NETWORK ANOMALY DETECTION

Course: (66219) Introduction to Machine Learning in Cybersecurity

Lecturer: Dr. Uri Itai

Assignee: Stas Susha

ABSTRACT

KEY TOPICS

- Importance of network security
- Crucial role of IDS in detecting malicious activities
- ML importance in network anomaly detection
- Experiment results on UNSW-NB15 dataset
- Future Work

INTRO

CYBER ATTACKS 2024

1. UnitedHealth - $872 Million Cyberattack

- **Industry sector**: Healthcare
- **Damage** : $872 million
- **Date**: April 2024
- **Attack type**: ransomware attack
- **Description**:
  - Attackers: a group known as AlphV or BlackCat
  - Affected systems: pharmacy services, payments platforms, and medical claims.
  - Disrupted operations period – over a week.
  - Stolen data ~6TB sensitive medical records
  - Company didn't expose the ransom payment, but media sources report a payment of $22 million in bitcoin to BlackCat
  - The attack is currently believed to have been executed via a vulnerable Citrix portal

1. UnitedHealth's $872 Million Cyberattack

Be in no doubt that ransomware continues to be a massive problem. A Q1 financial report from UnitedHealth Group in April 2024 revealed a massive $872 million loss attributable to ransomware.

The report states: "Cash flows from operations from the first quarter 2024 were $1.1 billion and were affected by approximately $3 billion due to the company's cyberattack response actions, including funding acceleration to care providers, and were additionally impacted due to the timing of public sector cash receipts."

Source: *Techradar – Top data breaches and cyber attacks in 2024*

CYBER ATTACKS 2024

2. Cryptocurrency Heist at DMM Bitcoin

- **Industry sector**: Finance
- **Damage** : 4,502.9 Bitcoin, approx. $308 million
- **Date**: May 31, 2024
- **Attack type**:
  unauthorized access, exploiting system vulnerabilities
- **Description**:
  - DMM Bitcoin - Japanese crypto currency exchange
  - Largest crypto attack in 2024 (8-largest ever)
  - Thieves obtained unauthorized access to corporate systems
  - The stolen Bitcoin was distributed to multiple different addresses, likely to evade detection and exchange blocks

Source: *SOCRadar – Major Cyber Attacks in Review: May 2024*

CYBER ATTACKS 2024

3. DDoS Attack on Internet Archive


The Internet Archive is fighting a major battle against DDoS attacks

News By Craig Hale published May 29, 2024

DDoS attack focuses on the Internet Archive

Source: *Techradar* – [The Internet Archive is fighting a major battle against DDoS attacks]

- **Industry sector**: Education/Research
- **Damage**: 3-day disrupted services
- **Date**: May 26, 2024
- **Attack type**: DDoS
- **Description**:
  - Internet Archive – non-profit research library housing million historical web pages
  - Attackers: anonymous gang called **SN_Blackmeta**
  - Attack involves tens of thousands fake info requests per second designed to flood the servers, which cause a data access problems.

CYBER THREATS STATS Q1-2024

Q1 2024 there was a 28% increase in cyber attacks on average comparing Q4 2023, and 5% Q1 YoY. (Check Point Report, Apr. 10)

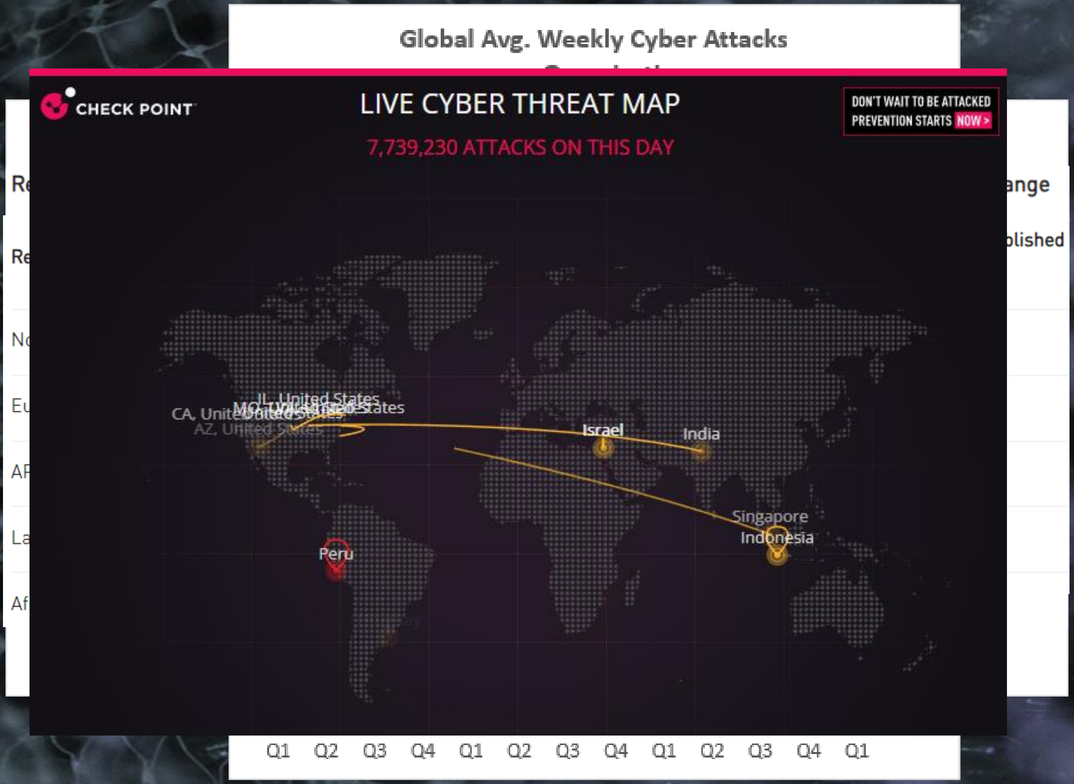
Top 3 industry sectors:
Education/Research (2454), Government/Military (1692), Healthcare(1605)

HW vendor industry cyber attacks +37% YoY

Africa saw a significant 20% increase in cyber attacks, while Latin America reported a 20% decrease year-on-year (YoY)

Ransomware attacks surge (1000 published attacks):
North America 59%, Europe (24%) and APAC (12%)

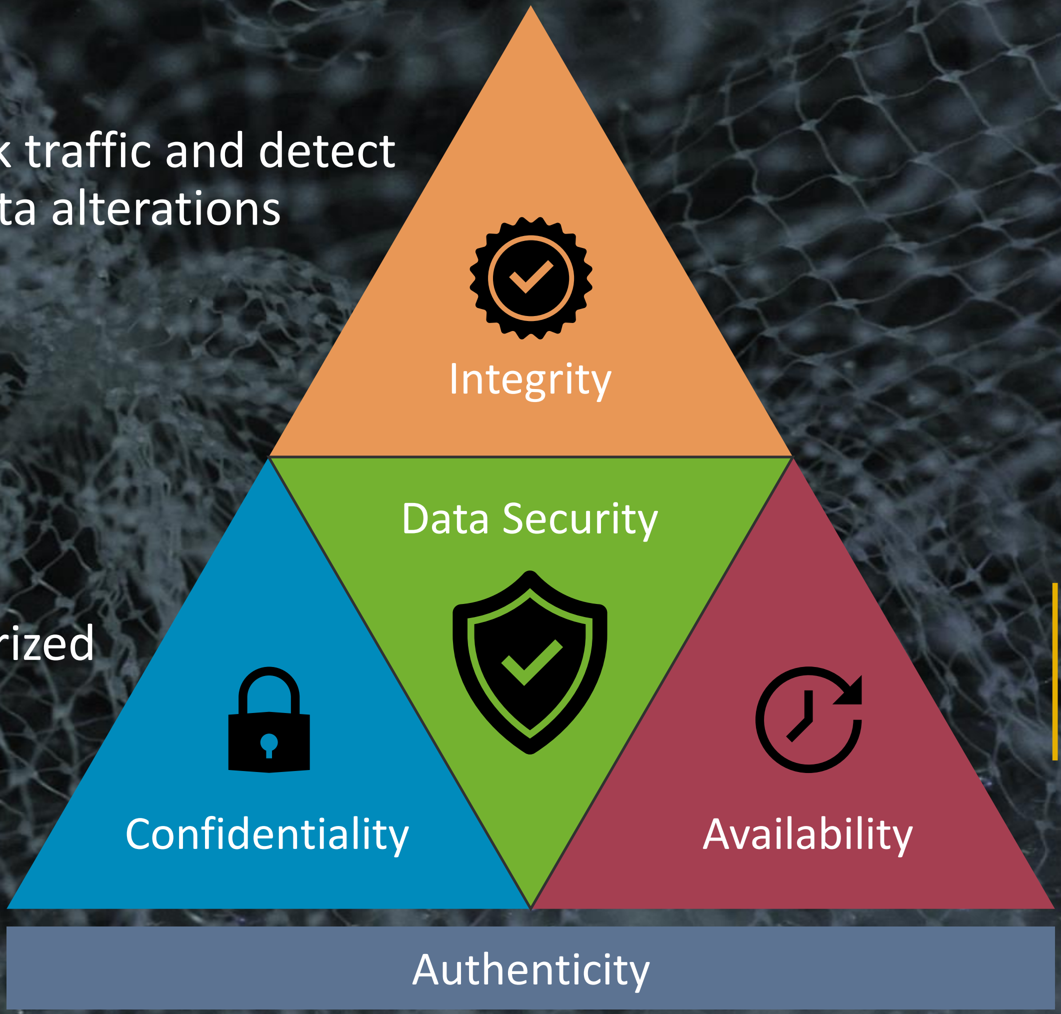
Europe +64% Q1 2024 compared to Q1 2023



WHY NETWORK SECURITY MATTERS?

