The application of artificial intelligence in internet security

Xiyu Cao

Department of Computer Science, Newcastle university, Newcastle, NE1 7RU, United Kingdom

C1027060@newcastle.ac.uk

Abstract. The global integration of the internet has led to a significant increase in the importance of cybersecurity. Artificial Intelligence (AI) has emerged as a viable solution for enhancing cybersecurity measures. AI has the potential to improve the speed and effectiveness of detecting and responding to cyber threats. This study explores the intersection of network security and AI, with a focus on the various ways in which AI can be used to enhance network security, such as intrusion detection, malware detection, and behavioural analytics. The study also examines the potential risks associated with AI in cybersecurity, including the possibility of AI being utilized for cyber-attacks. Additionally, the study discusses the challenges associated with implementing AI for network security, such as the lack of available large datasets for AI training, network infrastructure complexity, and the requirement for skilled AI professionals in cybersecurity. Ethical considerations arising from the use of AI in network security are also addressed. The study emphasizes the need for a balanced approach towards integrating AI into cybersecurity measures, taking into account potential benefits and challenges.

Keywords: artificial intelligence, internet security, machine learning.

1. Introduction

As the Artificial Intelligence (AI) continues to advance, the increasing utilization of AI in network security has become more prominent. It tracks the behaviour of a business network over time using deep learning and machine learning. It discovers and groups patterns on the network. The following stage is to investigate any infractions or security vulnerabilities and then respond. Patterns learned by artificial neural networks over time could enhance future security [1]. Potential dangers with characteristics similar to those listed are rapidly eliminated. It will be challenging for hackers to outwit AI since it is always under the continuous development. Human beings cannot know the attack on the network in advance, and this threat is real-time. And AI can respond to hacker attacks in the first time. It can quickly scan enormous volumes of data and traffic due to its automated nature. It may also detect and locate any threats hidden in a sea of high traffic [1]. Consequently, AI serves as one of the most effective security tools for the prevention of unexpected disruptions to company operations.

Internet security involves the implementation of measures aimed at preventing unauthorized access, use, disclosure, interruption, alteration, or destruction of computer systems, networks, and sensitive information. Traditional security approaches may no longer be enough in light of the rising complexity and sophistication of cyber threats. AI is increasingly being utilized in internet security to improve threat detection, prevention, and response. AI algorithms are capable of analysing massive amounts of data in real time and detecting anomalies or trends that may suggest a security problem. Machine learning algorithms, for example, can learn from previous data to identify and classify new sorts of risks. Natural Language Processing (NLP) can also be employed to analyse text-based communications and detect potential security issues such as phishing emails or social engineering assaults [1, 2]. AI can also be used to automate security duties and reactions, such as detecting and isolating infected devices. This can assist security professionals decrease their effort and respond to security problems more quickly. However, AI is not a panacea for internet security, and there are hazards connected with its use in this sector, such as bias in algorithmic decision-making or the possibility of attackers manipulating AI systems. As a result, it is critical to employ AI thoughtfully and responsibly, as well as to incorporate human oversight and experience in internet security practices.

The main purpose of this research is to provide the review of AI in some network defences. It will focus on the various defence methods and effects of AI.

2. Methodology

2.1. Overview of AI methods in network security

Machine learning-based intrusion detection system: Analysing and monitoring network traffic based on machine learning algorithms to quickly discover and block malicious traffic [3]. Intrusion detection systems can learn behavioural patterns of network traffic and identify anomalous traffic.

Deep learning-based intrusion detection system: Deep learning algorithms can learn high-level features of network traffic, such as the content and context of data packets [4]. By building deep learning models, malicious traffic can be more accurately detected and blocked.Network security defence based on reinforcement learning [5]: Reinforcement learning algorithms can learn network security defence strategies and continuously optimize strategies based on feedback. By establishing a reinforcement learning model, it is possible to quickly respond to new network attacks and improve network security.

Adaptive defence system: The adaptive defence system can automatically identify network attacks and adaptively adjust the defence strategy according to the characteristics of the attack [6]. For example, when a DDoS attack is detected, the adaptive defence system can automatically increase bandwidth and server resources to cope with the increase in attack traffic.

