Network Connection Management Based on the Integration of Artificial Intelligence for IT Operations and Threat Intelligence Databases

State University of Ceará (UECE), Brazil

Francisco V. J. Nobre, Ramon S. Araujo, Davi O. Alves,

Erik S. Nascimento, Lyedson S. Rodrigues, Rafael L. Gomes

UNIVERSIDADE ESTADUAL DO CEARÁ

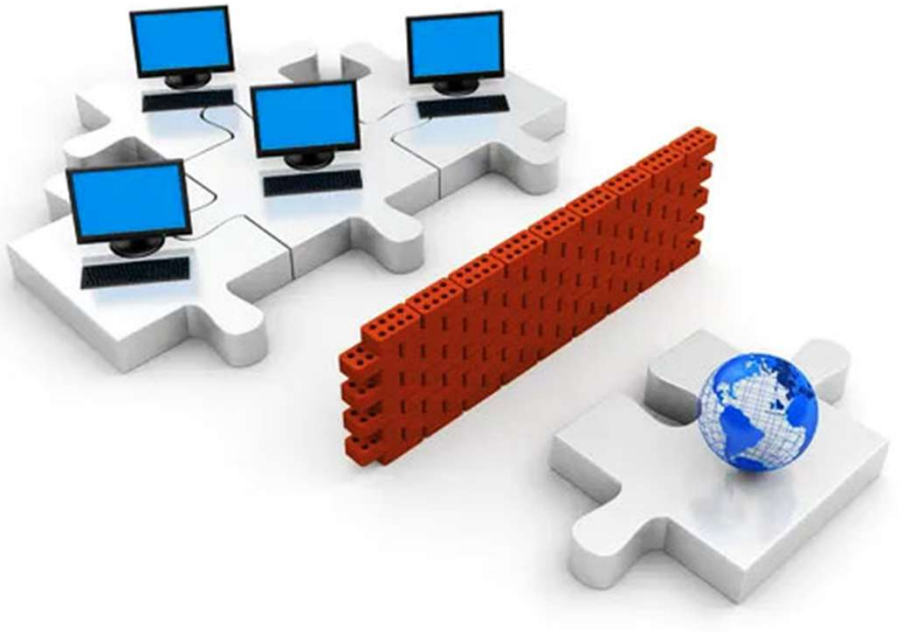
Introduction

Larces
Laboratório de Redes de Computadores e Segurança

Universidade Estadual do Ceará

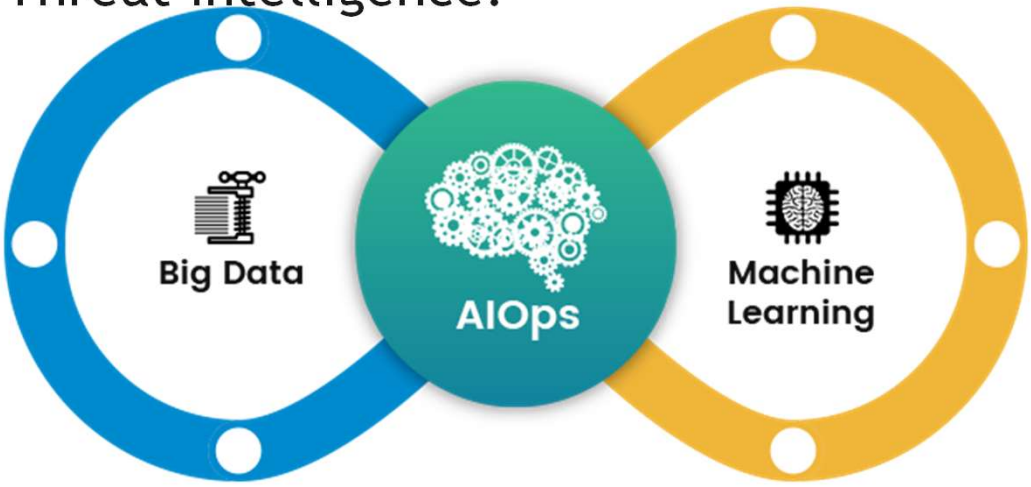
Introduction

- Information security is not just a necessity, but a prerequisite for protecting IT infrastructures and data.
- These network infrastructures are becoming increasingly complex and constant targets of cyber attacks.
- Traditional defenses, such as static denylists and manual filters, are no longer effective against dynamic and obfuscated threats.
- This reality demands security solutions that are adaptable, resilient, and capable of anticipating emerging threats.