Monitor network traffic and detect unauthorized data alterations

Identify/prevent unauthorized access to sensitive data



Helps to prevent service disruptions caused by attacks, such as denial-of-service (DoS)

Detect forged or malicious packets and ensure that communication originated from legitimate source

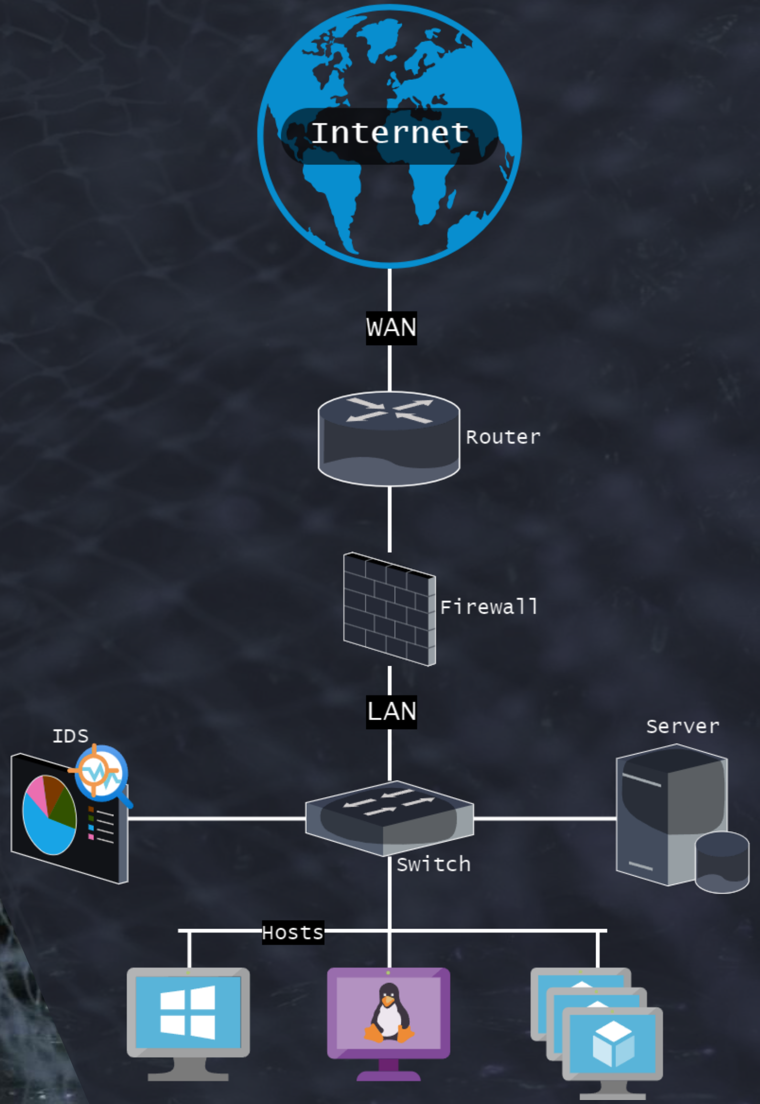
MALICIOUS TRAFFIC DETECTION (IDS)

Intrusion Detection Systems (IDS) – network security tool, acts as a protective line of defense against threats that can compromise system CIA.

IDS – software application or hardware device that continuously monitors the system or network

Looks for known threats, abnormal activities or policy violations

Alerts system administrator when detects security risks



DETECTION METHODS OF IDS

Signature-based detection (SIDS)

- Use fingerprint of known threats
- Efficient in detecting attacks with already known patterns
- Able to process high volume of network traffic
- Fail to identify new/unknown attacks in the network

Anomaly-based detection (AIDS)

- Use ML techniques to detect malicious traffic or patterns
- Require more processing resources
- Able to detect unknown attack types and anomaly behavior
- Lower detection rate and higher FP rate

MACHINE LEARNING
IN NETWORK SECURITY

ML IN NETWORK SECURITY

Improved Detection – ML models can recognize subtle patterns and anomalies that traditional IDS can miss

Continuous Learning – ML can learn and adapt to new threats and improve detection over time

Behavior Analysis – analyze behavior of users and systems to predict and prevent possible intrusions

Enhanced Threat Intelligence – ML can correlate data from multiple sources to provide a more comprehensive view of potential threats

DATASET

UNSW-NB15

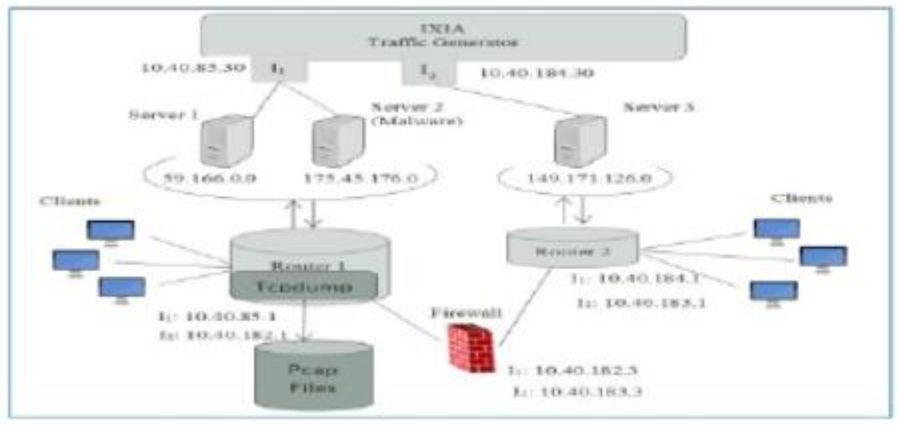
DATASET UNSW-NB15

UNSW-NB15 - comprehensive network intrusion dataset, which can be found here

Introduced by Dr. Nour Moustafa and Jilly Slay, researches from the University of New South Wales (UNSW), Australia. Visit this research paper.

Dataset creation

- The raw network packets were generated using the IXIA PerfectStorm tool in the Cyber Range Lab of the Australian Centre for Cyber Security (ACCS)
- This dataset combines real modern normal activities with synthetic contemporary attack behaviors.
- The simulation period was 16 hours on Jan 22, 2015 and 15 hours on Feb 17, 2015 for capturing 100 GB of raw traffic (pcap files)



DATASET UNSW-NB15

Dataset Size

- Full dataset a total of 2,540,044 records consists of 4 csv files
- Partial data set split into 2 files: train (175,341) and test (82,332) sets
  Note: the train/test dataset will be used for experiments

File	Size	Num of entries	Num of features
UNSW-NB15_1.csv	161.2MB	700,000	49
UNSW-NB15_2.csv	157.6MB	700,000	49
UNSW-NB15_3.csv	174.4MB	700,000	49
UNSW-NB15_4.csv	91.3MB	440,044	49
UNSW-NB15_features.csv	3.95KB	49	-
UNSW_NB15_training-set.csv	31536.15KB	175341	45
UNSW_NB15_testing-set.csv	15020.31KB	82332	45

DATASET UNSW-NB15

Features

- UNSW-NB15 dataset has 49 features (described in *UNSW-NB15_features.csv*)
- Data types:
  - Nominal (categorical)
  - binary (categorical)
  - numerical (integer/float)

Target

- label – 1:attack, 0:normal
- attack_cat – attack category (9)
  - **Fuzzers** - *cause a program or network owerhelm or crash by sending the randomly generated data*
  - **Analysis** - *uses port scans, vulnerability scans, spam files to gather info about the network*
  - **Backdoors** - *bypass security mechanisms to obtain unauthorized access to the host or data*
  - **DoS** - *Denial of Service, make a server or network services unavailable to users*
  - **Exploits** - *exploit the known OS or software vulnerabilities*
  - **Generic** - *cryptographic attack that targets the secret key used in encryption*
  - **Reconnaissance** - *discover all possible info to gain access to the target host or network*
  - **Shellcode** - *exploit attack uses a payload (small piece of code) to get unauthorized access*
  - **Worms** - *spread through the network by infecting multiple systems*

