Idea: Future Research
Volume 2, Issue 3, October 2024 Published by:
ISSN 2987-1565 (Online) | ISSN 2987-2715 (Print) Ideas for Future Research and Technology

Design and Construction of a Computer Network Security System Using the Intrusion Detection System (IDS) Method

Jonathan Demitrius
Program Studi Teknik Informatika, Fakultas Informatika dan Komputer, Universitas Kristen Indonesia Paulus, Sulawesi Selatan, Indonesia

Introduction

In the modern digital landscape, the rapid advancement of technology and the increasing reliance on interconnected systems have exposed organizations, businesses, and individuals to a wide range of cybersecurity threats. As the internet continues to evolve, so do the methods used by cybercriminals to exploit vulnerabilities in computer networks(Sabillon et al., 2016). These threats pose serious risks, including unauthorized access, data breaches, malware infections, and large-scale cyberattacks that can disrupt critical operations. The growing dependence on digital infrastructure, cloud computing, and online services has made cybersecurity a top priority for governments and enterprises worldwide(Srinivas et al., 2019).

Network security threats come in various forms, each with distinct characteristics and consequences(Roman et al., 2013). One of the most prevalent threats is malware, which includes viruses, worms, ransomware, and spyware. Malware can infect systems through phishing emails, malicious downloads, or unsecured network connections, leading to data theft, system corruption, and financial losses(Brown, 2011). Another significant threat is Distributed Denial-of-Service (DDoS) attacks, where cybercriminals flood a network with excessive traffic, rendering it unavailable to legitimate users. Such attacks can cause downtime for businesses, disrupt essential services, and result in economic losses(Rose et al., 2007).

Unauthorized access and data breaches also pose a major risk to network security(Cheng et al., 2017). Hackers often exploit weak passwords, unpatched software vulnerabilities, or social engineering tactics to gain access to sensitive information. In many cases, compromised data can be used for identity theft, financial fraud, or sold on the dark web. Furthermore, advanced persistent threats (APTs), which involve long-term, targeted cyberattacks, are increasingly being used by cybercriminal organizations and state-sponsored hackers to infiltrate high-value targets, such as government agencies and multinational corporations.

The impact of network security threats extends beyond financial damage. Data breaches can lead to reputational harm, loss of customer trust, and legal consequences

Corresponding Author: Jonathan Demitrius (jonathandemitrius@gmail.com)

due to regulatory violations(Martin et al., 2017). In critical sectors such as healthcare, banking, and national security, cyberattacks can have life-threatening implications, endangering patient records, financial systems, and government infrastructure. The increasing frequency and sophistication of these attacks have emphasized the need for robust cybersecurity measures to safeguard digital assets(Dupont, 2019).

To mitigate these risks, various security mechanisms have been developed, including firewalls, encryption, and authentication systems(Amara et al., 2017). However, these traditional security measures alone are often insufficient to detect and respond to advanced and emerging cyber threats. This has led to the increasing importance of Intrusion Detection Systems (IDS), which are designed to monitor network traffic, identify suspicious activities, and alert administrators to potential security breaches(Patel et al., 2010).

An IDS works by analyzing network traffic in real-time, detecting known attack signatures or anomalies, and providing early warnings of potential threats(Singh et al., 2017). There are two primary types of IDS: Host-based IDS (HIDS), which monitors activities on individual devices, and Network-based IDS (NIDS), which analyzes traffic across the entire network. The effectiveness of IDS depends on its ability to distinguish between normal and malicious activities while minimizing false positives and false negatives(Hachmi et al., 2019).

Despite the growing adoption of IDS, many organizations face challenges in implementing an efficient and reliable intrusion detection system(Benkhelifa et al., 2018). These challenges include high false alarm rates, difficulties in detecting zero-day attacks, and performance overhead. Therefore, designing and constructing an optimized IDS-based security system tailored to specific network environments is crucial for improving cybersecurity defenses.

This research aims to develop a network security system using the IDS method, focusing on designing an effective detection framework, implementing it in a real or simulated network environment, and evaluating its performance. By leveraging IDS technology, this study seeks to enhance network security, minimize cyber threats, and contribute to the broader field of cybersecurity research.

Research Problem Statement

As organizations increasingly rely on digital infrastructures and networked systems, cybersecurity threats have become a growing concern(Jang-Jaccard & Nepal, 2014). Cyberattacks such as malware infections, unauthorized access, Distributed Denial-of-Service (DDoS) attacks, and data breaches pose significant risks to businesses,

governments, and individuals. These threats can lead to financial losses, operational disruptions, legal consequences, and reputational damage. Despite the implementation of traditional security measures like firewalls, encryption, and authentication protocols, many systems remain vulnerable to sophisticated cyberattacks that continue to evolve(Jang-Jaccard & Nepal, 2014).

