NETWORK INTRUSION DETECTION USING MACHINE LEARNING

A COMPREHENSIVE ANALYSIS OF ML AND DL MODELS ON THE NSL-KDD DATASET

TEAM MEMBERS:

GOTAM SAI VARSHITH – 22BCE1605

PAVAN KRISHNA R -- 24BCE5294

MRINAL SWAIN -- 24BCE5357

WHAT IS NETWORK INTRUSION DETECTION?

- **Main Point:** It's a security guard for a computer network.
- **Explanation:** An Intrusion Detection System (IDS) is a tool that monitors network traffic to find suspicious activity or threats.
- **Analogy:** Think of an IDS as a security system that alerts you when someone tries to break into your house. A firewall is like a locked door, but an IDS watches for someone trying to pick the lock or sneak in.

TWO TYPES OF IDS(INTRUSION DETECTION SYSTEM)

- **Signature-Based:** Detects threats by looking for known patterns, like a virus signature. It's fast but can't find new, unknown threats.
- **Anomaly-Based:** Learns what "normal" network behavior looks like. Anything that deviates from this normal baseline is flagged as an anomaly or a potential attack. This is where machine learning and deep learning come in.

THE CHALLENGE: WHY USE MACHINE LEARNING?

- **The Problem:** Modern networks are huge and dynamic. New threats, called "zero-day attacks," emerge every day. Traditional, rule-based systems can't keep up.
- **The Solution:** We use Machine Learning (ML) to build an anomaly-based IDS.
- **How ML Helps:**
  - It can analyze massive amounts of data efficiently.
  - It can learn from past data to identify new and evolving threats.
  - It reduces the need for constant manual updates of security rules.

THE DATASET: NSL-KDD

- **What it is:** The NSL-KDD is a standard dataset used to test intrusion detection systems. It's a clean version of an older dataset called KDD Cup 1999.
- **What's inside:** It contains records of both normal network connections and various types of attacks.

KEY ATTACK CATEGORIES:

- **DoS (Denial of Service):** Flooding a server with traffic to make it unavailable.
- **Probe:** Scanning a network to find vulnerabilities.
- **R2L (Remote to Local):** An attacker gains local access to a machine from a remote location.
- **U2R (User to Root):** An attacker with user-level access tries to gain root (administrator) privileges.

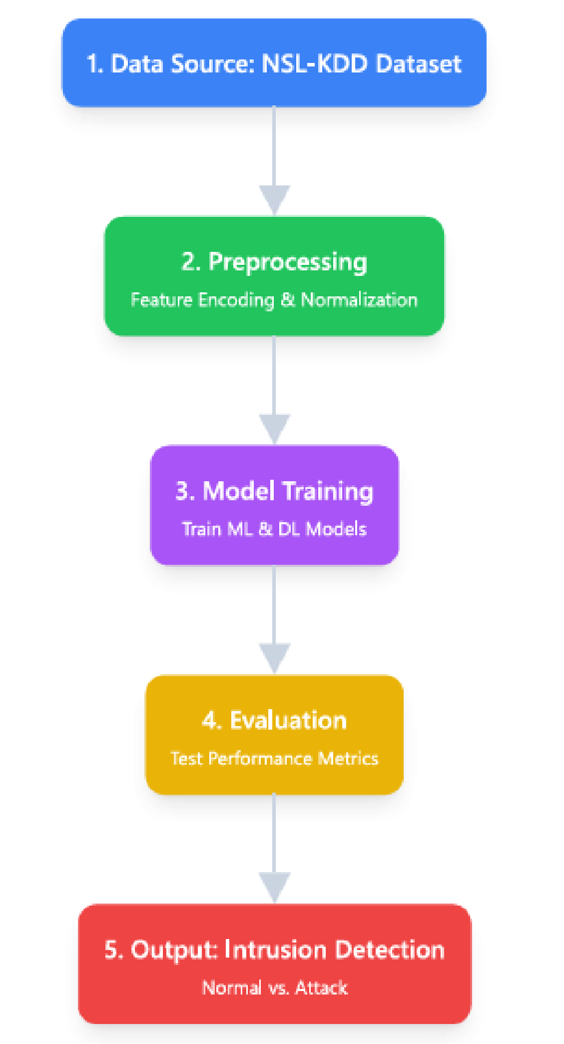
THE PROJECT'S APPROACH: ML VS. DL

- **Main Goal:** To compare how well different ML and DL algorithms can detect intrusions.
- **Methodology:**
  1. Data Preprocessing: We take the raw NSL-KDD data and prepare it for the models by cleaning, encoding, and normalizing the features.
  2. Model Training: We train a suite of different models on the prepared data.
  3. Evaluation: We test the trained models on new, unseen data to see how accurately they can classify connections as normal or as a specific attack type.