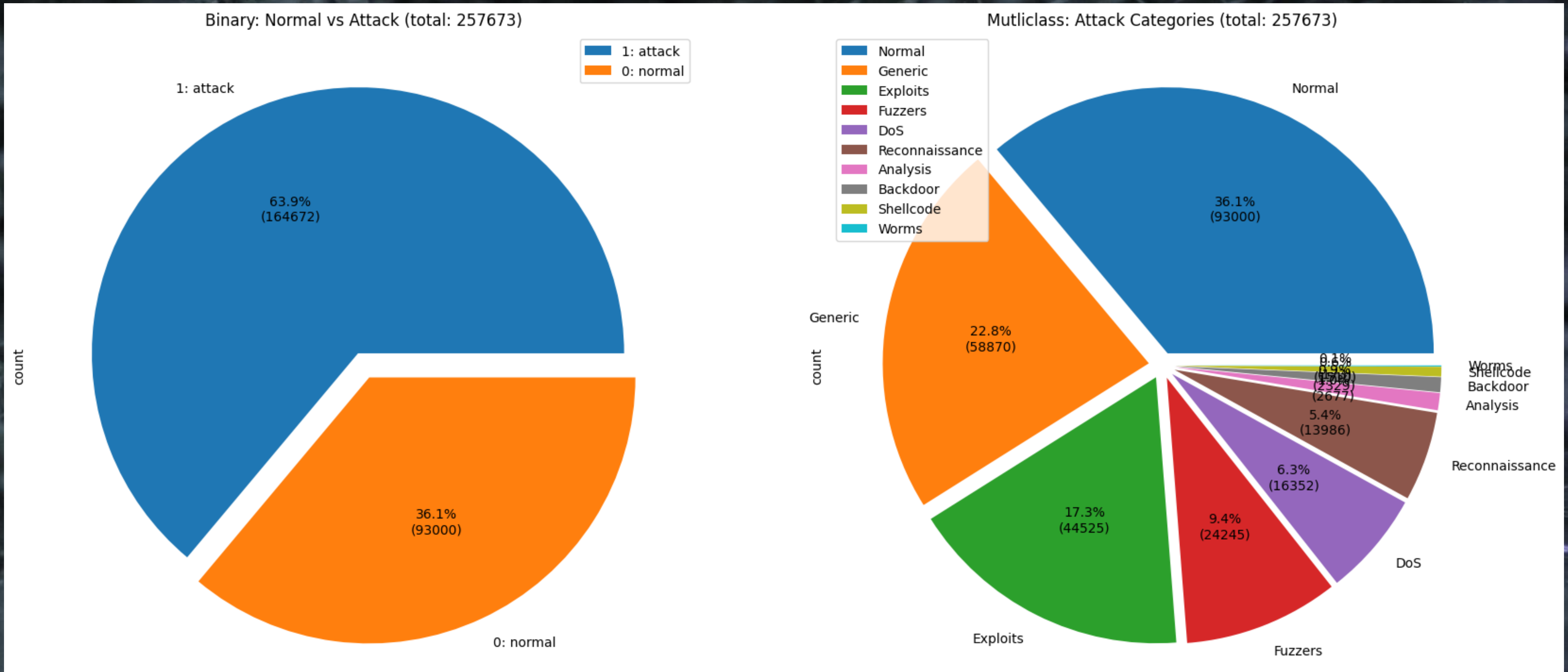
	Name	Type	Description
0	dur	float	Record total duration
1	proto	nominal	Transaction protocol
2	service	nominal	http, ftp, smtp, ssh, dns, ftp-data ,irc and ...
3	state	nominal	Indicates to the state and its dependent proto...
4	spkts	integer	Source to destination packet count
5	dpkts	integer	Destination to source packet count
6	sbytes	integer	Source to destination transaction bytes
7	dbytes	integer	Destination to source transaction bytes
8	rate	float	Ethernet data rates transmitted and received (...
9	sttl	integer	Source to destination time to live value
10	dttl	integer	Destination to source time to live value
11	sload	float	Source bits per second
12	dload	float	Destination bits per second
13	sloss	integer	Source packets retransmitted or dropped
14	dloss	integer	Destination packets retransmitted or dropped
15	sinpkt	float	Source interpacket arrival time (mSec)
16	dinpkt	float	Destination interpacket arrival time (mSec)
17	sjit	float	Source jitter (mSec)
18	djit	float	Destination jitter (mSec)
19	swin	integer	Source TCP window advertisement value
20	stcpb	integer	Source TCP base sequence number
21	dtcpb	integer	Destination TCP base sequence number
22	dwin	integer	Destination TCP window advertisement value
23	tcprtt	float	TCP connection setup round-trip time, the sum ...
24	synack	float	TCP connection setup time, the time between th...
25	ackdat	float	TCP connection setup time, the time between th...
26	smean	integer	Mean of the ?ow packet size transmitted by the...
27	dmean	integer	Mean of the ?ow packet size transmitted by the...
28	trans_depth	integer	Represents the pipelined depth into the connec...
29	response_body_len	integer	Actual uncompressed content size of the data t...
30	ct_srv_src	integer	No. of connections that contain the same servi...
31	ct_state_ttl	integer	No. for each state (6) according to specific r...
32	ct_dst_ltm	integer	No. of connections of the same destination add...
33	ct_src_dport_ltm	integer	No of connections of the same source address (...
34	ct_dst_sport_ltm	integer	No of connections of the same destination addr...
35	ct_dst_src_ltm	integer	No of connections of the same source (1) and t...
36	is_ftp_login	binary	If the ftp session is accessed by user and pas...
37	ct_ftp_cmd	integer	No of flows that has a command in ftp session.
38	ct_flw_http_mthd	integer	No. of flows that has methods such as Get and ...
39	ct_src_ltm	integer	No. of connections of the same source address ...
40	ct_srv_dst	integer	No. of connections that contain the same servi...
41	is_sm_ips_ports	binary	If source (1) and destination (3)IP addresses ...
42	attack_cat	nominal	The name of each attack category. In this data...
43	label	binary	0 for normal and 1 for attack records

EDA

UNSW-NB15

EDA UNSW-NB15

Target: Normal vs Attack (Binary & Mutli-class)

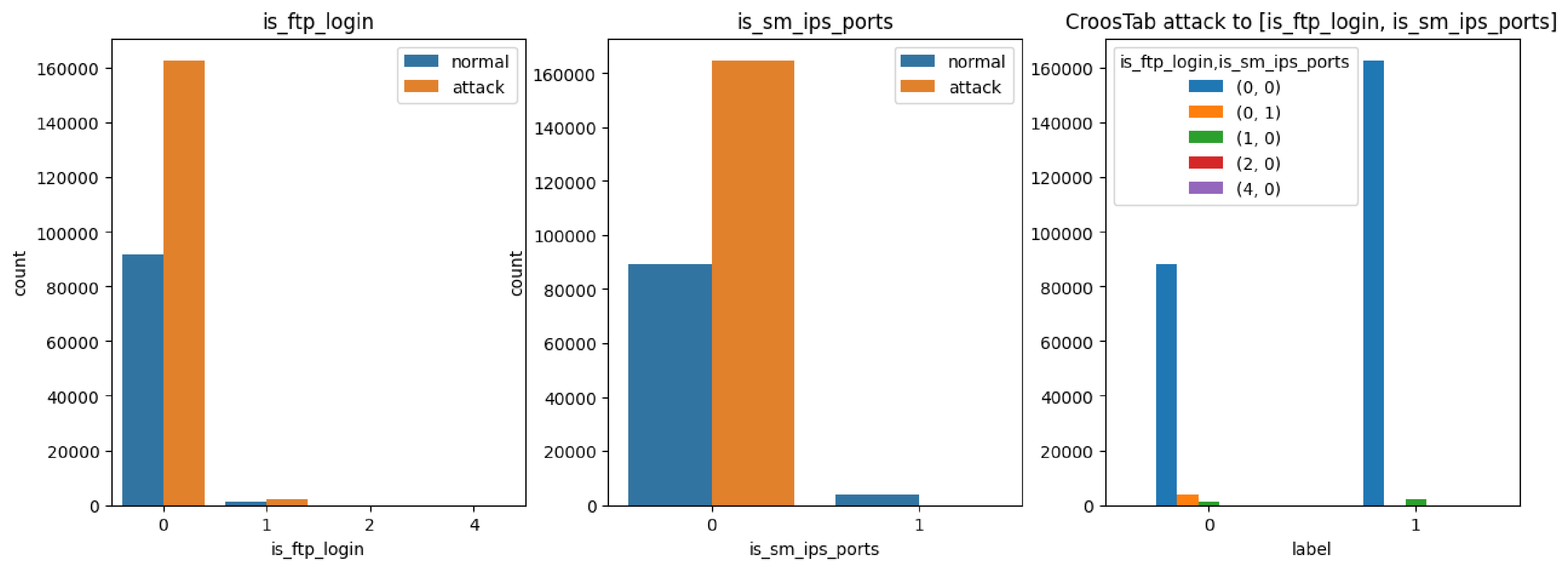


EDA UNSW-NB15

Categorical Features

- Count plots – counter based on normal/attack entries
- Cross-tab – to understand the relationship between categorical features (patterns, associations, dependencies)

is_ftp_login	0		1	2	4
is_sm_ips_ports	0	1	0	0	0
label					
0	88006	3678	1314	2	0
1	162744	0	1905	8	16

