate the efficiency of CNN-based intrusion detection for recognizing various attacks classes using datasets including such NSL-KDD and UNSW-NB 15. Several performance metrics, which add to the precision score, recall score, and F-measurement, have been compared to existing DL approaches. Mishra, Nivedita, et al. (2021) presented a review paper that compares and concentrates on Intrusion Detection models for mitigating DDoS attacks. In addition, the classification is according to Detection of intrusion Systems, various anomaly techniques, distinct Detection of intrusion System models based on the data information, and different ML and DL models for pre-processing also for malware detection. Finally, while addressing research challenges, proposed solutions, and future visions, a broader perspective was envisioned. Ferrag, Mohamed Amine, and colleagues (2021) provided a thorough categorization of intrusion detection systems in each technological innovation. They presented public datasets as well as frameworks for evaluating the performance of Agriculture 4.0's intrusion detection systems. Finally, they list the issues and possible future study areas for Agriculture 4.0 cyber security intrusion detection. Ferrag, Mohamed Amine, et al. (2021) suggested new methods and a sequential model based on the model's features. The proposed system can gather information from the network layer that is using dump packets from the layer using a system of application routines. Because they can create sequential data according to the language model, text-Convolutional Neural networks, and GRU methods were chosen. When compared to traditional methods, deep learning methods extract additional features from the given data, and results show that they have a higher F1 score. They concluded that a sequential prototype intrusion detection system based on DL can help to secure IoT servers.

III. Proposed Work

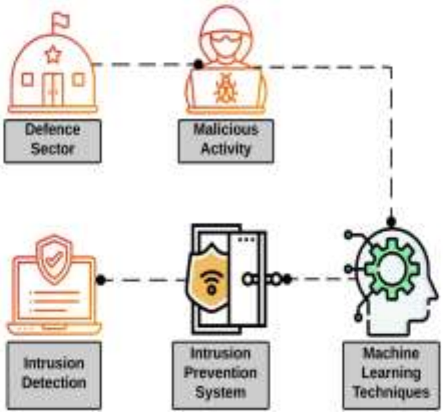

Fig. 1. Intrusion prevention system (IPS)

Malicious activity includes sending/distributing Viruses or information about the creation of Viruses, bouncing, flooding, mail bombing, denial of services, as well as other activities that disrupt or interfere with others' ability to use networks, systems, services, software, or equipment effectively. Machine learning is a field of study concerned with comprehending and developing methods for learning on its user data to improve performance on a set of tasks. It is considered a part of artificial intelligence. Machine learning employs two techniques: supervised learning, which involves training a model on established input and output data to help predict outputs, and unsupervised learning, which employs hidden patterns or structural components in the input data to predict future outputs.

In actual reality, the algorithm of subsidies distribution among the regional efforts aimed at boosting the military sectors by the algorithm output has shown to be a potent force, especially in bigger countries. Following equation (1), we may generally assume that regional authorities have supplied a T_L set of subsidized computations, which we shall refer to as types:

$$T_L = \sum_{m=1}^{c} \left\{ T_1(c_1, \ldots\ldots, c_n) + \sum_{m=1}^{T} T_l(c_1, \ldots\ldots\ldots, c_n) \right\} \quad (1)$$

The quality of funds supports D_l^n given to enterprise m in terms of rule T_l is the quantity of most recent financial statement performance indicators serves as a benchmark. The subsequent equation (2)

$$D_l^n = \sum_{l=1}^{T} T_l((c_1^n) \ \ , \ldots\ldots\ldots, (c_m^n) \quad (2)$$

Each subsidized allotment of the Defense Managing Zones Algorithm of subsidy allocation among the regional ventures is financially sound. To explain the equation (3) indicates that the total amount of a subsidy cannot be greater than the whole amount of such a budgetary provision.

$$\bar{E} = \sum_{n=1}^{N} D_l^n \leq D + \sum_{l=1}^{t} T_l((c_1^n) \qquad (3)$$

The$\bar{E}$ has been described as an algorithm for allocating funds among regional projects in the defense sector. The following equation (4) determines for each indicator the quantitative relationship between its value and the enterprise's performance measurements.

$$E_j = \sum_{j=1}^{E} E_j(c^1, c^2, \dots\dots\dots, c^N) + \sum_{l=1}^{n} D_l^n \leq D \;\; j = 1, \dots\dots.J, \qquad (4)$$

Each cash allotment can be represented by a modified worth $p_n(D_n,$ Dl). The following equation (5) will result in the maximum potential output growth thanks to the idea of acceptable resource allocations by incursion, which is concerned with creating a management plan.

$$D_l^n = \sum_{n=1}^{l} \pi^n\left(c^n, q_n(D_n, D_l^n)\right) \qquad (5)$$

To enhance the defense sector for intrusion on the condition by the equation (6).

$$C_m^n = \sum_{m\to n}^{c} \varphi_m^n\left((c^n) \;\; ,, q_n(D_n, D_n^l)\right), \qquad m1, \dots\dots., M \qquad (6)$$

