مجلة
كلية التــراث الجامعة

مجلة علمية محكمة
متعددة التخصصات نصف سنوية
العدد الحادي والأربعون
30 نيسان 2025

ISSN 2074-5621

رقم الايداع في دار الكتب والوثائق 719 لسنة 2011

مجلة كلية التراث الجامعة معترف بها من قبل وزارة التعليم العالي والبحث العلمي بكتابها المرقم
(ب 3059/4) والمؤرخ في (4/7 /2014)

Hybrid Intrusion Detection System Considering Dl And Ml Algorithms

Maha Ali Hussein[1], Sundos A. Hameed Alazawi[2], Haider K. Hoomod[3]

[1]Al-Mustansiriyah University, Baghdad, Iraq

[2]Department of Computer Science, College of Science, Al-Mustansiriyah University, Baghdad, Iraq

[3]Department of Computer Science, College of Education, Al-Mustansiriyah University, Baghdad, Iraq

Abstract

The increasing use of online services and products in government and business has led to a big increase in how much people use the Internet, which is managed by network operating systems. However, this also makes systems more vulnerable to harmful actions. Recently, there has been a big increase in the need for using strategies to improve the way we handle attack data to strengthen cybersecurity. These disciplines include vulnerability assessment, malware categorization, detection of intrusions, spam detection, and spoofed identifying. This article presents the crucial techniques for enhancing the selection and extraction of network attack data, with a specific emphasis on contemporary hybrid methods that use machine and deep learning algorithms.

Keywords: Deep Learning, Machine Learning, Hybrid IDS, Cybersecurity.

1. Introduction

The security of networks operating systems has become a major problem in the fast-changing field of information technology. The growing complexity of cyber threats is a significant obstacle to the effectiveness of conventional network operating system protection measures, thereby requiring the creation of more powerful intrusion detection systems. Rapid and efficient detection methods are necessary to safeguard the confidentiality and security of sensitive data in order to identify network anomalies, which may indicate malicious activity or unexpected issues. [1, 2]. Network attack efforts aim to breach cybersecurity systems to gain unauthorized access and manipulate network operating systems. Cybersecurity tools called intrusion-based intrusion detection systems try to find hacks by keeping an eye on system and network behaviour and labelling it as either normal or unusual. These systems try to find a good mix of having few false alarms (FAR) and catching many attacks (DR) [3].

The prevalence of cyberattacks is increasing, which means that information security must be protected by applying the CIA principles (Confidentiality, Integrity, and Availability) [4]. Two primary tactics for cybersecurity are signature-based identification and intrusion-based detection. While both strategies have proven effective, they do need regular database upgrades and thorough examination of attack data [5]. Anomalous network behavior is detected through the analysis of network traffic data. The intrusion-based detection approach is commonly employed for the purpose of identifying and mitigating network assaults, owing to its numerous advantages. [6].

Deep Learning (DL) approaches have shown exceptional achievements in several fields, such as natural language processing, computer vision, and, more recently, security of networks. Nonetheless, the intricate and ever-changing characteristics of network traffic patterns provide distinct obstacles for intrusion detection. The different and ever-changing properties of network data may provide challenges for conventional deep learning models in terms of efficiently adapting and applying their expertise. A variety of factors, including device breakdowns, network congestion, improper setups, malicious behaviour, or network intrusions that intercepted and interpret regular network services, can result in network abnormalities. [7].

2. Optimization Methods

Optimization strategies and approaches play a significant role in enhancing the accuracy of algorithms for classification and reducing the complexity of identifying and categorizing the problem efficiently. Data extraction and appropriate data selection facilitate improved data preparation in the design and creation of classification models, particularly for data sets that include mistakes or superfluous spaces [8, 9]. The optimizer's task involves making modifications during the searching and updating process until it achieves the desired values, which are deemed optimum for reaching the objective. The optimal solution relies on identifying the minimal and maximum solution and utilizing them to achieve the objective [8, 10]. Optimization is a crucial process in deep learning that aims to get the best possible solutions and features within a neural network [11, 12]. Most machine learning difficulties may be resolved by reconfiguring them or modifying the data to align with the characteristics of the problem and the functioning of the algorithm. The choice of optimization methods depends on the specific machine learning techniques employed, leading us to always seek the most suitable enhancement strategies in order to get optimal results [13].

