Chapter 9
Hybrid ML–LLM Pipeline for Non-Governance IT Audits

Kaung Myat Naing

http://orcid.org/0009-0003-8801-3067
Illinois Institute of Technology, USA

Talha Ali
Illinois Institute of Technology, USA

Mohammed Ouannass
Illinois Institute of Technology, USA

ABSTRACT

Organizations outside formal governance frameworks often lack cybersecurity audit tools, making anomaly detection and risk evaluation difficult. This paper presents an AI-enhanced auditing framework for non-governance IT environments. Using the UNSW-NB15 dataset, we evaluate four machine-learning models: Isolation Forest, Logistic Regression, Gradient Boosting, and XGBoost, identifying complementary strengths that motivate a two-stage filter for suspicious network flows. Flagged flows are aggregated into structured evidence and passed to a GPT-4-based large language model, which generates incident explanations, control mappings, and remediation suggestions. Results show the hybrid ML-LLM approach reduces audit workload, improves anomaly interpretation, and supports recommendations for private and small-scale IT systems. The study also highlights limitations including prompt sensitivity, false positives, and third-party AI risks. Overall, findings illustrate both the potential and challenges of deploying AI-driven audit pipelines to strengthen cybersecurity in non-governance settings.

DOI: 10.4018/979-8-3373-8252-4.ch009

1. INTRODUCTION

With the growth of the internet, cybersecurity and cybersecurity audits must evolve. While government systems have strict rules, private companies often operate with fewer regulations. This goes for both large corporations as well as small businesses. This creates a blind spot. Private companies face two major issues. They rely on complex supply chains. If a third-party vendor forgets to update their software, then the main company is vulnerable. They are also limited in the resources they can spend. The private sector favours innovation and risk. This allows them to grow quickly. This can result in a lack of auditing. The one-size-fits-all framework fails with smaller companies and businesses (Al-Dosari & Fetais, 2023). They require an AI system that can handle high demand and complexity. By creating an AI cybersecurity model that can detect anomalies and explain the issue in plain English as well as find solutions efficiently, this increases security for everyone as a whole (Wu & Tian, 2025). This includes users, small companies, and large companies. By making it efficient, we can lower prices to make it affordable (Al-Dosari & Fetais, 2023).

This study builds and tests a new hybrid AI Framework to automate the auditing process for private companies. This system works in two layers. The first layer is the filtering layer. Machine learning models scan huge amounts of data to quickly spot anomalies by using deep autoencoders and deep-learning-based intrusion detection systems (Benka et al., 2025; Zhang et al., 2025; Rhachi et al., 2025; Xu et al., 2025). The second layer uses large language models to look at the anomalies and then write a clear and easy-to-understand report explaining the risk (Palma et al., 2025; Rhachi et al., 2025). We evaluate this system not just on whether it works. There are three business factors to look out for: Is it necessary for audits? Is it efficient? How trustworthy is it?

The main innovation isn't just detecting viruses or suspicious network traffic. The main innovation is automating and modernising the pipeline. We can use tools that already exist to detect suspicious activity, but it still requires a human to understand the issue and then to formulate a report and solution for the issue. This also brings about the question of who should run these audits.

While developing this AI audit system isn't exactly necessary, it can help in all aspects of business. Larger corporations have the resources to spend on a cybersecurity auditing company. These companies can go through the entire system, which can take days. This can result in delays for the main corporation. They can afford to delay certain deadlines and still manage to stay afloat. Smaller companies, however, often cannot afford to pay for regular audits. This leaves them vulnerable to attacks from unsecured systems. By using AI for cybersecurity auditing, they will be able to afford routine audits, keeping the company as well as its clients safe.