IV. Experimental Results

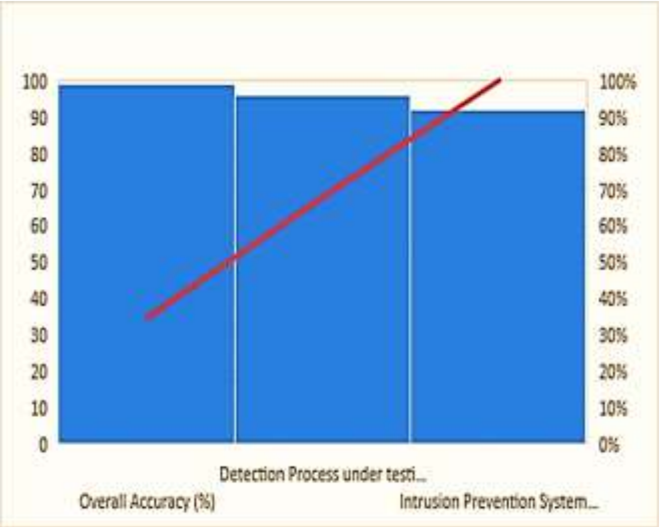

Fig. 2: Performance Analysis Computational ML model based on Intrusion Detection

An IPS is a networking tool (either hardware or software) that overcomes and manages a default network for illicit behavior and that takes action to prevent it, such as blocking and reporting, or dropping the functions, if it does occur. IPS is a security solution that provides active prevention. An IPS sit in the path of network traffic. The primary role is to prevent the system from intrusion. An intrusion prevention system (IPS) slows down entire traffic. An IPS is also known as an IDPS due to the services it provides. An IPS, in essence, sits in line with stable and secured network traffic and supervises it. It detects malicious network activity by analyzing intrusion signatures, generic behavior, and heuristic methods and takes the action of dropping all of the packets and obstructing the traffic. When such an event occurs, it also sends alerts to the administrator. The numerical analysis is presented in Table 1.

TABLE 1: Comparison of Result Analysis with the Existing Method

Algorithm	**Intrusion Prevention System Training (%)**	**Detection Process under testing (%)**	**Overall Accuracy (%)**
Intrusion Detection Algorithm	91.98	95.98	99.12
Existing Method:	85.98	90.59	91.87
Naïve Bayes			

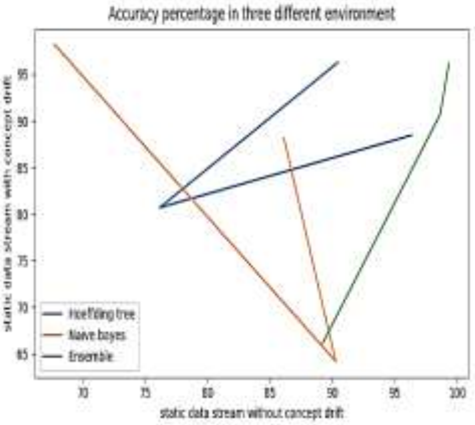

Fig. 3. Performance analysis of different algorithms based on Accuracy

The above Figure 3 depicts the accuracy variations in identifying the intrusion in any given network based on different algorithms. The analysis is performed over the static data of the given environment.

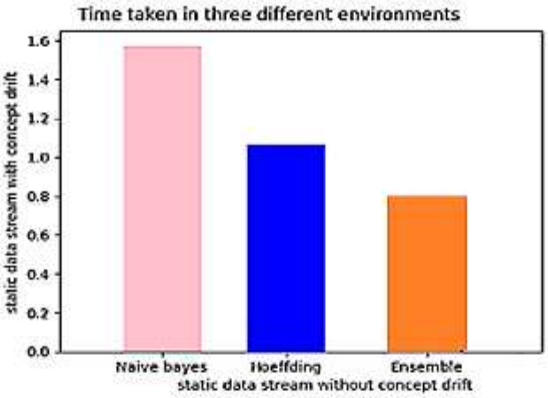

Fig. 4. Performance based on the time taken for intrusion detection

Performance analysis based on the time taken for the detection is presented in the Figure 4 in which the Naïve Bayes Algorithm has taken longer duration for identification than other proposed algorithm is presented. Kappa value Analysis is presented in the following Figure 5.

