AI IN INDUSTRY 2024/2025

Anomaly Detection in Network Cybersecurity

Vitaliia Stepashkina & Kimika Uehara

Motivation

Intrusion Detection Systems (**IDS**)

Growing sophistication of cyberattacks

As organizations increasingly rely on digital infrastructures, the volume and complexity of network traffic have grown exponentially

Traditional Signature-Based Detection Systems

Struggle to keep up with evolving attack vectors and zero-day vulnerabilities

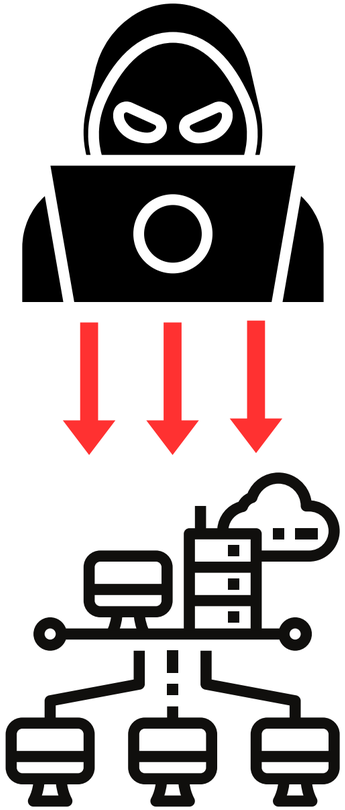
Anomaly Detection Systems

Focus on identifying deviations from normal behavior and offer the ability to detect previously unseen attacks

The Data: CSE-CIC-IDS2018

A collaborative project between the Communications Security Establishment (CSE) & the Canadian Institute for Cybersecurity (CIC) https://registry.opendata.aws/cse-cic-ids2018/

- Aims to provide a **comprehensive benchmark** for IDS.
- Captures **real labeled network traffic** with logs and 80 extracted features.
- Simulates both **legitimate and malicious behaviors** (DoS, Bruteforce, ...) across diverse protocols and applications
- High dimensional, time-series data



Attacker: 50 machines

Victim network: 420 machines and 30 servers, organized into 5 departments

Exploratory Data Analysis

Features

2097150 records (entries in the logging system)

78 features (excluding Timestamp and Label)

➡ **Duration, Number of packets, Number of bytes, Length of packets, etc.** calculated in forward and reverse directions