Context

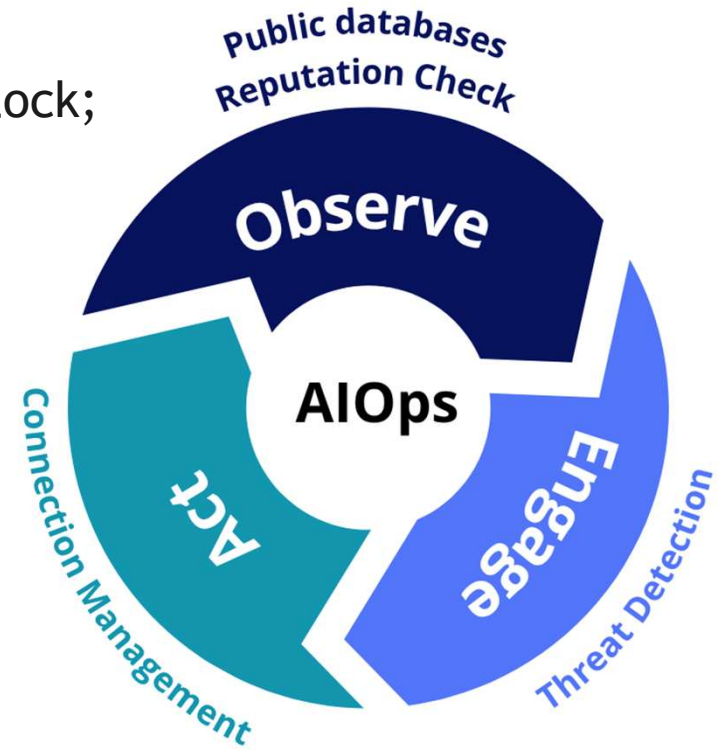
- AIOps (Artificial Intelligence for IT Operations) emerges as a promising approach to enhance security and automation.
  - AIOps is the application of AI and big data analytics, to automate, streamline, and optimize IT operations management processes and workflows.
  - Help IT teams manage the complexity and massive volume of data.
  - It lacks real-time integration with Threat Intelligence.



Objective

Propose an AIOps-driven solution for Network Connection Management:

- Integrates Machine Learning with multi-source threat intelligence databases;
- Classifies network connections as trusted, suspicious, or malicious
  - Based on IP risk (reputation);
- Automatically applies actions: allow, limit (tarpit), or block;
  - According to classification;
- Operates in real time with periodic evaluation cycles.



Related Work

Larces
Laboratório de Redes de Computadores e Segurança

Universidade Estadual do Ceará

Related Work

Author	Context	Approaches
Huang et al.	Malicious IP detection across multiple protocols.	Uses Graph Neural Networks (GNNs); notes high computational cost.
Usman et al.	IP reputation for malware analysis.	Hybrid pipeline with TI feeds and ML; constrained by sandbox evasion and high cost.
Yang & Lim / Wang et al.	Detection in encrypted traffic and domains.	Uses Deep Learning and K-means/CatBoost; limited CTI integration.
Tosun et al.	Identification of residential proxy traffic.	Host/flow-level detection with ML; distinct from CTI-integrated reputation scoring.
Our work	Connection management with multi-source TI.	AIOps solution automating actions, reaching up to 97.6% accuracy with strong real-time cost efficiency.

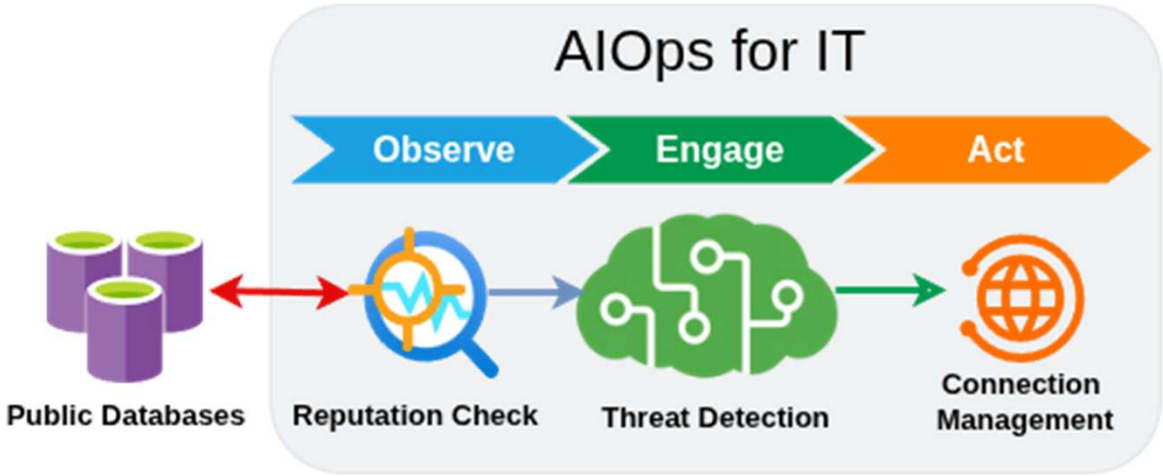
Novelty: Integrating diverse threat intelligence with efficient AI techniques enhances adaptive, real-time security detection.

