Ministry of Higher Education and Scientific Research

Higher Institute of Management and Information Technology, Kafr El-Sheikh

Graduation Project

Network Anomaly Detection for insider Attacks

Prepared by the Students

1- **Abdelhalim Mohsen Fathallah**
2- **Sameh Mahmoud El-Gebally**
3- **Asmaa Ibrahim Lila**
4- **Mohamed Ali AbdelMuti**
5- **Mahmoud Hossam elden El-gohary**

Supervised by

D. Amr E. Elshora **D. Ahmed Eltokhy**

2025

Chapter 1: Introduction

Chapter 1

Introduction

1.1 Introduction

The dawn of the fourth industrial revolution has been characterized by the unprecedented dominance of Artificial Intelligence (AI) and its advanced subset, Deep Learning (DL). Unlike traditional computing which relies on explicit, pre-defined instructions, AI has introduced a paradigm shift toward "learning from experience." By mimicking the neural structures of the human brain, Deep Learning models have demonstrated an extraordinary ability to process high-dimensional, unstructured data and extract meaningful patterns that are often invisible to human analysts. This technological leap has redefined efficiency across various domains, enabling machines to perform complex tasks such as natural language understanding, autonomous decision-making, and predictive modeling with a level of precision that continues to evolve at an exponential rate (1,2).

As global infrastructures become increasingly digitized, this AI-driven transformation has found its most critical application within the realm of **Cybersecurity**. The modern digital landscape is no longer a static environment; it is a dynamic, hyper-connected ecosystem where massive volumes of data are exchanged every second across cloud platforms, remote work-spaces, and distributed networks. Consequently, the "attack surface" for organizations has expanded significantly. While traditional security frameworks—such as firewalls and signature-based Intrusion Detection Systems (IDS)—were designed to defend against known, external "brute-force" attacks, they are proving to be increasingly inadequate in the face of modern, stealthy, and highly sophisticated cyber-threats. The sheer scale of network traffic today creates a "data deluge" that makes manual monitoring impossible, necessitating the deployment of intelligent, automated security architectures (3).

Within this complex security landscape, the **Insider Threat** has emerged as one of the most persistent and dangerous challenges for any organization. Unlike external hackers who must navigate through perimeter defenses, insiders already reside within the "circle of trust." These individuals—whether they are employees, contractors, or administrators—possess legitimate access credentials and a deep understanding of the organization's internal workflows. Because their activities are performed within a trusted environment, malicious actions such as unauthorized data exfiltration, privilege escalation, or system sabotage often blend seamlessly with routine daily operations. This makes the insider threat a "silent predator"; it does not leave the typical "digital fingerprints" that traditional security systems are programmed to look for, allowing attacks to remain undetected for months or even years, leading to catastrophic financial losses and irreversible reputational damage (4,5,6).

To address this critical vulnerability, this research focuses on the synergy between **Advanced Artificial Intelligence and Network Anomaly Detection (NAD)**. Instead of searching for specific "malicious signatures," which insiders can easily avoid, the proposed approach leverages the power of **Deep Learning (specifically Convolutional Neural Networks - CNNs)** to learn the unique "behavioral DNA" of the network. By modeling the baseline of normal user activity and network flows, the system becomes capable of identifying subtle deviations—anomalies—that signal a potential breach of trust. This project aims to design and implement an intelligent, adaptive framework that can distinguish between legitimate operational changes and malicious intent, providing a robust and proactive defense mechanism against the evolving threat of insider attacks in the modern digital enterprise (7,8).

1.2 Motivation

The motivation behind this project is driven by the urgent need to bridge the gap between traditional security capabilities and the evolving nature of internal cyber threats. The specific drivers include:

- Failure of Legacy Systems: Traditional security tools (like firewalls and signature-based IDS) are designed to stop external intruders but are "blind" to malicious activities performed by authorized users with legitimate credentials.
- The "Trusted" Vulnerability: Insider attacks are uniquely dangerous because they occur within the organization’s "circle of trust," allowing attackers to bypass perimeter defenses without triggering standard alarms.
- Complexity of Human Behavior: Unlike automated malware, human-driven attacks are subtle and inconsistent. There is a critical need for a system that can understand "normal behavior" and detect slight, suspicious deviations that human analysts might miss.

- The Data Deluge: Modern networks generate massive volumes of traffic logs every second. Manual monitoring is impossible, necessitating an AI-driven approach that can process big data and identify anomalies in real-time.
- High Cost of Failure: Insider threats often lead to the most expensive data breaches, causing irreversible financial loss and reputational damage. Developing a proactive, intelligent defense is no longer a luxury but a necessity for organizational survival.

1.3 Contributions

This project addresses five critical gaps in the field of Cybersecurity and AI-driven Network Monitoring. The specific contributions of this research are:

1. **Bridging the "Invisible Threat" Gap:** Solving the failure of traditional rule-based systems (firewalls/IDS) in detecting authorized users. By implementing **behavioral AI**, the project provides a solution for identifying "stealthy" insider attacks that do not leave known malicious signatures.
2. **Automating Feature Discovery:** Addressing the inefficiency of manual "Feature Engineering." The use of a **CNN architecture** solves the problem of human error and bias in selecting security indicators, as the model automatically learns the most relevant patterns from raw network flows.
3. **Solving Data Complexity via "Behavioral Imaging":** Resolving the difficulty of processing high-dimensional, unstructured network logs. The project introduces a method to transform sequential traffic into **matrix-based representations**, making complex network data "readable" and efficient for Deep Learning models.
4. **Reducing "Alert Fatigue" (False Positives):** Solving the common problem of excessive false alarms in anomaly detection. By developing a **Normal Behavior Profile (NBP)** with adaptive thresholding, the project provides a way to distinguish between legitimate network changes and actual malicious intent.
5. **Closing the Research-to-Real-Time Gap:** Addressing the performance bottleneck where Deep Learning models are often too slow for live networks. This project contributes a **low-latency framework**, proving that advanced AI can be scaled for near real-time detection in high-throughput environments.

1.4 Refrences

1. Artificial Intelligence & Deep Learning

[1] LeCun, Y., Bengio, Y., & Hinton, G. (2015). **Deep learning**. *Nature, 521*(7553), 436–444. https://doi.org/10.1038/nature14539

[2] Schwab, K. (2017). *The fourth industrial revolution*. World Economic Forum.

[3] Verizon. (2024). *Data breach investigations report (DBIR)*. Verizon Enterprise Solutions.

[4] IBM Security. (2024). *Cost of a data breach report*. IBM Corporation.

[5] Homoliak, I., Toffalini, F., Guarnizo, J. D., Elovici, Y., & Ochoa, M. (2019). **Insight into insiders: A survey of insider threat taxonomies, datasets, and detection techniques**. *ACM Computing Surveys*, *52*(2), Article 30. https://doi.org/10.1145/3303771

[6] Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). *The CERT guide to insider threats: How to prevent, detect, and respond to information technology crimes*. Addison-Wesley Professional.

[7] Wang, W., Zhu, M., Zeng, X., Ye, X., & Sheng, Y. (2017). **Malware traffic classification using convolutional neural networks**. In *Proceedings of the IEEE International Conference on Communications (ICC)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICC.2017.7996808

[8] Kwon, D., Kim, H., Kim, J., Suh, S. C., Kim, I., & Kim, K. J. (2019). **A survey of deep learning-based network anomaly detection**. *Cluster Computing, 22*(1), 949–961. https://doi.org/10.1007/s10586-017-1117-8