All columns are float/int, 8 columns with 2 unique values

1 column contains missing values

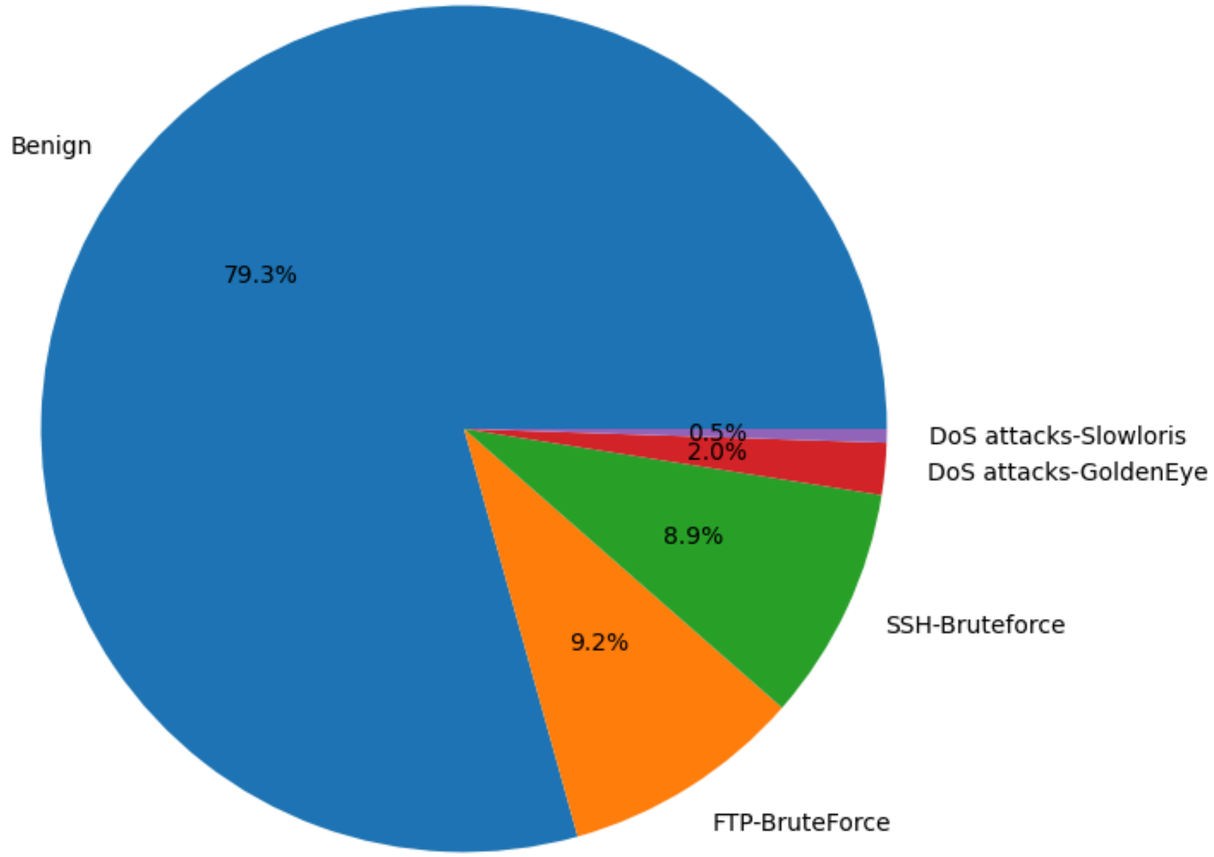
2 columns contain infinite values

Labels/Attack Scenarios

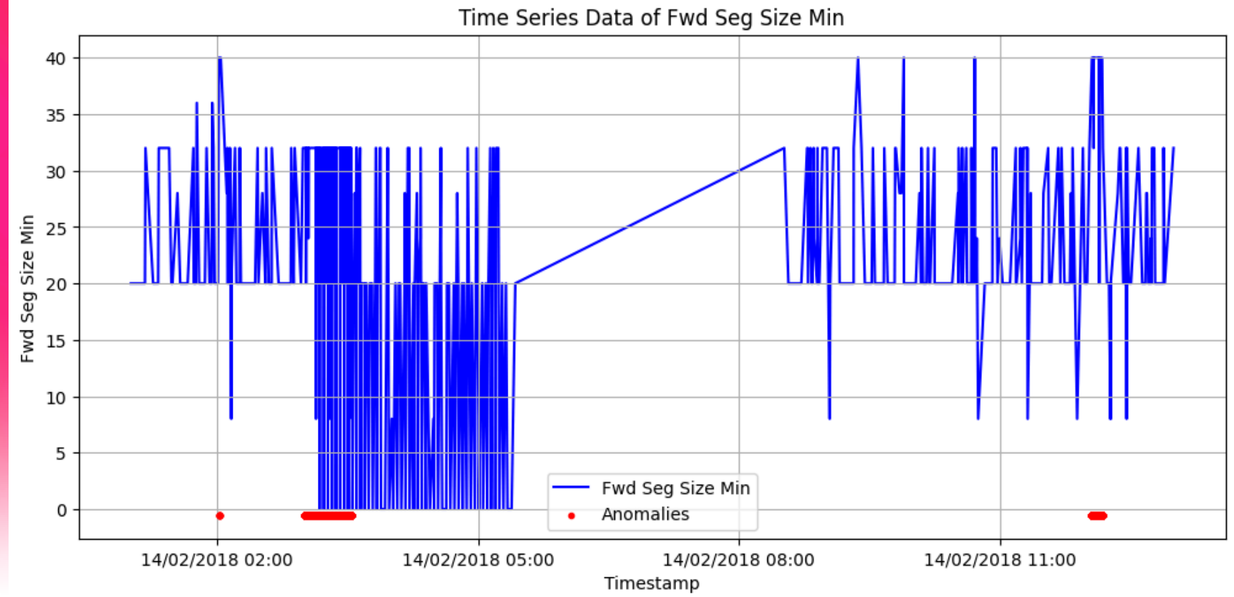
DoS Slowloris/GoldenEye: sends incomplete HTTP requests to the server at regular intervals to use up sockets

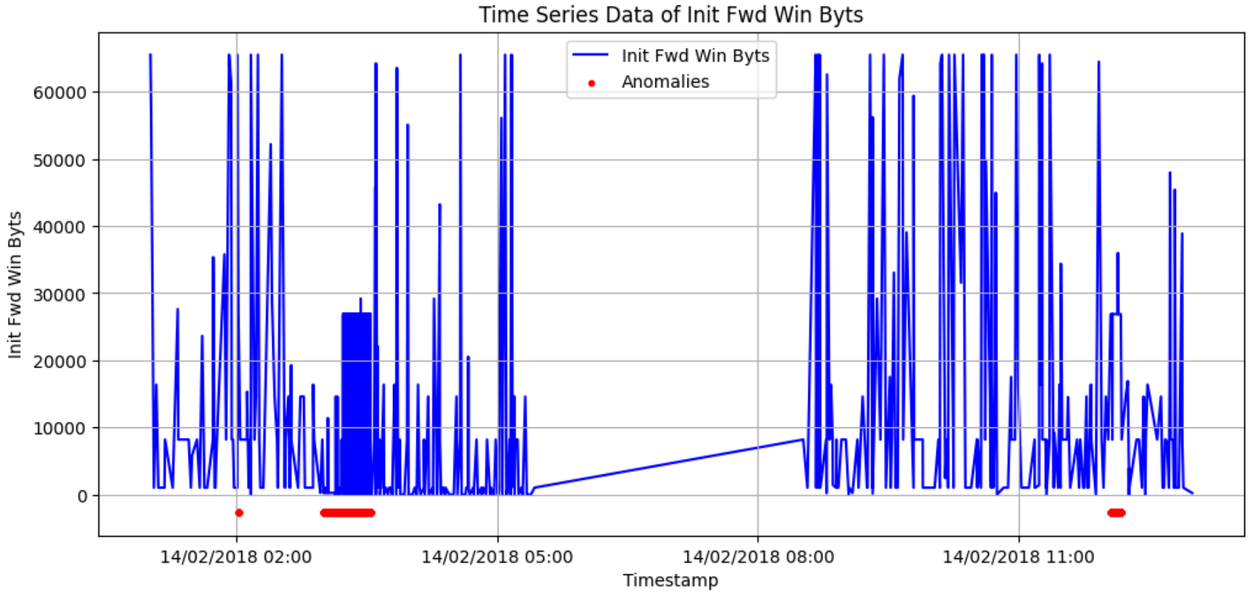
SSH/FTP-Bruteforce: Target weak credentials using dictionary attacks

