**System Call Analysis for Hybrid Host-Based Intrusion Detection Systems**

**Aryan Vats, Nitesh Jha, Shikhar Sharma**  
Computer Science and Engineering, NIIT University, Neemrana, India

**I. Background of the Study**

Cybersecurity threats have only gone better in today’s times, evolving in both frequency and sophistication. The older and more traditional defence mechanisms like firewalls and antivirus scanning softwares are often proven to be inadequate in detecting these advanced persistent threats, zero-day vulnerabilities and stealth based intrusions. Host-Based Intrusion Detection systems(HIDS) thus, play a vital role in the line of defence by monitoring the system behaviour at the Operating System level. Using System Call Analysis has emerged to become a powerful approach for implementing these HIDS’s as system calls reflect upon the operation behaviour of the applications and also provide detailed granular insights into the normal and abnormal activities happening in the system.

Our work is concerned in using three different comprehensive datasets-ADFA-LD (for Linux),ADFA-WD(for Windows),and ADFA-WD:SAA (Windows Stealth Attacks Addendum)- and uses these three datasets as backbone for the development and evaluation of a hybrid HIDS framework. The aim is to fix the gaps left by existing models, in the terms of the real-time performance, attack detection accuracy and handling the imbalanced datasets, an issue observed mostly in ADFA-WD dataset.

**II. Statement of the Problem**

Despite the ongoing progress going on in the research regarding HIDS systems, current systems still struggle to detect real-time stealthy and complex attacks, especially in cases of class imbalance and system noise in their training datasets not taken care of. High false-negative and false-positive rates, poor scalability, and limited adaptability to the current zero-day and stealthy attacks are the persistent issues in development of HIDS. Many detection systems today are not optimized for real-time performance, limiting their own practical deployment. This research works to develop a robust and adaptive HIDS system using system call analysis and hybrid machine learning techniques to overcome the above mentioned challenges.

**III. Objectives of the Study**

* To develop a hybrid HIDS framework that utilizes classical machine learning and deep learning techniques to better the intrusion detection accuracy of the HIDS systems.
* To design and evaluate the different feature extraction and feature selection methods for capturing the best semantic and temporal characteristics of system calls in Windows and Linux Operating Systems
* To assess the performance of these models on the diverse datasets of ADFA-LD,ADFA-WD and ADFA-WD:SAA.
* To implement these mechanisms for a real-time analysis and a minimal computational overhead and load.
* To incorporate the strategies of handling data imbalance problems in the imbalanced datasets for improvement in the detection of low-frequency critical attacks.

**V. Significance of the Study**

This Proposed HIDS system by us does a significant contribution to the field of cybersecurity by presenting a practical solution to the problem of host-based intrusion detection. By leveraging state-of-the-art feature engineering followed by machine learning techniques to address the key problems of detection in real time, scalability and data imbalance. Our findings have practical implications for designing a Host-based Intrusion Detection System that can be deployed in enterprises,government and even Cloud Based Environments. By integrating the datasets that were validated on the Linux and Windows datasets, our work supports cross-platform applicability, a crucial factor for today’s heterogenous IT infrastructures.

**VI. Scope and Limitations of the Study**

**Scope:**

* Focussed towards system call based intrusion detection inside the host environments with the help of three ADFA(Australian Defence Force Academy Datasets): ADFA-LD,ADFA-WD and ADFA-WD:SAA.
* Evaluates the performance of our applied machine learning and deep learning models like XGBoost,Stacked ensemble XGBoost,SVM,CNN and LSTM.
* Models are to be tested in the controlled experimental conditions for a better reproducibility and even consistency in the results
* Incorporating a system of multiple feature extraction techniques and evaluating them based on the metrics accuracy,precision,recall,f1-score and processing details.

**Limitations:**

* Datasets, though comprehensive, may not fully represent real-world conditions and attack diversity. Datasets,although comprehensive, may not represent the real-world conditions and a diversity observed in the attacks completely.
* Long system calls,despite still can lead to the introduction of computational overhead, which might affect the scalability.
* Models have not been validated on completely different and unknown datasets neither they have been deployed in live production environments, which limits their generalizability.
* Our study does not explore the external network based intrusion or cross-host coordination of different attacks.

**VII. Literature Review**

**ADFA-LD Dataset:**

* Feature selection, TF-IDF, and SVD have improved anomaly detection but often lack evaluation in dynamic environments.
* CNN-based context-aware feature extraction has shown superior accuracy but requires more generalized models for diverse datasets.

**ADFA-WD Dataset:**

* Stacking ensemble models and ensemble learning techniques have improved classification accuracy but face challenges in computational overhead and real-time deployment.

**ADFA-SAA Dataset:**

* SVM classifiers and deep neural networks have demonstrated higher accuracy for complex intrusion patterns, but imbalanced datasets and computational requirements remain issues.

**Identified Gaps:**

* Persistent data imbalance negatively impacts anomaly detection accuracy.
* Trade-off between detection speed and accuracy is a critical challenge.
* Scalability and generalization of deep learning models across environments need further improvement.
* High computational requirements limit real-world deployment of complex models4.

**VIII. Methodology**

**Data Sources:**

* ADFA-LD, ADFA-WD, and ADFA-WD:SAA datasets, representing Linux and Windows environments, including stealth attack scenarios.

**Feature Engineering:**

* Techniques include TF-IDF, SVD, and context-aware embeddings using CNNs to capture both semantic and temporal characteristics of system calls.

**Model Development:**

* Hybrid approach combining classical machine learning (Random Forest, SVM, Naïve Bayes) and deep learning (CNN, RNN, LSTM).
* Ensemble methods and stacking are used to leverage strengths of different models.

**Evaluation Metrics:**

* Accuracy, precision, recall, F1-score, and latency.
* Special attention to performance on imbalanced classes and real-time detection capabilities.

**Handling Data Imbalance:**

* Use of sampling techniques, loss function adjustments, and few-shot learning to improve detection of rare attacks124.

**IX. Results and Discussion**

* **Detection Accuracy:** Hybrid models consistently outperform individual models, particularly in detecting stealth and complex attacks.
* **Feature Extraction:** Advanced techniques (TF-IDF, SVD, CNN embeddings) significantly improve the ability to distinguish between benign and malicious behaviors.
* **Imbalanced Data:** Data balancing strategies lead to higher detection rates for underrepresented attack types.
* **Real-Time Performance:** Optimized models maintain low latency, supporting real-time deployment.
* **Cross-Platform Applicability:** The framework demonstrates robust performance across both Linux and Windows datasets124.

**X. Conclusion and Future Work**

This research presents a robust, hybrid HIDS framework leveraging system call analysis, advanced feature engineering, and hybrid machine learning techniques. The approach addresses key challenges in accuracy, real-time performance, and data imbalance, demonstrating practical applicability across diverse host environments.

**Future Directions:**

* Validation on unseen datasets and deployment in live production environments.
* Exploration of lightweight models for resource-constrained devices.
* Extension to network-based and cross-host intrusion detection scenarios124.