Network traffic analysis and visualization: Network traffic analysis and visualization can help network administrators better understand network traffic and attack behaviour. Through visualization technology, network traffic and attack behaviour can be displayed intuitively, helping administrators to discover and respond to network security problems more quickly.

2.2. Machine learning-based intrusion detection system

Intrusion detection systems powered by machine learning algorithms have gained significant attention due to their ability to effectively analyse and monitor network traffic to detect and prevent unwanted activity. Its primary working premise is to accept network traffic as input, then categories and predict using machine learning algorithms, and lastly output intrusion detection findings [7]. Specifically, the system is often separated into three phases: training, testing, and prediction. During the training phase, the system is taught the behavioural patterns of network traffic by utilizing known samples of normal and malicious traffic. During the testing phase, the system is tested with new samples and the system’s performance is reviewed. During the prediction stage, the system receives network traffic data, classifies and predicts it using the trained model, and finally delivers intrusion detection findings [7]. Support vector machines, naive Bayes, decision trees, random forests, neural networks, and other machine learning techniques are extensively used for classification and prediction problems. These algorithms may learn network traffic characteristics such as size, frequency, source and destination addresses, protocols, and then classify and predict network traffic to detect intrusions. The quality and quantity of training data influence the performance and accuracy of machine learning algorithms, therefore obtaining a significant amount of training data is critical. Furthermore, machine learning algorithms must be regularly optimized and changed in order to respond to various types of cyber threats and changing network settings.

2.3. Deep learning-based intrusion detection system

An advanced intrusion detection system that uses deep learning algorithms to automatically extract advanced features and classify and anticipate network traffic is known as an AI deep learning-based intrusion detection system. Deep learning algorithms, when compared to typical machine learning algorithms, may automatically uncover more complex and abstract features, enhancing detection accuracy and resilience.

In most cases, neural networks are used to process network traffic data for intrusion detection. Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-term Memory Networks (LSTM), and other neural networks are commonly employed [8]. To achieve high-precision intrusion detection, these networks can automatically learn complicated features and extract meaningful information from vast amounts of network data.

However, intrusion detection systems based on deep learning also face some challenges, such as the need for a large amount of training data, the need for powerful computing resources and algorithm optimization, etc. Therefore, in practical applications, it is necessary to weigh these factors and choose an appropriate model and algorithm to achieve intrusion detection [8, 9].

2.4. Network security defense based on reinforcement learning

AI network security defence based on reinforcement learning is a new type of security defence. This method utilized reinforcement learning algorithms to enable the system to learn how to fight against network attacks and continuously optimizes its own defence strategies. The specific implementation methods of network security defence based on reinforcement learning include: AI network security defence based on reinforcement learning is a new type of security defence. This method utilized reinforcement learning algorithms to enable the system to learn how to fight against network attacks and continuously optimizes its own defence strategies [10]. The specific implementation methods of network security defence based on reinforcement learning include building a reinforcement learning model, construction of attack simulation environment, training reinforcement learning model. First, it is necessary to build a reinforcement learning model suitable for network security defence, including state, action, reward function, etc. Then using simulation technology to build a simulation environment that can simulate different attack methods, and train and evaluate the reinforcement learning model. Through repeated experiments in the attack simulation environment, the reinforcement learning model can continuously learn and optimize its own defence strategy [10]. Lastly, In the actual network environment, use the trained reinforcement learning model for detection and defence in real time.

