GLOBUS

Cosmos Journal of Engineering & Technology
A Refereed Research Journal
Vol 12 / No 1 / Jan-Jun 2022 ISSN: 2231-4210

EVOLUTIONARY TRENDS IN MACHINE LEARNING-BASED INTRUSION DETECTION: CHALLENGES AND OPPORTUNITIES

*Priyanka Rani

**Dr Dev Ras Pandey

Paper Received: 28.04.2022 / **Paper Accepted**: 26.06.2022 / **Paper Published**: 01.07.2022
Corresponding Author: Priyanka Rani; doi:10.46360/cosmos.et.620221011

Abstract

The incorporation of machine learning into intrusion detection systems represents a crucial new frontier in the process of strengthening digital defences in this day and age, when cyber-attacks are continually evolving in terms of both their level of sophistication and their frequency. The purpose of this research study is to investigate the evolutionary tendencies that have emerged within this ever-changing environment. It also investigates the potential and challenges that come when utilising machine learning for the purpose of intrusion detection. They provide potential capabilities to adapt, learn, and detect novel dangers, overcoming the constraints of traditional rule-based systems.

Keywords: Machine Learning, IDS, Cyber-Attacks, Network.

Introduction

The incorporation of machine learning makes it possible for intrusion detection systems to surpass the capabilities of traditional rule-based systems, which frequently struggle to keep up with the speed at which attack vectors are changing. IDS models that are based on machine learning have the ability to continuously learn from fresh data, which allows them to improve their accuracy and effectiveness over time. They are exceptionally skilled in the analysis of enormous amounts of data in real time, which allows them to quickly identify and respond to any security breaches.

However, in the midst of this progress, important obstacles have emerged. These challenges include concerns regarding the quality of the data, scalability, adversarial assaults, and the necessity of striking a balance between accuracy and real-time processing. The purpose of this paper is to negotiate these hurdles while also putting light on the revolutionary prospects given by machine learning-based intrusion detection. These opportunities range from the discovery of threats at an early stage to the possibility of implementing adaptive and proactive defence. In order to chart the course for effective machine learning-driven intrusion detection systems in the midst of a threat landscape that is constantly shifting, this research seeks to delineate a path towards more robust, adaptive, and resilient cybersecurity frameworks. This will be accomplished by analysing the current methodologies, analysing the evolving trends, and outlining the road ahead.

When it comes to the field of cybersecurity, the combination of machine learning and intrusion detection has emerged as a crucial technique for resisting the unrelenting evolution of cyber threats. The purpose of this study is to investigate the potential and problems that are inherent to the application of machine learning for intrusion detection. This research will begin by doing an investigation of the evolutionary trajectory that has occurred within this area. The landscape of defence mechanisms has been changed as a result of promising breakthroughs in anomaly detection, pattern recognition, and predictive analytics. These advancements have occurred concurrently with the rapid evolution of machine learning algorithms. However, in order to successfully navigate through this transition, it is necessary to face crucial hurdles. These challenges include the requirement for labelled datasets, the hostile landscape, and the pursuit of real-time adaptation.

Literature Review

Alqahtani (2020) [1] The rapid expansion of computer connectivity and the proliferation of computer-related applications in recent years have led to an ongoing difficulty in ensuring cyber-security. Additionally, it requires a robust security system to defend against a multitude of cyber threats. Hence, the task at hand involves identifying discrepancies and malicious activities within a computer network, and subsequently creating an intrusion detection system (IDS) that effectively contributes to the overall cyber-security efforts. An intrusion detection system that relies on machine learning techniques within the field of artificial intelligence has been successfully developed. This paper utilises several widely-used machine learning classification algorithms, including Bayesian Network, Naive Bayes classifier, Decision Tree, Random Decision Forest, Random Tree, Decision Table, and Artificial Neural Network, to identify intrusions caused by intelligent services in the field

**Research Scholar, Kalinga University, Naya Raipur, Chhattisgarh, India.*
***Supervisor, Kalinga University, Naya Raipur, Chhattisgarh, India.*

of cyber-security. Ultimately, we assess the efficacy of different experiments on datasets pertaining to cyber-security, which encompass multiple types of cyber-attacks. Additionally, we examine the usefulness of performance metrics such as precision, recall, f1-score, and accuracy.

Sohi (2021) [2] The integrity of data transmitted over the Internet is at risk due to sophisticated malware, including organised botnets and polymorphic worms. Zero-day attacks, such as these threats, have the ability to modify their behaviour multiple times in their early stages in order to evade network intrusion detection systems (NIDS). Indeed, even meticulously crafted and regularly updated signature-based network intrusion detection systems (NIDS) are unable to identify zero-day threats. This is because they lack a comprehensive signature database that can adapt to sophisticated attacks on the Internet. It is crucial to evaluate an NIDS (Network Intrusion Detection System) using a malicious traffic dataset that not only includes known assaults but also captures the features of unknown, zero-day attacks to some degree. The research recognises that generating such traffic is a significant challenge when assessing the performance of NIDS.

