Project Report

Title: AI-Based Intrusion Detection and Prevention System (IDPS)

INTRODUCTION

With the rapid growth of digital communication, cyberattacks have become a major threat to organizations and individuals. Traditional Intrusion Detection and Prevention Systems (IDPS) rely heavily on signature-based methods, which can only detect known attack patterns. However, modern attackers use advanced techniques, including zero-day attacks, that bypass such systems.

This project proposes the design and development of an **AI-powered IDPS** that uses **machine learning (ML)** for anomaly detection. The system will learn normal network behavior and detect deviations in real-time, enabling it to not only identify but also prevent malicious activities proactively.

OBJECTIVES

- To design an intelligent IDPS using AI and ML.
- To detect both known and unknown (zero-day) attacks.
- To provide real-time alerts and automated prevention.
- To improve overall network resilience and security.

PROCEDURE

Step 1: Dataset Collection & Preprocessing

- Use datasets like **NSL-KDD** or **CICIDS2017**.
- Clean and preprocess data (remove duplicates, normalize values).

Step 2: Model Training

- Train machine learning models (Random Forest, SVM, or Neural Networks).
- Establish a baseline of normal vs. abnormal traffic.

Step 3: System Deployment

- Integrate the trained model with a real-time network monitoring environment.
- Collect live traffic for classification.

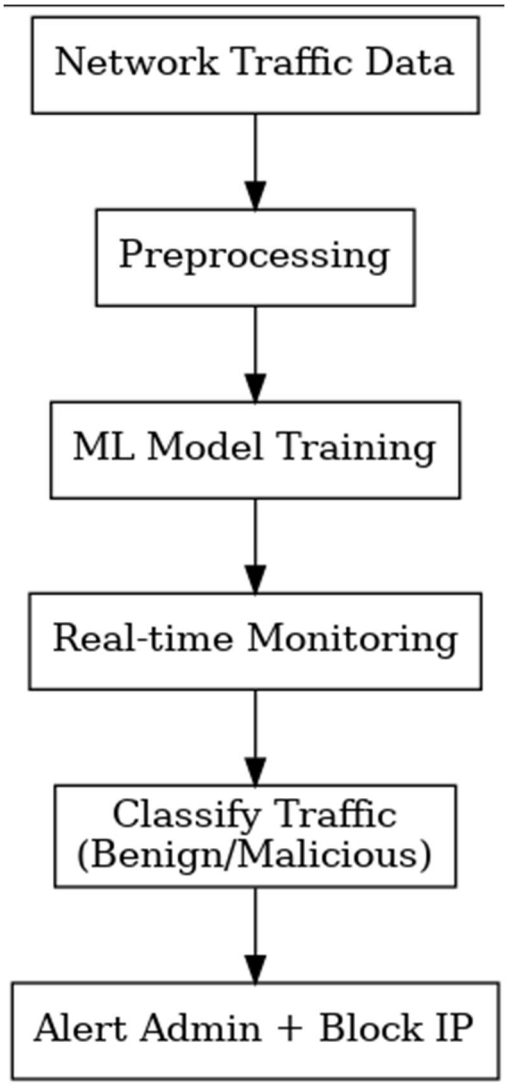
Step 4: Detection & Prevention

- Detect anomalies and generate alerts.
- Take preventive actions such as blocking suspicious IPs.

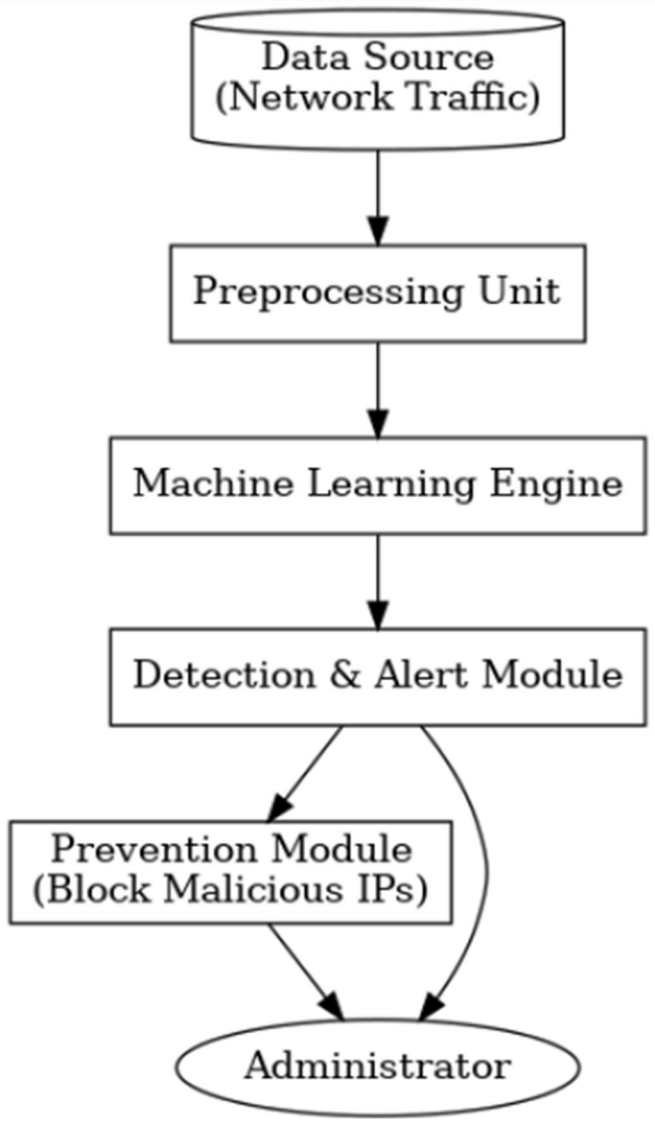
Step 5: Evaluation

- Measure accuracy, precision, recall, and false-positive rate.
- Fine-tune model for better performance.

FLOWCHART OF THE PROPOSED SYSTEM



SYSTEM ARCHITECTURE DIAGRAM



USES

- Detects both known and unknown attacks.
- Reduces manual monitoring with automated actions.
- Improves speed and accuracy of threat detection.
- Enhances organizational cybersecurity posture.

ADVANTAGES

- **Real-Time Detection:** Immediate response to threats.
- **Adaptive:** Learns new attack patterns.
- **Scalable:** Can handle large network traffic.
- **Proactive Prevention:** Stops attacks before damage occurs.

Approach to Implementation

- Select dataset → preprocess data → train ML model.
- Use Python libraries (**Scikit-learn, TensorFlow, PyTorch**).
- Deploy in real-time using packet sniffing tools (**Wireshark, Scapy**).
- Integrate with firewall for automatic blocking.
- Test with simulated attack scenarios.

Conclusion

The proposed AI-based IDPS will provide an **intelligent, adaptive, and proactive security solution**. By combining anomaly detection with automated prevention, the system can protect against sophisticated and zero-day attacks, significantly enhancing network security and resilience.