INTRODUCTION

As modern networks grow in size and complexity, so do cyberattacks. Traditional signature-based Intrusion Detection Systems (IDS) such as Snort and Suricata rely on predefined rules to detect known threats. While effective against known attacks, they fail to detect:

- *Zero-day attacks*
- *Previously unseen behaviors*
- *Polymorphic and evolving malware*
- *High-volume modern DoS/DDoS attacks*

To overcome these limitations, **Machine Learning–based IDS (ML-IDS)** systems have emerged. Instead of using predefined signatures, ML-IDS learns patterns from real network traffic and automatically identifies malicious behaviour. It demonstrates how ML can classify traffic into:

1. **Benign vs Attack (Binary IDS)**
2. **Type of attack (Multiclass IDS)**

WHY MACHINE LEARNING IDS?

Machine Learning IDS is chosen because:

1. Detects Unknown Attacks

ML models analyse statistical properties of traffic (packet sizes, durations, flags, IATs, etc.).Thus they detect **new, previously unseen attacks**.

2. Learns Behavior, Not Signatures

Instead of matching signatures, ML IDS learns patterns of:

- *DoS traffic*
- *Port scanning*
- *Brute force login attempts*
- *Botnet activity*
- *Web-based attacks*

3. High Accuracy and Automation

Algorithms like Random Forest, SVM, and Neural Networks perform complex pattern analysis, giving:

- *High precision*
- *Low false negatives*
- *Consistent automated detection*

4. Scalable to Large Networks

They can analyse millions of flows using statistical summaries without needing deep packet inspection.

5. Real-Time Detection

Once trained, ML-based IDS offers **fast inference** — ideal for real-time monitoring.

DATASET USED AND WHY THIS DATASET:

We used **balanceddata.csv**, prepared from the **CIC-IDS** family of datasets — popular benchmark datasets for ML IDS research.

This dataset is chosen because:

1. Contains Modern Attack Types

Includes:

- *DoS Hulk, DoS GoldenEye, Slowloris*
- *FTP-Patator & SSH-Patator (brute force)*
- *PortScan*
- *Botnet*
- *Web Attack variants*
- *Infiltration*

These are **realistic**, modern and varied attacks.

2. Balanced for ML Training

The dataset supplied already has controlled class distribution. This avoids ML bias and improves evaluation stability.

3. Rich Features (79 features initially)

Includes:

- *Flow duration*
- *Total packets (Fwd/Bwd)*
- *Packet length stats*
- *Inter-arrival times*
- *Content/flag features*
- *Window sizes*
- *Bulk operation data*

These features are known to be effective for distinguishing attack traffic.

MODELS USED & WHY:

1. Random Forest Classifier (RF)

- *Handles high-dimensional tabular data well*
- *Robust to noise and missing values*
- *Provides feature importance*
- *Excellent baseline for network traffic classification*
- *Achieved best performance in this project (≈98.6% binary accuracy)*

2. Logistic Regression (LR)

- *Simple, interpretable linear model*
- *Good for explaining feature weights*
- *Fast & efficient*
- *Serves as benchmark against more complex models*

3. Support Vector Machine (SVM – RBF Kernel)

- *Captures non-linear patterns*
- *Effective in high-dimensional spaces*
- *Works well on smaller datasets*
- *Produces strong decision boundaries for binary IDS*

4. Artificial Neural Network (ANN)

- *Learns complex patterns*
- *Multi-layer structure captures high-level representations*
- *Suitable for multiclass attack classification*
- *Produces probability outputs for ensemble fusion*

5. Ensemble Decision System

Combines **RF + LR + SVM + ANN** results using majority vote.

Benefits:

- *Reduces individual model weaknesses*
- *Improves robustness*
- *Enhances consistency for real-time IDS*

This forms a “mini SIEM-style” decision engine.