Analysis

The incorporation of machine learning into intrusion detection systems represents a crucial new frontier in the process of strengthening digital defences in this day and age, when cyber-attacks are continually evolving in terms of both their level of sophistication and their frequency. The purpose of this research study is to investigate the evolutionary tendencies that have emerged within this ever-changing environment. It also investigates the potential and challenges that come when utilising machine learning for the purpose of intrusion detection. They provide potential capabilities to adapt, learn, and detect novel dangers, overcoming the constraints of traditional rule-based systems. Machine learning algorithms are always advancing, and their capabilities are becoming more and more promising.

However, in the midst of this progress, important obstacles have emerged. These challenges include concerns regarding the quality of the data, scalability, adversarial assaults, and the necessity of striking a balance between accuracy and real-time processing. The purpose of this paper is to negotiate these hurdles while also putting light on the revolutionary prospects given by machine learning-based intrusion detection. These opportunities range from the discovery of threats at an early stage to the possibility of implementing adaptive and proactive defence. In order to chart the course for effective machine learning-driven intrusion detection systems in the midst of a threat landscape that is constantly shifting, this research seeks to delineate a path towards more robust, adaptive, and resilient cybersecurity frameworks. This will be accomplished by analysing the current methodologies, analysing the evolving trends, and outlining the road ahead.

When it comes to the field of cybersecurity, the combination of machine learning and intrusion detection has emerged as a crucial technique for resisting the unrelenting evolution of cyber threats. The purpose of this study is to investigate the potential and problems that are inherent to the application of machine learning for intrusion detection. This research will begin by doing an investigation of the evolutionary trajectory that has occurred within this area. The landscape of defence mechanisms has been changed as a result of promising breakthroughs in anomaly detection, pattern recognition, and predictive analytics. These advancements have occurred concurrently with the rapid evolution of machine learning algorithms. However, in order to successfully navigate through this transition, it is necessary to face crucial hurdles. These challenges include the requirement for labelled datasets, the hostile landscape, and the pursuit of real-time adaptation.

Through this study, an attempt is made to unravel these complexities while also shedding light on the immense opportunities that are given by machine learning-based intrusion detection. This research also aims to drive the conversation towards cybersecurity paradigms that are adaptable, resilient, and anticipatory. The combination of machine learning with intrusion detection represents a big step forward in the field of cybersecurity.

This convergence offers a paradigm shift away from rule-based systems that are static and towards defence mechanisms that are adaptive and learning-driven. In this paper, we look into the dynamic growth of this combination, exploring the obstacles that arise when utilising machine learning for intrusion detection as well as the potential that are gradually becoming available. The idea of discovering, classifying, and reducing risks in real time is becoming more and more tangible as machine learning algorithms continue to undergo continual evolution. However, in the midst of this progress, there is a spectrum of challenges: the search for high-quality labelled data, the sensitivity to adversarial manipulation, and the requirement to strike a balance between accuracy and processing efficiency. In order to shed light on the revolutionary potential of machine learning in strengthening intrusion detection systems and paving the way for proactive and resilient cybersecurity frameworks,

this study makes an effort to negotiate these challenges.

Challenges

- A issue that continues to exist is the acquisition of labelled data for the purpose of training machine learning models. For the construction of a strong model, quality data is absolutely necessary.
- Interpretability of Models: Complex machine learning models frequently lack interpretability, which makes it difficult to comprehend the decision-making processes they employ, which is essential for cybersecurity.
- Adversarial Attacks: Threat actors have the ability to manipulate machine learning models, which can result in incorrect classifications or allow them to avoid detection, which is a huge difficulty.
- The implementation of machine learning models at a large scale within networks requires a significant amount of computational resources and infrastructure. Scalability and resource allocation must be considered.
- Continuous Learning and Adaptation: If machine learning models are to be able to respond to new threats, they need to be constantly retrained and updated, which presents a number of logistical issues.

Opportunities

- Detection of Emergencies Early on Machine learning models are very effective at recognising novel dangers and anomalies, which enables early detection and proactive actions.
- Defence systems That Are Adaptive These models are able to learn and adapt to ever-changing dangers, which allows them to improve defence systems against dynamic attacks.
- Through the utilisation of previous data, machine learning models are able to forecast prospective dangers, which enables preventative measures to be taken in order to reduce risks.
- Strong Network Security: The incorporation of machine learning-driven defences strengthens networks against a wide variety of cyber attacks that are always growing.
- Automation and Efficiency: Machine learning models automate threat detection duties, which frees up human resources for more strategic cybersecurity endeavours which in turn increases efficiency.