Proposal

Larces
Laboratório de Redes de Computadores e Segurança

Universidade Estadual do Ceará

Proposal Overview



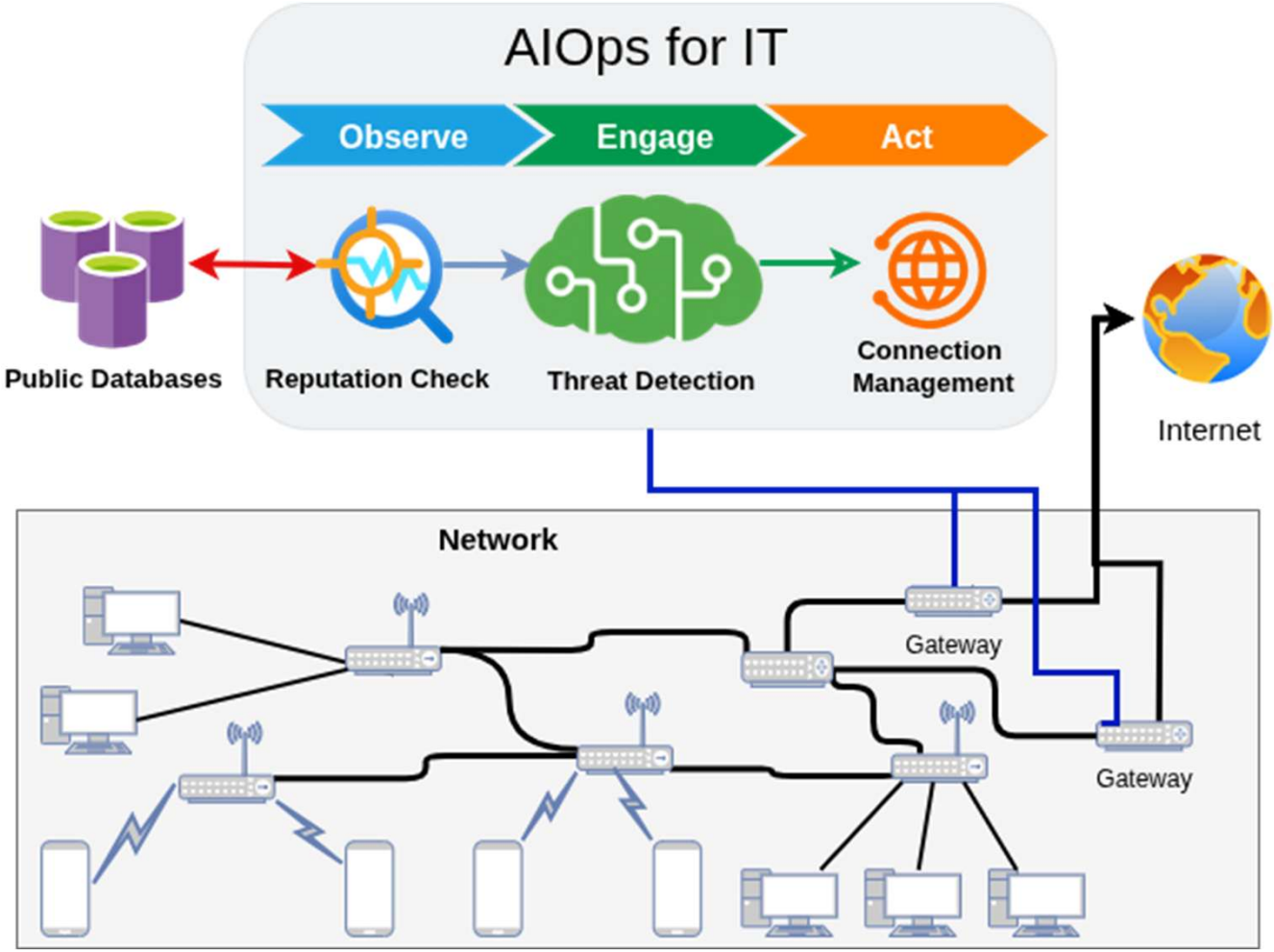
Reputation Check: Queries public databases (AbuseIPDB, VirusTotal, Pulsedive, IPVoid) to obtain information about a given IP (reputation scores, reports, etc.).

Threat Detection: An ML model classifies the IP into one of three categories: Trusted (Allowlist), Suspicious (Suspect), or Malicious (Denylist).