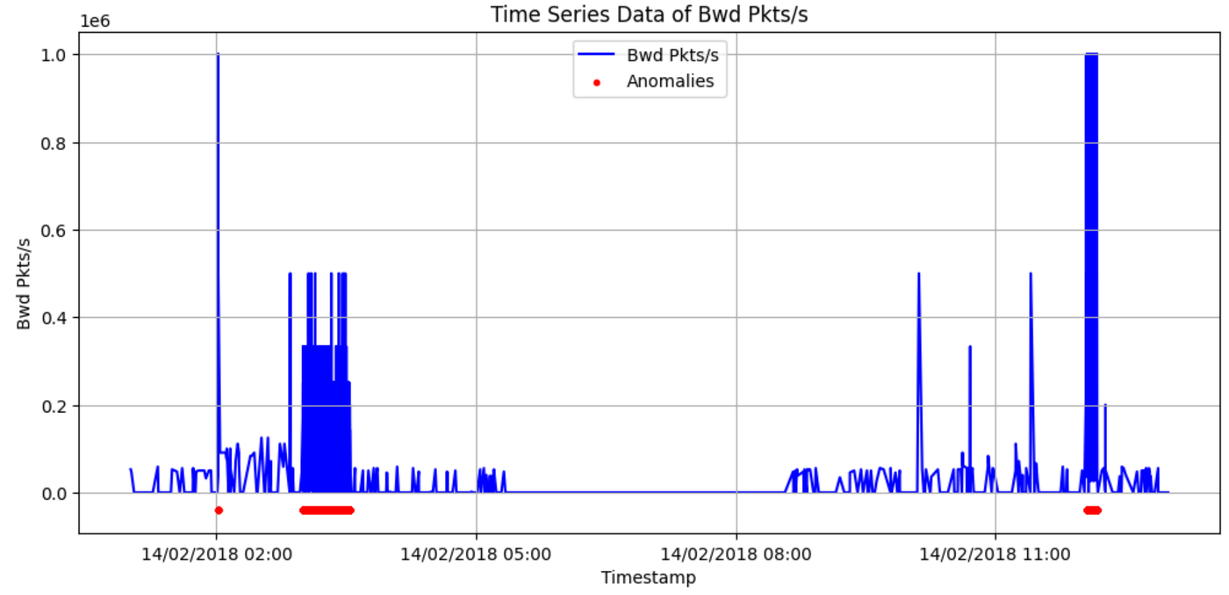
➡ Benign (0) or Anomalous (1)

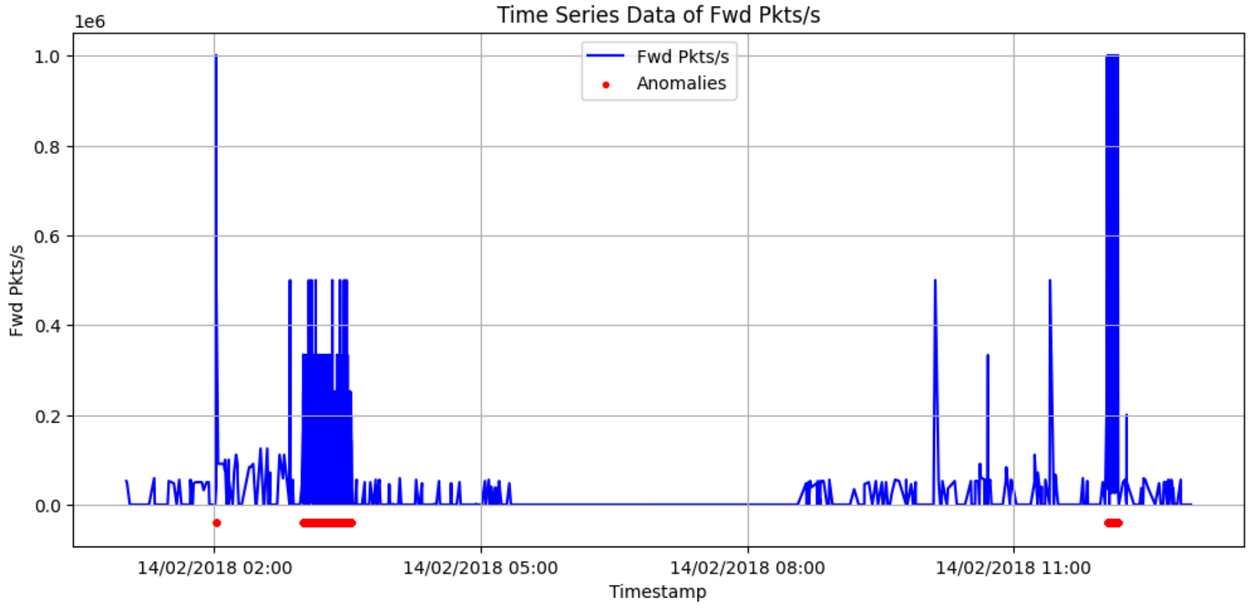


Time Series

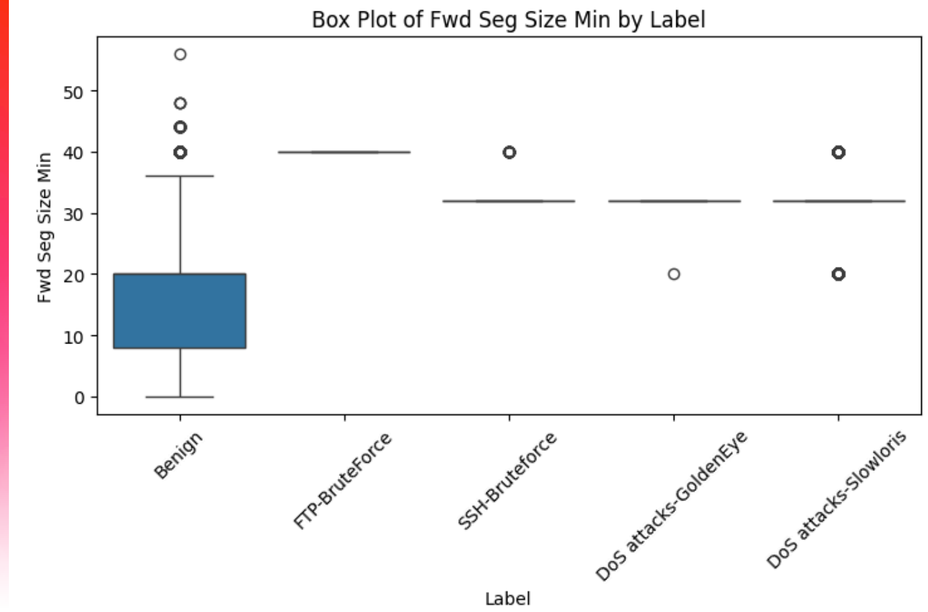

Time Series Data of Fwd Seg Size Min
Fwd Seg Size Min
Anomalies
Fwd Seg Size Min
Timestamp
14/02/2018 02:00
14/02/2018 05:00
14/02/2018 08:00
14/02/2018 11:00