ALGORITHM STEPS / PSEUDOCODE:

DATA PREPROCESSING PHASE:

```
START
Load balanceddata.csv → df

Extract:
    - AttackType (string)
    - BinaryLabel (0/1)
    - AttackTypeEncoded (integer class)

Drop all label columns from feature matrix

For each feature column:
    If non-numeric → convert to float (coerce NaN)
    Replace +inf or -inf with NaN

Impute all NaN values using median of that column

Clip outliers:
    lower = 0.5 percentile
    upper = 99.5 percentile
    Clip values to [lower, upper]

Drop constant (zero-variance) features

Scale dataset using StandardScaler
END
```

MODEL TRAINING PHASE:

```
Split X and labels into train/test (80/20)

Train Random Forest (rf_binary, rf_multi)
Train Logistic Regression (lr_binary, lr_multi)
Train SVM (svm_binary, svm_multi)

Build ANN (binary):
    64 → 32 → 1 layers (sigmoid output)

Build ANN (multiclass):
    64 → 32 → num_classes layers (softmax)

Compile & train both networks for 10 epochs
```

EVALUATION PHASE:

```
For each model:
    Make predictions on X_test
    Compute:
        - Accuracy
        - Confusion Matrix
        - Classification Report
        - ROC (binary)
        - Feature Importance (model-specific)
    Plot heatmaps and curves
```

LIVE IDS DEMO PHASE:

```
FUNCTION run_live_demo(user_input):
    Prepare JSON/list input
    Fill missing fields with dataset mean
    Scale with StandardScaler

    For each classifier:
        Compute probability P(Attack)
        Convert to prediction (0/1)

    Multiclass prediction:
        Use ANN (softmax)
        Determine attack subtype
        Map subtype → attack family (DoS, Web Attack, Botnet)

    Ensemble decision:
        If sum(predictions) >= 2:
            Final Result = ATTACK
        Else:
            Final Result = BENIGN

    Print:
        - Per-model predictions
        - Attack family probabilities
        - Final ensemble label
END
```

PROGRAM:

INPUT / OUTPUT:

The dataset contains two broad categories: **Benign** traffic and various **Attack** types such as DoS, DDoS, Brute Force, Web Attacks, PortScan, Infiltration, and Botnet. For demonstration purposes, only three representative classes—**Benign**, **DoS**, and **PortScan**—are used to illustrate the functioning of the ML-based IDS.

1. BENIGN SAMPLE (Correctly Detected):

A **benign sample** is a network record that represents **normal, safe user activity**. It shows **legitimate traffic patterns** without any malicious behaviour or attacks.In ML-IDS, benign samples help the model learn what *normal* looks like, so it can detect deviations as attacks.