Connection Management: Applies rules to the firewall based on the classification. Actions include blocking, allowing, or degrading the connection (Tarpit) for suspicious IPs.

Proposal Deployment

The system automates real-time threat detection by leveraging diverse public threat intelligence and a machine learning model to classify and enforce adaptive actions against network connection attempts.



Features Collected

- AbuseIPDB:
  - Confidence score regarding the probability of maliciousness.
  - The total number of malicious reports for the IP.
  - The count of unique users who reported the IP.
- IPVoid:
  - The number of IPVoid detection services that flagged the IP as a threat.
- Pulsedive:
  - Overall risk assessment for the IP.
- VirusTotal:
  - Reputation score of the IP.
  - Count of engines classifying the IP as malicious.
  - Count of engines classifying the IP as suspicious.
  - Count of engines that found no threats.
  - Count of engines classifying the IP as harmless.

Dataset Composition

Collection: 2,499 IP addresses were collected from four public threat databases.

Composition: The dataset includes malicious IPs from AbuseIPDB and trusted IPs from sources like Google, Amazon, and Microsoft to serve as a "ground truth".

Dataset Pre-Processing

Data Cleaning: The initial step involved removing rows with missing values from any of the databases and eliminating duplicate data entries to ensure dataset quality.

Feature Transformation: Numeric features were normalized using min-max scaling. Non-numeric categorical features were also properly encoded for the models.

Class Balancing with SMOTE: To address class imbalance, the SMOTE (Synthetic Minority Oversampling Technique) was applied exclusively to the training set.

Score Calculation

The definition of the classification Score is based on the following metrics:

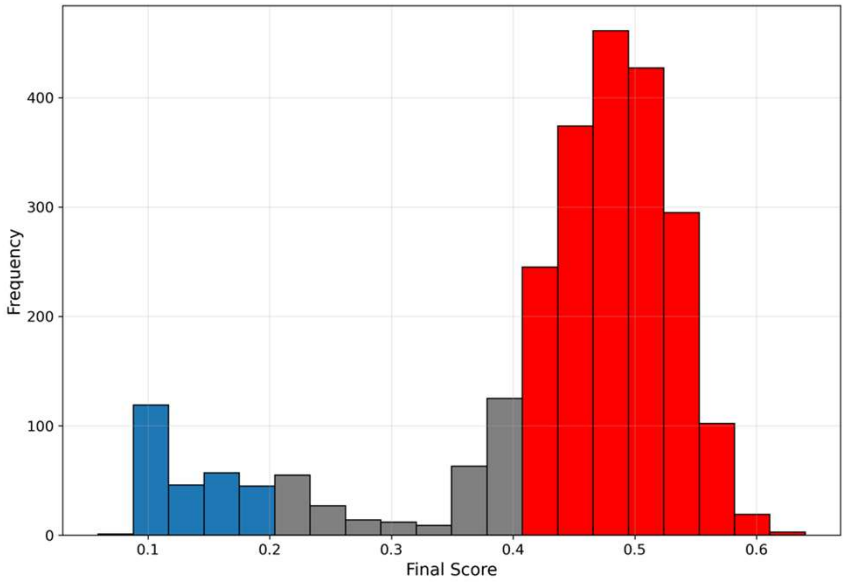
- **Variance (V):** $V = (1/n)\ \Sigma(xi - \bar{x})^2$
- **Average Correlation ($\bar{r}$):** $\vec{ri} = (1/(m-1))\ \Sigma|Ri,j|$
- **Importance (I):** $Ii = (Vi + \vec{ri})/2$
- **Importance Normalization (N):** $Ni = Ii/\Sigma Ij$

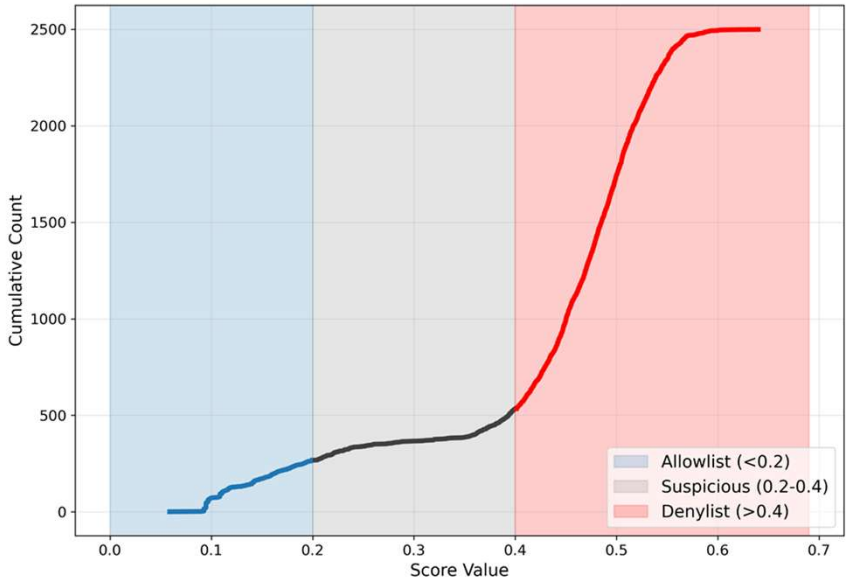
The **Score** is the sum of the weighted values of all characteristics and classifies the IPs:

$$Score = \Sigma ni.Ni$$

The Score quantifies IP risk by calculating a weighted sum of normalized threat intelligence features, using variance and correlation to determine feature importance for classification thresholds.

Score for Classification





Based on the score, the IP addresses are classified as follows:

- Allowed IPs: Score < 0.2 (Trusted IPs)
- Suspicious IPs: 0.2 ≤ Score ≤ 0.4 (IPs requiring monitoring)
- Blocked IPs: Score > 0.4 (Malicious IPs)

Experiments

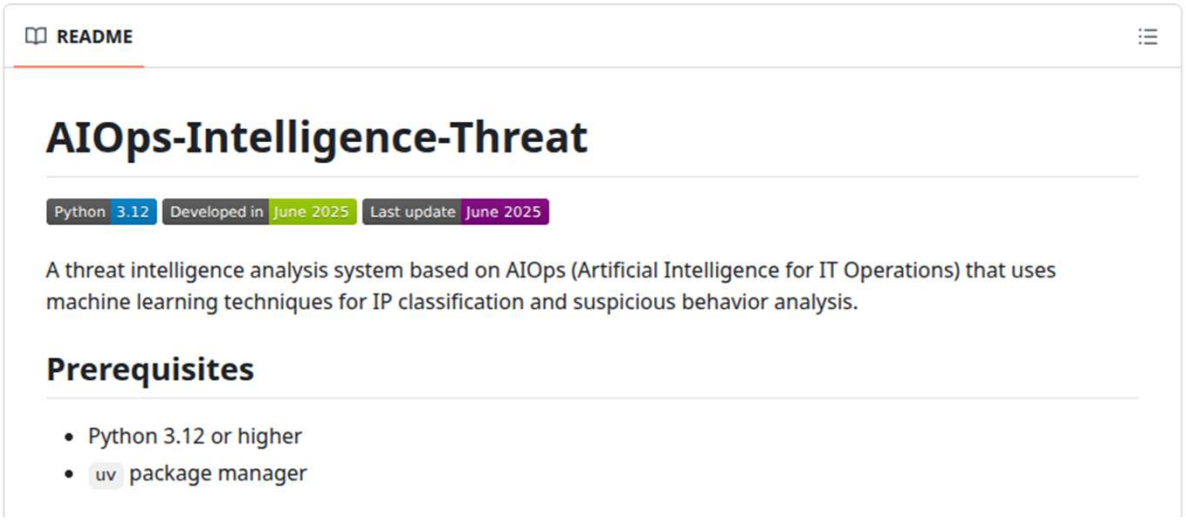
Larces
Laboratório de Redes de Computadores e Segurança

Universidade Estadual do Ceará

Setup and Models

- **Models Evaluated:** 7 Machine Learning algorithms were analyzed, including Decision Tree (DT), Random Forest (RF), CNN, SVM, and Neural Networks (NN).
  - The hyperparameters of each model were optimized using Grid Search with cross-validation to balance complexity and generalizability.
- **Metrics:** The evaluation considered Accuracy, F1-Score, Recall, and, crucially, Execution Time (training time).
- **Real-World Environment:** The solution was deployed to the network gateway of the Computer Science building (on a TP-Link TL-SG105E switch) to measure its performance and overhead in a real-world scenario. High-frequency monitoring is performed in ~7 ms, while database queries (~3 s), which are the main source of latency, occur only once per IP address.

Code and Dataset Available



README

AIOps-Intelligence-Threat

Python 3.12 | Developed in June 2025 | Last update June 2025

A threat intelligence analysis system based on AIOps (Artificial Intelligence for IT Operations) that uses machine learning techniques for IP classification and suspicious behavior analysis.

Prerequisites

- Python 3.12 or higher
- `uv` package manager

https://github.com/LarcesUece/AIOps-Intelligence-Threat

Performance of ML Models

With models like CNN achieving over 97% in both Accuracy and F1-Score when balanced, the NN and KNN models, despite a slightly lower score, were considered suitable for real-time deployment due to its balance between efficiency and speed.