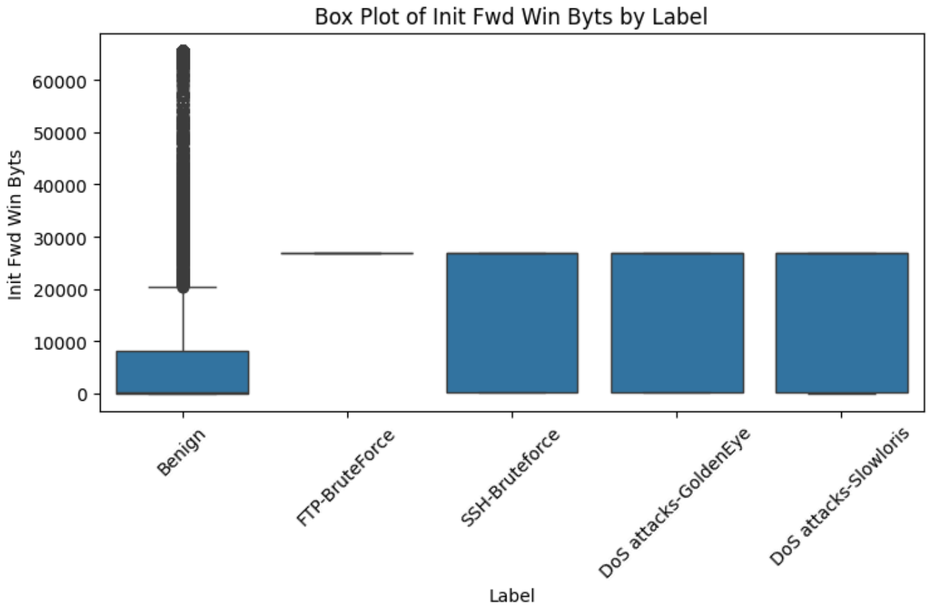

Time Series Data of Init Fwd Win Byts
Init Fwd Win Byts
Anomalies
Init Fwd Win Byts
Timestamp
14/02/2018 02:00
14/02/2018 05:00
14/02/2018 08:00
14/02/2018 11:00

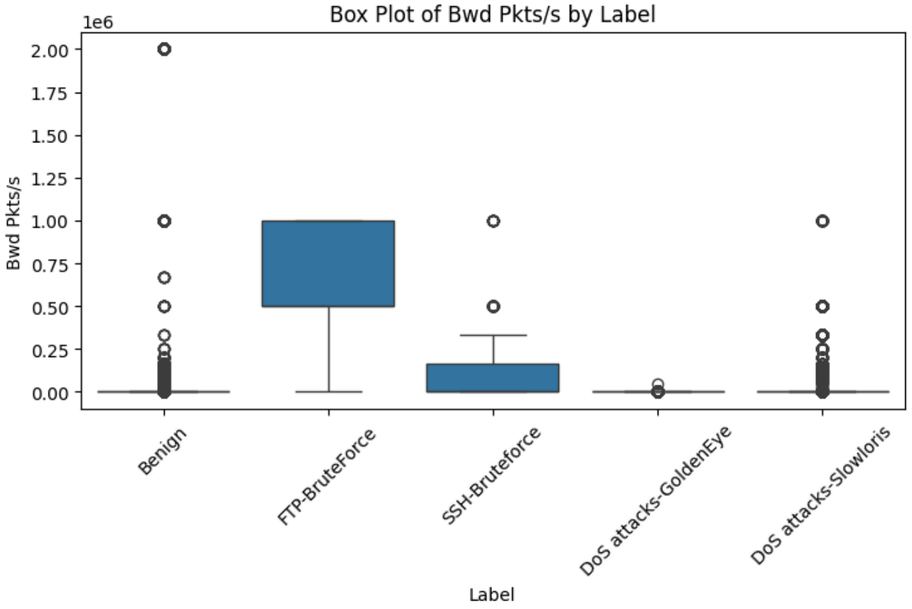

Time Series Data of Bwd Pkts/s
1e6
Bwd Pkts/s
Anomalies
Bwd Pkts/s
Timestamp
14/02/2018 02:00
14/02/2018 05:00
14/02/2018 08:00
14/02/2018 11:00

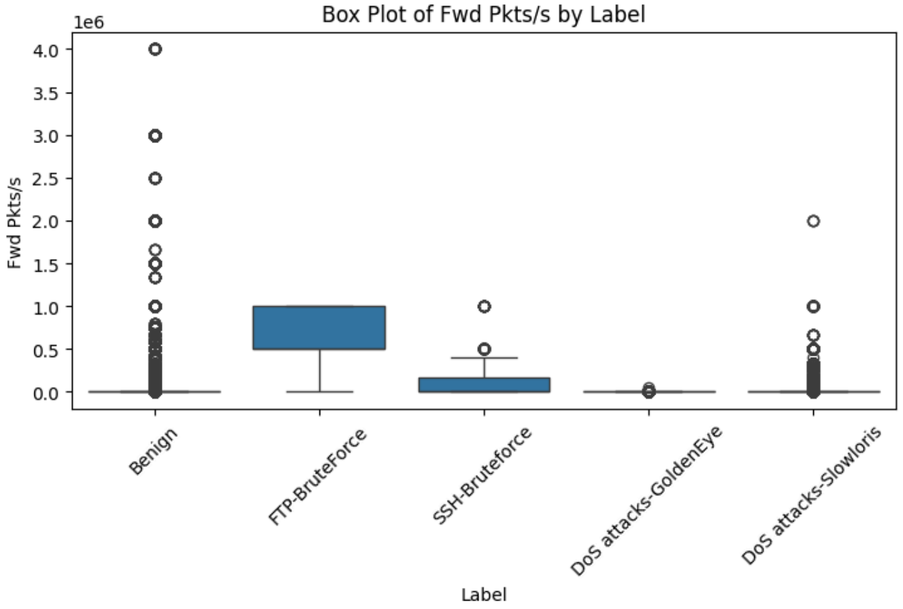

Time Series Data of Fwd Pkts/s
1e6
Fwd Pkts/s
Anomalies
Fwd Pkts/s
Timestamp
14/02/2018 02:00
14/02/2018 05:00
14/02/2018 08:00
14/02/2018 11:00

