International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 04 April-2026 | Impact Factor: 3.5

Development of AEOSARS: An AI Enhanced Offline Security Audit Reporting System for Air Gaped Cybersecurity Environments

KAVITHA C[1], SASHWATH Y[2], NITHISH M[3], GUNASEKARAN V[4]
[1]*Kavitha C, Sri Ramakrishna Engineering College*
[2]*Sashwath Y, Sri Ramakrishna Engineering College*
[3]*Nithish M, Sri Ramakrishna Engineering College*
[4]*Gunasekaran V, Sri Ramakrishna Engineering College*

How to Cite this Article:

C, K., Y, S., M, N. & V, G. (2026). Development of AEOSARS: An AI Enhanced Offline Security Audit Reporting System for Air Gaped Cybersecurity Environments. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.192

https://doi.org/10.55041/ijcope.v2i4.192

Abstract: The AI Enhanced Offline Security Audit Reporting System (AEOSARS) is a desktop application that automates the lengthy task of technical vulnerability reporting. Unlike traditional deep exploitation scanners, this system targets flaws in configuration files and system logs. It combines a rule-based detection engine with audit reports while keeping data secure in sensitive environments. This paper explains the system's "Chain of Evidence" chunking architecture and how it effectively reduces the time cybersecurity analysts spend on manual reporting.

Index Terms: Cybersecurity Audit, Offline AI, Rule-Based Detection, Security Reporting Automation, Air-Gapped Systems, Vulnerability Evidence.

I. INTRODUCTION

As software systems and network infrastructures grow more complex, cybersecurity auditing becomes essential for organizations. Security audits help identify weaknesses, misconfigurations, and possible attack paths before they can be exploited by malicious actors. Traditional auditing often requires multiple independent tools, such as vulnerability scanners, network traffic analyzers, and penetration testing frameworks. These tools typically require manual setups and expert interpretation of their outputs.

Many current security platforms depend on online resources for vulnerability intelligence. This reliance makes them unsuitable for environments with restricted access, like internal enterprise networks, research labs,

defense infrastructures, and other air-gapped systems.

To address these challenges, this research proposes an Offline Auditor. This intelligent auditing platform conducts automated security assessments without needing a continuous internet connection. The system combines various scanning tools and uses artificial intelligence to interpret scan results and create organized security reports. Users can start security scans using conversational prompts. Based on the prompt, the system chooses suitable tools, runs them, processes the results, and generates reports that include vulnerability descriptions, risk severity, affected components, and suggested solutions.

This approach simplifies the cybersecurity auditing process. It also makes advanced analyses easier for users with limited expertise.

II. RELATED WORK

Many tools and frameworks exist for vulnerability scanning and network security assessments. Well-known tools like vulnerability scanners, packet analyzers, and penetration testing frameworks can effectively identify security weaknesses in systems and networks.

Network analysis tools review application traffic and highlight suspicious activities. These tools allow security analysts to capture packets, evaluate protocols, and detect anomalies in communication patterns. Similarly, vulnerability scanners can find outdated software versions, misconfigured services, and known security issues.

However, most existing solutions have several limitations. Many tools operate independently and require manual correlation of results from different sources. This process can be slow and demands extensive expertise from security professionals.

Another issue is many modern cybersecurity platforms rely on cloud-based vulnerability databases and online analysis tools. These needs make them unsuitable for offline or restricted environments.

The proposed Offline Auditor system overcomes these limitations by integrating multiple security tools into one platform and using AI to automatically interpret scan results and generate detailed reports. The system provides an automated auditing workflow that significantly reduces the time and effort needed for security assessments.

III. SYSTEM ARCHITECTURE

The architecture of the Offline Auditor platform uses a modular layered design to ensure scalability, ease of maintenance, and effective handling of security data. The system has four main layers:

User Interface Layer:
This layer features an interactive chat interface where users can request various types of security scans. They can input prompts for vulnerability scans, traffic analysis, or application security assessments. The interface displays scan results, visualizations, and generated security reports.

AI Processing Layer:
This layer analyzes user prompts using natural language processing techniques. It determines the type of security scan needed and matches the request with suitable scanning tools. It also reviews scan outputs and extracts meaningful security insights.

Security Tool Integration Layer:
This layer connects the system with various cybersecurity tools used for scanning and analysis. These tools perform tasks like network scanning, traffic capture, vulnerability detection, and service enumeration. The outputs from these tools are collected and sent to the AI analysis engine.