Even though there are many optimization algorithms, we will only talk about the ones that are based on the population principle. We will focus on the chosen method for improving search techniques. Some examples are genetic algorithms, swarm optimization methods, and the Corona virus program used today. Genetic algorithms are a type of genetic algorithms that are mostly used to find the best solution to a problem. Genetic Algorithm (GA) is a form of observational research that replicates the mechanism of natural selection [14]. One type of stochastic optimization is particle swarm optimization. It uses the smart behavior of individuals and groups in animal populations, like a flock of birds or fish, to find the best solution for a problem, like finding food or moving to a better place. [15, 16].

3. Intrusion Detection System

A network intrusion detection approach is often integrated by an Intrusion Detection System (IDS) into a framework that includes other interconnected sub-components. This combination creates an efficient independent system that can perform all the necessary duties for intrusion detection. The topic covers several kinds of Intrusion Detection Systems (IDSs) and presents many IDSs, along with their structures and components [17].

4. Types of Intrusion Detection Systems

Intrusion detection systems are available in several forms and may identify potentially harmful behavior through a range of approaches and capabilities. Typically, IDSs may be categorized into five kinds based on their varied tastes [18]: A network intruder detection system is carefully placed across a network to show what data is coming in and going out from all the devices on the network. It looks at traffic in the neighborhood and connects it to the signs and symptoms of assaults that have already been identified. When strange behavior is found, an alert is sent to start a similar investigation of the norm. To keep your computer and other devices safe, you need a host intruder detection system. This system works on all hosts and devices in your network, whether they are connected to the internet or not. This thing saves all a computer's files and keeps track of what each one is doing. It can find any move on the computer, like changing or destroying files. A certain kind of security device is often put on a web server to keep an eye on how networked devices talk to online resources. Things sent through HTTP and HTTPS are looked at. You can also get protection that listens to how people and apps talk to each other. As the orders are sent back to the people who sent them, it checks the messages that were sent through special methods for certain apps.

5. IDS Detection Methods

Depending on the kind of intrusion detection system, the security solution will rely on many detection techniques. A Signature-based Intrusion Detection System (SIDS) compares patterns to pre-established signs of unwanted access in order to identify and categorize them [19]. These novel zero-day attacks can be recognized using the Anomaly-Based Intrusion Detection System (AIDS) [20]. Anytime traffic deviates from this typical behaviour, the system flags it as suspicious. Hybrid Intrusion Detection system can flag new and existing intrusion strategies [21]. It is exactly what its name suggests: it's a mix of two or more types of IDSs. In the hybrid type, the strengths of two systems are combined: Signature-based intrusion detection and Anomaly-Based intrusion detection [21, 22].

6.Related works

The security solution will depend on several detection methods, depending on the type of intrusion detection system. The purpose of a Signature-based Intrusion Detection System (SIDS) is to identify and categorize trends by comparison with pre-established signs of unlawful access.

In 2020, Kaiyuan et al. [24], A network intruder detection system is made up of Convolutional Neural Networks (CNNs), bidirectional long short-term memory (BiLSTM), and hybrid sampling. The hybrid method tries to improve the accuracy and speed of community intrusion detection by using both Convolutional Neural Network (CNN) and Bidirectional Long Short-Term Memory (BiLSTM) approaches to successfully look at network information. The version still stands out because it's too hard to understand.

In 2020, Jahanzaib et al. [25], The purpose of the safety protection design presented in this study was to maintain the security of a software-defined network's control layer. This platform combines the techniques of Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) to create an intrusion detection system (IDS) that is both proficient and potent. This paper examines the scalability issues that Software-Defined Networks (SDNs) face with their centralized control intelligence, particularly as these networks get larger and more complex.