Feature Distributions









Data Preprocessing

Step 1

Remove columns with missing values & rows with infinite values

Step 2

Standardize the data using sklearn StandardScaler

Step 3

Split the data using the sliding windows technique

- Window size = 40
- Extract features from a sequence of data
- Preserve context between adjacent data points

Step 4

Split the data into training, validation & test set

- Training & validation: only benign data
- Test: mix of benign & anomalous data (around 6:4)

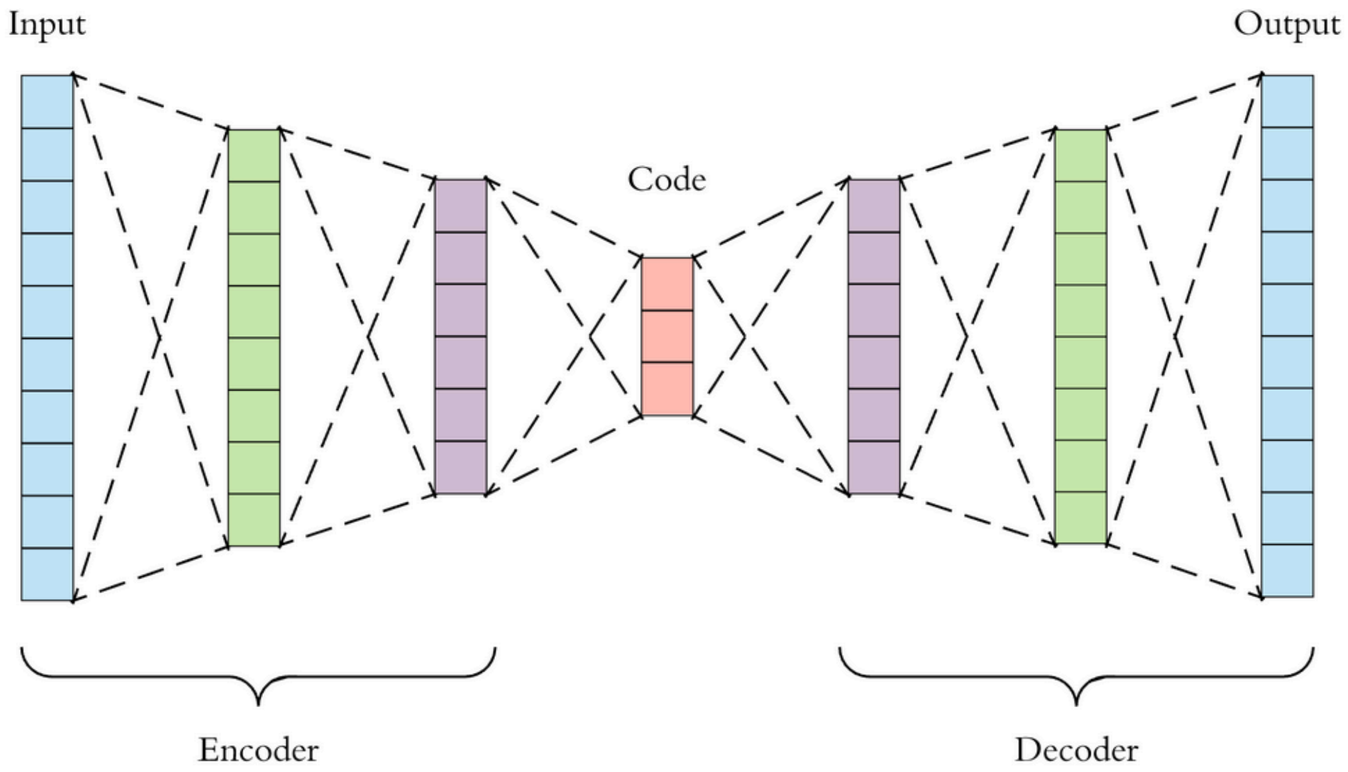
Neural networks approaches

Introducing to solutions

Autoencoder

Detects unknown attacks by focusing on deviations

Goal: Minimize reconstruction error between input and output



Input & output

Windows of Data:

- 77 Features
- Window Size of 40 timestamps.

Reconstruction loss

$$\mathcal{L}_{\text{reconstruction}} = \frac{1}{B}\sum_{i=1}^{B} \text{MSE}(X_i, \hat{X}_i)$$

Encoder

Compresses input into a smaller latent space representation.

Structure:

- 3 layers of 1D **convolution**:
  - 77 → 50 → 34 → 16 (feature reduction).
- **Activation**: LeakyReLU

Decoder

Reconstructs the original input from the latent representation.