Input JSON:

```
#1 in dataset
sample_output = run_live_demo_json({
  "Destination Port": 53," Flow Duration": 204," Total Fwd Packets": 2,
  " Total Backward Packets": 2,"Total Length of Fwd Packets": 60,
  " Total Length of Bwd Packets": 316," Fwd Packet Length Max": 30,
  " Fwd Packet Length Min": 30," Fwd Packet Length Mean": 30,
  " Fwd Packet Length Std": 0,"Bwd Packet Length Max": 158,
  " Bwd Packet Length Min": 158," Bwd Packet Length Mean": 158,
  " Bwd Packet Length Std": 0,"Flow Bytes/s": 1843137.255,
  " Flow Packets/s": 19607.84314," Flow IAT Mean": 68,
  " Flow IAT Std": 112.5833025, " Flow IAT Max": 198," Flow IAT Min": 3,
  "Fwd IAT Total": 3," Fwd IAT Mean": 3," Fwd IAT Std": 0," Fwd IAT Max": 3,
  " Fwd IAT Min": 3,"Bwd IAT Total": 3, " Bwd IAT Mean": 3," Bwd IAT Std": 0,
  " Bwd IAT Max": 3," Bwd IAT Min": 3,"Fwd PSH Flags": 0," Bwd PSH Flags": 0,
  " Fwd URG Flags": 0," Bwd URG Flags": 0," Fwd Header Length": 64,
  " Bwd Header Length": 64,"Fwd Packets/s": 9803.921569,
  " Bwd Packets/s": 9803.921569," Min Packet Length": 30,
  " Max Packet Length": 158," Packet Length Mean": 81.2,
  " Packet Length Std": 70.10848736," Packet Length Variance": 4915.2,
  "FIN Flag Count": 0," SYN Flag Count": 0," RST Flag Count": 0,
  " PSH Flag Count": 0," ACK Flag Count": 0," URG Flag Count": 0,
  " CWE Flag Count": 0," ECE Flag Count": 0," Down/Up Ratio": 1,
  " Average Packet Size": 101.5," Avg Fwd Segment Size": 30,
  " Avg Bwd Segment Size": 158," Fwd Header Length.1": 64,
  "Fwd Avg Bytes/Bulk": 0," Fwd Avg Packets/Bulk": 0," Fwd Avg Bulk Rate": 0,
  " Bwd Avg Bytes/Bulk": 0," Bwd Avg Packets/Bulk": 0,"Bwd Avg Bulk Rate": 0,
  "Subflow Fwd Packets": 2," Subflow Fwd Bytes": 60," Subflow Bwd Packets": 2,
  " Subflow Bwd Bytes": 316,"Init_Win_bytes_forward": -1,
  " Init_Win_bytes_backward": -1," act_data_pkt_fwd": 1,
  " min_seg_size_forward": 32,"Active Mean": 0," Active Std": 0,
  " Active Max": 0," Active Min": 0,"Idle Mean": 0," Idle Std": 0,
  " Idle Max": 0," Idle Min": 0})
```

Output:

```
1/1 ━━━━━━━━━━━━━━━━━━━━ 0s 36ms/step
1/1 ━━━━━━━━━━━━━━━━━━━━ 0s 37ms/step
------------------------------------------------------------
Per-model binary predictions (pred, p(class=1)):
  RandomForest        : 0   (p1=0.0150)
  LogisticRegression  : 0   (p1=0.0000)
  SVM                 : 0   (p1=0.0000)
  ANN                 : 0   (p1=0.0303)
------------------------------------------------------------
Attack CATEGORY (family-level):
  Predicted: BENIGN   (prob=0.9882)
------------------------------------------------------------
ENSEMBLE FINAL: 0 -> BENIGN
Votes: [0, 0, 0, 0] Consensus: majority
------------------------------------------------------------
```

2. DoS ATTACK DETECTION:

A **Denial of Service (DoS) attack** is when an attacker floods a system or network with excessive requests.

This overloads the server's resources, making it **slow, unstable, or completely unavailable** to real users.

In ML-IDS, DoS attacks appear as **abnormally high traffic patterns** that help the model learn to detect disruptions.