Smys, S., Abul Basar, and Haoxiang Wang 2020 [22], Proposed an intrusion detection machine for IoT networks that use a hybrid convolutional neural network version to efficaciously perceive numerous styles of attacks. The proposed paradigm is relevant to a huge spectrum of Internet of Things (IoT) packages. The proposed studies effort is assessed and contrasted with traditional system gaining knowledge of and deep mastering fashions. The experimental effects imply that the counseled hybrid model exhibits extra susceptibility to attacks inside the IoT community.

Balyan, Amit Kumar, et al. 2022 [26], The authors delivered a hybrid network-based intrusion detection system that utilizes a hybrid optimization method, which incorporates genetic, particle swarm, and random woodland techniques. Hybrid optimization processes were hired to improve the exceptional of secondary information and extract new statistics with more advantageous accuracy. The efficacy of the proposed device was evaluated by using using machine getting to know strategies on NSL-KDD preferred datasets. The researchers have shown that the proposed method attained an accuracy of up to 98.979% on the NSL-KDD dataset.

Bangui, Hind, and Barbora Buhnova. 2022 [27], Make recommendations for an independent IDS that makes use of centralized systems' advantages to collect and train large amounts of data. We examine the merits of highly promising bio-inspired optimization techniques, namely Ant Colony and Ant Lion Optimization, in order to identify the most appropriate fact representation strategy for the specified device class. As a classifier, we use the Deep Forest policy set to reliably and accurately detect intrusive activities while reducing the number of false positives. The results of the experiment demonstrate that the proposed approach may potentially improve the accuracy and execution speed of lightweight intrusion detection systems.

Nguyen, Xuan-Ha, et al. 2022 [28], You can see Realguard here. It is a network intrusion detection system (NIDS) that uses Deep Neural Networks (DNN) to protect IoT devices on the network. It works directly on local ports. Our idea is unique because it can correctly detect a number of cyber threats in real time with very little computer power. A simple way for extracting features and a very good attack detection model based on deep neural networks are used to do this. Realworld datasets let us test Realguard, and it was able to spot 10 different types of threats in real time. Port checks, Botnets, and FTP-Patators were some of these. Our best rival only gets 98.85% of the time right, so this one is better with an average of 99.57%. Besides, our plan works well on routers that are simple, like the Raspberry PI, and can handle a lot of packets at once, around 10,600 per second.

Roy, Souradip, et al. 2022 [29], Suggest a brand new intrusion detection version that use system mastering to correctly identify cyber-attacks and abnormalities in IoT networks with little resources. By imposing a chain of optimizations consisting of getting rid of multicollinearity, employing sampling techniques, and reducing dimensionality, our version is able to figuring out the most important traits for detecting intrusions with plenty reduced training facts and education time. The recommended methodology was assessed through extensive experimentation using the CICIDS2017 and NSL-KDD databases. The results of the experiment on two widely used datasets demonstrate that our model has a high detection rate and a low false alarm rate. It surpasses cutting-edge models in several overall performance parameters and continuously classifies widespread cyber-attacks. Crucially, the recommended model is light-weight and may be applied on IoT nodes which have constrained power and storage capacities, not like widespread intrusion detection systems that want quite a few resources.

Guezzaz, Azidine, et al. 2022 [30], A machine learning-based hybrid intrusion detection system (IDS) is demonstrated to offer edge protection for the Industrial Internet of Things (IIoT). This novel technique uses Principal Component Analysis (PCA) and K-Nearest Neighbor (K-NN) in tandem to identify and report abuse incidents and other issues. To facilitate decision-making and improve identification, the K-NN classifier was introduced. The PCA improved feature building and instruction. Based on our findings, our proposed Framework outperforms existing frameworks in several aspects. When applied to two sets of data, the model performs admirably. On the NSL-KDD dataset, it has a 99.10% accuracy rate, a 98.4% recognition rate, and a 2.7% false alarm rate. It finds 97.6% of the objects in the Bot-IoT collection, makes the correct decision 98.2% of the time, and only makes mistakes 2.9% of the time.

Alharbi, Sarah, and Arshiya Khan. 2023 [31], A proposition turned into made to rent EDS (Event Detection System) for intrusion detection with the aid of combining signature-based intrusion detection technologies with anomaly-based totally ones. In addition, the researchers applied Elasticsearch, an open-supply protection data control platform, to assess the statistics produced with the aid of intrusion detection systems. The effectiveness of the proposed gadget turned into assessed through carrying out several types of assaults, consisting of port scanning and denial of service assaults. The evaluation discovered that the system plays well and is capable of detecting cybersecurity attacks.

