International Journal of Computing and Artificial Intelligence

E-ISSN: 2707-658X
P-ISSN: 2707-6571
IJCAI 2022; 3(2): 109-112
Received: 29-06-2022
Accepted: 03-08-2022
www.computersciencejournals.com/ijcai

Akhila Reddy Yadulla
Department of Information Technology, University of the Cumberlands, USA

Corresponding Author:
Akhila Reddy Yadulla
Department of Information Technology, University of the Cumberlands, USA

Building smarter firewalls: Using AI to strengthen network security protocols

Akhila Reddy Yadulla

DOI: https://www.doi.org/10.33545/27076571.2022.v3.i2a.133

Abstract
The traditional firewalls are gradually becoming inadequate in keeping us secure against the sophisticated and fast-changing cyber threats in this evolving cybersecurity landscape. In this research attempt, the incorporation of Artificial Intelligence techniques in the building of more innovative firewalls with the capability to improve the network security protocols was investigated. The study aims to explore the application of AI techniques for threat detection, anomaly detection, and traffic filtering to improve the need for firewall performance and decrease the number of false positives. Moreover, the research investigates the capability of AI to enhance the scalability, performance, and reusability of firewalls in how networks function. This paper provides a mechanism for a thorough analysis of AI-driven firewall solutions and how they further network security and identify future automated adaptive security systems.

Keywords: Artificial intelligence, firewalls, network security, machine learning, cybersecurity, threat detection, anomaly detection, intrusion detection, deep learning

1. Introduction
Digital security protocols from the past no longer work well enough to defend against advanced computer system threats since Katiyar and colleagues published their report in 2024. New AI technology lets us build better firewalls that adapt effortlessly to screen various cyber dangers. Static rules and signatures-protected legacy firewalls allow attackers to easily avoid polymorphic malware and zero-day attacks, as well as APT tools [1]. The outdated ways of safeguarding networks cannot monitor traffic in real-time nor spot strange behavior since threats evolve and allow danger to enter our systems. Through their ability to keep learning from fresh data and detect emerging threat patterns, the AI-powered firewalls create a preemptive defense system for recognized as well as unidentified cyber-attacks [2].
A differentiation must be made between what artificial intelligence is and what it brings to the table in terms of modern cybersecurity methods of assessment, identification, prevention, and elimination of various cyber threats. There is a need to enhance threat detection and response as the threats evolve, and AI techniques are capable of enhancing the process. Artificial neural networks are one of the key components of cybersecurity that can be applied, for example, for anomaly detection, classification of malicious programs to understand and combat them, and network intrusion detection to avoid unauthorized access. They make it possible to have better and enhanced ways of protecting computer systems with relative ease from current and new threats [3].
AI has great potential to boost the efficiency of the set detection and response methods, thus improving overall cyber security. AI in cyber security is observed to play a more important role in the enhanced or appropriate identification of threats, responses to the threats, and thus, the enhanced movements towards the formation of more effective defense mechanisms. Modern systems based on AI do not only identify attacks and cyber threats but also closely study them, evaluate the obtained information, and develop further strategies for countering them. This gives it a cybersecurity environment that actively adapts to all the latest threats, which, in essence, helps it maintain a strong security posture against all the threats out there [4].
Machine learning-based firewalls can go through large bitstreams and unravel enigmatic patterns of mischievous nature like traffic bursts, intruder intrusions, and the flow of virals. These firewalls use machine learning techniques to complement their ability to detect normal

behavior of the network; hence, when there is a recognition of something new, they are capable of identifying it as a threat and blocking it. Such learning capabilities highly increase the firewall's effectiveness in identifying complicated attacks that could go unnoticed by standard signature-based mechanisms [5]. It is equally important to note that AI also intervenes with an enormous number of cyber threats because it can identify, prevent, and reduce the impact of a large number of these threats. There are tremendous advancements in technology these days, and the transformation of the working of all the fields and the cyber security domain cannot ignore the importance of AI.

2. Literature Review

The modern digital environment requires cybersecurity to be a fundamental matter because digital security challenges are continually evolving toward higher complexity. Networks and sensitive data need better innovative strategies than conventional security methods can provide to keep up with evolving changes [6]. The detection and response to security threats now require AI because AI techniques produce both faster and smarter threat security methods.

Much like a major evolution, Artificial Intelligence, together with machine learning, has entered cybersecurity frameworks to introduce new methods that both discover and counter cyber threats effectively. Modern cybersecurity practices heavily rely on Artificial Intelligence because it generates advanced detection mechanisms that prevent and reduce various cyber threats [7]. New detection systems exhibit an improved ability to adapt and enhance resilience, which allows these systems to fight continually changing cyber threats. The main present difficulties consist of reducing false detection outcomes while improving real-world detection model precision [8].