Input JSON:

```
#250 in dataset
sample_output = run_live_demo_json(
{
  "Destination Port": 80," Flow Duration": 20998592," Total Fwd Packets": 2,
  " Total Backward Packets": 1,"Total Length of Fwd Packets": 13,
  " Total Length of Bwd Packets": 0," Fwd Packet Length Max": 13,
  " Fwd Packet Length Min": 0," Fwd Packet Length Mean": 6.5,
  " Fwd Packet Length Std": 9.192388155,"Bwd Packet Length Max": 0,
  " Bwd Packet Length Min": 0," Bwd Packet Length Mean": 0,
  " Bwd Packet Length Std": 0,"Flow Bytes/s": 0.619089127,
  " Flow Packets/s": 0.142866722," Flow IAT Mean": 10500000,
  " Flow IAT Std": 14800000," Flow IAT Max": 21000000," Flow IAT Min": 65,
  "Fwd IAT Total": 21000000," Fwd IAT Mean": 21000000," Fwd IAT Std": 0,
  " Fwd IAT Max": 21000000," Fwd IAT Min": 21000000,"Bwd IAT Total": 0,
  " Bwd IAT Mean": 0," Bwd IAT Std": 0," Bwd IAT Max": 0," Bwd IAT Min": 0,
  "Fwd PSH Flags": 1," Bwd PSH Flags": 0," Fwd URG Flags": 0,
  " Bwd URG Flags": 0," Fwd Header Length": 64," Bwd Header Length": 32,
```

```
  "Fwd Packets/s": 0.095244481," Bwd Packets/s": 0.047622241,
  " Min Packet Length": 0," Max Packet Length": 13," Packet Length Mean": 6.5,
  " Packet Length Std": 7.505553499," Packet Length Variance": 56.33333333,
  "FIN Flag Count": 0," SYN Flag Count": 1," RST Flag Count": 0,
  " PSH Flag Count": 0," ACK Flag Count": 1," URG Flag Count": 0,
  " CWE Flag Count": 0," ECE Flag Count": 0," Down/Up Ratio": 0,
  " Average Packet Size": 8.666666667," Avg Fwd Segment Size": 6.5,
  " Avg Bwd Segment Size": 0," Fwd Header Length.1": 64,
  "Fwd Avg Bytes/Bulk": 0," Fwd Avg Packets/Bulk": 0," Fwd Avg Bulk Rate": 0,
  " Bwd Avg Bytes/Bulk": 0," Bwd Avg Packets/Bulk": 0,"Bwd Avg Bulk Rate": 0,
  "Subflow Fwd Packets": 2," Subflow Fwd Bytes": 13," Subflow Bwd Packets": 1,
  " Subflow Bwd Bytes": 0,"Init_Win_bytes_forward": 229,
  " Init_Win_bytes_backward": 235," act_data_pkt_fwd": 0,
  " min_seg_size_forward": 32,"Active Mean": 0," Active Std": 0,
  " Active Max": 0," Active Min": 0,"Idle Mean": 0," Idle Std": 0,
  " Idle Max": 0," Idle Min": 0
}
)
```

Output:

```
1/1 ━━━━━━━━━━━━━━━━━━━━ 0s 36ms/step
1/1 ━━━━━━━━━━━━━━━━━━━━ 0s 30ms/step
------------------------------------------------------------
Per-model binary predictions (pred, p(class=1)):
  RandomForest        : 1   (p1=0.8000)
  LogisticRegression  : 1   (p1=0.9967)
  SVM                 : 1   (p1=0.9417)
  ANN                 : 1   (p1=0.9693)
------------------------------------------------------------
Attack CATEGORY (family-level):
  Predicted family: DoS   (prob=0.6359)
    DoS             -> 0.6359
    Brute Force     -> 0.2878
    ATTACK          -> 0.0348
    BENIGN          -> 0.0255
------------------------------------------------------------
ENSEMBLE FINAL: 1 -> ATTACK
Votes: [1, 1, 1, 1] Consensus: majority
------------------------------------------------------------
```

3. PORTSCAN DETECTION:

PortScan detection identifies when an attacker rapidly checks multiple ports on a system to find open or vulnerable ones.

This scanning creates **unusual connection patterns**, such as many short, repeated requests to different ports.

ML-IDS models flag these patterns as **suspicious reconnaissance activity**, helping prevent later attacks.

