IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN: 2349-2163
Volume 11, Issue 12, December 2024 https://www.ijirae.com/archives

Network Security Intrusion Detection Methods Combining Optimization Algorithms and Neural Networks

Abhishek Gupta
Department of Design, Data Science Cyber Security
Greater Noida Institute of Technology (Engg. Institute),
Greater Noida, India
Abhishek Kumar
Department of Design, Data Science Cyber Security
Greater Noida Institute of Technology (Engg. Institute),
Greater Noida, India
Abhishek Kumar Singh
Department of Design, Data Science Cyber Security
Greater Noida Institute of Technology (Engg. Institute),
Greater Noida, India
Uma Shanker Yadav
Department of Design, Data Science Cyber Security
Greater Noida Institute of Technology (Engg. Institute),
Greater Noida, India
Ishrat Ali
Department of Design, Data Science Cyber Security
Greater Noida Institute of Technology (Engg. Institute),
Greater Noida, India
Dr.Shivani Dubey
Professor, Department of Design, Data Science Cyber Security
Greater Noida Institute of Technology (Engg. Institute), Greater Noida, India
shivanidubey@gniot.net.in

Publication History
Manuscript Reference No: IJIRAE/RS/Vol.11/Issue12/DCAE10093
Research Article | Open Access | Double-Blind Peer-Reviewed | Article ID: IJIRAE/RS/Vol.11/Issue12/DCAE10093
Received:10,November 2024,Revised: 21,November 2024,Accepted: 30, November 2024, Published Online: 15,December 2024. https://www.ijirae.com/volumes/Vol11/iss-12/14.DCAE10093.pdf
Article Citation: Abhishek, Abhishek, Abhishek, Uma, Ishrat, Dr.Shivani (2024), Network Security Intrusion Detection Methods Combining Optimization Algorithms and Neural Networks. IJIRAE:: International Journal of Innovative Research in Advanced Engineering, Volume 11, Issue 11 of 2024 pages 974-979
Doi:> https://doi.org/10.26562/ijirae.2024.v1112.14
BibTeX Key: Abhishek@2024Network

Abstract: Cyber-attacks are becoming increasingly common and sophisticated, and the security of net-works is a pressing concern for companies everywhere. To spot and stop attempts to access network resources without authorization, intrusion. There is, however, a problem that many traditional IDS methods can generate a lot of false alarms. This means that it misidentifies safe activity as a threat and is not readily accepted by security teams for which real issues. Scalability and resistance to evolving threats a hybrid approach of a neural network combined with an adaptive algorithm was used in this paper focuses on improvement the performance and accuracy of the intrusion detection system proposed by us. Combining genetic algorithms and particle swarm optimization with neural networks using a framework optimized for comprehensive performance is present in this tutorial. More to the point, parameters and training procedures for Deep learning models in intrusion detection tasks. The objective of this research paper model is to make a false alarm the rate should be decreased, search accuracy increased and in real-time network environments, the system should adapt easily. Experimental results show that the combination of optimization algorithms and neural networks outperforms traditional IDS methods.
Keywords: Intrusion Detection (IDS), Optimization Algorithm, Machine learning

I. INTRODUCTION

Cyber security is nowadays one of the most primordial needs in the world. It is because of the dangerous impacts of cyberspace that have come to be experienced worldwide. It is well aware that threats in cyberspace are increasing day by day. As a result of this advancement, more complicated and intertwined problems arise. That proves to be a challenge to most, if not all, of the security strategies put in place. An intrusion detection system (IDS) is also pertinent to prevent any unauthorized access to the network or any malicious activities being carried out in the system.

Such systems provide passive detection, but these passive systems can be greatly enhanced with the help of certain processing intelligence techniques and algorithms. Advanced Optimization Algorithms and Neural Networks This article explores new approaches that combine these technologies to improve the accuracy and efficiency of intrusion detection. Given the flexibility of neural networks and the focused nature of neural networks in using optimization algorithms. We aim to propose such a framework that helps in detecting threats at a higher level while being able to cut down on false positives. By examining the varied ease of, performing and stressfulness, we attempt to provide solutions to the threats that are being experienced in the network security systems [1].