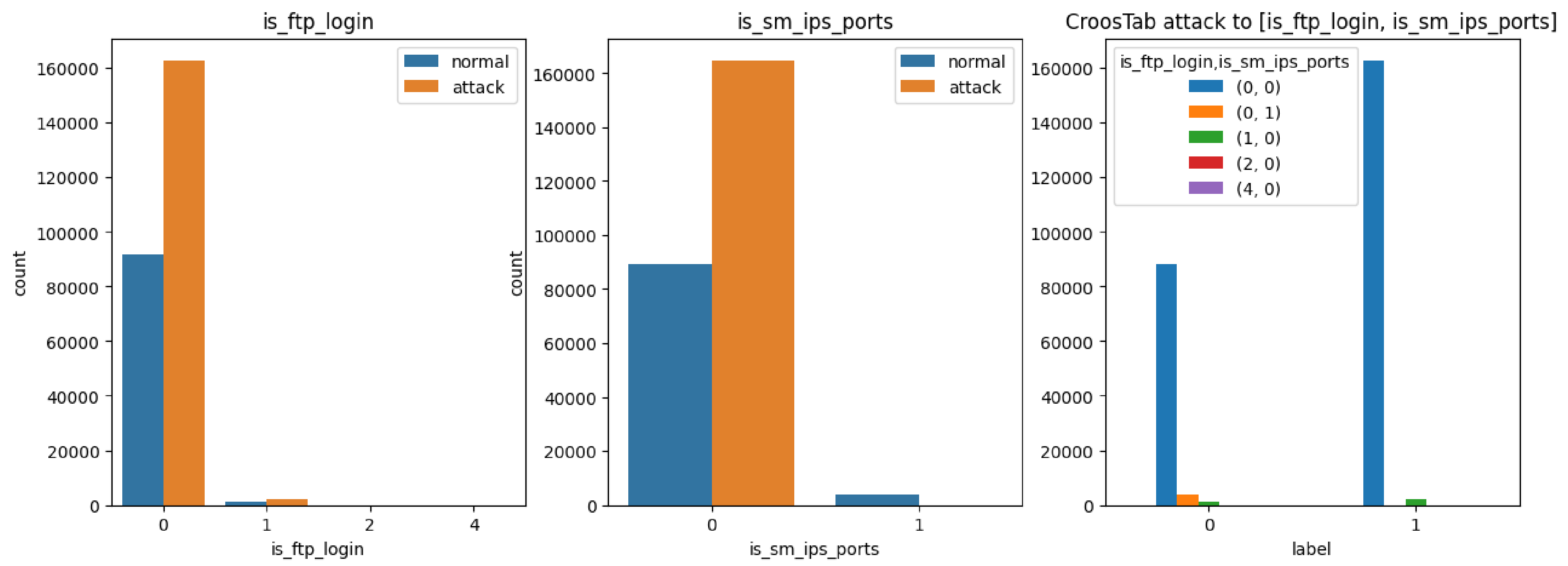


EDA UNSW-NB15

Categorical Features

- Count plots – counter based on normal/attack entries
- Cross-tab – to understand the relationship between categorical features (patterns, associations, dependencies)

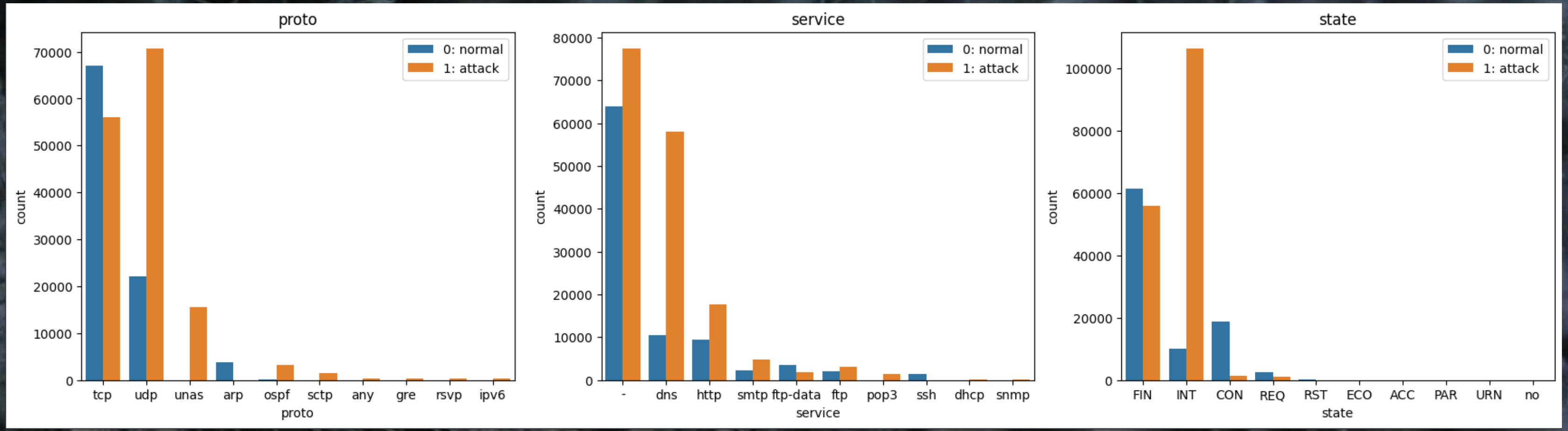
is_ftp_login	0		1	2	4
is_sm_ips_ports	0	1	0	0	0
label					
0	88006	3678	1314	2	0
1	162744	0	1905	8	16



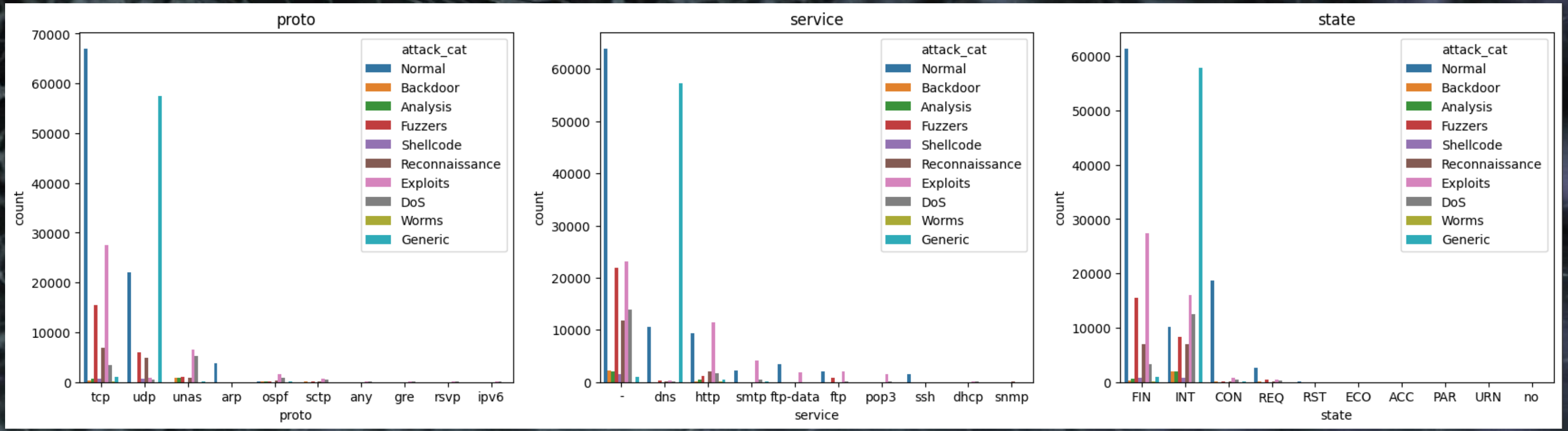
EDA UNSW-NB15

Categorical Features

Binary



Multi-class



Cross-tab

```
mask = (data['all']['attack_cat'] == 'Generic') & (data['all']['proto'] == 'udp') & (data['all']['service'] == 'dns') & (data['all']['state'] == 'INT')
print(pd.crosstab(data['all'].loc[mask, 'attack_cat'], [data['all'].loc[mask, 'proto'], data['all'].loc[mask,'service']]))
```

✓ 0.0s

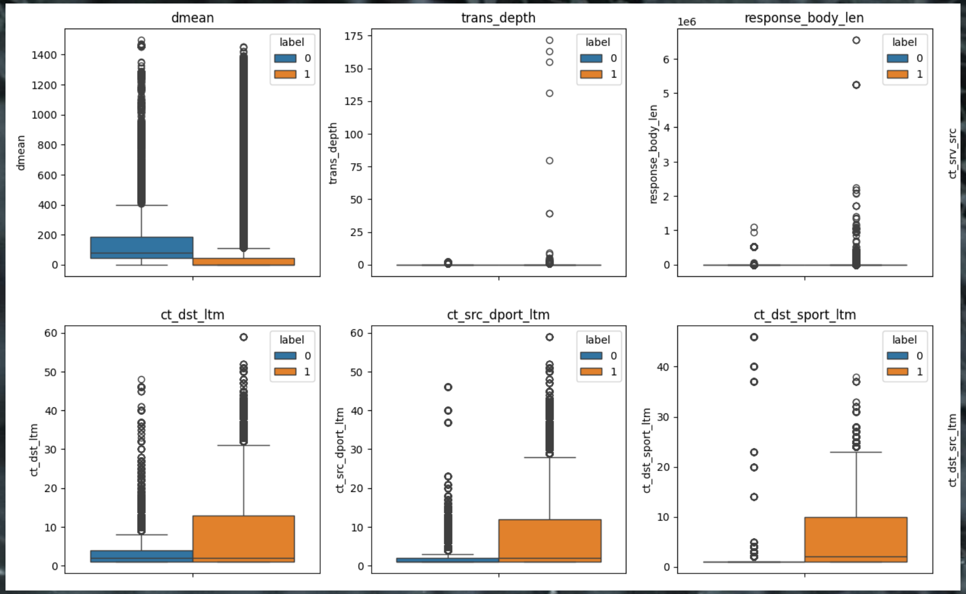
```
proto        udp
service      dns
attack_cat
Generic    57276
```

