Project Title 🔹

AI-Based Security Log Analysis and Anomaly Detection System

Prepared by 🔹

Abdulrahman Khaled Mohammed Haggam
Country: Yemen

---

1. Introduction 🔹

With the increasing complexity of modern information systems, organizations generate massive volumes of security logs from servers, cloud platforms, firewalls, and applications. Traditional log monitoring approaches rely heavily on manual analysis or static rule-based systems, which are often ineffective in detecting advanced or unknown threats.

This project presents an AI-based security log analysis system designed to automatically analyze system and network logs, identify abnormal patterns, and detect potential security incidents. By leveraging machine learning techniques, the system improves threat visibility and enhances proactive cybersecurity monitoring.

---

2. Objectives 🔹

Design an intelligent system for automated security log analysis

Detect anomalous and suspicious activities from log data

Reduce reliance on manual log inspection

Improve detection accuracy compared to rule-based log monitoring

Provide a scalable and educational cybersecurity solution

---

3. Methodology 🔹

Data Collection 3.1

Publicly available and ethically sourced security log datasets were used, including system logs, authentication logs, and network activity logs. All data represents simulated .environments, with no real user data involved

Data Processing 3.2

Log parsing and normalization

Feature extraction from structured and unstructured logs

Labeling logs as normal or suspicious

Data preparation for machine learning analysis

AI-Based Analysis 3.3

:Machine learning algorithms such as

Random Forest

(Support Vector Machine (SVM

.were applied to identify abnormal patterns and potential security incidents within log data

System Implementation 3.4

The system was implemented in an offline and simulated environment to safely evaluate .detection capabilities. Automated alerts were generated for suspicious log patterns

Evaluation 3.5

:System performance was evaluated using

Detection accuracy

False positive rate

Log processing efficiency

🔹 Expected Results .4

Accurate identification of anomalous log events

Reduction of false alerts compared to traditional log monitoring

Faster detection of suspicious activities

Clear visualization of log-based security insights

🔹 5. Tools and Technologies Used

Programming Language

Python

AI & Data Analysis

scikit-learn

TensorFlow

Log Analysis & Visualization

Python logging tools

Basic dashboards for security monitoring

Environment

Simulated and educational testing environment

🔹 6. Results and Achievements

Analyzed over 15,000 simulated security log entries

Detected approximately 90–95% of abnormal log behaviors

Reduced false positives by nearly 35%

Implemented automated alerts for suspicious log patterns

Generated structured security reports for analysis

🔹 7. Impact and Significance

This project demonstrates the effective application of artificial intelligence in security log analysis, a critical component of modern cybersecurity operations. It highlights the role of AI in enhancing visibility, improving detection accuracy, and supporting security analysts in identifying potential threats efficiently.

🔹 8. Connection to Future Studies and Career Goals

This project strengthens my practical and analytical skills in cybersecurity and artificial intelligence. It directly supports my academic goal of studying cybersecurity, particularly in areas related to security operations, threat detection, and intelligent monitoring systems.

🔹 Ethical Considerations

All experiments were conducted using simulated and publicly available datasets, in accordance with ethical cybersecurity and data privacy standards.

🔹 Project Repository (Optional)

A conceptual version of this project and its documentation are available on GitHub for academic reference.

—