

DEVELOPMENT OF A MACHINE LEARNING MODEL FOR EARLY DETECTION OF MALICIOUS WEB ATTACKS IN INFORMATION SYSTEMS

Kerimov K

Abstract

The rapid growth of web-based information systems has significantly increased cybersecurity risks and the number of malicious web attacks targeting digital infrastructures. Traditional security systems based on static rules and signature analysis are often unable to detect sophisticated and previously unknown cyber threats. This study focuses on the development of a machine learning model for the early detection of malicious web attacks in information systems. The proposed framework applies intelligent data analysis and pattern recognition methods to identify suspicious activities within web traffic and user behavior. Machine learning algorithms such as Decision Trees, Random Forest, and Support Vector Machines are used to classify web activities as normal or malicious. Feature extraction and anomaly detection techniques are integrated into the system to improve detection accuracy and reduce false-positive rates. Experimental analysis demonstrates that machine learning technologies can effectively detect cyber threats at early stages before significant damage occurs. The proposed model provides scalable and adaptive protection mechanisms for modern web environments and contributes to the development of intelligent cybersecurity systems.

Keywords: machine learning, cybersecurity, malicious web attacks, intrusion detection, anomaly detection, web security, artificial intelligence, pattern recognition

Introduction

The increasing use of web technologies in government institutions, financial organizations, healthcare systems, and educational platforms has made cybersecurity one of the most important challenges in modern information technologies. Web applications process sensitive information and support critical

services; therefore, they are common targets for cybercriminals. Modern malicious attacks such as SQL injection, phishing, malware injection, and distributed denial-of-service attacks continue to evolve in complexity and sophistication.

Traditional cybersecurity approaches rely heavily on predefined signatures and static rule-based detection systems. Although such methods are effective against known threats, they often fail to identify zero-day attacks and obfuscated malware. Consequently, intelligent and adaptive cybersecurity solutions have become necessary for protecting modern information systems.

Machine learning technologies provide powerful tools for detecting malicious activities by analyzing network traffic, user behavior, and abnormal system operations. Machine learning algorithms can identify hidden patterns in data and distinguish between legitimate and malicious activities without requiring explicit programming. Decision Trees and Random Forest algorithms are widely used because of their high classification accuracy and interpretability, while Support Vector Machines are effective for identifying complex attack structures.

The proposed machine learning model focuses on early threat detection through behavioral analysis and anomaly recognition. The framework monitors HTTP requests, session activities, packet structures, and authentication attempts to identify suspicious actions in real time. Feature extraction methods are used to select the most informative parameters for attack classification and system optimization. The practical importance of this study lies in its ability to strengthen web application security and reduce the risks associated with cyberattacks. Intelligent cybersecurity systems based on machine learning technologies can improve digital infrastructure protection, support automated monitoring, and enhance incident response processes. The findings demonstrate that machine learning methods can significantly improve cybersecurity efficiency in modern web-based information systems.

References

1. Bishop C. M. *Pattern Recognition and Machine Learning*. Springer, 2006.
2. Goodfellow I., Bengio Y., Courville A. *Deep Learning*. MIT Press, 2016.

3. Stallings W. *Network Security Essentials*. Pearson Education, 2017.
4. Buczak A. L., Guven E. "Machine Learning Methods for Cyber Security." *IEEE Communications Surveys & Tutorials*, 2016.
5. Chandola V., Banerjee A., Kumar V. "Anomaly Detection: A Survey." *ACM Computing Surveys*, 2009.