EDA UNSW-NB15

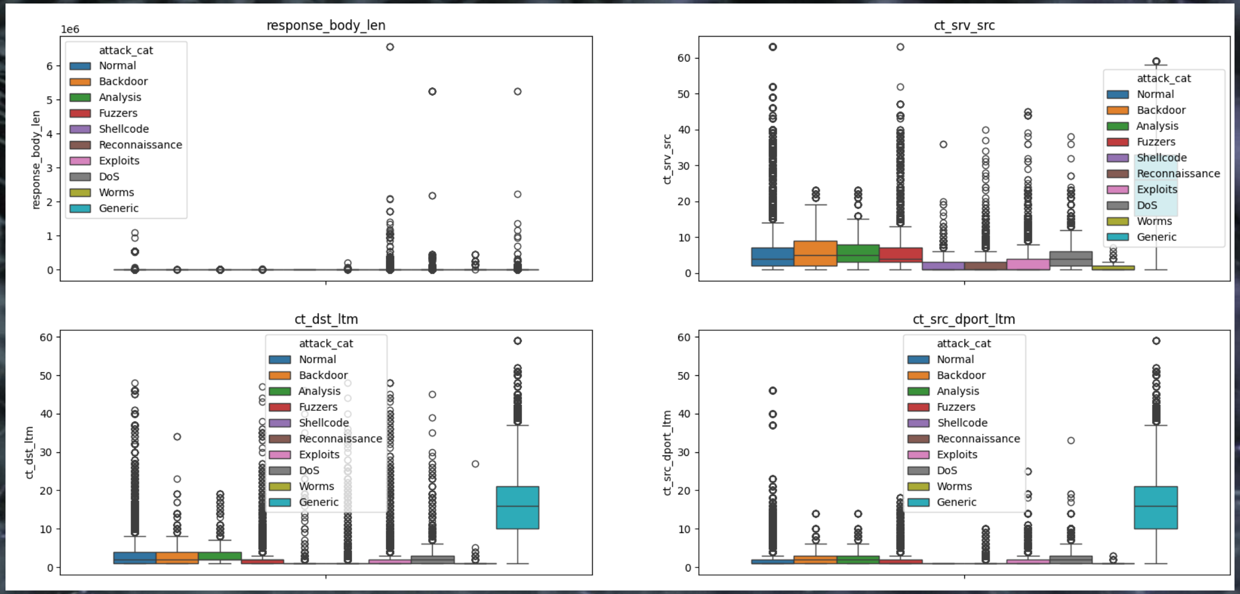
Numeric Features

- Box plot – visualize IQR distribution of continuous features

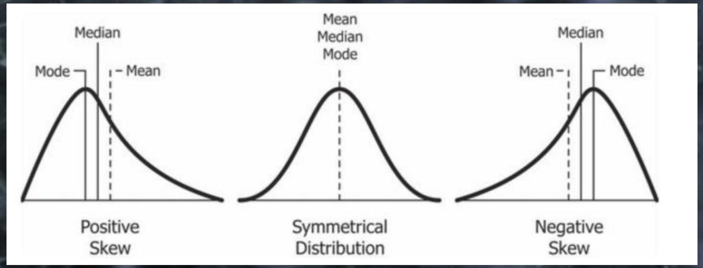
Binary



Multiclass



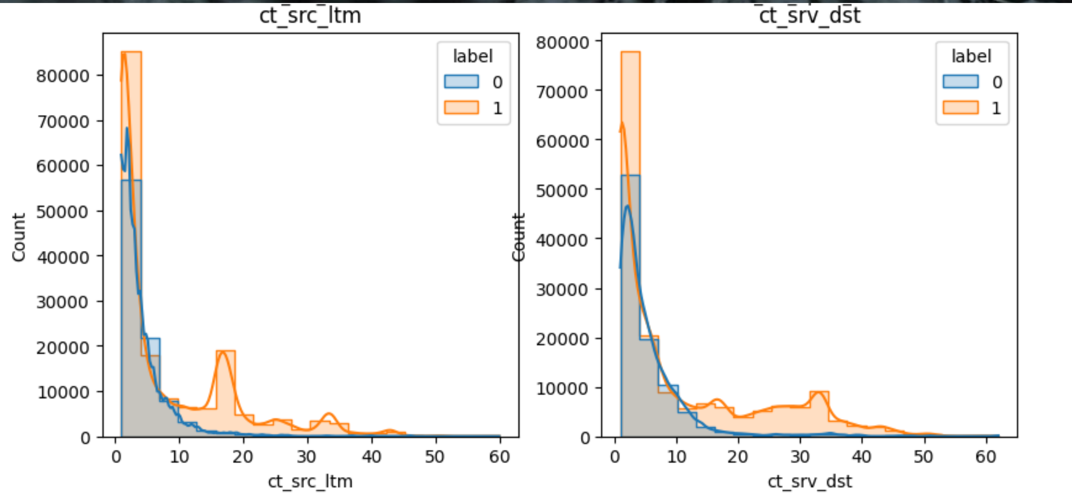
EDA UNSW-NB15



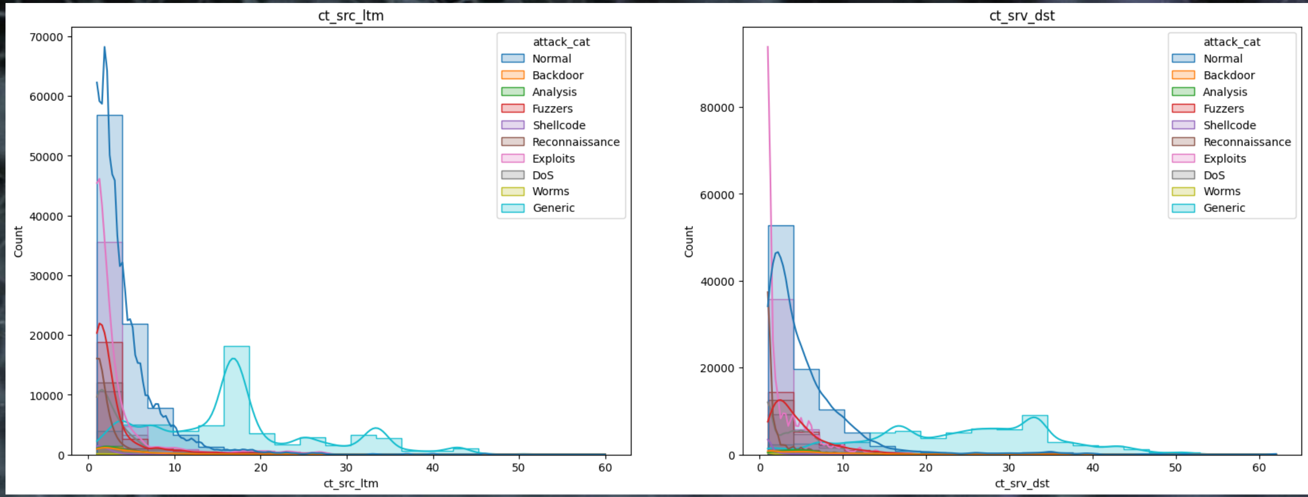
Numeric Features

- Histogram – distribution of numeric features
  - Distribution of data with different bin sizes to see other patterns
  - Identify peaks
  - Skewness detection (left, right, normal)

Binary (Skewed right)



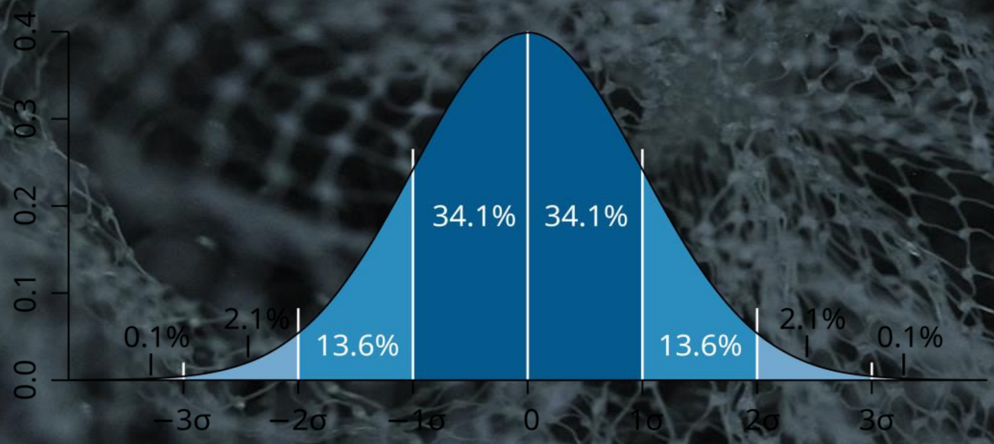
Muti-class (Skewed right)