Ahmad, Ijaz, et al. 2024 [32], The layout's shape makes it easy to put in place processes for feature selection and fact processing. The study also made a category version that uses a single guide vector device (SVM) method and is fine-tuned using three different optimization techniques. If you want to improve something, you could use Artificial Rabbits Optimization (ARO), Nuclear Reactor Optimization (NRO) or Particle Swarm Optimization (PSO). These techniques are used to carefully test a lot of different choices and make sure they work so that the Support Vector Machine (SVM) can find malware better. Our proposed framework functioned as anticipated when tested against eleven well-known system algorithms for learning and three new ensembles (ARO-SVM, NRO-SVM, and PSO-SVM) following numerous tests. The NRO-SVM Algorithm is currently the most optimal option due to its efficacy ratio of 97.8%, F1 rating of 97%, and recollect rate of 99%. It also shows that the number of false hits and rejections has gone down. Also, our method successfully found and stopped attacks that were caused by malware, which shows that it has a good chance of finding new risks.

Table 1 offers a concise review of the technique hired in current strategies that integrate device mastering and deep studying algorithms for intrusion detection structures, at the side of the corresponding optimization strategies.

Table 1: Summary of the methodology for IDS using Hybrid techniques

Authors	Methodology	Hybrid Techniques	Dataset	Results
Jan, Sana Ullah, et al. 2019 [23]	A lightweight attack detection strategy injects meaningless data into an IoT network.	support vector machine (SVM) classifier based on SVM, mix of two or three in complicated features		deliver acceptable results when it comes to correctly categorizing and identifying.
2020, Kaiyuan et al. [24]	Networks IDS	Bidirectional Long Short-Term Memory (BiLSTM) in a Convolutional Neural Network (CNN)		high complexity
2020, Jahanzaib et al. [25]	Architecture for security protection created especially to safeguard a software-defined network's control layer. IDSS	The Long Short-Term Memory (LSTM) as well Convolutional Neural Network (CNN) are used together to do this job.		Centralized control intelligence is currently suffering from scalability issues in SDNs, especially for large and complex networks.
2020, Smys, S., Abul Basar, and	IoT network for intrusion detection system	both deep learning models and conventional machine learning.		It offers many uses for the Internet of Things and is more vulnerable to threats in the IoT system.

Authors	Methodology	Hybrid Techniques	Dataset	Results
Haoxiang Wang [22]				
2022, Balyan, Amit Kumar, et al. [26]	network-based intrusion detection system	optimization algorithm that combines genetic, particle swarm, and random forest methods.	NSL-KDD	accuracy of up to 98.979 percent on the extract new data with features that work more accurately.
2022, Bangui, Hind, and Barbora Buhnova. [27]	easy-to-use system for detecting threats across multiple devices	Deep Learning offers two optimization algorithms that are inspired by nature: Ant Lion Optimization and Ant Colony Optimization.		It could make lightweight intruder detection systems more quickly and accurate, which would make them more reliable. Using unified systems to learn and get information from huge amounts of data.
2022, Nguyen, Xuan-Ha, et al. [28]	Deep neural networks (DNN) are used in an attack detection system that is built right into local ports to protect Internet of Things (IoT) devices.	A simple way to get important information and a fast method to find harmful actions using advanced computer networks.		Efficiently identify various online attacks as they happen while using minimal computer resources. Achieve an average precision of 99.57%.
2022, Roy, Souradip, et al. [29]	new methods for finding unauthorized access and unusual behavior in internet-of-things networks with limited resources	Using machine learning to effectively spot cyber-attacks	CICIDS2017 and NSL-KDD	The system is easy to carry and can work on small devices with low power and storage. We need to find the key characteristics to spot unauthorized access. It requires much smaller amounts of data for training and