II. INTRUSION DETECTION

An IDS is important for the supervision of specified systems or networks in order to identify any anomalies or security breaches that can take place. IDS can be categorized broadly in terms of two specific types, one being the Host based IDS (HIDS) and then also the Network based IDS (NIDS).HIDS is aimed at the single hosts and keeps track of intrusions through their operating system logs and system activity. On the other hand, NIDS is network traffic based, having the capability of capturing packets that traverse the network and being able to detect many forms of attacks which HIDS are unable to detect such as some IP based DoS attacks. But, while NIDS can certainly read the packet header, they do not operate through the host o/s thus make it easier for other forms of detection instead. Moreover, hybrid IDS are the incorporation of HIDS and NIDS methods and thus utilizing both teachings' benefits. There are various types of detection methods used by the IDS system: for instance, there is misuse detection which detects known threats; there is an anomaly detection which detects deviations. Detection techniques commonly employed include statistical approaches, ML (machine learning), or data mining, all of which form responses to security incidents [2].

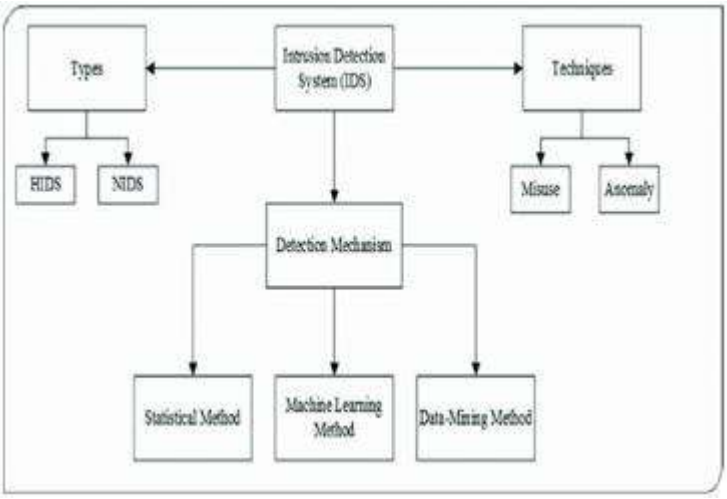

Fig.1: Intrusion Detection System (IDS)

III. MISUSE DETECTION

Misuse detection is the technique of detecting those unauthorized or malicious behaviors in a system or network. It concentrates on knowing known patterns of attacks within sequences of commands or documented harmful behaviors. Thus, the issue with misuse detection is that it relies on predefined signatures or rules that describe how specific attacks occur, thus allowing security systems to detect these behaviors in real time. The process usually makes use of intrusion detection systems (IDS) that monitor the network traffic or system activities and identifies known attack signatures. On detecting a match, the system creates alerts to notify administrators for suitable action to be taken to neutralize the threat that may arise. This system becomes effective in detecting established vulnerabilities as well as known exploits but has a limitation of failing to indicate novel attacks or sophisticated ones that don't match existing signatures. This addition of misuse detection is sometimes combined with anomaly detection techniques that identify unusual patterns of behavior that might be indicative of a breach. Together, it establishes a richer security posture by addressing known and unknown threats by safeguarding organizational digital assets from multiple cyber threats [3].

IV. ANOMALY DETECTION

Anomaly detection refers to the process by which abnormal patterns or behaviors are identified in the data that are not expected. The application of this technique can be found in almost all domains, including cyber security, finance, and even health, in terms of helping to identify potential problems and dangers. For example, in Cyber security, anomaly detection monitors activities on a computer network or system. It actually watches out for the behaviors that diverge from the normal activity on the system, such as sudden spikes in data traffic or bizarre login attempts. These anomalies can quickly alert organizations to possible security breaches or attacks. To detect anomalies, first, the systems must understand what normal behavior is, based on historical data. After base lining a record, any significant deviation from that base can be tagged as anomalous. It may catch newer, unknown threats that others may not. Therefore, while useful; anomaly detection may be producing false alarms whereby normal behavior is mistakenly identified as a threat.