The recent development of detection systems shows a rise in resilience and adaptivity in such systems, which can become a powerful factor for solving problems arising in the continuously changing space of cybersecurity threats. Most of the current challenges are in minimizing false positives and improving the precision of detection models in the real world. The next step for future work should include more work on the accuracy and reliability of AI-driven models, enabling the development of new comprehensive cybersecurity solutions able to manage the ever-increasing complexity of cyber threats [9].

3. Theoretical Frameworks for Network Security

The introduction of artificial intelligence brought automated security technologies alongside intelligent systems that used to be out of reach for cybersecurity. Artificial intelligence systems enabled economic sectors to simplify their tasks related to data security management. The integration of Artificial Intelligence advances beyond standard technological advancement to create an operational formal change that reinforces cybersecurity measures against growing cyber threats. AI utilizes analytical tools to detect unconventional actions, which then function as an alert system for impending security threats that security personnel utilize to stop unauthorized system entry, leading to decreased loss potential.

3.1 Supervised Learning Models: Training and Evaluating AI Models with Labelled Datasets

The process of supervised learning involves acquiring labeled datasets after model development through training. AI's core application in cybersecurity empowers organizations to work through extensive data collections from network activities, system events, and user actions to discover security breaches that signal attacks [11]. The autonomous learning powers of particular machine learning algorithms strengthen their ability to distinguish harmless from threatening activities by processing large datasets of information. Continuous training across multiple datasets helps models improve their ability to detect suspicious activity patterns, which leads to better proactive security measures. The engineered algorithm system scrutinizes network traffic and system logs and tracks user behavior patterns in order to identify malicious activity through anomaly detection measures.

3.2 The Role of Artificial Intelligence in Modern Intrusion Detection Systems

Modern cybersecurity heavily relies on Intrusion Detection Systems, making Artificial Intelligence a primary factor in their development since these systems perform threat detection and response operations through machine learning. Security analysts use analytical results to identify unusual behavior patterns because those patterns may warn about harmful attacks and enable them to create preemptive security measures [12].

Using classification algorithms to examine network parameters as well as throughput and error logs allows for detecting anomalies. AIDS-based IDS systems improve their attack detection expertise by integrating new data, which results in better abilities to find complex threats while adding new detection patterns and behavioral indicators [13].

3.3 Improving Firewall Efficacy with AI

Network security relies on firewalls as their primary defense mechanisms that protect systems from unauthorized entry and dangerous network traffic. The standard firewall operating methods depend on existing rules, but these prove easily outdated due to evolving modern cyber threats. Firewall systems that utilize AI gain enhanced flexibility along with smart capabilities, which allows them to automatically react to current dangers in security networks. The decision-making quality of firewalls improves through AI-enabled implementation of advanced analytics, which helps evaluate network activity risks before implementing security policies [14].

4. The Transformative Power of AI-Driven Cybersecurity

The implementation of artificial intelligence within firewall systems has become researchers' focus since it aims to increase their performance against modern cyber security threats. The main research direction centers on developing machine learning algorithms that make firewall systems able to recognize and adjust automatically to fresh patterns of network-based attacks. Deep learning models, especially recurrent neural networks together with long short-term memory networks, show the ability to detect anomalies and intrusions accurately while monitoring network traffic and user behavior data records [8].

Firewalls powered by AI technology become more skilled at detecting new threats because they persistently learn from data through which their detection abilities improve steadily with the passing of time. Research teams have established

reinforcement learning-based frameworks that explain the firewall decision-making process through Markov decision processes so firewalls can automatically enhance their security settings while reducing risks independently without needing human supervision [3].

The cybersecurity domain is experiencing an evolving change because it merges state-of-the-art artificial intelligence automation solutions. AI-powered technology provides firewalls together with intrusion detection systems and additional security tools with enhanced abilities to stop and identify numerous threatening cyber incidents [6].

I adoption in cybersecurity occurs due to the requirement of active defense systems that adjust and become durable enough to match the ever-evolving security threats. Security systems enhanced by AI technology extend their alert management capabilities by placing their detection alerts into priority order after performing a risk severity assessment. Thus, security teams can allocate their scarce resources to handle the foremost threats without misdiagnosing non-threatening situations. Remote detection systems became better by using AI in cybersecurity because they enabled stronger intrusion detection through advanced tactics that extend past traditional signature matching methods into adaptive protection methods [8].

