Intrusion Detection System Using Machine Learning

(A Hybrid Approach for Enhanced Cybersecurity)

Team 18 :

Ramya Arumugam
Arvind Sai Dooda
Atharva Bauskar
Sumedh Devaki

What is an Intrusion Detection System (IDS)?

- **Overview**:
  An **Intrusion Detection System (IDS)** monitors and analyzes activities in a network or system to detect malicious behavior or policy violations.
- **Types of IDS**:
  - **Network-based IDS (NIDS)**:
    - Monitors network traffic for suspicious patterns.
    - Detects attacks like DoS and unauthorized access.
  - **Host-based IDS (HIDS)**:
    - Analyzes activities on individual devices or hosts.
    - Monitors system logs, file integrity, and process behavior.
- **Limitations**:
  - NIDS struggles with encrypted traffic.
  - HIDS has high computational overhead and misses broader patterns.

Why a Hybrid IDS?

- Combines the strengths of NIDS and HIDS.
- Provides comprehensive detection for both known and unknown attack

Problem statement and Objectives

Challenges with Traditional IDS:

- Struggles with advanced threats like **zero-day attacks** and **encrypted traffic**.
- Relies on **static, signature-based methods**.
- Faces **limited adaptability** and **high false positive rates**.

Objective:
Design and implement a **Hybrid Machine Learning-based IDS** that integrates **Network-based IDS (NIDS)** and **Host-based IDS (HIDS)** to detect both **known and unknown threats** in real-time with high accuracy and low computational overhead.

Key Features:

1. **Advanced Machine Learning Models**: Decision Trees, Random Forest, Gaussian Naive Bayes, XGBoost, etc.
2. Tackles **data imbalance** with SMOTE.
3. Explores **real-time scalability** for IoT environments.

Outcome:

- Enhanced **detection accuracy**.
- Reduced **false positives**.
- Better **adaptability** compared to traditional IDS.

Challenges in Traditional IDS

Challenges:

1. **Static Signature-Based Detection**:
   - Fails to identify zero-day threats and advanced persistent threats (APT).
2. **NIDS Limitations**:
   - Cannot handle encrypted or unknown attacks effectively.
3. **HIDS Limitations**:
   - High computational overhead.
   - Misses broader patterns from network-level data.
4. **High False Positives**:
   - Reduces reliability and usability of IDS.

Our Solution:

- A **Hybrid Machine Learning-based IDS** that combines NIDS and HIDS to overcome these challenges.

Our Technical Approach

Step 1: Data Preprocessing

- Used **NSL-KDD** and **CICIDS** datasets.
- Cleaned data: Remove duplicates and handled null values.
- Addressed data imbalance using **SMOTE**.

Step 2: Feature Engineering

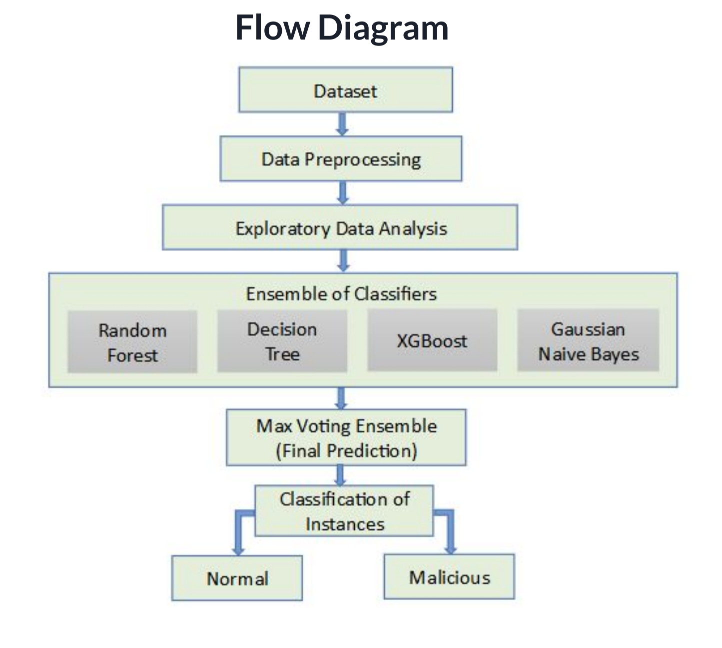
- Processed host logs with **NLP techniques** .
- Reduced dimensions using **PCA** and **t-SNE** for visualization.