It is thus necessary that organizations combine other security strategies with anomaly detection to give a more precise response to the issues presented. Over and above, maintaining security and safeguarding systems from harm through anomaly detection remains an important tool [4].

V. IDS CHALLENGES

Intrusion Detection Systems (IDS) face numerous and big challenges. On close examination, one of these is the high rate of false positives and false negatives - which can cause alert fatigue as well as a decline in confidence that the system can detect anything. Equally important, though, is that cyber threats are not static: they keep evolving. Attackers use ever more sophisticated means - including encryption and social engineering techniques for example - thus IDS must be able to keep pace in an ongoing fashion. The resource intensity can also be overwhelming: IDS usually must comb through huge volumes of network traffic, and so need big super computers to do this efficiently without causing performance bottlenecks in high-speed environments. Complexity in deployment is still another problem: put simply an IDS is no good unless you can correctly configure and then manage it tactically over time which all takes experience. Also, the function of integrating IDS with other security tools -such as firewalls, Security Information and Event Management (SIEM) systems - facilitates complete threat detection but is difficult. The last problem to solve is privacy concerns (there will be regulation enough!) caused by collecting data on network traffic: IDS captures all sorts of things in the net fishing expedition. This must be better referred to as rules when it takes place and how one's responsibilities stand. To counter pose these difficulties is important to get better results out of IDS as a bulwark against Cyber attacks [5].

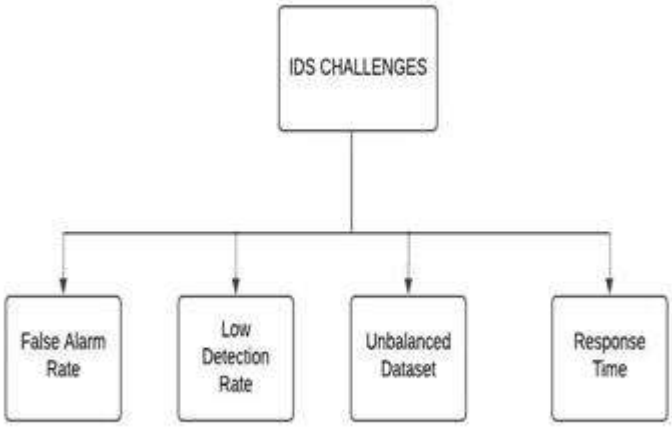

Fig.2 : IDS Challenges

VI. MACHINE LEARNING

Machine learning (ML) is a portion of fake insights that permits frameworks to learn from information, recognize designs, and make choices with small human input. ML calculations can move forward at an errand as they see more information, as contradicted to requiring express programming enlightening for each task. The starting of the concept of machine learning dates back to the 1950s [6]. The Dartmouth Conference in 1956 set up counterfeit insights as a field. Early endeavors centered on symbol-based thinking and logic-based procedures. In the 1960s and 70s, we had calculations like the perceptron, a basic demonstrate for categorizing things into two classes. It went into decrease in the 1970s due to need of intrigued coupled with computers being able to do more things without utilizing machine learning. In the 1980s, intrigued picked up once more with the reemergence of neural systems that had a down to earth utilize and with back engendering getting to be prevalent as a strategy for preparing systems. At that point back vector machines got to be fantastically well known amid the 1990s and the field really took off [7]. Machine learning advanced greatly in the 2000s due to expanded computing control and superior calculations, and at that point when indeed bigger sums of information got to be accessible much appreciated to Open Accessibility of advanced data through Web (PAWS) age, customarily hand-coded frameworks started to be supplanted. The taking after decade we got great at PowerPoint slides almost self-driving cars as major breakthroughs happened in this space such as convolutional neural systems and repetitive neural systems. Since at that point machine learning has come on jumps and bounds having an ever developing affect on society [8].