One of the major challenges in network security is the ability to detect and respond to cyber threats in real-time(Wang & Lu, 2013). Many security breaches occur due to delayed threat detection, allowing attackers to infiltrate networks, compromise sensitive data, and disrupt critical operations before administrators can respond. Traditional security mechanisms, while effective in blocking known threats, often fail to identify new or complex attack patterns. Furthermore, organizations struggle with high false positive and false negative rates in intrusion detection, making it difficult to differentiate between legitimate network activity and malicious attacks.

Intrusion Detection Systems (IDS) have emerged as a critical component of modern cybersecurity frameworks(Anwar et al., 2017). IDS can monitor network traffic, analyze patterns, and detect potential security threats before they escalate. However, designing an effective IDS-based security system remains a challenge due to factors such as system complexity, resource consumption, and adaptability to emerging threats. Many existing IDS solutions are either too rigid, relying on predefined attack signatures, or too sensitive, generating excessive false alarms that overwhelm security teams(Alkadi et al., 2020).

Given these challenges, this research seeks to address the problem of designing and constructing a robust computer network security system using the IDS method(Garcia-Teodoro et al., 2009). The study aims to develop an IDS framework that enhances threat detection capabilities while minimizing false positives and negatives. Additionally, the research will explore how IDS can be effectively integrated into real-world network environments, ensuring optimal performance in detecting and mitigating cyber threats. By analyzing different IDS techniques and evaluating their effectiveness, this study will contribute to the ongoing efforts to strengthen network security and protect digital assets from malicious attacks.

Novelty of Research

The growing complexity of cyber threats and the increasing reliance on digital infrastructure have made network security a critical area of research. While various security mechanisms, including firewalls and encryption, play a role in protecting networks, Intrusion Detection Systems (IDS) have emerged as an essential component in identifying and mitigating cyberattacks. However, existing IDS implementations

often suffer from limitations such as high false positive rates, inability to detect zero-day attacks, and inefficient resource utilization. These challenges create a gap in current cybersecurity defenses, highlighting the need for an improved IDS-based security system that offers higher accuracy, adaptability, and efficiency(Khraisat et al., 2019).

This research introduces a novel approach to designing and constructing a network security system using an optimized IDS framework. Unlike traditional IDS implementations that rely solely on signature-based detection, which is ineffective against new or evolving threats, this study explores a hybrid approach that combines signature-based, anomaly-based, and machine learning techniques for enhanced threat detection(Aldweesh et al., 2020). By integrating real-time monitoring, adaptive threat analysis, and automated response mechanisms, the proposed system aims to minimize detection errors and improve the accuracy of identifying cyber threats.

Additionally, this research seeks to address one of the primary weaknesses of conventional IDS solutions the high false alarm rate by implementing intelligent filtering and correlation techniques that refine threat classification. This ensures that legitimate network activities are not mistakenly flagged as malicious, reducing the burden on security administrators and improving overall system efficiency(Neumann, 2000). Furthermore, the study will explore the feasibility of integrating IDS with cloud-based security frameworks and IoT networks, expanding its applicability beyond traditional enterprise environments.

Another key aspect of this study's novelty is its focus on real-world deployment and performance evaluation. Many existing IDS models are tested in controlled environments that do not fully represent the complexities of live networks(Elrawy et al., 2018). This research will implement and assess the proposed IDS system in a simulated or real network infrastructure, measuring its effectiveness in detecting various types of attacks while maintaining optimal network performance. The results will contribute valuable insights into the practical application of IDS in modern cybersecurity frameworks.

By advancing IDS technology through enhanced detection methods, adaptive learning, and practical implementation strategies, this research offers a significant contribution to the field of network security. The findings will help organizations strengthen their cyber defenses, reduce security vulnerabilities, and develop more resilient network infrastructures against emerging threats.

Plan for the results and discussion of this research

The results and discussion section of this research will focus on analyzing the effectiveness, performance, and practical implementation of the proposed Intrusion Detection System (IDS)-based network security system. The findings will be structured into key areas that address the research objectives and provide insights into the system's efficiency in detecting and mitigating cyber threats. The plan for this section includes the following components:

1. System Implementation and Testing Results
    - Description of the IDS framework implemented in the study, including its architecture, detection methods (signature-based, anomaly-based, or hybrid), and deployment model (host-based, network-based, or cloud-integrated).
    - Details of the testing environment, whether it is a controlled laboratory setup, a real-world enterprise network, or a simulated network scenario.
    - Overview of datasets used for IDS training and evaluation, such as publicly available cybersecurity datasets (e.g., KDD Cup 99, NSL-KDD, CIC-IDS 2017) or real-time network traffic logs.
    - Configuration and specifications of the hardware and software used in the IDS deployment.

