Expanded Research Paper Sections

# I. Background of the Study

Cybersecurity threats have evolved significantly over the years, growing in both frequency and sophistication. Traditional defense mechanisms such as firewalls and antivirus software are often inadequate in detecting and preventing advanced persistent threats, zero-day vulnerabilities, and stealth-based intrusions. In this context, Host-Based Intrusion Detection Systems (HIDS) serve as a vital line of defense by monitoring system behavior at the operating system level. System call analysis has emerged as a powerful approach for implementing HIDS because system calls reflect the operational behavior of applications and can provide granular insights into both normal and abnormal activities. This study leverages three comprehensive datasets—ADFA-LD (Linux), ADFA-WD (Windows), and ADFA-WD:SAA (Windows Stealth Attacks Addendum)—to develop and evaluate a hybrid HIDS framework. The aim is to bridge the gaps left by existing models, particularly in terms of real-time performance, detection accuracy, and handling of imbalanced datasets.

# II. Statement of the Problem

Host-based intrusion detection remains a challenging domain due to the difficulty in accurately identifying sophisticated attacks in diverse and dynamic environments. Existing models often suffer from high false-positive rates, poor scalability, and an inability to adapt to zero-day and stealth attacks, especially when datasets are imbalanced. Furthermore, many detection systems are not optimized for real-time performance, limiting their applicability in operational settings. This research seeks to develop a robust, real-time, and adaptive HIDS framework that addresses these challenges using system call analysis and hybrid machine learning techniques.

# III. Objectives of the Study

The specific objectives of this research include:

1. To develop a hybrid machine learning framework that combines classical and deep learning techniques for enhanced intrusion detection accuracy.

2. To design and evaluate effective feature extraction and selection methods that capture the semantic and temporal characteristics of system calls.

3. To assess the performance of the proposed models using diverse datasets (ADFA-LD, ADFA-WD, ADFA-WD:SAA).

4. To implement mechanisms for real-time analysis with minimal latency and computational overhead.

5. To incorporate strategies for handling imbalanced datasets to improve detection of low-frequency but critical attacks.

# IV. Hypotheses (if applicable)

H1: A hybrid detection model integrating machine learning and deep learning will outperform individual models in detecting complex and stealthy attacks.

H2: Feature extraction techniques such as TF-IDF, SVD, and CNN-based embeddings will enhance the model’s ability to distinguish between benign and malicious behavior.

H3: Using data balancing methods and few-shot learning will significantly improve detection rates for underrepresented attack classes.

# V. Significance of the Study

This study contributes significantly to the field of cybersecurity by presenting an advanced and practical solution for host-based intrusion detection. It leverages state-of-the-art feature engineering and machine learning techniques to address key challenges such as real-time detection, system scalability, and data imbalance. The findings have practical implications for designing HIDS that can be deployed in enterprise, government, and cloud-based environments. By integrating models validated on both Linux and Windows datasets, the research also supports cross-platform applicability, a critical factor in today’s heterogeneous IT infrastructures.

# VI. Scope and Limitations of the Study

Scope:

- The research focuses on system call-based intrusion detection within host environments using three ADFA datasets: ADFA-LD, ADFA-WD, and ADFA-WD:SAA.

- It evaluates the performance of machine learning and deep learning models including Random Forest, SVM, CNN, and LSTM.

- The models are tested under controlled experimental conditions to ensure reproducibility and consistency in results.

- The study incorporates multiple feature extraction techniques and evaluates them based on accuracy, precision, recall, and processing latency.

Limitations:

- The datasets used, though comprehensive, may not fully represent real-world conditions and attack diversity.

- Long system call sequences can introduce computational overhead, affecting scalability.

- The models have not been validated on completely unseen datasets or deployed in live production environments, which limits generalizability.

- The study does not consider external network-based intrusions or cross-host coordination of attacks.