VII. MACHINE LEARNING IN IDS

Machine learning (ML) is evidently significant in Intrusion Detection Systems (IDS) as it facilitates their ability to cope with cyber threats. While most traditional IDS use rules-based detection to determine the existence of possible attacks, these systems are limited in scope as they do not account for emerging or advanced threats [9]. Machine Learning plays a role in this area by using methods that use the data to learn, and the system recognizes what is considered normal behavior and any intrusion that attempts to breach the system could be an attack. The primal contribution of ML to the IDS is its unrivaled ability to process inputs almost instantaneously. It means that the possible dangers will be most likely contained and mitigated before they cause any harm. Secondly, ML systems are dynamic, which means that they improve with time; as they are exposed to different attacks or new sources of information, they sharpen their detection abilities.

This dynamic learning is essential in combating threats that are continuously changing with time .In addition, this machine learning is used to alleviate the problem of false positive detection, which is the detection of non-threats that may inundate security personnel. Systems of this kind learn from previous use and become more and more proficient in separating relevant behavior from behavior that is truly threatening and thus allowing security teams to concentrate on real risks. In general, there is a strong reinforcement of security systems against network based attacks when machine learning concepts are applied to intrusion detection systems [10].

VIII. OPTIMIZATION ALGORITHM IN IDS

An optimization algorithm is a method by which the best solution to a particular problem is found from a limited set of candidate solutions. It also assists in decision making by focusing on maximizing or minimizing any specific concerns such as costs, time, or assets. This field has many applications in the fields of mathematics, computer sciences, and engineering (and so forth).For example, it may be able to help companies plan the best way for delivery trucks to travel the shortest physical distances, resource allocation, or anything else. Common optimization algorithms are linear programming, genetic algorithms, and gradient descent. Thanks to these algorithms, it is now possible to improve on current processes and rely on evidence when making decisions [11].

a) Genetic Algorithms

Genetic Algorithms (GAs) are optimization methods based on natural selection. They operate by simulating evolution, where a population of candidate solutions is generated. These solutions are compared based on performance, and the best ones are then used to generate new solutions using some crossover and mutation method. GAs iteratively searches for the best solution across generations. John Holland first introduced GAs in the 70s when he was exploring the use of evolutionary principles in computer science. Since the 1980s, the advantage of using GAs has been seen in various fields, including designing and artificially intelligent AI. In the Intrusion Detection System (IDS), GAs can optimize the detection of Cyber attacks. They help select optimal features or rules for identifying malicious activities by dynamically updating and optimizing detection models over time. Through optimal parameter combinations, GAs enhances IDS performance in attack detection and reduces false alarms, making the systems more efficient and reliable for network protection [12].

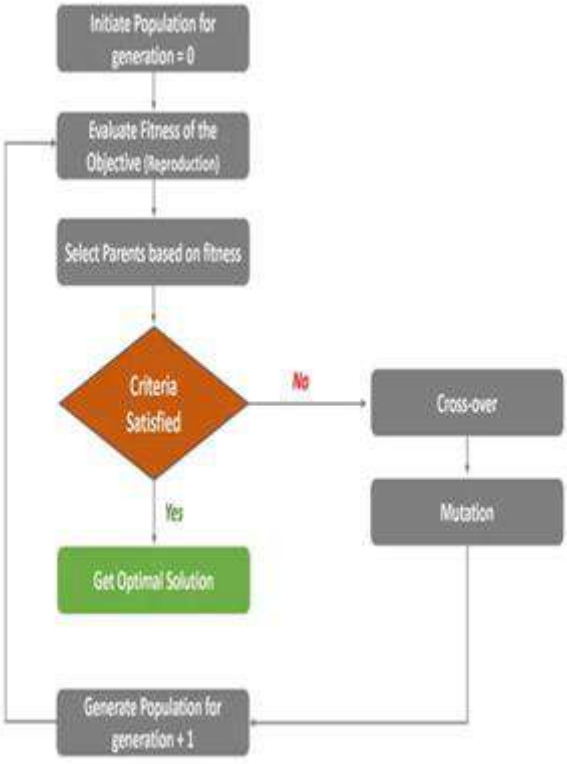

Fig.3: Flowchart of Genetic Algorithm

b) Particle Swarm Optimization Algorithms(PSO)