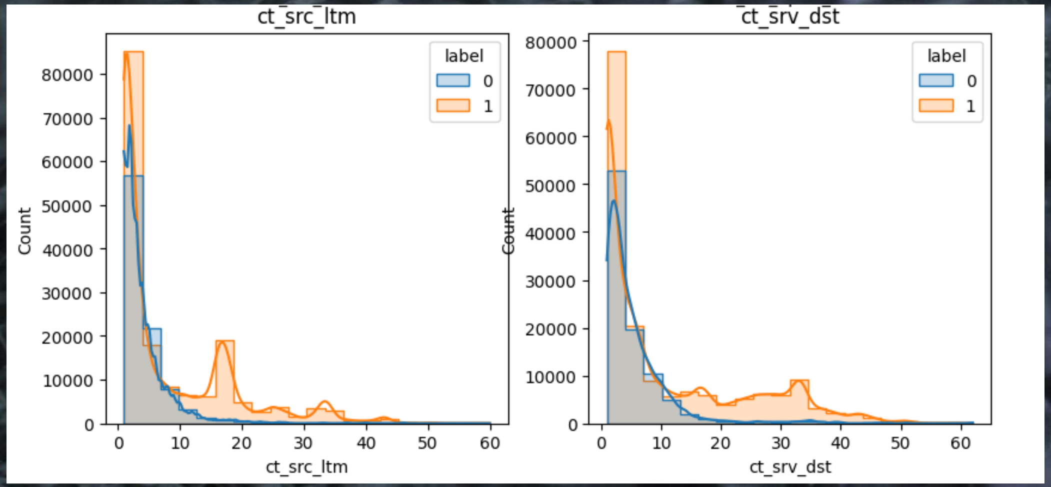


EDA UNSW-NB15

Numeric Features

- STD – how data points deviate from the mean





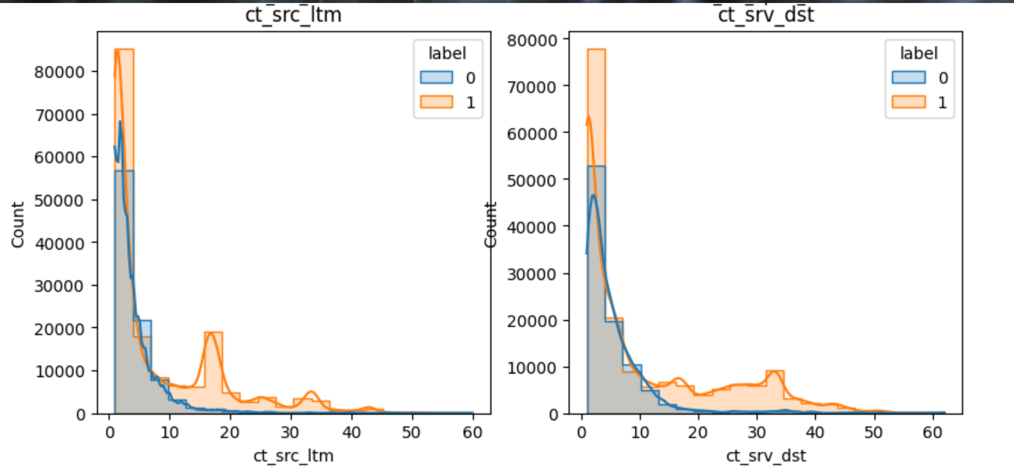

```
# STD
print(f"STD: {data['all']['ct_src_ltm'].std()}")
[45] ✓ 0.0s
··· STD: 8.396266203511304
```

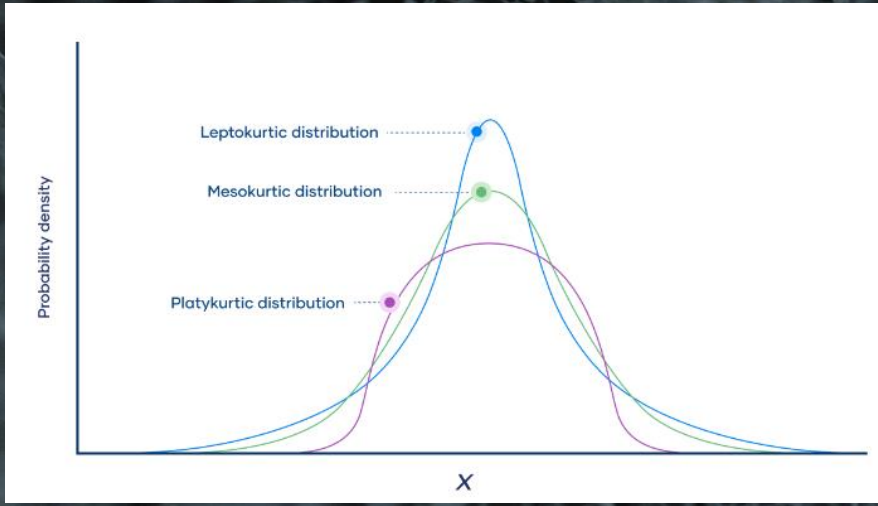
STD 8.4 – high variability in the data

EDA UNSW-NB15

Numeric Features

- Kurtosis – measure shape and tail of data (3 – normal distribution, excess kurtosis 0)
  - Platykurtic – low kurtosis (thin tails)
  - Mesokurtic – medium kurtosis (medium tails)
  - Leptokurtic – high kurtosis (fat tails)





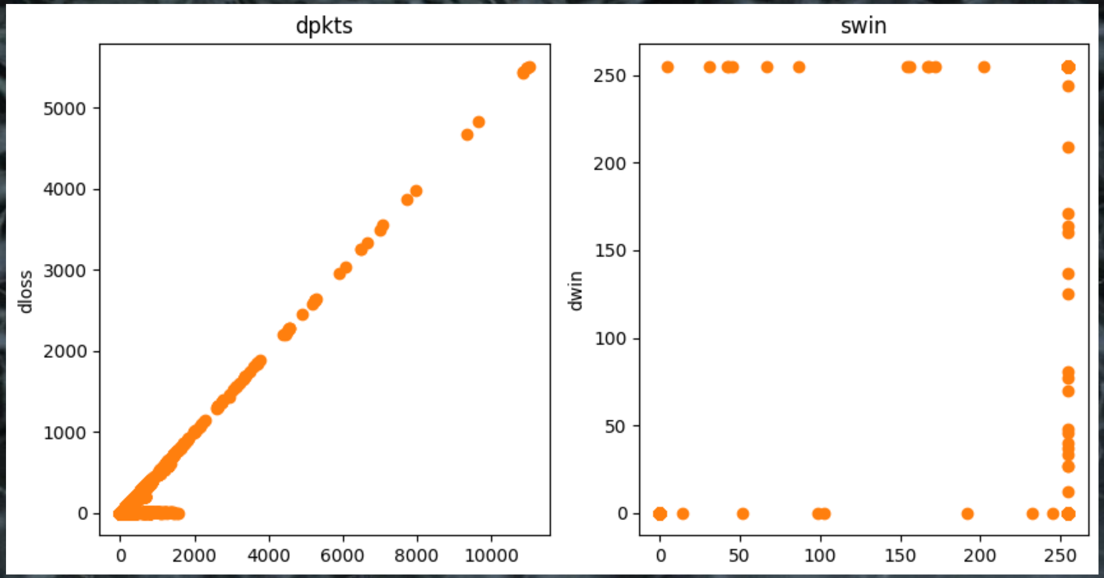

```
# Kurtosis
print(f"Kurtosis: {data['all']['ct_src_ltm'].kurt()}")
[44] ✓ 0.0s
... Kurtosis: 4.085590083858209
```

Kurtosis 4.09 – fat tails (leptokurtic)

EDA UNSW-NB15

Numeric Features

- Scatter plot – relationship between two numerical features
  - Correlation: strong/weak, linear/non-linear
  - Identify outliers
  - Distribution understanding – spread, cluster