2. Threat Detection and Classification Analysis
    - Evaluation of the IDS's ability to detect various types of cyber threats, including malware, DDoS attacks, unauthorized access attempts, and zero-day vulnerabilities.
    - Assessment of the accuracy and efficiency of the detection model, including false positive rates (FPR) and false negative rates (FNR) to determine how well the system distinguishes between normal and malicious activities.
    - Performance comparison between the proposed IDS system and existing IDS models or security mechanisms.

3. System Performance and Optimization
    - Analysis of system resource usage, including CPU, memory, and network bandwidth consumption, to determine whether the IDS introduces significant performance overhead.
    - Response time analysis to measure how quickly the IDS identifies and reacts to potential threats.
    - Effectiveness of automated alerts and incident response mechanisms, if integrated into the IDS.

- Optimization strategies applied, such as machine learning-based anomaly detection, filtering techniques to reduce false alarms, or adaptive learning models.

4. Comparative Evaluation with Existing Solutions
   - Comparison of the proposed IDS framework with traditional security approaches, such as firewalls and conventional intrusion prevention systems.
   - Discussion of advantages and limitations of the proposed system in terms of security coverage, detection capability, and usability.
   - Examination of existing IDS research studies and where this research contributes new insights or improvements.

5. Practical Applications and Future Considerations
   - Discussion on the real-world applicability of the IDS model for enterprises, government agencies, and cloud service providers.
   - Feasibility of integrating the IDS into IoT environments, industrial control systems, and smart infrastructure.
   - Recommendations for further enhancements, including AI-driven threat detection, adaptive learning mechanisms, and blockchain-based security frameworks.
   - Exploration of future cybersecurity challenges and how IDS technology can evolve to address emerging threats.

The discussion will conclude with a summary of key findings, emphasizing the effectiveness of the proposed IDS in improving network security. It will highlight the strengths and limitations of the system, suggest areas for future research, and underscore the significance of IDS-based security solutions in protecting digital infrastructures.

References

Aldweesh, A., Derhab, A., & Emam, A. Z. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. *Knowledge-Based Systems*, *189*, 105124.

Alkadi, O., Moustafa, N., & Turnbull, B. (2020). A review of intrusion detection and blockchain applications in the cloud: approaches, challenges and solutions. *IEEE Access*, *8*, 104893–104917.

Amara, N., Zhiqui, H., & Ali, A. (2017). Cloud computing security threats and attacks

with their mitigation techniques. *2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, 244–251.

Anwar, S., Mohamad Zain, J., Zolkipli, M. F., Inayat, Z., Khan, S., Anthony, B., & Chang, V. (2017). From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions. *Algorithms*, *10*(2), 39.

Benkhelifa, E., Welsh, T., & Hamouda, W. (2018). A critical review of practices and challenges in intrusion detection systems for IoT: Toward universal and resilient systems. *IEEE Communications Surveys & Tutorials*, *20*(4), 3496–3509.

Brown, B. C. (2011). *How to Stop E-mail Spam, Spyware, Malware, Computer Viruses, and Hackers from Ruining Your Computer Or Network: The Complete Guide for Your Home and Work*. Atlantic Publishing Company.

Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *7*(5), e1211.

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity*, *5*(1), tyz013.

Elrawy, M. F., Awad, A. I., & Hamed, H. F. A. (2018). Intrusion detection systems for IoT-based smart environments: a survey. *Journal of Cloud Computing*, *7*(1), 1–20.

Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*, *28*(1–2), 18–28.

Hachmi, F., Boujenfa, K., & Limam, M. (2019). Enhancing the accuracy of intrusion detection systems by reducing the rates of false positives and false negatives through multi-objective optimization. *Journal of Network and Systems Management*, *27*, 93–120.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993.

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, *2*(1), 1–22.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, *81*(1), 36–58.

Neumann, P. G. (2000). Practical architectures for survivable systems and networks. *Prepared by SRI International for the US Army Research Laboratory*.

Patel, A., Qassim, Q., & Wills, C. (2010). A survey of intrusion detection and prevention systems. *Information Management & Computer Security*, *18*(4), 277–290.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266–2279.

Rose, A., Oladosu, G., & Liao, S. (2007). Business interruption impacts of a terrorist attack on the electric power system of Los Angeles: customer resilience to a total blackout. *Risk Analysis: An International Journal*, *27*(3), 513–531.

Sabillon, R., Cano, J. J., & Serra-Ruiz, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security, 2016, 4 (6)*.

Singh, R., Kumar, H., Singla, R. K., & Ketti, R. R. (2017). Internet attacks and intrusion detection system: A review of the literature. *Online Information Review*, *41*(2), 171–184.

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, *92*, 178–188.

Wang, W., & Lu, Z. (2013). Cyber security in the smart grid: Survey and challenges. *Computer Networks*, *57*(5), 1344–1371.