5. Methodology

Advanced artificial intelligence techniques have led to a fundamental change in cybersecurity at this time. Artificial Intelligence technologies power firewalls, intrusion detection systems, and other security systems, which substantially boost their ability to discover and stop various types of cyber threats.

The objective of this research study is to examine how artificial intelligence technology boosts network security protocols, particularly through firewall enhancement. The research methodology consists of reviewing the latest AI-based cybersecurity solutions from published literature.

The key aspects explored in this research paper include:

1. This study examines how AI boosts the ability of modern intrusion detection systems through its integration, together with analyses of machine learning algorithm applications for detecting abnormal network behaviors.
2. A firewall system utilizing AI decision systems receives adaptive security policy abilities to defend against developing cyber threats.
3. Artificial intelligence-based methods alongside deep learning and reinforcement learning enable firewall creation to become stronger and more resilient for efficient prevention of new attack paths.
4. Researchers have employed a literature review procedure that combines academic journal articles with industry reports and white papers for their study.
5. The research follows a systematic review of academic journal articles and white papers together with industry reports as its methodological methodology.

Findings from this study enhance researchers' and practitioners' comprehension of AI-based network security protocol strengthening and yield practical knowledge for cyber security experts. The analysis in this research paper thoroughly examines how artificial intelligence evolves network security protocols, particularly by fortifying firewall systems.

6. The Unfolding Potential of AI-Powered Cybers

The modern firewall system has received major enhancement through its integration with artificial intelligence and machine learning techniques, according to reviews of existing literature.

Artificial intelligence models have brought revolutionary changes to cybersecurity because they enhance network security protocol innovation and deployment [14]. Research teams have identified the vast potential AI-based security platforms present for this issue, hence creating heightened curiosity and capital expenditure in this space. Firewalls stand among the most crucial domains where AI brings substantial positive changes.

7. Conclusion

Artificial intelligence can advance network security protocols by strengthening firewall systems, which ought to be considered a promising approach for battling ongoing cyber threats. Next-generation firewalls employ machine learning together with deep learning and reinforcement learning to improve their ability to learn continuously while maintaining superior security against attackers. This research paper demonstrates how AI finds many different applications in securing computer systems and illustrates its transformative capability in cybersecurity. The study presented in this document demonstrates AI's many cybersecurity uses, which display the technology's revolutionary capabilities.

8. References

1. Sharma A, Singh A. Artificial intelligence in cybersecurity: applications and challenges. Springer; c2020.
2. Daruvuri R. An improved AI framework for automating data analysis. World J Adv Res Rev. 2022;13(1):863-866.
3. Zhao H, Wang X, Liu J. Deep learning for intrusion detection in firewall systems. J Netw Secur. 2021;45(2):115-130.
4. Kasula VK. Empowering finance: Cloud computing innovations in the banking sector. Int. J Adv Res Sci Commun Technol. 2022;2(1):877-881. DOI: 10.48175/IJARSCT-12467I.
5. Garg S, Gupta A. AI-enhanced firewall for network defense: a review of trends and techniques. Int. J Comput Appl. 2020;181(1):27-35.
6. Li W, Chen G. Adaptive security using AI in network firewalls: a case study of machine learning integration. IEEE Access. 2019;7:13472-13485.
7. Kumar A, Bansal S. Anomaly detection in network traffic using AI-driven firewalls. J Cybersecurity Priv. 2022;8(3):45-57.
8. Davis R, Harris D. Leveraging AI for real-time cyber threat detection and mitigation in firewalls. In: Proceedings of the International Conference on Cybersecurity; c2020. p. 210-218.
9. Konda B. The impact of data preprocessing on data mining outcomes. World J Adv Res Rev. 2022;15(3):540-544.
10. Xu Y, Zhou J. Machine learning techniques for network security: a focus on smarter firewalls. Int. J Inf Secur. 2021;19(4):233-245.
11. Singh H, Verma M. Enhancing firewall efficacy with AI: a comparative study of traditional vs. AI-driven

systems. Int J Comput Networks. 2020;72(1):90-103.
12. Patel R, Raghav S. AI-driven firewalls for preventing distributed denial of service (DDoS) attacks. J Cyber Def Secur. 2022;12(2):88-101.
13. Mehta P, Sharma K. Designing self-learning firewalls using AI for dynamic network security. Cybersecurity Technol Appl. 2021;33(4):145-159.
14. Yenugula M. Google Cloud Monitoring: A comprehensive guide. J Recent Trends Comput Sci Eng. 2022;10(2):40-50.