Particle Swarm Optimization (PSO) is a solution concept inspired by the social behavior of birds and fish in developing a climbing algorithm. It is a heuristic where group potential projects, called particles, explore the search space for the best solution, and each particle uses its knowledge and that of neighbors to correct the neighborhood. In 1995, PSO was invented and primarily designed by James Kennedy and Russell Eberhart. Due to its simplicity and power in solving various engineering problems, it has adapted over the years, thanks to its increasing usage. Every aspect of IDS flow results from cyber signature analysis, especially the educated selection of features and parameters for future system use. PSO methodology is used for effective navigation of different configurations, identifying critical aspects that maximize threat detection accuracy. This leads to increased detection rates, decreased false positives, and enhances IDS performance. Additionally, PSO allows AI/ML inside Detector to select parameters uniquely to address emerging threats efficiently. Overall, using PSO helps security systems preserve networks more effectively [13].

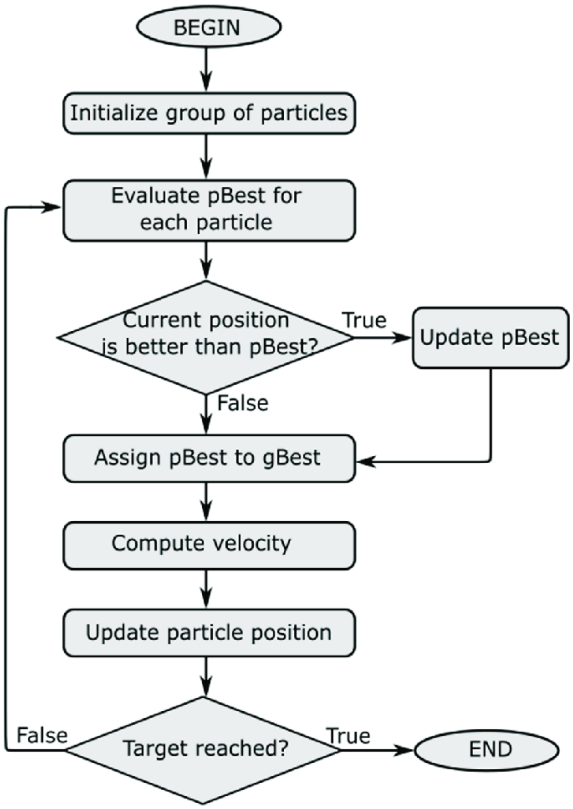

Fig.4: Flowchart of Particle Swarm Optimization Algorithm

c) Ant Colony Optimization Algorithms-

Ant Colony Optimization (ACO) is a method of optimization that works based on the fact that ants in the real world go through the shortest path when collecting food. It mimics ants finding the shortest route to food sources by leaving a trail of pheromones on the ground. Other ants then follow these pheromone trails, resulting in the reinforcement of paths leading to food. Gradually, the algorithm converges on this behavior in order to uncover optimal solutions to highly complex problems.ACO was introduced by Marco Dorigo in 1992 as part of his doctoral degree program documentation [14]. It became one of the most popular techniques to solve combinatorial optimization problems, such as the traveling salesman problem and routing in a network, due to its performance. In Intrusion Detection Systems (IDS), ACO is the optimization mechanism used for detecting cyber threats by enhancing the selection of features and rules to identify the activities of attackers. Through mimicking ant activity by following or bundling pathways, ACO effectively searches for optimal intrusion indicators within vast datasets. Thus, it increases the precision of IDS by focusing only on pertinent characteristics, reducing false alarms and improving recognition and identification performance overall [15].