2.5. Adaptive defense system

Adaptive defence system is a network security defence system based on machine learning and artificial intelligence technology, which can monitor network traffic and behaviour in real time, and automatically respond and defend according to abnormal behaviour. The core idea of the adaptive defence system is to constantly adjust the defence strategy according to the dynamic changes of the network environment, to deal with new threats. It can learn normal behaviour patterns in the network through machine learning algorithms, detect abnormal behaviours, and respond and defend quickly according to the characteristics of abnormal behaviours [11]. An adaptive defence system usually includes the following components: data acquisition and processing, machine learning algorithms, risk assessment and response, and feedback and optimization. AI first monitors and collects network traffic, logs, and other security events in real time, and then processes and stores the data. Then use machine learning algorithms to establish normal behaviour models and detect abnormal behaviours for real-time security defence [12]. According to the analysis results of machine learning algorithms, risk assessment is performed on abnormal behaviours, and corresponding response measures are taken, such as blocking or restricting network access, isolating infected hosts, etc. According to the defence effect and the actual situation, optimize and improve the machine learning algorithm so that it can better adapt to new threats.

2.6. Network traffic analysis and visualization

Network traffic analysis and visualization is a commonly used technical method in the field of network security. It can help network administrators and security experts monitor and diagnose network traffic and discover potential security threats [13].

Network traffic analysis and visualization mainly includes the following aspects: traffic capture, traffic filtering and classification, traffic analysis and visualization display AI captures network traffic data through network sniffing tools or network traffic collectors, and performs real-time monitoring and analysis. Then filter and classify the captured network traffic, distinguish normal traffic from abnormal traffic, and extract useful data features [13, 14]. Then conduct an in-depth analysis of the traffic data to discover potential security threats in the traffic, such as network attacks, virus spread, and malware. Finally, the analysis results are presented graphically through visualization tools to help network administrators and security experts understand network traffic more intuitively and quickly discover anomalies and risks. Commonly used network traffic analysis and visualization tools include Wireshark, Tcpdump, Zeek, ELK Stack, etc [15]. These tools can provide a variety of visualization methods, such as line charts, histograms, scatter plots, etc., and can also perform data statistics and report generation, which is convenient for network administrators and security experts to conduct comprehensive analysis and monitoring of network security.

3. Discussion

Machine learning-based intrusion detection systems have demonstrated effectiveness in detecting intrusion events in network environments. The effectiveness of such systems largely depends on various factors, including the selection of algorithms, datasets, and feature engineering techniques. Typically, known attack types, such as port scans and denial of service attacks, can be effectively detected using machine learning algorithms. Furthermore, machine learning algorithms have the capability to identify new types of attacks, including zero-day vulnerabilities. Compared to traditional intrusion detection systems, machine learning-based intrusion detection systems are capable of achieving higher detection accuracy while simultaneously reducing the false alarm rate [16].

But at the same time, AI using Machine learning-based intrusion detection system also has shortcomings. First of all, it will be limited by the amount of data, and machine learning algorithms require a large amount of data for training [17]. However, it is difficult for an intrusion detection system to obtain enough data because intrusion events do not occur frequently. Therefore, insufficient data volume may prevent machine learning algorithms from accurately identifying new attack patterns. Secondly, due to the complex and diverse characteristics of intrusion events, machine learning algorithms are prone to overfitting. When an algorithm overfits, it takes noise and abnormal data in the training set as features, causing the performance of the algorithm to degrade in practical applications. In a real cyber-attack and defence, the attacker can deliberately scramble the input data so that the machine learning algorithm cannot classify it correctly. These attacks are called adversarial attacks. Adversarial attacks can be achieved by adding noise, modifying data, etc. These attacks are difficult to detect by machine learning algorithms.

There are several ways to improve the use of machine learning-based intrusion detection systems: Using multiple machines learning models and fusing their results can improve the accuracy and robustness of the intrusion detection system [18]. Or combine artificial intelligence and machine learning, combine artificial intelligence and machine learning, and use expert knowledge or rules to guide the learning process of machine learning algorithms, which can improve the accuracy and explain ability of the algorithm. Techniques such as adversarial training can also be used to make machine learning algorithms robust to adversarial attacks. Adopt data privacy protection technology, such as data encryption, differential privacy, etc., to protect user privacy. In addition, data sharing technologies, such as federated learning, can also be used to disperse and store data on different devices to reduce the risk of data leakage [19, 20].