Authors	Methodology	Hybrid Techniques	Dataset	Results
				takes less time to train.
2022, Guezzaz, Azidine, et al. [30]	IDS for Edge-Based IIoT Security	K-Nearest Neighbor (K-NN) and Principal Component Analysis (PCA) techniques are used to identify improper use and odd patterns.	NSL-KDD Bot-IoT	The accuracy, detection rate, and false alarm rate on the NSL-KDD dataset are 99.10%, 98.4%, and 2.7%, respectively. Accuracy is 98.2%, detection rate is 97.6%, and false alarm rate is 2.9% on the Bot-IoT dataset.
2023, Alharbi, Sarah, and Arshiya Khan. [31]	use EDS in intrusion detection	Signature-based intrusion detection tools along with anomaly-based ones.		the efficiency of the system is good and capable of detecting cybersecurity attacks.
2024, Ahmad, Ijaz, et al. [32]	framework is lightweight for IDS	The Support Vector Machine (SVM) algorithm is incrementally modified using the three methodologies of Artificial Rabbits Optimization (ARO), Nuclear Reactor Optimization (NRO), and Particle Swarm Optimization (PSO).		We identified and prevented assaults that had a high likelihood of success due to malicious software. Our machine attained a F1 rating of 97%, a success rate of 97.8%, and a recall rate of 99%. It additionally committed fewer errors in terms of disregarding legitimate threats or misidentifying them.

6. Conclusion

In this paper it take a look at used prior studies on hybrid structures that applied deep studying strategies and techniques for community intrusion detection, in mixture with machine studying algorithms. Network traffic data sets, such as NSL-KDD, CICIDS2017, and Bot-IoT dataset, are commonly utilized for intrusion detection purposes.

Regarding deep learning algorithms, the majority of researchers have predominantly utilized convolutional neural networks (CNNs) due to their ability to easily establish parameters for network layers and the potential to manipulate them in order to get optimal accuracy outcomes in intrusion detection. Additionally, one researcher utilized the Long Short-Term Memory algorithm. In order to get better outcomes, some researchers have concentrated on utilizing optimization algorithms to acquire ideal characteristics of the data, such as genetic, particle swarm, and random forest techniques.

To stop attacks fast, you need systems that can find intrusions in real time. It would be good to do more study on ways to lower delay in deep learning and machine learning-based intruder detection systems, especially in distributed systems.

7. Acknowledgments

The authors would like to express their thanks to the Department of Computer Science, College of Science, Mustansiriyah University, for supporting this work.

References

1. Chen, L., et al. Zyell-nctu nettraffic-1.0: A large-scale dataset for real-world network anomaly detection. in 2021 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW). 2021. IEEE.
2. Fernandes, G., et al., A comprehensive survey on network anomaly detection. Telecommunication Systems, 2019. 70: p. 447-489.
3. Mishra, S., et al., Swarm intelligence in anomaly detection systems: an overview. International Journal of Computers and Applications, 2021. 43(2): p. 109-118.
4. Abdulhameed, A.A., R.J. Al-Azawi, and B.M. Al-Mahdawi, Modeling Web Security Analysis Attacks with CySeMoL Tool. Al-Mustansiriyah Journal of Science, 2020. 31(3): p. 101-109.
5. K., S.H. and A., A.A. (2021) ‘A vehicle id identification architecture: A parallel-joining WSN algorithm’, Iraqi Journal of Science, pp. 267–270. doi:10.24996/ijs.2021.si.1.37.
6. Abdulhammed, R., et al. Efficient network intrusion detection using pca-based dimensionality reduction of features. in 2019 International symposium on networks, computers and communications (ISNCC). 2019. IEEE.
7. Hussein, M.A., Kadhim, L.E. and Abdulameer, A.A. (2023) ‘Optimum placement of nodes in networks of wireless sensors’, AIP Conference Proceedings, 2591, pp. 020019-1-020019–6. doi:10.1063/5.0119640.
8. Abiodun, E.O., et al., A systematic review of emerging feature selection optimization methods for optimal text classification: the present state and prospective opportunities. Neural Computing and Applications, 2021. 33(22): p. 15091-15118.
9. Yi, D., J. Ahn, and S. Ji, An effective optimization method for machine learning based on ADAM. Applied Sciences, 2020. 10(3): p. 1073.

