

AN ARTIFICIAL INTELLIGENCE–BASED FRAMEWORK FOR IDENTIFYING CYBER THREATS IN WEB APPLICATIONS

Kerimov K

Abstract

The development of web technologies and online communication platforms has created new cybersecurity challenges related to the increasing number of cyber threats targeting web applications. Traditional intrusion detection systems often fail to identify advanced attacks because they rely on static rules and predefined signatures. This study presents an artificial intelligence–based framework for identifying cyber threats in web applications using machine learning and pattern recognition technologies. The proposed system analyzes network traffic behavior, user activities, and web request anomalies to detect malicious actions in real time. Artificial intelligence algorithms such as Neural Networks, Random Forest, and Support Vector Machines are integrated into the framework to improve threat classification performance. Experimental results demonstrate that AI-driven security systems achieve higher detection accuracy and better adaptability compared to conventional cybersecurity methods. The study confirms the effectiveness of artificial intelligence technologies for strengthening web application security and preventing modern cyberattacks.

Keywords: artificial intelligence, cybersecurity, web applications, cyber threats, machine learning, intrusion detection, neural networks, anomaly detection

Introduction

Web applications have become essential components of modern digital infrastructures and support critical services in healthcare, banking, education, e-commerce, and government administration. However, the rapid growth of web technologies has also increased the vulnerability of digital systems to cyberattacks. Cybercriminals use sophisticated methods such as phishing, SQL injection, malware

distribution, and cross-site scripting attacks to exploit weaknesses in web applications.

Traditional cybersecurity systems are often ineffective against dynamic and previously unseen threats because they rely mainly on predefined attack signatures. As cyberattacks become more complex, intelligent security solutions capable of adaptive learning and behavioral analysis are becoming increasingly important.

Artificial intelligence technologies provide effective tools for identifying suspicious activities and detecting abnormal patterns in web environments. AI-based cybersecurity systems can analyze large-scale datasets, learn from attack behaviors, and improve detection capabilities through continuous training. Neural Networks are particularly effective for recognizing nonlinear attack patterns, while Random Forest and Support Vector Machine algorithms improve classification accuracy.

The proposed AI-based framework analyzes HTTP requests, session activities, packet structures, and user behaviors to detect malicious activities within web applications. Feature selection and anomaly detection methods are integrated into the framework to optimize system performance and reduce false-positive alerts. The findings of this study demonstrate that artificial intelligence technologies can significantly improve web application security and support the development of adaptive cybersecurity infrastructures. AI-driven security systems provide scalable and intelligent protection mechanisms capable of responding dynamically to evolving cyber threats.

References

1. Goodfellow I., Bengio Y., Courville A. *Deep Learning*. MIT Press, 2016.
2. Bishop C. M. *Pattern Recognition and Machine Learning*. Springer, 2006.
3. Stallings W. *Cryptography and Network Security*. Pearson Education, 2018.
4. Sommer R., Paxson V. "Machine Learning for Intrusion Detection Systems." *IEEE Symposium on Security and Privacy*, 2010.
5. Alpaydin E. *Introduction to Machine Learning*. MIT Press, 2020.