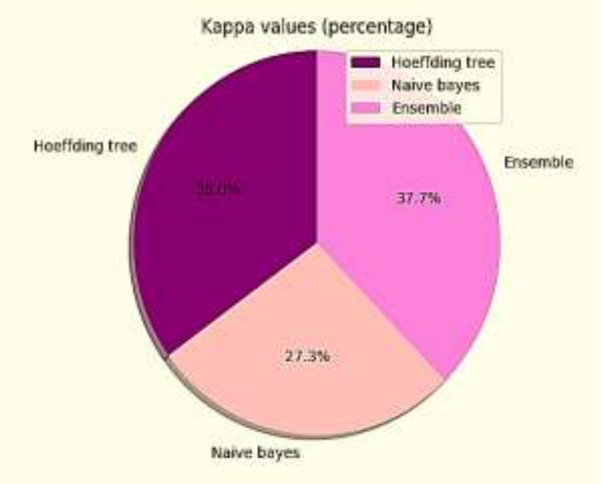

Fig. 5. Kappa Value Analysis

V. Conclusion

The proposed Intrusion Prevention System (IPS) is a security device that keeps an eye out for and tries to stop hostile activities on a network and system. Sensing and perception layer security concerns and vulnerability evaluations exist, as well as information security risks that differ from traditional network era characteristics. Nonetheless, ML methods have fundamentally altered the assessment of cybersecurity threats. To detect network anomalies, the system employs a variety of techniques, along with intrusion detection and managing the flow of identification. Nonetheless, the system has some kind of limitations, such as the integrity of the entire data controllence used to produce the input with its output. New ML methods are becoming progressively popular as a result of the need for quicker and more useful evaluation using the data.

References

[1] U. S. Musa, M. Chhabra, A. Ali and M. Kaur, "Intrusion Detection System using Machine Learning Techniques: A Review," 2020 International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, pp. 149-155, 2020,

[2] A. Sayghe, J. Zhao and C. Konstantinou, "Evasion Attacks with Adversarial Deep Learning Against Power System State Estimation," 2020 IEEE Power & Energy Society General Meeting (PESGM), Montreal, QC, Canada, pp. 1-5, 2020, doi: 10.1109/PESGM41954. 2020.9281719.

[3] Chaabouni, Nadia, et al. "Network intrusion detection for IoT security based on learning techniques." IEEE Communications Surveys & Tutorials, vol. 21.3, pp. 2671-2701, 2019.

[4] Maleh, and Yassine, "Machine learning techniques for IoT intrusions detection in aerospace cyber-physical systems," Machine Learning and Data Mining in Aerospace Technology. Springer, Cham, pp. 205-232, 2020.

[5] Kim, and Jiyeon, et al. "CNN-based network intrusion detection against denial-of-service attacks." Electronics, vol. 9.6, p. 916, 2020.

[6] Liu, Qi, VeitHagenmeyer, and Hubert B. Keller. "A review of rule learning-based intrusion detection systems and their prospects in smart grids," IEEE Access, vol. 9, pp. 57542-57564, 2021.

[7] Potluri, Sasanka, Shamim Ahmed, and Christian Diedrich. "Convolutional neural networks for the multi-class intrusion detection system," International Conference on Mining Intelligence and Knowledge Exploration. Springer, Cham, 2018.

[8] Mishra, Nivedita, and Sharnil Pandya. "Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review." IEEE Access, vol. 9, pp. 59353-59377, 2021.

[9] Ferrag, and Mohamed Amine, et al. "Cyber security intrusion detection for agriculture 4.0: Machine learning-based solutions, datasets, and future directions," IEEE/CAA Journal of Automatica Sinica, vol. 9.3, pp. 407-436, 2021.

[10] Zhong, Ming, Yajin Zhou, and Gang Chen. "Sequential model-based intrusion detection system for IoT servers using deep learning methods," Sensors, vol. 21.4, p. 1113, 2021.

[11] M. Khant, D. Gouwanda, A.A. Gopalai, K.H. Lim, and C.C. Foong, "Estimation of Lower Extremity Muscle Activity in Gait Using the Wearable Inertial Measurement Units and Neural Network," Sensors vol. 23, p. 556, 2023, https://doi.org/10.3390/s23010556.

[12] Sitharthan, R., Vimal, S., Verma, A., Karthikeyan, M., Dhanabalan, S. S., Prabaharan, N., ... & Eswaran, T. (2023). Smart microgrid with the internet of things for adequate energy management and analysis. Computers and Electrical Engineering, 106, 108556.

[13] M. Monica, P. Sivakumar, S. J. Isac, and K. Ranjitha, "PMSG based WECS: Control techniques, MPPT methods and control strategies for standalone battery integrated system," In AIP Conference Proceedings, AIP Publishing LLC, vol. 2405, no. 1, p. 040013, April 2022.

[14] Moshika, A., Thirumaran, M., Natarajan, B., Andal, K., Sambasivam, G., & Manoharan, R. (2021). Vulnerability assessment in heterogeneous web environment using probabilistic arithmetic automata. IEEE Access, 9, 74659-74673.

[15] Vemuri, Ratna Kumari, Pundru Chandra Shaker Reddy, Puneeth Kumar, Jayavadivel Ravi, Sudhir Sharma, and Sivakumar Ponnusamy. "Deep learning based remote sensing technique for environmental parameter retrieval and data fusion from physical models," Arabian Journal of Geosciences, vol. 14, no. 13, pp. 1-10, 2021.

[16] K. Sridharan, and P. Sivakumar, "A systematic review on techniques of feature selection and classification for text mining," International Journal of Business Information Systems, vol. 28, no. 4, pp. 504-518, 2018.

[17] M. Buvana, K. Loheswaran, K. Madhavi, S. Ponnusamy, A. Behura, and R. Jayavadivel, "Improved resource management and utilization based on a fog-cloud computing system with IOT incorporated with classifier systems," Microprocessors and Microsystems, p. 103815, 2021.