Crimson Publishers
Wings to the Research

Mini Review

Expansion of Cyberspace and Critiques of Cybersecurity

Elhamahmy ME*

Department of Information Technology, Chief Expert of Cybersecurity at National Telecommunications Regulatory Authority NTRA, Egypt

ISSN: 2832-4463

***Corresponding author:** Elhamahmy ME, Chief Expert of Cybersecurity at National Telecommunications Regulatory Authority NTRA, Egypt

Submission: January 08, 2024
Published: February 09, 2024

Volume 3- Issue 4

How to cite this article: Elhamahmy ME*. Expansion of Cyberspace and Critiques of Cybersecurity. COJ Rob Artificial Intel. 3(4). COJRA. 000567. 2024.
DOI: 10.31031/COJRA.2024.03.000567

Abstract

The expansion of cyberspace has seen significant growth, incorporating mobile phone networks, IoT device networks, and interconnected systems with traditional internet computer networks. The proliferation of smartphones and high-speed mobile internet technologies has substantially increased internet-connected devices. This evolution has created a more complicated cyber space, expanding beyond conventional computer networks. Along with the big data traffic that traverse this expanded cyber space with a big velocity, as well as advanced technology such as generative artificial intelligence which resulted in more risk and cybersecurity threats. This article emphasizes the network security threats and the critiques of defense systems. The effectiveness in addressing network risks lies in recognizing the primary concern of network providers and users, ensuring network functionality while adapting to inevitable changes. Toward a zero-trust network security model which aim at the first priority to secure the data.

Keywords: Internet networks security; Intrusion detection system; Big data; Machine learning; AI

Introduction

Integration of IoT devices has led to a surge in interconnected devices, generating vast amounts of data for analytics and automation. Simultaneously, the expansion of traditional internet computer networks and widespread adoption of cloud computing services has reinforced global interconnectedness [1]. The convergence of mobile, IoT and traditional internet technologies has formed an interconnected ecosystem supporting diverse applications. However, this enlargement presents challenges, including an increased attack surface for malicious actors, necessitating continuous advancements in cybersecurity measures. Despite security concerns, network expansion persists, emphasizing a balanced approach that recognizes the utility of the network while implementing adaptable, modular and functional security solutions aligned with evolving network services and architecture. Acknowledging tensions between network professionals and security experts, collaboration is underscored to develop effective network security strategies.

Intrusion detection system (IDS)

The IDS serves as a security mechanism identifying and reporting malicious activities within network traffic or system operations. It categorizes into Network-based IDS (NIDS) and Host-based IDS (HIDS). NIDS monitors network traffic for potential threats, while HIDS installed on devices serves as a last line of defense against cyber-attacks after perimeter defenses like firewalls [2]. IDS can also be classified based on detection techniques: signature-based (S-NIDS) and anomaly-based (A-NIDS) methods. The A-NIDS can detect zero-day attacks as it is trained on a dataset differentiating between the normal and malicious packets. It uses machine learning as well as deep learning algorithms. Critiques of modern IDS, particularly in big data environments, include challenges related to size, velocity, encrypted payloads, and the integration of artificial intelligence.

These challenges encompass issues such as limited visibility, adversarial attacks, complexity, scalability, and resource intensiveness, emphasizing the need for innovative solutions to enhance the effectiveness of intrusion detection systems [1]. There is a lot of issues discussed in the literature about the used dataset for A-NIDS. Such as it is an artificial data packets which generated in labs but not taken from a real environment. Another issue is it reflects the packet headers content only but does not include the packet payload. So that deep learning algorithms such as CNN, RNN, LSTM and others may be used to train an A-NIDS model [2]. However, the A-NIDS still not relied on the real environment. Another main issue of using the machine learning algorithm as a multi-classifier for A-NIDS is the evaluation issues. the attack that belongs to a certain class may be incorrectly predicted as a wrong class of attacks; it is still predicted as an attack but of a wrong class. We could not consider this case either false positive nor false negative as it contradicted the terminology definition of false positive and false negative. When the model predicts an attack as another type of attack [3].

Big data challenges

The big data challenges encountered by intrusion detection systems (IDS) are multifaceted and require careful consideration. Traditional NIDS may face difficulties in handling the massive volumes and high velocity of data associated with big data environments. The sheer size and speed of data influx can overwhelm NIDS capabilities, potentially leading to delays in identifying and responding to threats. Encrypted payloads pose another significant hurdle for NIDS. With the growing use of encryption to secure communications, the ability of NIDS to inspect encrypted payloads is limited. This limitation means that potential threats within encrypted data streams remain concealed, making it challenging for traditional NIDS to analyze and detect malicious activities effectively. The integration of generative artificial intelligence introduces new risks, particularly in the form of adversarial attacks. Sophisticated attackers may manipulate or deceive AI algorithms, rendering NIDS vulnerable to such manipulations and potentially compromising their overall effectiveness. The integration challenges between NIDS, big data platforms, and AI technologies are noteworthy. Ensuring seamless interoperability and efficient data exchange between these components requires substantial effort and resources. Scalability concerns also arise as the volume of data and the complexity of AI models increase, potentially leading to limitations in traditional NIDS scalability. Resource intensiveness, particularly in terms of computational resources, can impact the performance of NIDS in resource-intensive environments. Analyzing large volumes of data in real-time and employing AI algorithms demand significant computational power, potentially resulting in performance issues and latency challenges for NIDS.

Zero-trust architecture

The fundamental principles of Zero Trust are straightforward: Never trust, always verify. In practical terms, this entails authenticating and authorizing each user before granting access to any resource, regardless of their location within or outside the network perimeter. Every user request is subject to real-time authentication, authorization, and encryption. Zero Trust provides a level of protection that other models may lack. It serves as a barrier against malware infiltration, enhances security for remote workers without compromising productivity, streamlines security operations center management through increased automation, and expands visibility into potential threats for more effective proactive remediation and response. This approach challenges the traditional notion of implicit trust within networks, fostering a more secure and adaptive cybersecurity model.

Conclusion

In summary, the critiques of network-based intrusion detection systems against big data, encrypted payloads, and new risks of artificial intelligence highlight the need for innovative solutions. Addressing these challenges involves exploring advanced technologies, refining detection techniques, and ensuring seamless integration to enhance the overall effectiveness of intrusion detection systems in modern, data-intensive environments. Along with using zero-trust architecture in order to secure the data. This approach challenges the traditional notion of implicit trust within networks, strengthening the cybersecurity model.

References

1. Reddy SS, Nishoak K, Shreya JL, Vishwambhar YR, Venkanna U (2023) A P4-based adversarial attack mitigation on machine learning models in data plane devices. Journal of Network and Systems Management 32(1).
2. Ramadan RA, Emara AH, Al Sarem MH, Elhamahmy M (2021) Internet of drones intrusion detection using deep learning. Electronics 10(21): 2633.
3. Elhamahmy ME, Hesham NE, Imane AS (2010) A new approach for evaluating intrusion detection system. Artificial Intelligent Systems and Machine Learning 2(11): 290-298.