Input JSON:

```
#1062 in dataset
sample_output = run_live_demo_json(
{
  "Destination Port": 3389," Flow Duration": 24," Total Fwd Packets": 1,
  " Total Backward Packets": 1,"Total Length of Fwd Packets": 2,
  " Total Length of Bwd Packets": 6," Fwd Packet Length Max": 2,
  " Fwd Packet Length Min": 2," Fwd Packet Length Mean": 2,
  " Fwd Packet Length Std": 0,"Bwd Packet Length Max": 6,
  " Bwd Packet Length Min": 6," Bwd Packet Length Mean": 6,
  " Bwd Packet Length Std": 0,"Flow Bytes/s": 333333.3333,
  " Flow Packets/s": 83333.33333, " Flow IAT Mean": 24, " Flow IAT Std": 0,
  " Flow IAT Max": 24," Flow IAT Min": 24,"Fwd IAT Total": 0,
  " Fwd IAT Mean": 0," Fwd IAT Std": 0," Fwd IAT Max": 0," Fwd IAT Min": 0,
  "Bwd IAT Total": 0," Bwd IAT Mean": 0," Bwd IAT Std": 0," Bwd IAT Max": 0,
  " Bwd IAT Min": 0,"Fwd PSH Flags": 0," Bwd PSH Flags": 0,
  " Fwd URG Flags": 0," Bwd URG Flags": 0," Fwd Header Length": 24,
  " Bwd Header Length": 20,"Fwd Packets/s": 41666.66667,
  " Bwd Packets/s": 41666.66667," Min Packet Length": 2,
  " Max Packet Length": 6," Packet Length Mean": 3.333333333,
  " Packet Length Std": 2.309401077," Packet Length Variance": 5.333333333,
  "FIN Flag Count": 0," SYN Flag Count": 0," RST Flag Count": 0,
  " PSH Flag Count": 1," ACK Flag Count": 0," URG Flag Count": 0,
  " CWE Flag Count": 0," ECE Flag Count": 0," Down/Up Ratio": 1,
  " Average Packet Size": 5," Avg Fwd Segment Size": 2,
  " Avg Bwd Segment Size": 6," Fwd Header Length.1": 24,
  " Fwd Avg Packets/Bulk": 0," Fwd Avg Bulk Rate": 0," Bwd Avg Bytes/Bulk": 0,
  " Bwd Avg Packets/Bulk": 0,"Bwd Avg Bulk Rate": 0,"Subflow Fwd Packets": 1,
  " Subflow Fwd Bytes": 2," Subflow Bwd Packets": 1," Subflow Bwd Bytes": 6,
  "Init_Win_bytes_forward": 1024," Init_Win_bytes_backward": 0,
  " act_data_pkt_fwd": 0," min_seg_size_forward": 24,"Active Mean": 0,
  " Active Std": 0," Active Max": 0," Active Min": 0,"Idle Mean": 0,
  " Idle Std": 0," Idle Max": 0," Idle Min": 0
}
)
```

Output:

```
1/1 ━━━━━━━━━━━━━━━━━━━━ 0s 139ms/step
1/1 ━━━━━━━━━━━━━━━━━━━━ 0s 104ms/step
------------------------------------------------------------
Per-model binary predictions (pred, p(class=1)):
  RandomForest        : 1   (p1=1.0000)
  LogisticRegression  : 1   (p1=0.9660)
  SVM                 : 1   (p1=0.9521)
  ANN                 : 1   (p1=0.9409)
------------------------------------------------------------
Attack CATEGORY (family-level):
  Predicted family: PortScan   (prob=0.7985)
    PortScan        -> 0.7985
    Botnet          -> 0.0764
    BENIGN          -> 0.0539
    Brute Force     -> 0.0344
------------------------------------------------------------
ENSEMBLE FINAL: 1 -> ATTACK
Votes: [1, 1, 1, 1] Consensus: majority
------------------------------------------------------------
```

CONCLUSION

This project successfully demonstrates a **Machine Learning–based Intrusion Detection System (IDS)** using algorithms. The system uses real NetFlow-derived features to classify network traffic into benign and multiple attack types.

Key achievements:

- *High binary accuracy (98.59% for Random Forest)*
- *Strong multiclass accuracy (95.30% for Random Forest)*
- *Robust data pre-processing pipeline*
- *Four diverse ML models + ensemble decision logic*
- *Live demo accepting JSON or feature list input*
- *Feature importance analysis for explainability*

This demonstrates that **Machine Learning is a powerful approach for modern network security**, capable of detecting both known and unknown threats by learning behaviour patterns instead of relying on signatures.