PERFORMANCE OF ML MODELS WITHOUT SMOTE

Model	Accuracy	F1-Score	Recall	H. Mean	Ex. Time
KNN	0.972	0.970	0.972	0.972	0.7
ET	0.970	0.970	0.970	0.971	3.8
RF	0.960	0.961	0.960	0.961	16.6
SVM	0.960	0.962	0.960	0.964	2.8
DT	0.942	0.944	0.942	0.944	0.5
CNN	0.826	0.853	0.826	0.875	5.0
NN	0.790	0.697	0.790	0.697	0.5

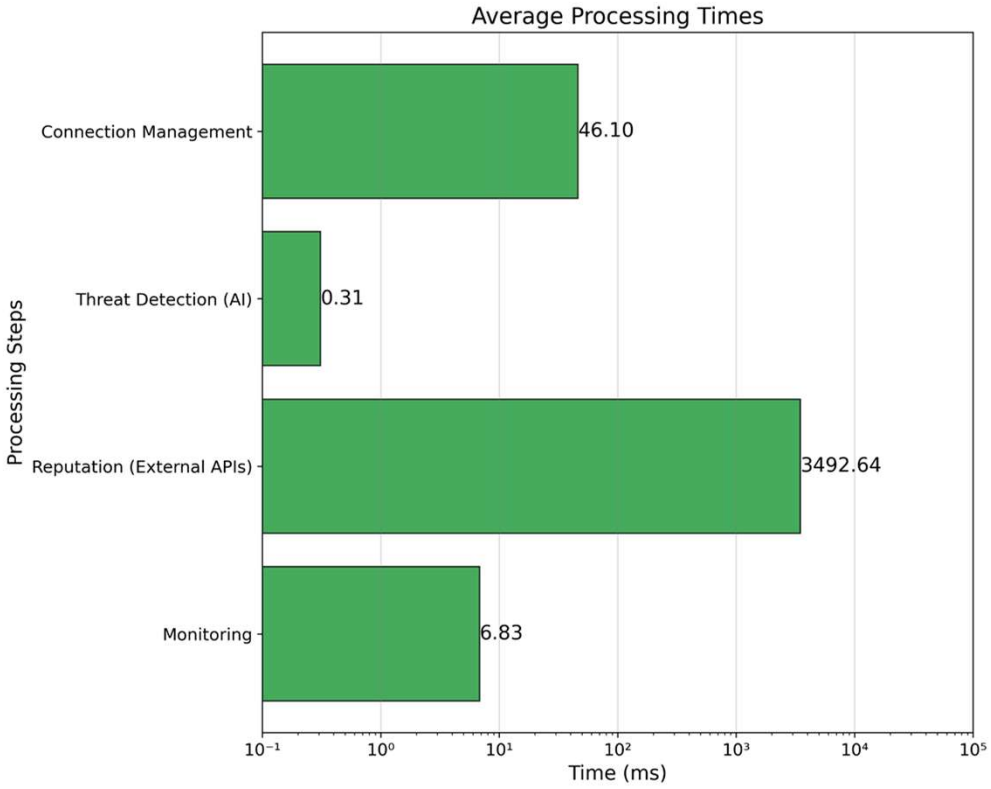
INFERENCE TIME OF MACHINE LEARNING MODELS

