

ABSTRACT

AI-Driven Real-Time Cyberattack Detection and Mitigation System

This project focuses on creating an AI-powered system that can detect, analyze, and mitigate cyberattacks in real time. The system uses machine learning algorithms to quickly find the root cause of an attack, helping organizations recover faster and minimize damage. Instead of relying on manual investigations, this tool automates the process, making cybersecurity more efficient and proactive.

One of the key features is Attack Path Mapping, which provides a visual representation of how an attack spreads through a network. This helps security teams identify compromised areas and understand how the attack evolved. Additionally, Code-Level Tracing pinpoints the exact line of code or system configuration that led to the vulnerability, allowing for a quick fix to prevent further issues.

The system also integrates with Security Information and Event Management (SIEM) tools, improving its ability to collect and analyze security data. Its self-healing feature can automatically fix common security weaknesses, reducing the burden on IT teams. Moreover, the real-time forensics feature captures and analyzes logs as an attack happens, providing valuable insights for quick decision-making.

By combining AI, automation, and real-time analysis, this system enhances cybersecurity, reducing risks, financial losses, and system downtime.