Data and Report Generation Layer:
This layer stores results and creates organized security reports. It categorizes detected vulnerabilities by severity and generates visual representations, such as vulnerability distribution charts and risk summaries.

The layered architecture allows efficient interaction among components and secure handling of sensitive security data.

IV. METHODOLOGY

User Prompt Processing:
The auditing process begins when a user submits a prompt for a security scan. The AI module analyzes the prompt to determine the type of security assessment needed, such as network scanning, traffic inspection, or vulnerability analysis.

Automated Tool Selection:
Based on the interpreted prompt, the system selects the necessary security tools for the requested analysis. The tools run automatically with preset configurations suitable for the tested environment.

Data Collection and Preprocessing:
During the scanning process, the system collects network traffic data, service information, and vulnerability indicators from the running tools. The gathered data is cleaned and organized for further analysis.

Vulnerability Detection and Classification:
The AI analysis module processes the collected data and identifies potential security vulnerabilities. Detected vulnerabilities are classified by severity, such as critical, high, medium, and low. The system also determines the root cause and affected components of each vulnerability.

Automated Report Generation:
Once the analysis is complete, the system generates a structured security audit report. The report includes several sections like:
- Executive Summary
- List of detected vulnerabilities
- Severity classification
- Detailed vulnerability descriptions
- Root cause analysis
- Recommended remediation strategies
- Visual representations of risk levels

These reports help organizations quickly understand their security status and prioritize their mitigation efforts.

V. RESULTS AND ANALYSIS

The Offline Auditor system was tested in simulated network setups to evaluate its effectiveness in detecting vulnerabilities and generating automated security reports. The evaluation focused on three key performance aspects: detection ability, reporting efficiency, and usability.

Experimental results showed that the system detected common vulnerabilities, such as open ports, insecure services, outdated software versions, and suspicious network traffic patterns. The AI analysis module efficiently processed the scan outputs and generated structured reports without needing manual interpretation.

Compared to traditional manual auditing workflows, the Offline Auditor significantly reduced the time taken to create comprehensive security reports. The chat-based interface also simplified interactions with security tools, enabling users to conduct complex security assessments using straightforward prompts.

Overall, the system showed better effectiveness in vulnerability detection and reporting while remaining suitable for offline environments.

VI. CONCLUSION AND FUTURE WORK

This paper introduced the Offline Auditor, an AI-powered cybersecurity auditing platform designed to automate vulnerability scanning and security report generation in offline settings. The system combines various security tools and uses artificial intelligence to analyze scan results and create detailed reports.

By providing a single interface for security scanning and automated report generation, the Offline Auditor simplifies the cybersecurity auditing process and reduces the need for expert manual analysis. The platform especially benefits organizations operating in restricted or air-gapped networks with limited internet access.

Future work will focus on improving the system with advanced machine learning techniques for spotting anomalies, adding more security tools for deeper analyses, and enhancing visualization options for better representation of security risks. Additional improvements may include predictive vulnerability analysis and automated remediation recommendations.

REFERENCES

[1] National Institute of Standards and Technology, Guide for Conducting Risk Assessments, NIST Special Publication 800-30, Gaithersburg, MD, USA, 2022.

[2] Open Web Application Security Project, OWASP Top 10: The Ten Most Critical Web Application Security Risks, OWASP Foundation, 2023.

[3] Gary McGraw, Software Security: Building Security In, Addison-Wesley Professional, Boston, MA, USA, 2006.

[4] Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed., Wiley, 2020.

[5] Ian Goodfellow, Yoshua Bengio, and Aaron Courville, Deep Learning, MIT Press, Cambridge, MA, USA, 2016.

[6] A. Sharma, R. Gupta, and P. Kumar, "Automated vulnerability detection using machine learning techniques," IEEE Access, vol. 9, pp. 124567–124578, 2021.

[7] L. Wang, S. Jajodia, and A. Singhal, "Network vulnerability analysis and security risk assessment," IEEE Security & Privacy, vol. 8, no. 6, pp. 44–52, 2020.

[8] H. Holm, M. Ekstedt, and D. Andersson, "Empirical analysis of system vulnerabilities and security risk evaluation," Computers & Security, vol. 34, pp. 31–43, 2019.

[9] J. Kim and Y. Lee, "AI-assisted cybersecurity analysis for automated security auditing systems," Journal of Information Security and Applications, vol. 60, pp. 102870, 2021.