# AI-Powered Insider Threat Detection: A Machine Learning Approach

The project uses the CICIDS 2018 dataset to detect insider threats with AI.

**by M. Haris Jamal**

# Understanding Insider Threats & Project Goals

### Insider Threats

Malicious or accidental threats originating within an organization.

### Cybersecurity Concern

Hard to detect and often cause significant damage and data leaks.

### Project Aim

Develop AI system to detect threats using machine learning models.

### CICIDS 2018 Dataset

A benchmark dataset for realistic network traffic and attack scenarios.

# Literature Review: ML for Intrusion Detection

### Common Algorithms

- Random Forest
- Support Vector Machines (SVM)
- Convolutional Neural Networks (CNN)

### Preprocessing Importance

Data cleaning, encoding, and feature engineering are crucial for accuracy.

### Research Insights

Most detection methods balance accuracy and computation efficiency.

# Dataset & Exploratory Data Analysis

## CICIDS 2018 Dataset

Includes benign and multiple attack types with network flow features.

Used Pandas, Seaborn, Matplotlib, and Plotly for data analysis.

## Attack Distribution

Visualized attack type frequencies to understand dataset balance.

# Data Preprocessing Steps

## Handle Missing Values

Ensured data completeness by filling or removing gaps.

## Encode Labels

Converted categorical data into numerical for model input.

## Balance Dataset

Addressed class imbalance to improve detection accuracy.

## Normalize & Split

Normalized features and divided data into training/testing sets.

# Model Development: Random Forest & CNN

## Random Forest

- Used ensemble decision trees with tuned hyperparameters.
- Evaluated by accuracy, confusion matrix, classification report.
- Feature importance identified key predictors.

## Convolutional Neural Network

- Conv1D layers, pooling, dense layers, ReLU activation.
- Trained over epochs with batch size and Adam optimizer.
- Monitored training/validation accuracy and loss.

# Results: Model Performance Comparison

## Random Forest

- High precision and recall on most classes.
- Strong interpretability through feature importance.

## CNN Model

- Better at complex pattern recognition in traffic.
- Training requires more computation time and data.

# Conclusions & Future Directions

### Key Findings

AI models detect insider threats effectively with balanced data.

### Impact

Machine learning offers scalable, automated threat detection tools.

### Future Work

Explore real-time deployment and integration with security platforms.

# References & Resources

- CICIDS 2018 Dataset – University of New Brunswick
- Research on ML models for intrusion detection
- Python libraries: Pandas, Seaborn, Matplotlib, Plotly
- Scikit-learn Random Forest and TensorFlow CNN implementations

CYFERSEUDNCE
CYTERSUPRESSTUILECT
CYYEERSTFY RONLESS-TAKETORS
CYBERSECURINT POFACE
CYBERSTICI RESAEARCH PAPES
Appezn Attesecigns
Tory he dunicke loying!
Pore resyit to Cypereapiher Ixjniel
Mcliletsioy and Frojians Fsiity...