ALGORITHMS USED FOR NETWORK INTRUSION DETECTION

Type	Algorithms Used in Project
Traditional Machine Learning (ML)	• K-Nearest Neighbours (KNN) • Linear/Quadratic Discriminant Analysis (LDA/QDA) • Linear/Quadratic Support Vector Machine (LSVM/QSVM)
Deep Learning (DL)	• Multi-Layer Perceptron (MLP) • Autoencoder • Long Short-Term Memory (LSTM)

ARCHITECTURE DIAGRAM



1. **Data Source:** The project starts with the NSL-KDD dataset, a benchmark for network intrusion detection.
2. **Preprocessing:** The raw data is cleaned and prepared. This involves encoding text-based features into numbers and normalizing the data's scale.
3. **Model Training:** The prepared data is used to train different models, including both traditional Machine Learning algorithms and advanced Deep Learning models.
4. **Evaluation:** The trained models are tested on new, unseen data to measure their performance using metrics like accuracy and precision.
5. **Output:** The final result is a system that can reliably classify new network traffic as either Normal or an Attack.

DEEP DIVE: THE ALGORITHMS

- **Multi-Layer Perceptron (MLP):**
  - **Concept:** A basic neural network with multiple layers. It learns to find complex, non-linear patterns in the data to make classifications.
  - **Why it works:** It's a powerful general-purpose classifier that can learn to distinguish between different types of network traffic.

DEEP DIVE: THE ALGORITHMS

- **Long Short-Term Memory (LSTM):**
  - **Concept:** A special type of neural network that can remember past information.
  - **Why it works:** Network traffic is a sequence of events. LSTMs are perfect for this because they can remember what happened 10 or 100 packets ago, which is crucial for detecting complex attacks that unfold over time.

DEEP DIVE: THE ALGORITHMS

- **Autoencoder:**
  - **Concept:** An unsupervised deep learning model that learns to compress data and then reconstruct it.
  - **How it works for IDS:** You train it only on normal network traffic. When a new, normal connection comes in, the autoencoder can reconstruct it perfectly. But when an attack (an anomaly) comes in, the autoencoder struggles to reconstruct it, resulting in a high reconstruction error. This error is the signal that an intrusion has been detected.

THE NOVELTY OF THIS PROJECT

- **What makes it unique?** This project isn't just a simple application of ML models. It's loosely based on a research paper that combines two unique ideas:
  - **Statistical Analysis:** It uses statistical techniques to extract the most important and relevant features from the raw data. This is a crucial step that improves model performance and efficiency.
  - **Autoencoder-Driven Detection:** It uses the autoencoder not just for anomaly detection, but as a core component of the system to identify optimized features. The reconstruction error from the autoencoder becomes a powerful feature for the final classification step.
- **In simple terms:** We are not just throwing data at a model. We are intelligently preparing the data and using a special deep learning model (**Autoencoder**) to find the best possible features, which makes the final classification more accurate.

RESULTS & CONCLUSION

- **The Findings:** This project shows that deep learning models like **Autoencoders** and **LSTMs** can achieve very high accuracy in detecting both known and unknown network intrusions on the NSL-KDD dataset.
- **Key Takeaway:** While traditional ML models like KNN and SVM perform well, deep learning models often have an edge, especially when dealing with complex, time-series data and the need to detect novel attacks without explicit rules.
- **Future Improvements:**
  - Test on a newer dataset to handle modern traffic patterns.
  - Integrate a real-time detection pipeline to make the system more practical.
  - Further optimize the deep learning models for even higher accuracy.
- This project is a powerful demonstration of how the latest advances in deep learning can be applied to solve critical security challenges in the real world.

REFERENCES

- **The NSL-KDD Dataset:** Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 dataset. In Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications.
- **Autoencoders for NIDS:** Ieracitano, C., Adeel, A., Morabito, F. C., & Hussain, A. (2020). A novel statistical analysis and autoencoder driven intelligent intrusion detection approach. Neurocomputing, 387, 51-62.
- **LSTMs for Intrusion Detection:** Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2017). A survey on intrusion detection systems and the role of deep learning. Journal of Cyber Security, 6(1), 1-15.
- **MLP in IDS:** Al-Jarrah, O., Al-Duyyami, A., Al-Duweish, K., Al-Mutairi, A., & Al-Zahrani, A. (2019). An analysis of machine learning algorithms for network intrusion detection system using NSL-KDD dataset. International Journal of Computer Science and Network Security, 19(5), 143-150.