

Research Issues 3

Task 10

Abdulaziz Alarfaj



الملخص التنفيذي - Executive Summary

Automated Cybersecurity Compliance and Threat Response Using AI, Blockchain & Smart Contracts
(Lampis Alevizos & Vinh Thong Ta, 2024)

<https://arxiv.org/abs/2409.08390>

1. Background and Objective - الخلفية والاهداف

Cybersecurity compliance and real-time threat response remain major challenges for organizations worldwide due to evolving attack techniques and human error.

Traditional security frameworks often rely on manual policy enforcement and lack scalability in dynamic environments.

This research project aims to design an automated cybersecurity compliance and threat response system by integrating Artificial Intelligence (AI), Blockchain, and Smart Contracts. The goal is to improve enforcement consistency, reduce human dependencies, and enhance response efficiency against emerging threats

2. Methodology - المنهجية

The researchers adopted an **applied systems design and simulation methodology**. The proposed framework consists of three integrated components:

AI Engine: Analyzes cyber threat intelligence data to detect compliance violations and emerging threats in real time.

Blockchain Ledger: Maintains immutable logs of compliance actions and security events for transparency and auditability.

Smart Contracts: Automate enforcement of security policies based on predefined rules, ensuring uniform policy application across systems.

The effectiveness of the framework was evaluated through simulation scenarios comparing automated enforcement with traditional methods.

3. Key Findings / Results - النتائج

The study's outcomes demonstrated significant improvements in several areas:

Faster Threat Response: The AI-enabled system detected non-compliance and responded faster than manual processes.

Improved Compliance Rates: Automated enforcement reduced inconsistencies caused by human error.

Audit Transparency: Blockchain logging provided clear, tamper-proof records of compliance and threat events, facilitating audits.

Overall, the framework showed enhanced scalability and adaptability compared to conventional compliance enforcement approaches.

4. Recommendations - التوصيات

The researchers provide the following practical and strategic recommendations:

Adopt AI-Driven Compliance Tools: Organizations should invest in AI-powered compliance monitoring to proactively detect and manage security gaps.

Use Immutable Logging for Accountability: Blockchain can strengthen trust and reduce disputes by ensuring tamper-proof audit trails.

Leverage Smart Contracts for Automation: Embedding policies into smart contracts reduces manual oversight and standardizes enforcement across distributed systems.

Further Empirical Testing: Real-world implementation and longitudinal studies are recommended to validate scalability and performance in operational environments.

5. Conclusion - الخلاصة

This research project offers an innovative approach to addressing core challenges in cybersecurity policy compliance and threat response.

By integrating AI, blockchain, and smart contracts, the authors propose a scalable model that improves enforcement efficiency and strengthens organizational defense capabilities.

The study contributes valuable insights for both cybersecurity practitioners and researchers seeking automated, resilient security solutions in complex digital infrastructures.