10. Emami, H., Anti-coronavirus optimization algorithm. Soft Computing, 2022. 26(11): p. 4991-5023.
11. Al-Betar, M.A., et al., Coronavirus herd immunity optimizer (CHIO). Neural Computing and Applications, 2021. 33(10): p. 5011-5042.
12. Sun, R., Optimization for deep learning: theory and algorithms. arXiv preprint arXiv:1912.08957, 2019.
13. Sun, S., et al., A survey of optimization methods from a machine learning perspective. IEEE transactions on cybernetics, 2019. 50(8): p. 3668-3681.
14. Misra, P. and A.S. Yadav. Impact of preprocessing methods on healthcare predictions. in Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE). 2019.
15. Wang, D., D. Tan, and L. Liu, Particle swarm optimization algorithm: an overview. Soft computing, 2018. 22: p. 387-408.
16. Pourpanah, F., et al., A review of artificial fish swarm algorithms: Recent advances and applications. Artificial Intelligence Review, 2023. 56(3): p. 1867-1903.
17. Bhuyan, M.H., D.K. Bhattacharyya, and J.K. Kalita, Network anomaly detection: methods, systems and tools. Ieee communications surveys & tutorials, 2013. 16(1): p. 303-336.
18. Abdulganiyu, O.H., T. Ait Tchakoucht, and Y.K. Saheed, A systematic literature review for network intrusion detection system (IDS). International journal of information security, 2023. 22(5): p. 1125-1162.
19. Einy, S., C. Oz, and Y.D. Navaei, The anomaly-and signature-based IDS for network security using hybrid inference systems. Mathematical Problems in Engineering, 2021. 2021(1): p. 6639714.
20. Jin, S., J.-G. Chung, and Y. Xu. Signature-based intrusion detection system (IDS) for in-vehicle CAN bus network. in 2021 IEEE international symposium on circuits and systems (ISCAS). 2021. IEEE.
21. Maseno, E.M., Z. Wang, and H. Xing, A systematic review on hybrid intrusion detection system. Security and Communication Networks, 2022. 2022(1): p. 9663052.
22. Smys, S., A. Basar, and H. Wang, Hybrid intrusion detection system for internet of things (IoT). Journal of ISMAC, 2020. 2(04): p. 190-199.
23. Jan, S.U., et al., Toward a lightweight intrusion detection system for the internet of things. IEEE access, 2019. 7: p. 42450-42471.
24. Jiang, K., et al., Network intrusion detection combined hybrid sampling with deep hierarchical network. IEEE access, 2020. 8: p. 32464-32476.
25. Malik, J., et al., Hybrid deep learning: An efficient reconnaissance and surveillance detection mechanism in SDN. IEEE Access, 2020. 8: p. 134695-134706.
26. Balyan, A.K., et al., A hybrid intrusion detection model using ega-pso and improved random forest method. Sensors, 2022. 22(16): p. 5986.
27. Bangui, H. and B. Buhnova, Lightweight intrusion detection for edge computing networks using deep forest and bio-inspired algorithms. Computers and Electrical Engineering, 2022. 100: p. 107901.

28. Nguyen, X.-H., et al., Realguard: A lightweight network intrusion detection system for IoT gateways. Sensors, 2022. 22(2): p. 432.
29. Roy, S., et al., A lightweight supervised intrusion detection mechanism for IoT networks. Future Generation Computer Systems, 2022. 127: p. 276-285.
30. Guezzaz, A., et al., A Lightweight Hybrid Intrusion Detection Framework using Machine Learning for Edge-Based IIoT Security. Int. Arab J. Inf. Technol., 2022. 19(5): p. 822-830.
31. Alharbi, S. and A. Khan. Ensemble Defense System: A Hybrid IDS Approach for Effective Cyber Threat Detection. in 2023 33rd International Telecommunication Networks and Applications Conference. 2023. IEEE.
32. Ahmad, I., et al., A Hybrid Optimization Model for Efficient Detection and Classification of Malware in the Internet of Things. Mathematics, 2024. 12(10): p. 1437.