

AN INTELLIGENT PATTERN RECOGNITION–BASED APPROACH FOR DETECTING VIRAL THREATS IN WEB-BASED INFORMATION SYSTEMS

*Shoraimov Khusanboy Uktamboevich, Muxsinov Shamil Shavkatovich,
Nurdullayev Alisher Niyatilla o'g'li*

Abstract

The rapid expansion of web-based information systems has significantly increased cybersecurity challenges associated with malicious web threats. This study proposes an intelligent approach for detecting viral threats in web environments using pattern recognition techniques. Modern cyber threats such as Cross-Site Scripting (XSS), malicious iframe injections, obfuscated JavaScript code, unauthorized web-shell deployment, and suspicious URL manipulations are considered as the primary research objects.

The proposed model integrates web traffic monitoring, behavioral analysis, and intelligent classification mechanisms to improve threat detection capabilities in real time. A multi-stage detection architecture is developed to identify suspicious patterns by analyzing HTTP/HTTPS requests, URL structures, JavaScript fragments, and web server log activities. Unlike traditional signature-based protection systems, the proposed approach enables the identification of previously unknown or dynamically modified web threats through structural and semantic pattern analysis.

Experimental findings demonstrate that the proposed intelligent framework improves the accuracy of web threat detection, minimizes false identification rates, and reduces response time against malicious activities. The developed model contributes to strengthening cybersecurity in web-based information systems and provides an effective mechanism for protecting digital infrastructures against emerging cyber threats.

Keywords: cybersecurity, web malware, pattern recognition, intelligent detection, web threats, XSS attack, web-shell, JavaScript obfuscation, anomaly detection, web monitoring.

Introduction

In recent years, web-based information systems have become fundamental components of digital transformation across government services, finance, education, healthcare, and e-commerce sectors. While these systems provide operational flexibility and accessibility, they also introduce new cybersecurity vulnerabilities. The increasing complexity of malicious cyberattacks targeting web applications has become one of the major concerns in ensuring information security.

Among modern web threats, malicious JavaScript injections, XSS attacks, hidden iframe redirections, and web-shell exploitation represent highly dangerous attack vectors capable of compromising system integrity and confidentiality. Conventional security solutions primarily rely on signature-based detection methods, which often fail to identify unknown or polymorphic threats. As cyberattacks continue to evolve, intelligent and adaptive threat detection mechanisms become increasingly necessary.

Therefore, developing an intelligent detection framework capable of identifying both known and previously unseen web threats is a critical research challenge. This study introduces a pattern recognition-based approach for analyzing suspicious activities in web-based environments and improving cybersecurity resilience.

Research Methodology

The research methodology is based on monitoring web server activities and analyzing network interactions through HTTP/HTTPS requests, URL parameters, JavaScript code fragments, and user session behaviors. To improve detection efficiency, a multi-stage intelligent model was designed using pattern recognition principles.

The proposed methodology includes the following stages:

- collection and monitoring of web-related data;
- preprocessing and normalization of suspicious content;
- identification of malicious behavioral patterns;
- intelligent threat classification;
- automated response and blocking mechanisms.

A probabilistic risk assessment mechanism was additionally integrated into the framework to determine the severity level of detected threats and prioritize mitigation strategies.

Results and Discussion

Experimental evaluation showed that the proposed intelligent detection framework significantly enhances the ability to identify web-based malicious activities. Particularly, high performance was achieved in detecting XSS attacks, iframe manipulations, and obfuscated JavaScript malware.

The experimental results indicate that the proposed model improves detection accuracy while reducing system response time compared to traditional signature-based systems. Furthermore, the framework demonstrated strong capabilities in identifying previously unknown threats through pattern similarity analysis, making it suitable for dynamic cybersecurity environments.

Conclusion

This study proposed an intelligent pattern recognition-based model for detecting viral threats in web-based information systems. The developed approach provides an effective mechanism for identifying malicious activities at early stages and enables automated response against suspicious behavior in real time.

The practical implementation of the proposed model can significantly enhance cybersecurity resilience in digital infrastructures and contribute to securing web-based platforms against evolving cyber threats.

References

- [1] Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2019.

- [2] Web Application Security. O'Reilly Media, 2020.
- [3] Machine Learning and Security. O'Reilly Media, 2018.
- [4] Practical Malware Analysis. No Starch Press, 2019.
- [5] OWASP Foundation. *OWASP Web Security Testing Guide (WSTG)*, 2024.
- [6] European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape Report*, 2024.
- [7] Cisco Systems. *Cisco Annual Cybersecurity Report*, 2024.
- [8] Palo Alto Networks. *Unit 42 Threat Intelligence Report*, 2024.
- [9] Check Point Software Technologies. *Cyber Attack Trends Report*, 2024.