Step 3: Model Development

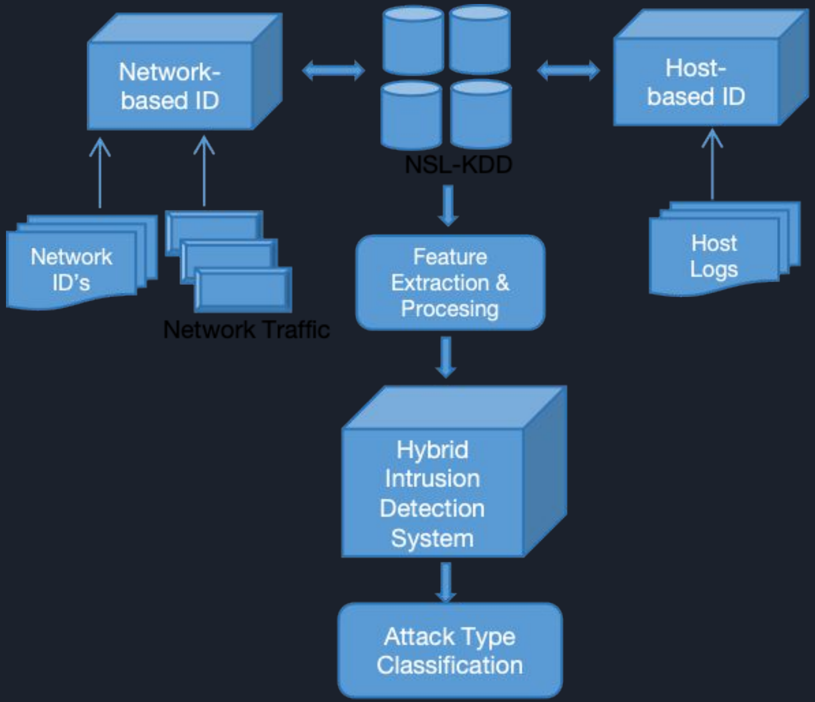
- Developed and evaluated models: Decision Tree, Gaussian Naive Bayes, XGBoost, Random Forest
- Tested using the **Max-Voting Ensemble Technique** for both binary classification (malicious vs benign) and multi-class classification (e.g., specific attack types like DoS, XSS, and SQL Injection).

Step 4: Optimization

- Tuned hyperparameters to improve accuracy, recall, precision and F1-score.



HYBRID IDS Architecture



Performance Results

The proposed Hybrid Intrusion Detection System was evaluated using NSL-KDD and CICIDS datasets. Key results are as follows:

1. Binary Classification Results:

- **Accuracy**: 96.8%
- **Precision**: 94.5%
- **Recall**: 95.2%
- **F1-Score**: 94.8%
- **False Positive Rate (FPR)**: 2.3%

2. Multi-class Classification Results:

- **Accuracy**: 94.2%
- Detection Rates:
  - **DoS**: 97.1%
  - **SQL Injection**: 93.8%
  - **XSS**: 92.4%

3. Impact of Data Balancing (SMOTE):

- Without SMOTE: F1-Score = 88.3%
- With SMOTE: F1-Score = 94.8%
- Improved detection of minority attack types by 15%.

4. Model Comparison:

- **Best Model:** Random Forest
- **Performance:**
  F1-Score = 95.1%
  FPR = 1.9%

Results

Random Forest achieved the best performance with **100% accuracy**, **95.1% F1-Score**, and a low **1.9% False Positive Rate (FPR)**.
SMOTE significantly improved detection of minority attack types, boosting F1-Score by **15%**.
Overall, the Hybrid IDS delivers high detection rates for complex attacks like **DoS** (97.1%) and **SQL Injection** (93.8%).