4. Conclusion

The utilization of Artificial Intelligence (AI) in network security has the potential to revolutionize the field of cybersecurity. It can help detect and respond to cyber threats more efficiently and effectively, thereby enhancing network security. However, the implementation of AI for network security also poses several challenges, including the availability of large datasets, the complexity of network infrastructure, and the need for skilled AI professionals. Moreover, the ethical considerations that arise with the use of AI in network security must also be taken into account. As AI continues to advance, there is a growing concern about the possibility of AI being used for malicious purposes, such as cyber-attacks. It is crucial to have proper regulations and ethical guidelines in place to prevent such scenarios. Overall, a balanced approach towards the integration of AI into network security is necessary. AI can complement traditional cybersecurity measures and enhance their effectiveness, but it should not replace human decision-making entirely. Together, AI and human experts can create a robust defense against cyber threats, ensuring the safety and security of the interconnected world.

References

[1] Khalaf B A Mostafa S A Mustapha A et al. 2019 Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods IEEE Access 7: 51691-51713

[2] Lv Z Han Y Singh A K et al. 2020 Trustworthiness in industrial IoT systems based on artificial intelligence IEEE Transactions on Industrial Informatics 17(2): 1496-1504

[3] Wu H Han H Wang X et al. 2020 Research on artificial intelligence enhancing internet of things security: A survey Ieee Access 8: 153826-153848

[4] Zaman S Alhazmi K Aseeri M A et al. 2021 Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey Ieee Access 9: 94668-94690

[5] Uras M Cossu R Ferrara E et al. 2020 Wifi probes sniffing: an artificial intelligence based approach for mac addresses de-randomization 2020 IEEE 25th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD) IEEE 1-6

[6] Ferrag M A Maglaras L Moschoyiannis S et al. 2020 Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study Journal of Information Security and Applications 50: 102419

[7] Berman D S et al 2019 A Survey of Deep Learning Methods for Cyber Security. Information 2019 10 122

[8] Shaukat K Luo S Varadharajan V et al. 2020 A survey on machine learning techniques for cyber security in the last decade IEEE Access 8: 222310-222354

[9] Apruzzese G Colajanni M Ferretti L et al. 2018 On the effectiveness of machine and deep learning for cyber security 2018 10th international conference on cyber Conflict (CyCon) 371-390

[10] Kwon D Kim H Kim J et al. 2019 A survey of deep learning-based network anomaly detection Cluster Computing 22: 949-961

[11] Olowononi F O Rawat D B Liu C 2020 Resilient machine learning for networked cyber physical systems: A survey for machine learning security to securing machine learning for cps IEEE Communications Surveys & Tutorials 23(1): 524-552

[12] Alzahrani S Hong L 2018 Detection of distributed denial of service (DDoS) attacks using artificial intelligence on cloud 2018 IEEE World Congress on Services (SERVICES) IEEE 35-36

[13] Spanaki K Karafili E Despoudi S 2021 AI applications of data sharing in agriculture 4.0: A framework for role-based data access control International Journal of Information Management 59: 102350

[14] Sasturkar A Yang P Stoller S D et al. 2011 Policy analysis for administrative role-based access control Theoretical Computer Science 412(44): 6208-6234

[15] Wickramaarachchi G T Qardaji W H Li N 2009 An efficient framework for user authorization

queries in RBAC systems Proceedings of the 14th ACM symposium on Access control models and technologies 23-32

[16] Hasebe K Mabuchi M Matsushita A 2010 Capability-based delegation model in RBAC Proceedings of the 15th ACM symposium on Access control models and technologies 109-118

[17] Buczak A L Guven E 2015 A survey of data mining and machine learning methods for cyber security intrusion detection IEEE Communications surveys & tutorials 18(2): 1153-1176

[18] Liu H Lang B 2019 Machine learning and deep learning methods for intrusion detection systems: A survey applied sciences 9(20): 4396

[19] Li J 2018 Cyber security meets artificial intelligence: a survey Frontiers of Information Technology & Electronic Engineering 19(12): 1462-1474

[20] Boutaba R Salahuddin M A Limam N et al. 2018 A comprehensive survey on machine learning for networking: evolution, applications and research opportunities Journal of Internet Services and Applications 9(1): 1-99