Structure:

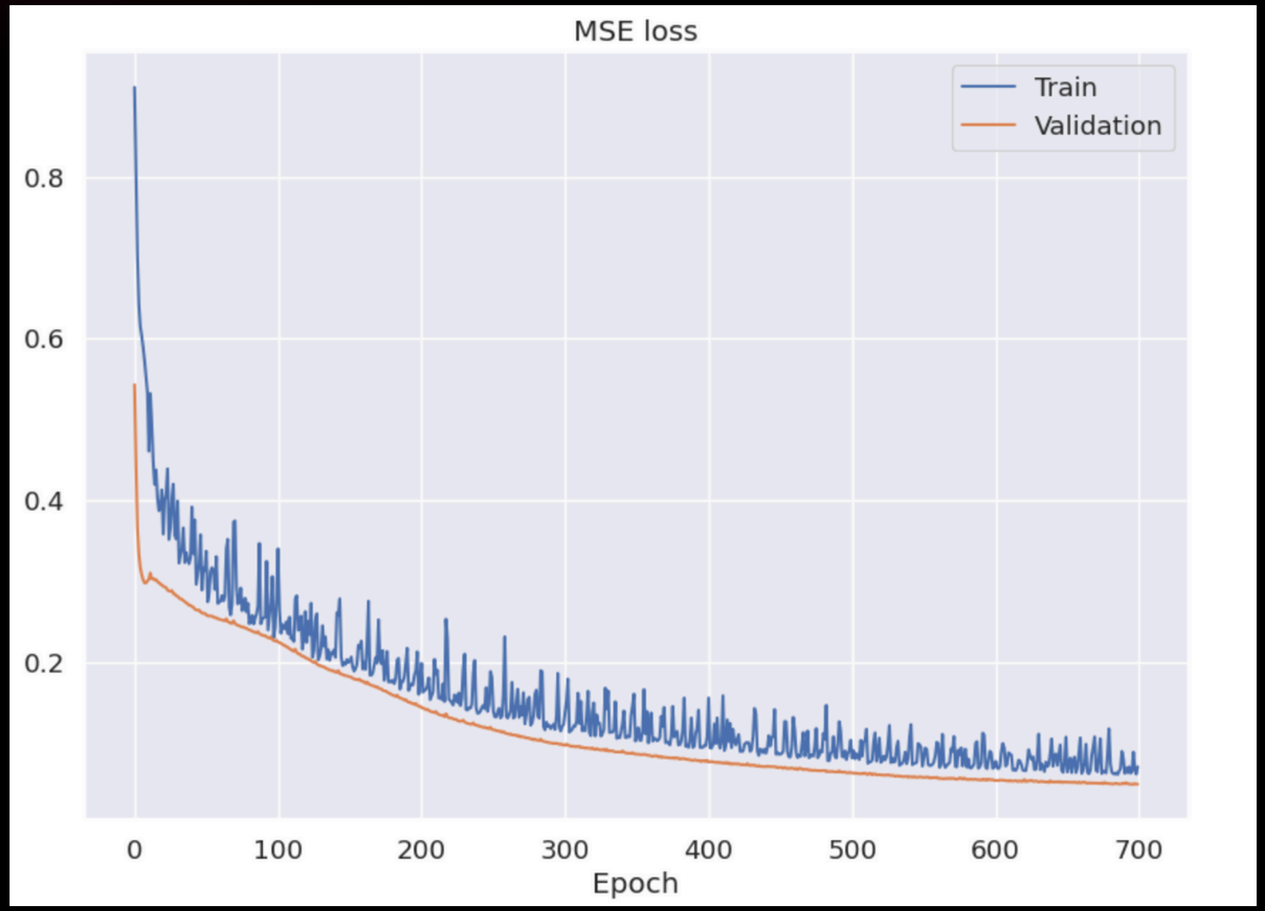
- 3 layers of 1D transposed **convolution**
  - 16 → 34 → 50 → 77 (restoring original dimensions).
- **Dropout** (20%) for regularization.
- **Activation**: LeakyReLU

Training AE

Technical side

Normal Data: Autoencoder learns to reconstruct typical patterns.
Anomalous Data: Reconstruction errors are significantly higher due to unfamiliar patterns.

