Unified AI-Enhanced Endpoint Threat Detection and Response System with Attack Simulation Framework

Nirupam.E.S
Department of Computer Science and Engineering B.S.Abdur Rahman Crescent Institute of Science and Technology, India

Akask Kanna. A
Department of Computer Science and Engineering B.S.Abdur Rahman Crescent Institute of Science and Technology, India

Valarmathi. P
Professor, Department of Computer Science and engineering B.S.Abdur Rahman Cresecent Institute of Science and Technology, India

Abstract

The rapid evolution of cyber threats has rendered traditional signature-based endpoint security mechanisms increasingly ineffective. Modern attacks such as zero-day exploits, fileless malware, and advanced persistent threats operate stealthily, often bypassing conventional defenses and remaining undetected for extended periods. Endpoint Detection and Response (EDR) systems aim to address these challenges by continuously monitoring endpoint activities and enabling rapid incident response. However, many existing EDR solutions rely heavily on static rules and lack mechanisms to validate their detection capabilities under realistic attack conditions. This paper presents a Unified AI-Enhanced Endpoint Detection and Response System integrated with an Attack Simulation Framework. The proposed system combines rule-based detection for known threats with machine learning-based anomaly detection to identify previously unseen attacks. Endpoint telemetry is centrally collected and analyzed using a Security Information and Event Management (SIEM) platform, enabling real-time correlation, automated response, and forensic analysis. Furthermore, a controlled attack simulation framework is incorporated to safely evaluate detection accuracy and response effectiveness. Experimental results indicate improved threat detection accuracy, reduced response time, and enhanced endpoint visibility.

Index Terms

Endpoint Detection and Response, Artificial Intelligence, SIEM, Anomaly Detection, Attack Simulation, Cybersecurity