

ADAPTIVE MONITORING MODEL FOR DETECTING ANOMALOUS ACTIVITIES IN WEB-BASED INFORMATION SYSTEMS

Shoraimov Khusanboy Uktamboevich, Muxsinov Shamil Shavkatovich,

Nurdullayev Alisher Niyatilla o'g'li

Abstract

This thesis proposes an adaptive monitoring model for detecting anomalous activities in web-based information systems. The growing number of cyber threats targeting web applications, including malicious scripts, session hijacking, unauthorized access attempts, and abnormal traffic manipulations, highlights the necessity of improving web monitoring mechanisms. The research focuses on developing an adaptive approach for real-time detection of suspicious activities through web traffic analysis and behavioral monitoring.

The proposed model integrates traffic monitoring, user session analysis, statistical anomaly detection, and risk evaluation mechanisms into a unified framework. Unlike traditional signature-based security systems, the developed approach enables the identification of previously unknown and dynamically evolving cyber threats through abnormal behavioral pattern analysis. Experimental evaluation demonstrates improvements in anomaly detection accuracy and response efficiency in web environments.

The proposed monitoring framework contributes to strengthening cybersecurity in web-based infrastructures and provides an effective solution for early-stage threat detection and automated monitoring of suspicious activities..

Keywords: web monitoring, anomaly detection, cybersecurity, web traffic analysis, adaptive model, malicious activity, behavioral monitoring, web security, session analysis, cyber threats.

Introduction

The rapid development of digital technologies has significantly increased the role of web-based information systems in government administration, financial institutions, education, healthcare, and e-commerce sectors. However, the expansion

of web technologies has simultaneously increased cybersecurity challenges related to malicious activities and unauthorized access attempts. Modern web environments are frequently targeted by cyber threats such as malicious scripts, traffic manipulation, session hijacking, and unauthorized access to server resources.

Traditional cybersecurity mechanisms mainly rely on signature-based detection approaches, which are effective for identifying known threats but demonstrate limited performance against dynamically evolving or previously unseen malicious activities. As cyberattacks become increasingly sophisticated, adaptive and intelligent monitoring systems capable of identifying abnormal behavioral patterns in real time become essential.

Therefore, the development of adaptive monitoring approaches for identifying anomalous activities in web-based systems represents an important scientific and practical challenge in modern cybersecurity research.

Research Methodology

The research methodology is based on monitoring web server logs, HTTP/HTTPS traffic flows, URL parameters, and user session activities. To identify suspicious behavior patterns, an adaptive monitoring framework was developed for distinguishing normal and anomalous activities within web-based systems.

The proposed methodology includes the following stages:

- collection of web traffic and server-related information;
- monitoring and analysis of user session behavior;
- comparison of normal and anomalous activities;
- risk evaluation based on suspicious indicators;
- automated detection and response to malicious activities.

Statistical and heuristic techniques were applied to analyze behavioral deviations and identify abnormal patterns associated with cyber threats.

Results and Discussion

The experimental findings demonstrated that the proposed adaptive monitoring model significantly improves the efficiency of anomaly detection in web environments. In particular, suspicious session behavior, malicious URL manipulations, and abnormal traffic activities were identified with higher accuracy compared to conventional monitoring methods.

The developed framework reduced response time to suspicious activities and improved real-time monitoring performance. Furthermore, the adaptive nature of the proposed model enabled the detection of emerging threats that could not be effectively recognized by traditional rule-based systems.

Conclusion

This study proposed an adaptive monitoring model for detecting anomalous activities in web-based information systems. The developed framework provides an efficient mechanism for monitoring web traffic, identifying suspicious behavior patterns, and detecting malicious activities in real time.

The implementation of the proposed approach can contribute to improving cybersecurity resilience in web infrastructures and strengthening protection mechanisms against evolving cyber threats.

References

- [1] Cybersecurity Essentials. Wiley, 2021.
- [2] Artificial Intelligence for Cybersecurity. Springer, 2023.
- [3] Hands-On Machine Learning for Cybersecurity. Packt Publishing, 2019.
- [4] Applied Cyber Security and the Smart Grid. Syngress, 2021.
- [5] National Institute of Standards and Technology (NIST). *Cybersecurity Framework (CSF 2.0)*, 2024.
- [6] European Union Agency for Cybersecurity (ENISA). *Cyber Threat Landscape: Emerging Attacks Report*, 2024.
- [7] SANS Institute. *Emerging Web Threat Detection Techniques*, 2024.
- [8] Fortinet. *Global Threat Landscape Report*, 2024.

[9] Trend Micro. *Cyber Risk and Threat Intelligence Report*, 2024.