Optimizer: AdamW
Scheduler: ReduceLROnPlateau
Epochs: 700
Lr: 0.0001

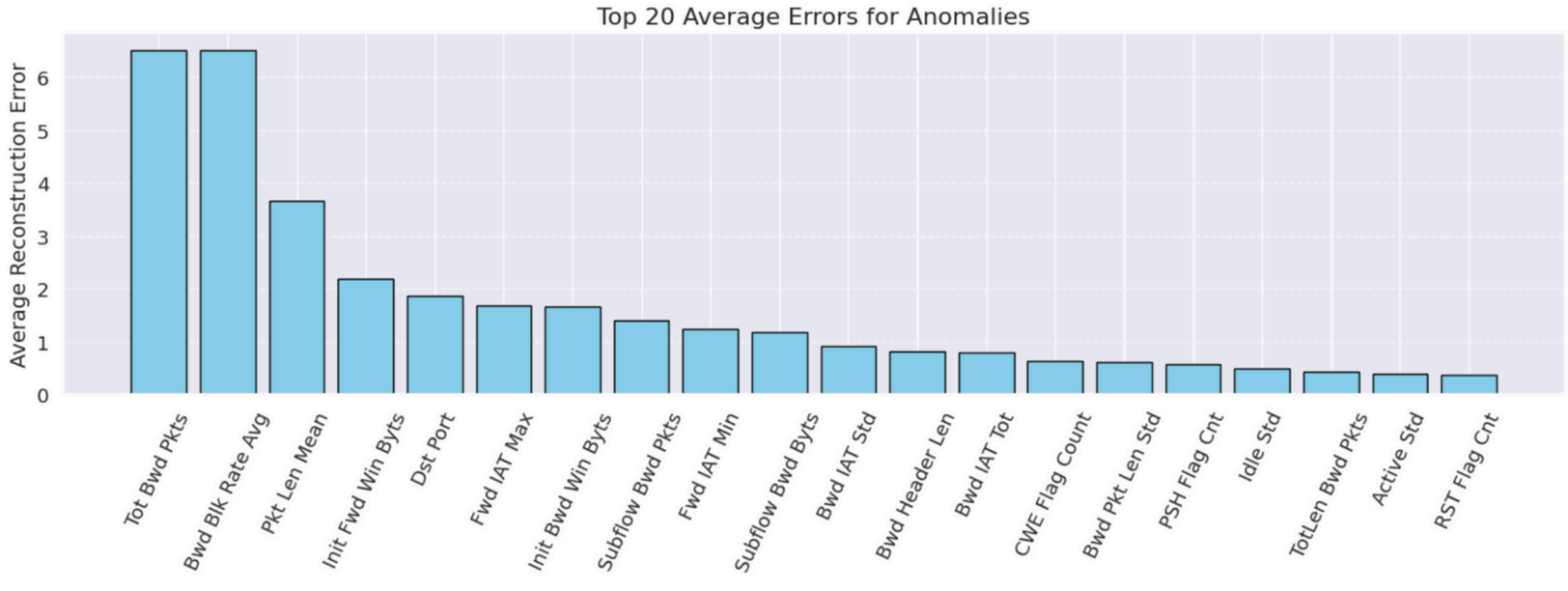


Results

AE final version

ROC_AUC	0.87
F1_score	0.8378
Recall	0.959
Precision	0.743

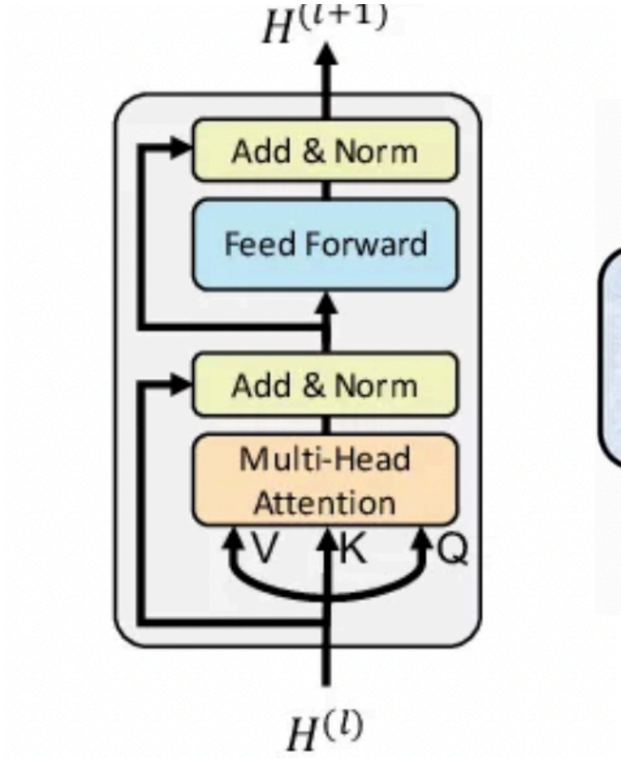
← fixed

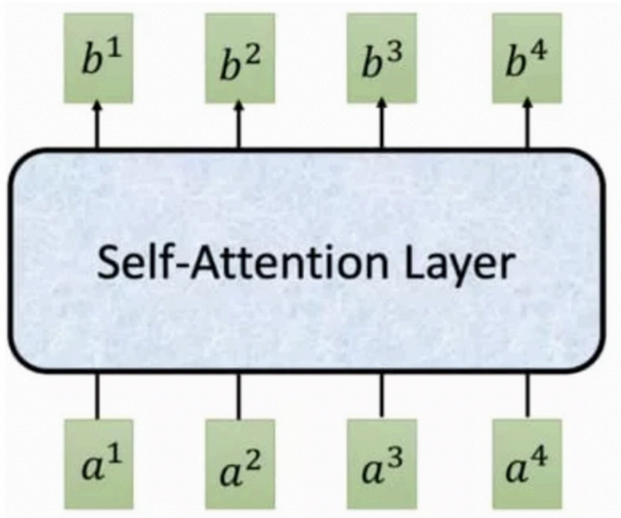


Autoencoder #2

with Transformer layers

Global Context Awareness + **High Performance**
(captures long-range dependencies) (SOTA)





Input & output

Windows of Data:

- 77 Features
- Window Size of 40 timestamps.

Reconstruction loss

$$\mathcal{L}_{\text{reconstruction}} = \frac{1}{B}\sum_{i=1}^{B}\text{MSE}(X_i, \hat{X}_i)$$

AE + Transformer

Final tuned structure

Input Transformation

- **Linear Projection:** Projects **77 features into** an embedding space (**32** dimensions).
- **Positional Encoding**

Encoder

- **4 Layers** with multi-head self-attention and feedforward sub-layers
- **Multi-Head Attention: 8** heads to capture relationships
- **Hidden layer size of 256**

Decoder

- **4 Layers:** similar structure to the encoder
- **Multi-Head Attention: 8** heads for reconstruction
- **Feedforward Dimension of 256**