IX. CONCLUSION

To wrap up, when we combine optimization algorithms with neural networks, we see a significant boost in how well intrusion detection systems work. In this paper we have tried to improve at spotting cyber threats and do so faster as well. This combination allows these systems to adjust on the fly to new and tricky attacks. As we continue to study and test these methods in the real world, we will make them even better. This results in stronger protection for network security in the future. The research aimed to examine the current algorithms utilized to create intrusion detection systems and explain how they have been applied to guarantee everyone's safety in cyberspace. Some of the key things that were considered include the datasets used to come up with the algorithms, what Deep learning algorithms have been used in IDS, the attacks covered in the datasets, and the problems that the models developed intended to solve.

REFERENCES

1. Z.Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," Transactions on Emerging Telecommunications Technologies, vol. 32, no. 1, Jan. 2021.
2. D.E.Kim and M. Gofman, "Comparison of shallow and deep neural networks for network intrusion detection," in Proc. 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), 2018, pp. 204–208.
3. Y.Zhong et al., "HELAD: A novel network anomaly detection model based on heterogeneous ensemble learning," Computer Networks, vol. 169, 107049, Mar. 2020.
4. M.Pandey et al., "The transformational role of GPU computing and deep learning in drug discovery," Nat. Mach. Intell., vol. 4, no. 3, pp. 211–221, 2022.

5. V.K. Quy, A. Chehri, N. M. Quy, N. D. Han, and N. T. Ban, "Innovative trends in the 6G Era: A comprehensive survey of architecture, applications, technologies, and challenges," IEEE Access, vol. 11, pp. 39824–39844, 2023.
6. I.Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in Proc. 4th International Conference on Information Systems Security and Privacy, SCITEPRESS - Science and Technology Publications, 2018, pp. 108–116.
7. Z.Inayat, A. Gani, N. B. Anuar, M. K. Khan, and S. Anwar, "Intrusion response systems: Foundations, design, and challenges," Journal of Network and Computer Applications, vol. 62, pp. 53–74, Feb. 2016.
8. K.Kurniabudi, D. Stiawan, D. Darmawijoyo, M. Y. B. Idris, B. Kerim, and R. Budiarto, "Important features of CICIDS-2017 dataset for anomaly detection in high dimension and imbalanced class dataset," Indonesian Journal of Electrical Engineering and Informatics (IJEEI), vol. 9, no. 2, May 2021.
9. A.Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, "Hybrid intrusion detection system based on the stacking ensemble of C5 decision tree classifier and one class support vector machine," Electronics (Basel), vol. 9, no. 1, 173, Jan. 2020.
10. S.Waskle, L. Parashar, and U. Singh, "Intrusion detection system using PCA with random forest approach," in Proc 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), 2020, pp. 803–808.
11. S.Dhaliwal, A. A. Nahid, and R. Abbas, "Effective Intrusion detection system using XGBoost," Information, vol. 9, no. 7, 149, Jun. 2018.
12. H.Yao, D. Fu, P. Zhang, M. Li, and Y. Liu, "MSML: A novel multilevel semi-supervised machine learning framework for intrusion detection system," IEEE Internet Things J., vol. 6, no. 2, pp. 1949–1959, Apr. 2019.
13. G.Liu, H. Zhao, F. Fan, G. Liu, Q. Xu, and S. Nazir, "An enhanced intrusion detection model based on improved KNN in WSNS," Sensors, vol. 22, no. 4, 1407, Feb. 2022.
14. H.Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection systems: A survey," Applied Sciences, vol. 9, no. 20, 4396, Oct. 2019.
15. E.U.H.Qazi, A. Almorjan, and T. Zia, "A One-dimensional Convolutional Neural Network (1D-CNN) based deep learning system for network intrusion detection," Applied Sciences, vol. 12, no. 16, 7986, Aug. 2022.