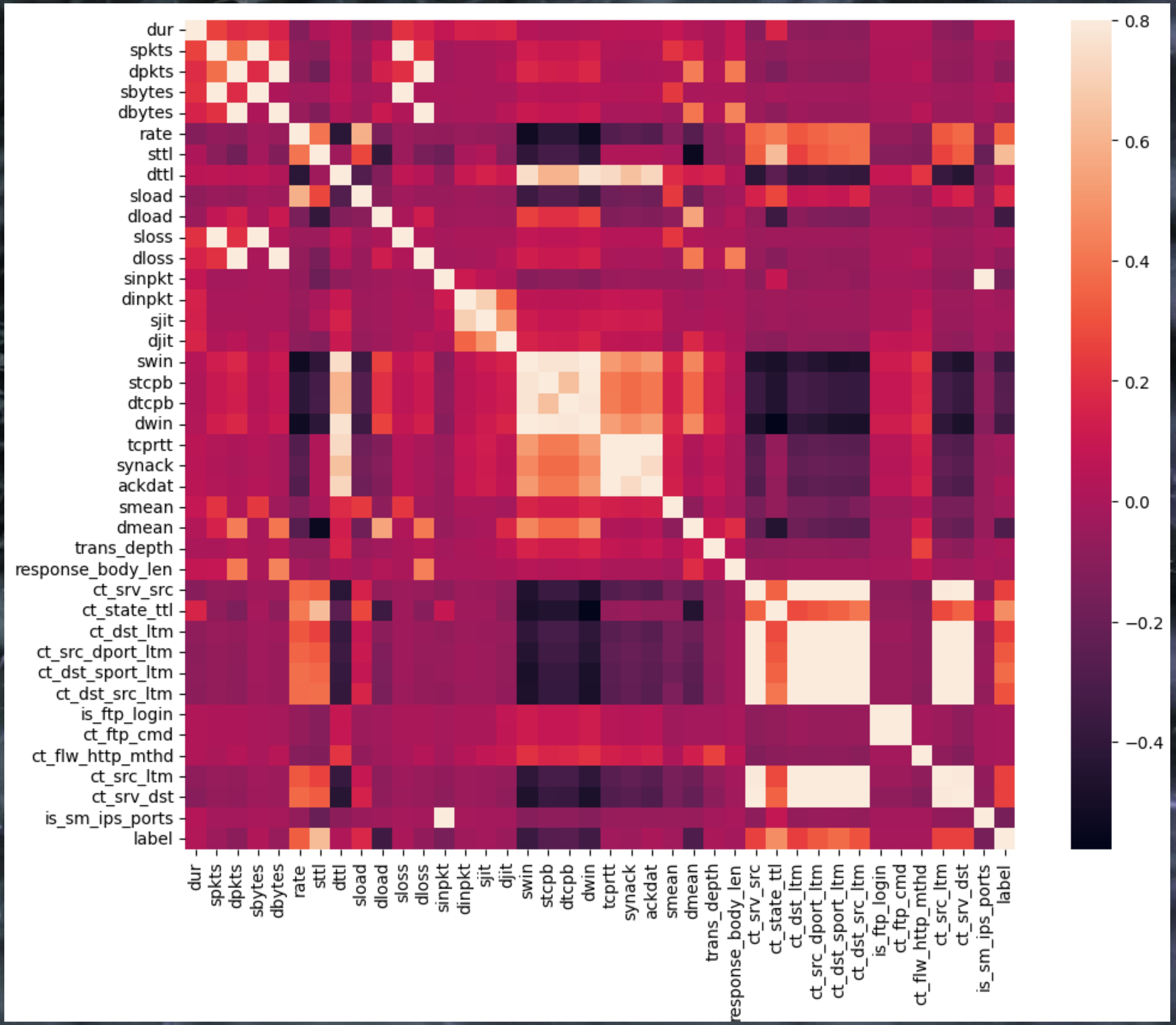
EDA UNSW-NB15

Numeric Features

- Correlation matrix
  - Understanding of feature relationship (
    0-weak, -1 strong negative, +1 strong positive
  - Important for feature selection

- Methods
  - Pearson – linear relationship between 2 numeric features
  - Spearman – monotonic relationship, increasing or decreasing between 2 variables using ranked data

Pearson linear correlation



EDA UNSW-NB15

Brief Summary

- Secure protocols such as SSH has low number of attacks
- DNS protocol has many ‘Generic’ attacks
- Most of the normal traffic appear in FIN state (session finished)
- Many attacks during INT - session initialization sate
- Most lieanrly correlated features:
  [sbytes, sloss], [dpkts, dbytes, dloss], [sttl, ct_state_ttl, label], [stime, dtime], [tcprtt, synack, ackdat], [ct_srv_src, ct_dst_src_ltm, ct_srv_dst], [ct_dst_ltm, ct_src_ltm, ct_src_dport_ltm, ct_dst_sport_ltm]
- Feature **dload** has highest correlation with target

DATA PREPROCESSING

UNSW-NB15

DATA PRE-PROCESSING UNSW-NB15

Clean Data:

- Fill missing values (median – for skewed data)
- Remove duplicates
- Drop highly correlated features
  Note: For detailed info, please, visit this the article in Medium.
  - Redundancy
  - Multicollinearity – may affect linear models
  - Computation efficiency
  - Model interpretability – complex to interpret importance of highly correlated features
  - Feature importance stability – small change in dataset can lead to significant variations in feature importance

```
# Select highly correlated features
corr_matrix = temp_data.corr().abs()
# Select upper triangle of correlation matrix
upper = corr_matrix.where(np.triu(np.ones(corr_matrix.shape), k=1).astype(bool))
# Find index of feature columns with correlation greater than 0.9
to_drop = [column for column in upper.columns if any(upper[column] > 0.95)]
print(to_drop)
```

[87] ✓ 1.2s

```
['sbytes', 'dbytes', 'sloss', 'dloss', 'dwin', 'ct_src_dport_ltm', 'ct_dst_src_ltm', 'ct_ftp_cmd', 'ct_srv_dst']
```

DATA PRE-PROCESSING UNSW-NB15

Feature Engineering

- Create new features
  Combine source and destination data bytes to single column

```
# combine source and destination bytes
data2['sd_bytes'] = data2['sbytes'] + data2['dbytes']
data2.shape
```

✓ 0.0s

```
(162745, 45)
```

EDA UNSW-NB15

Scaling Data

- Standard Scaler

$$z = \frac{x - \mu}{\sigma}$$

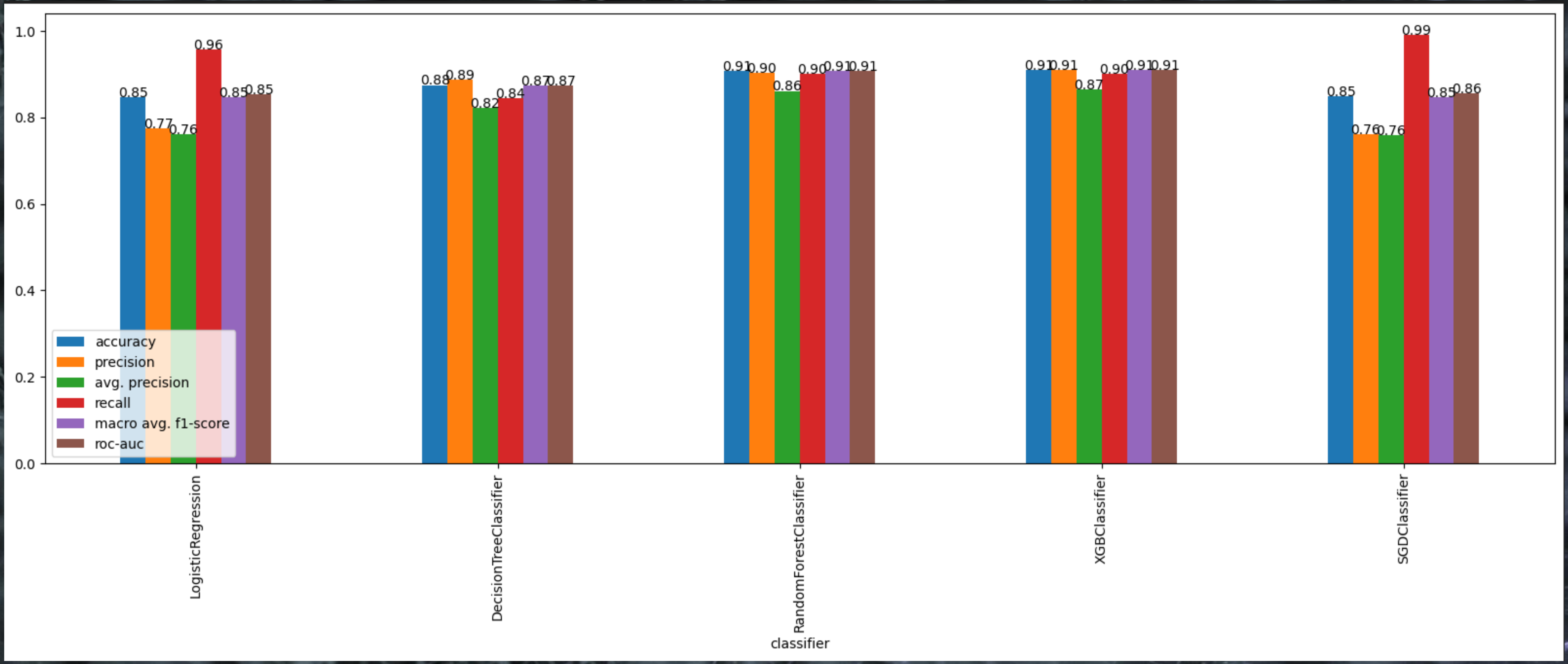
  - Applied for numerical features
  - All columns will be standardized with mean 0 and std 1
    Important for scale sensitive algorithms such as SVM and KNN
  - Performance – better performance with scaled data

- One-hot encoder
  - Encodes categorical features
  - Allows to use ML models that require numeric input
  - Avoids ordinality problem. E.g. Monday/Tuesday/etc. as 1,2,3
  - Disadvantage – increasing dimensionality