Autoencoder + Transformer

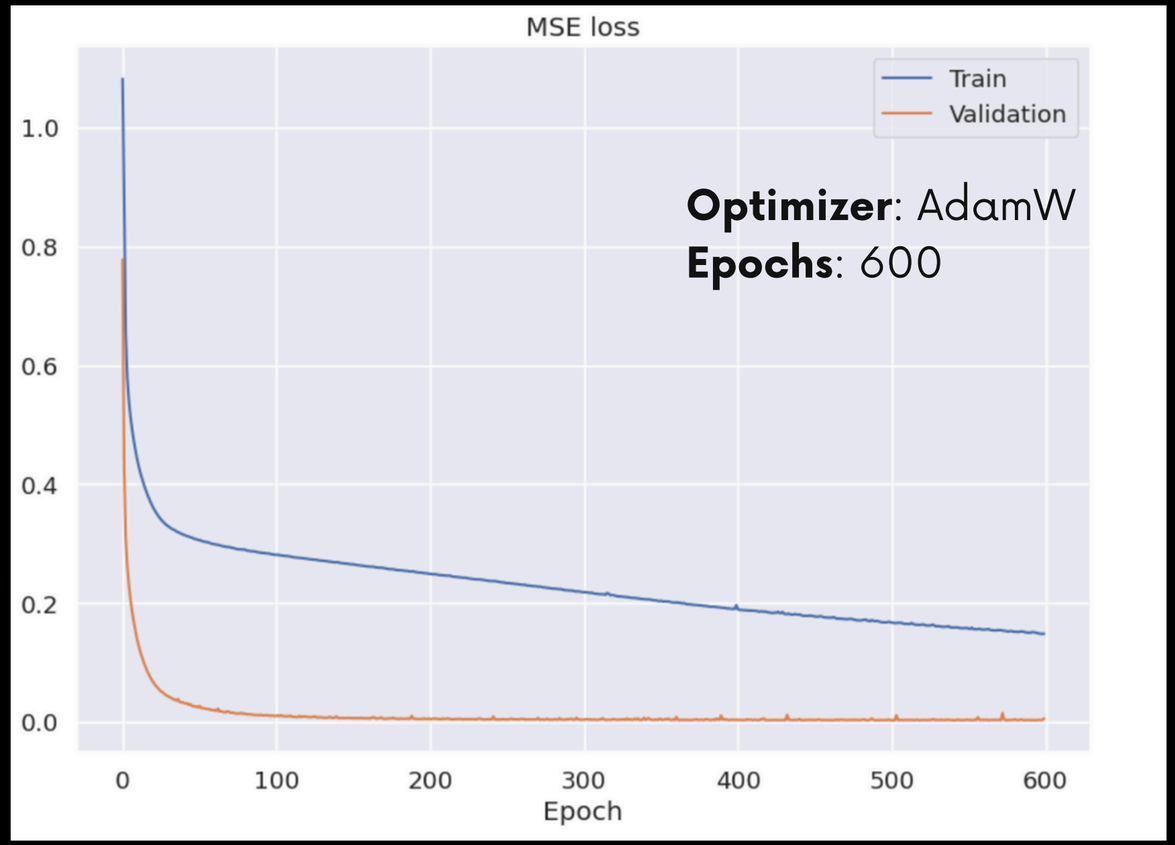
technical tweaks

+

Learning Rate Scheduling with Warmup

Warmup Phase: increases lr from 1e-9 to 3e-4 in 20 epochs

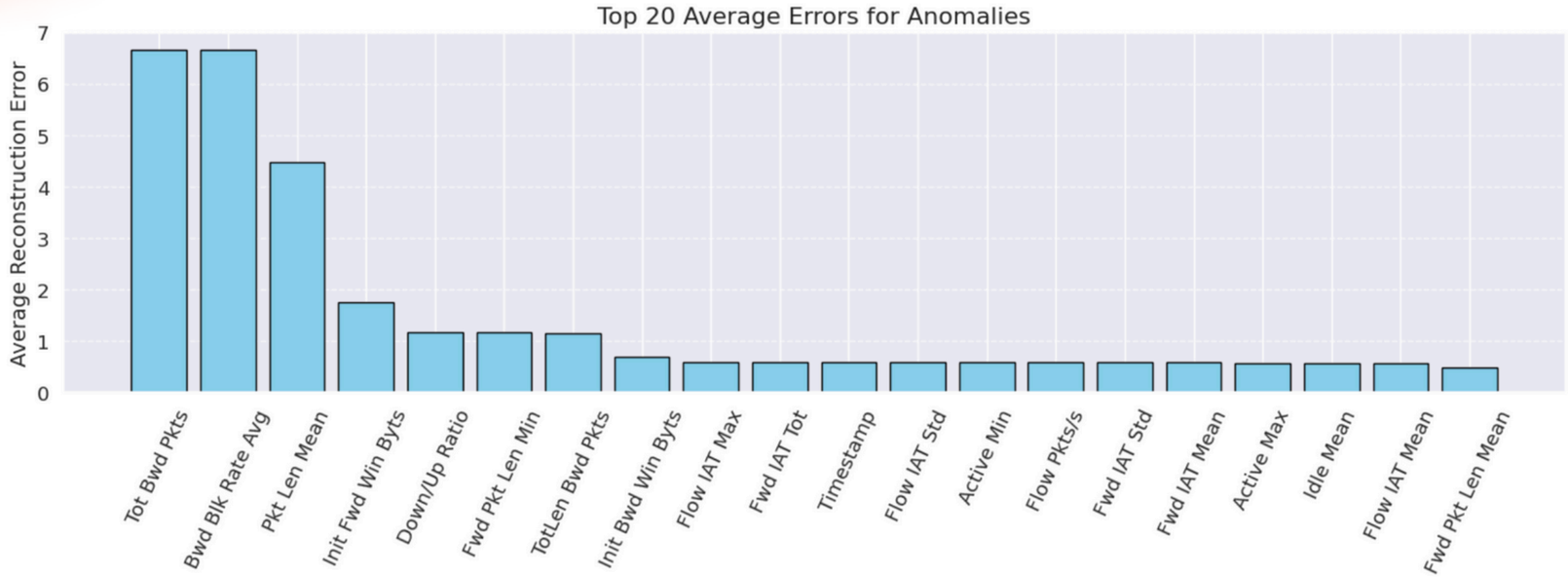
Decay Phase: Transitions to a multi-step scheduler reducing lr by 0.7x at [60, 120, 180, 250, 350, 450]



Results

AE + Transformer
final version

ROC_AUC	0.963	+10.6%
F1_score	0.9106	+8.6%
Recall	0.9503	← fixed
Precision	0.874	+17.6%



Future Pathways

1. **Hybrid Models:**

   Try out other options: implement **VAE**, combine model with **LSTMs**

2. **Forecasting-based Anomaly Detection:**

   Time-Series Transformers, Temporal Fusion Transformers

3. **Graph Neural Networks:**

   Identify anomalous relationships in network traffic, using Graph Convolutional Networks (**GCNs**) or Graph Attention Networks (**GATs**)

4. **Contrastive Learning for Representation:**

   Use techniques like **SimCLR** or **TS-TCC**

Do you have any questions?