In order to strike a balance between these obstacles and the opportunities that machine learning presents in intrusion detection systems, it is necessary to make concentrated efforts in research, to collaborate between data scientists and cybersecurity professionals, and to continuously progress both technology and techniques. Within the context of the ever-changing digital landscape, this synergy is absolutely necessary in order to fully exploit the potential of machine learning for the development of proactive and resilient cybersecurity frameworks.

Conclusion

When it comes to strengthening defences against the constantly shifting panorama of cyber threats, adaptive machine learning technologies in cybersecurity represent a cornerstone that should not be overlooked. These methods include dynamic methodologies that make it possible for systems to learn, adapt, and respond independently to new dangers that are present inside complex networks. In the field of cybersecurity, where traditional static defences frequently fail to meet the challenge of the rapid evolution of threats, adaptive machine learning is a powerful tool that may be used to foster resilience and proactive defence methods.

There are many different ways in which adaptability can be demonstrated within machine learning methodologies, with the most popular example being in the context of intrusion detection systems (IDS). These systems make use of adaptive algorithms that are able to continuously learn from the data that is being received, thereby recognising both patterns and abnormalities as well as potential dangers. The adaptability of these models resides in their capacity to develop over time, so gradually improving their comprehension of typical network behaviour while simultaneously identifying aberrations that are suggestive of malevolent activity in a short amount of time. This component of continuous learning is essential for proactively discovering novel attack vectors or zero-day threats that are able to circumvent existing signature-based detection approaches.

In the field of adaptive machine learning for cybersecurity, both supervised and unsupervised learning techniques play critical roles. When it comes to categorising and classifying network behaviour, supervised learning algorithms perform exceptionally well. These algorithms are trained on labelled datasets, which allows them to differentiate between benign and dangerous activity. On the other hand, unsupervised learning methods, such as clustering or anomaly detection, make it possible for systems to recognise deviations from established norms without relying on predetermined labels. This allows for the discovery of new dangers or subtle

anomalies that might be able to avoid standard detection mechanisms.

Additionally, reinforcement learning techniques show promise in adaptive cybersecurity because they enable systems to make decisions based on interactions with their environments. This is a significant advancement in the field. Reinforcement learning agents acquire knowledge through the process of trial and error, modifying their actions in order to maximise the rewards or outcomes they receive. This enables them to create adaptive responses to dangers that are constantly changing and evolving.

The application of adaptive machine learning strategies in the field of cybersecurity, on the other hand, provides a variety of obstacles. The quality and quantity of data continue to be of utmost importance; the acquisition and maintenance of high-quality labelled datasets for the purpose of training adaptive models can frequently be difficult due to the variety and number of cyber threats they include. Furthermore, there is a substantial concern regarding the possibility of assuring the durability and robustness of these models in the face of destructive attacks. It is possible for adversaries to take advantage of flaws in these models, which could result in incorrect classifications or allow them to avoid detection by manipulating input data.

Conflict of Interest

There is no conflict of interest in this manuscript by the authors.

References

1. Alqahtani, H., Sarker, I.H., Kalim, A., Minhaz Hossain, S.M., Ikhlaq, S. & Hossain, S. (2020). Cyber intrusion detection using machine learning classification techniques. In Computing Science, Communication and Security: First International Conference, COMS2 2020, Gujarat, India, March 26–27, 2020, Revised Selected Papers 1 (pp. 121-131). Springer Singapore.
2. Sohi, S.M., Seifert, J.P. & Ganji, F. (2021). RNNIDS: Enhancing network intrusion detection systems through deep learning. Computers & Security, 102, 102151.
3. Moualla, S., Khorzom, K. & Jafar, A. (2021). Improving the performance of machine learning-based network intrusion detection systems on the UNSW-NB15 dataset. Computational Intelligence and Neuroscience, 1-13.
4. Azwar, H., Murtaz, M., Siddique, M. & Rehman, S. (2018). Intrusion detection in secure network for cybersecurity systems using machine learning and data mining, In 2018 IEEE 5th international conference on engineering technologies and applied sciences (ICETAS), (pp. 1-9), IEEE.
5. Dang, Q.V. (2021). Improving the performance of the intrusion detection systems by the machine learning explainability. International Journal of Web Information Systems, 17(5), 537-555.
6. Khan, M.A., Rehman, A., Khan, K.M., Al Ghamdi, M.A. & Almotiri, S.H. (2021). Enhance Intrusion Detection in Computer Networks Based on Deep Extreme Learning Machine. Computers, Materials & Continua, 66(1).
7. Kilincer, I.F., Ertam, F. & Sengur, A. (2021). Machine learning methods for cyber security intrusion detection: Datasets and comparative study. Computer Networks, 188, 107840.