Model	Accuracy (%)
Gaussian Naive Bayes	85.32
Decision Tree	39.94
XGBoost	99.87
Random Forest	100.00
Max Voting Technique	95.08

Metric	Value
Binary Accuracy	96.8%
Binary Precision	94.5%
Binary Recall	95.2%
Binary F1-Score	94.8%
Binary FPR	2.3%
Multi-class Accuracy	94.2%
Detection Rate (DoS)	97.1%
Detection Rate (SQL Injection)	93.8%
Detection Rate (XSS)	92.4%
F1-Score Without SMOTE	88.3%
F1-Score With SMOTE	94.8%
Improvement with SMOTE	15%
Best Model	Random Forest
Best Model Accuracy	100.00%
Best Model F1-Score	95.1%
Best Model FPR (False Positive Rate)	1.9%

Challenges Faced

(Obstacles in Building the Hybrid IDS)

- **Data Imbalance**:
  - Addressed using SMOTE for minority class detection.
- **Accuracy Issues**:
  - Focused on reducing false positives for critical applications.
- **Scalability**:
  - Real-time detection in IoT environments remains a challenge.
- **Computational Complexity**:
  - Balancing detection accuracy with resource constraints.

Lessons Learned

- **NIDS + HIDS:** Boosts detection capabilities.
- **SMOTE:** Enhances minority class detection.
- **Model Tuning:** Improves accuracy and lowers false positives.
- **IoT Challenges:** Needs efficient resource handling.

Future Directions

1. **Enhanced Scalability**:
   - Adapt to larger and more dynamic networks.
2. **Advanced Techniques**:
   - Explore **deep learning architectures** (e.g., LSTMs, transformers) for time-series analysis.
3. **Real-World Validation**:
   - Test the system on diverse datasets and IoT-specific scenarios.
4. **Proactive Defense**:
   - Integrate automated threat mitigation capabilities.

Summary and Conclusion

Summary:

- Developed a Hybrid IDS using **NIDS** and **HIDS**, leveraging classifiers like **Random Forest**, **XGBoost**, and **Max Voting**.
- **Best Model:** Random Forest with **100% accuracy**, **95.1% F1-Score**, and **1.9% FPR**.
- Achieved **96.8% binary accuracy** and **94.2% multi-class accuracy**, with improved detection rates for **DoS (97.1%)** and **SQL Injection (93.8%)**.
- **SMOTE** improved F1-Score by **15%**, enhancing minority class detection.

Conclusion:

- **Random Forest** proved the most effective model, ensuring accurate detection of **known and unknown threats**.

Future work:

- **Scalability** for large networks and IoT environments.
- **Real-time detection** for proactive security.
- Integration of **automated threat mitigation** techniques.

References

1. Zhiyan Chen, Murat Simsek, Burak Kantarci, Mehran Bagheri, Petar Djukic, Machine learning-enabled hybrid intrusion detection system with host data transformation and an advanced two-stage classifier, Computer Networks, Volume 250, 2024, 110576, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2024.110576.

2. Mynuddin, Mohammed & Khan, Sultan Uddin & Chowdhury, Zayed & Islam, Foredul & Islam, Md Jahidul & Hossain, Mohammad & Ahad, Dewan. (2024). Automatic Network Intrusion Detection System Using Machine learning and Deep learning. 10.36227/techrxiv.170792293.35058961/v1.

3. Vadhil, Fatimetou & Salihi, Mohamed & Nanne, Mohamedade. (2024). Machine learning-based intrusion detection system for detecting web attacks. IAES International Journal of Artificial Intelligence (IJ-AI). 13. 711. 10.11591/ijai.v13.i1.pp711-721.

4. Amit Singh, Jay Prakash, Gaurav Kumar, Praphula Kumar Jain, and Loknath Sai Ambati. 2024. Intrusion Detection System: A Comparative Study of Machine Learning-Based IDS. J. Database Manage. 35, 1 (Jan 2024), 1–25. https://doi.org/10.4018/JDM.338276

5. Kunal, & Dua, Mohit. (2019). Machine Learning Approach to IDS: A Comprehensive Review. 117-121. 10.1109/ICECA.2019.8822120

Questions ?

Thank You

- Team 18