ML MODELS

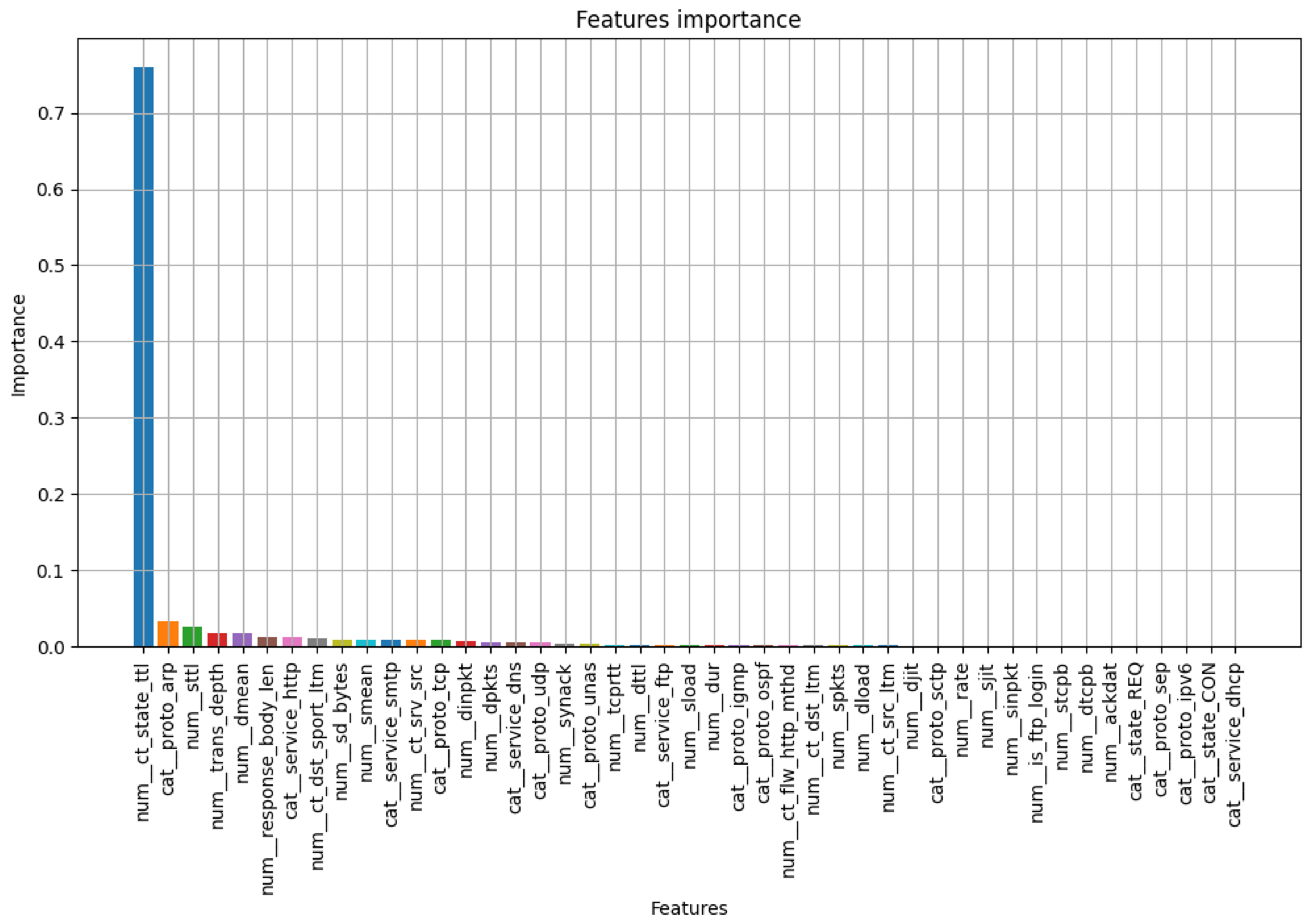
UNSW-NB15

ML MODELS



	classifier	accuracy	precision	avg. precision	recall	macro avg. f1-score	roc-auc
0	LogisticRegression	0.847543	0.774037	0.761353	0.957767	0.846995	0.853049
1	DecisionTreeClassifier	0.875022	0.886727	0.822291	0.843987	0.874307	0.873471
2	RandomForestClassifier	0.907808	0.903845	0.861377	0.901266	0.907540	0.907482
3	XGBClassifier	0.910020	0.909167	0.865608	0.899969	0.909723	0.909518
4	SGDClassifier	0.848182	0.760782	0.758250	0.991180	0.846918	0.855325

FEATURE IMPORTANCE - XGBOOST



EVALUATION METRICS

F1-Score

- $F1 = \frac{2 \cdot precision \cdot recall}{precision + recall}$
- Harmonic mean of precision and recall
- Useful when you want to consider both false positives and false negatives

Recall – True Positive Rate

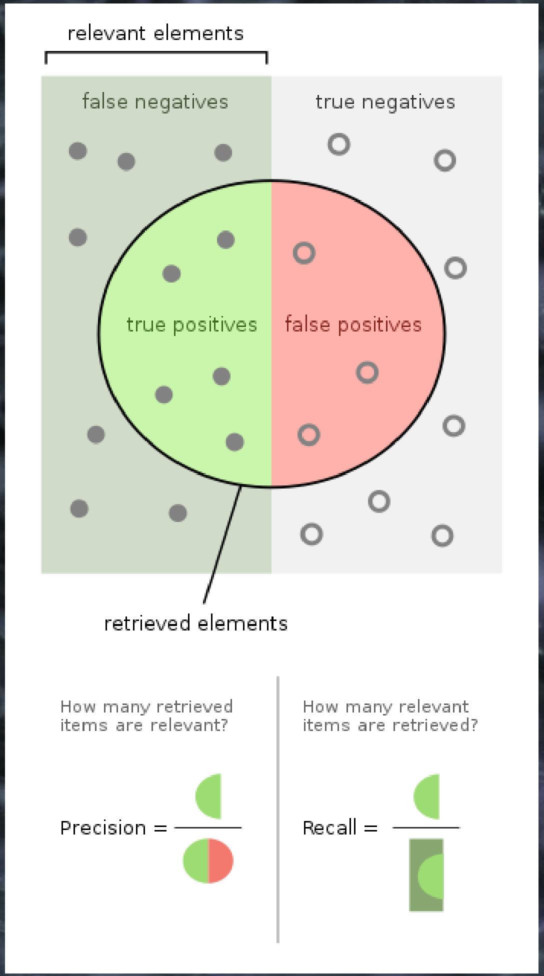
- $Recall = \frac{True\ Positives}{True\ Positives + Flase\ Negatives}$
- Proportion of actual positive cases correctly predicted by model (hit rate)

Precision – Positive Predictive Value

- $Precision = \frac{True\ Positives}{True\ Positives + Flase\ Positives}$
- Proportion of actual positive cases that are actually positive.

Accuracy – Positive Predictive Value

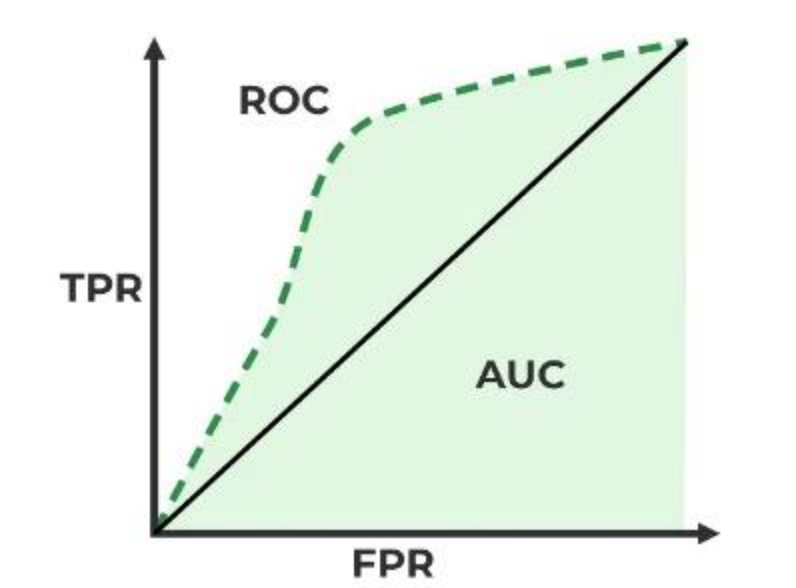
- $Accuracy = \frac{True\ Positives + True\ Negatives}{Total\ Samples}$
- Overall correctness of the model



EVALUATION METRICS

ROC-AUC

- Range from 0 to 1 (0.5 – random match, 1 – perfect match)
- Higher value better performance
- ROC-AUC shows how well the classifier distinguish between 2 classes



SUMMARY

FUTURE WORK

- Use other data set such as KDD, NSL-KDD, 2017-SUEE, etc.
- Multi-class classification
- Experiment with unsupervised learning, such as K-means, DBSCAN
- Enhance feature engineering
- Reduce feature span: PCA, t-SNE, Auto-Encoder
- Use more advanced technics – LDA, LSTM, GANs, Graph Based approach

REFERENCES

REFERENCES

- Nour Moustafa, Jill Slay. UNSW-NB15: A Comprehensive Data set for Network Intrusion Detection systems
  Military Communications and Information Systems Conference (MilCIS), 2015. IEEE, 2015

- Nour Moustafa, Jill Slay.
  The evaluation of Network Anomaly DetectionSystems: Statistical analysis of the UNSW-NB15data set and the comparison with the KDD99 dataset
  Information Security Journal: A Global Perspective (2016)

- Shweta More, Moad Idrissi, Haitham Mahmoud and A. Taufiq Asyhari.
  Enhanced Intrusion Detection Systems Performance with UNSW-NB15 Data Analysis
  Faculty of Computing, Birmingham City University and Department of Data Science, Monash University, Indonesia. February 2024

- Subrata Maji
  Building an Intrusion Detection System on UNSW-NB15 Dataset Based on Machine Learning Algorithm
  Medium, Sep 19, 2020

- Christian Cawley. Top data breaches and cyber attacks in 2024
  TechRadar, May 22, 2024

- CheckPoint - Live Cyber Threat Map

- Check Point Team. Shifting Attack Landscapes and Sectors in Q1 2024 with a 28% increase in cyber attacks globally
  Check Point Blog. *April 10, 2024*

- Zeinab Zoghi and Gursel Serpen.
  UNSW-NB15 Computer Security Dataset: Analysis through Visualization
  Electrical Engineering & Computer Science, University of Toledo, Ohio, USA. 27 June, 2023

- Pictures: Photo by Uriel SC on Unsplash

THANK YOU