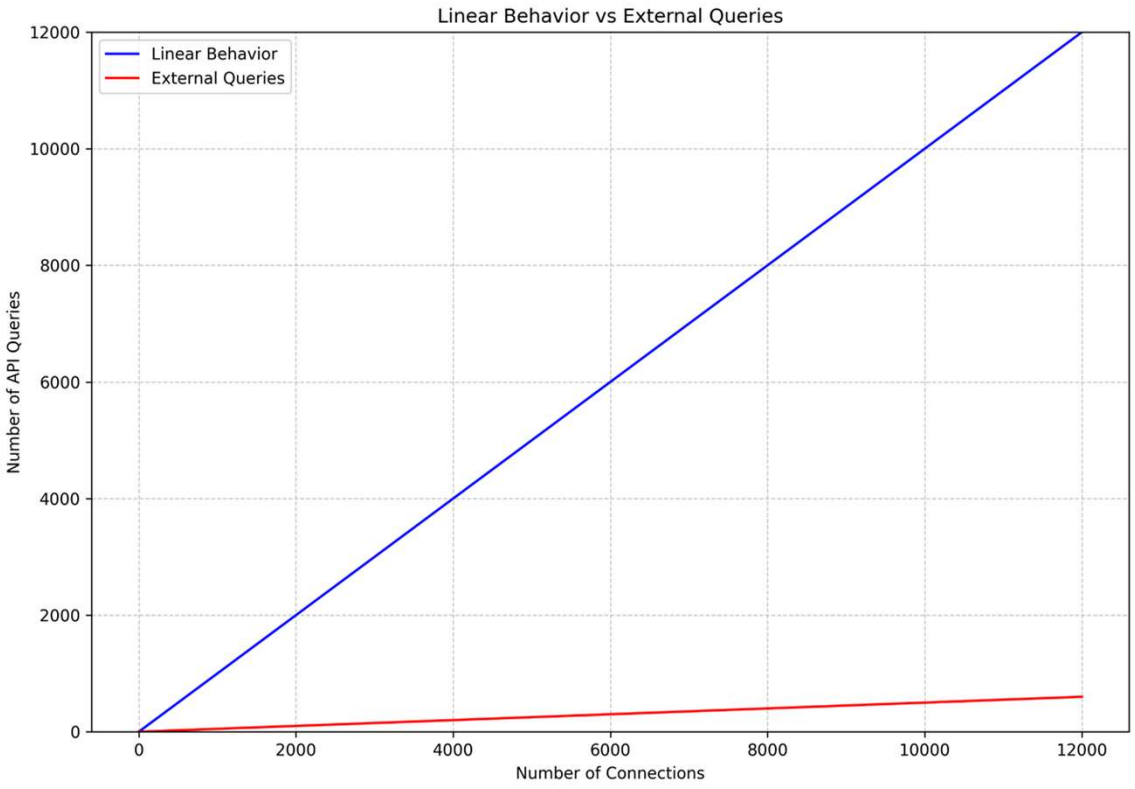
Model	Inference Time (s)
SVM	0.0028
KNN	0.0040
NN	0.0047
RF	0.0133
ET	0.0393
DT	0.1287
CNN	0.2925

PERFORMANCE OF ML MODELS WITH SMOTE

Model	Accuracy	F1-Score	Recall	H. Mean	Ex. Time
CNN	0.976	0.977	0.976	0.978	6.4
SVM	0.972	0.973	0.972	0.975	10.2
NN	0.971	0.971	0.969	0.975	1.9
RF	0.968	0.969	0.968	0.969	23.0
ET	0.968	0.969	0.968	0.969	3.3
KNN	0.958	0.960	0.958	0.961	1.2
DT	0.936	0.940	0.936	0.939	0.5

Performance of Execution Time



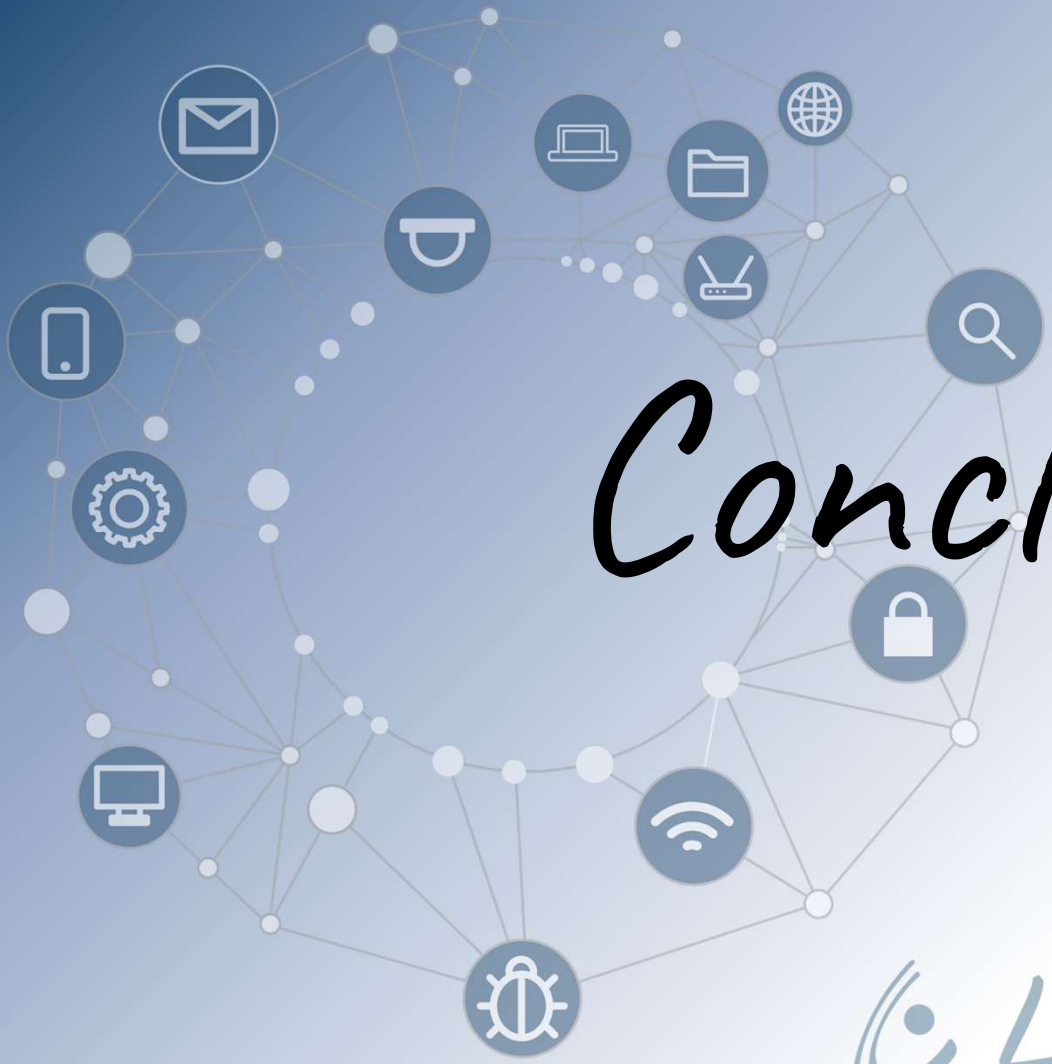


The average processing time is dominated by the multi-source threat intelligence queries (around 3.5 seconds), but the high-frequency Threat Detection (AI) step is very fast (0.31 ms), ensuring minimal impact on real-time network performance.

The Ideal Model for Real-Time Deployment

Based on the experimental results, the Neural Network (NN) model stands out as the most balanced and production-ready option.

- Accuracy is slightly lower than CNN
- Efficiency up to faster than CNN and faster than KNN.
- NN model provides the best trade-off between accuracy, latency, and computational cost, making it the most suitable choice for real-time AIOps threat response.



Conclusion

Larces
Laboratório de Redes de Computadores e Segurança

Universidade Estadual do Ceará

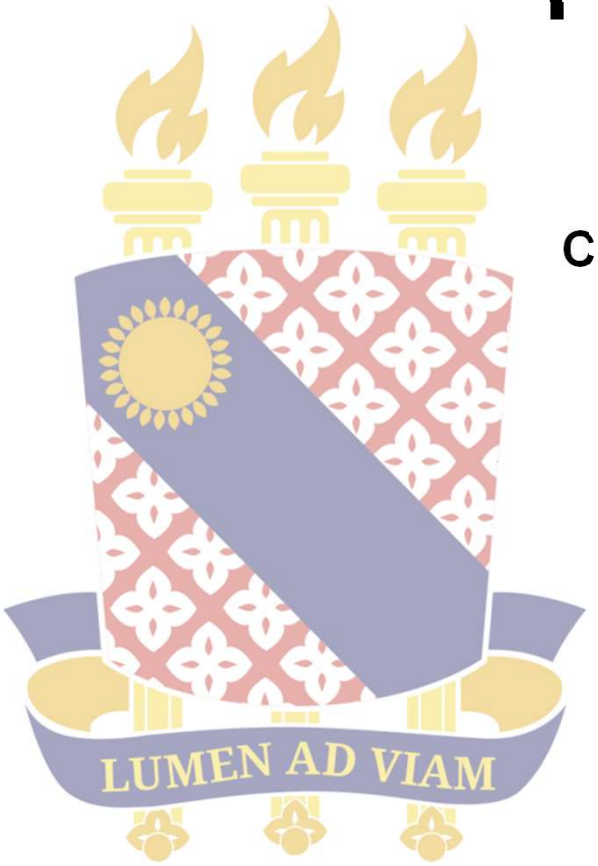
Conclusion

- The proposed architecture effectively classifies IP risks into allowlist, denylist, and suspicious categories, achieving high accuracy with minimal operational overhead in a real environment.
- The NN model was chosen for real-time deployment, offering fast execution and competitive accuracy compared to more complex models like CNN and KNN.
- Contributions:
  - Real-time actions integrated into AIOps lifecycle.
  - Public dataset and open-source code for reproducibility.
  - Validation in real-world environment.

Future Work

- Improving the fusion of heterogeneous threat data using advanced AI to enhance the accuracy and robustness of behavioral classification.
- Creation of a new, more robust dataset with a larger number of IP addresses and new databases.
- Analyze the behavior of IPs from the collected databases over a time interval using time series analysis to identify temporal patterns and predict future risks.
- Develop an ensemble-based machine learning system, combining the strengths of the different models evaluated (DT, RF, CNN, etc.) to further improve detection accuracy and robustness.

Thank you !



Contatos:

larces@uece.br
larces.uece.br