IOT Security Gateway

Intrusion Detection In IOT Nets

Intelligent
Embedded
Systems Lab

universität freiburg

How detection is done?

Methods and Models

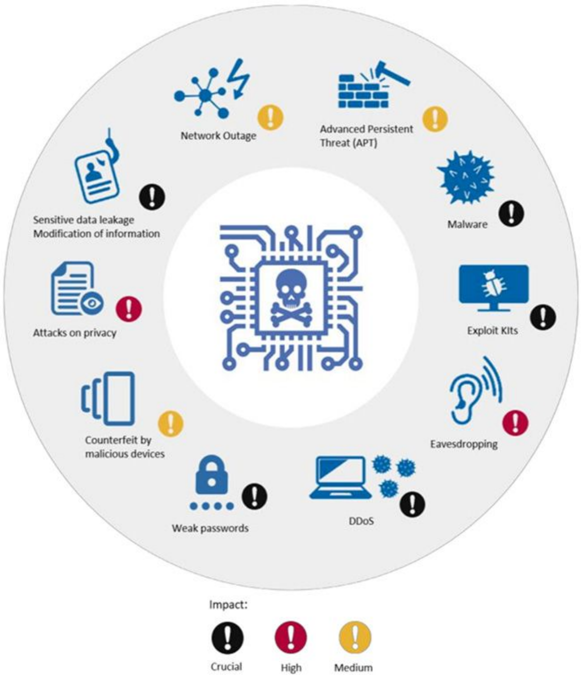
Results

References

Intelligent Embedded Systems Lab

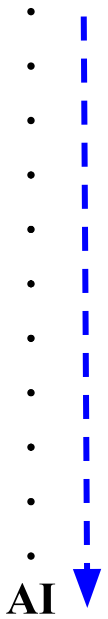
universität freiburg

How detection is done?

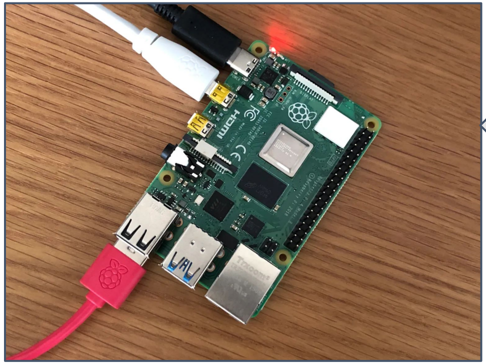


[1]

- Heuristic Analysis
- Signature-Based Detection



Real and Infected IOT Devices



[6]

[6]

3 Real IOT Devices : [4]

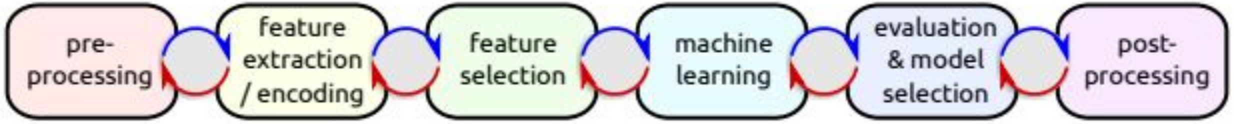
- Philips HUE smart LED lamp
- Amazon Echo home intelligent personal assistant
- Somfy smart doorlock

[4]

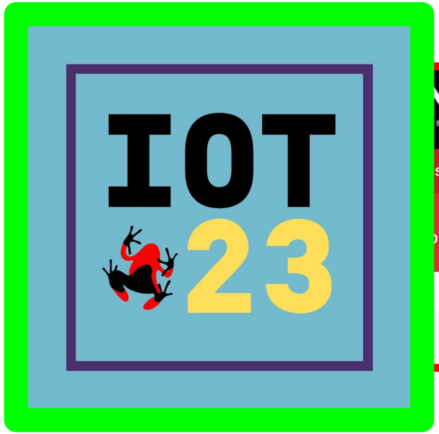
[4]

[4]

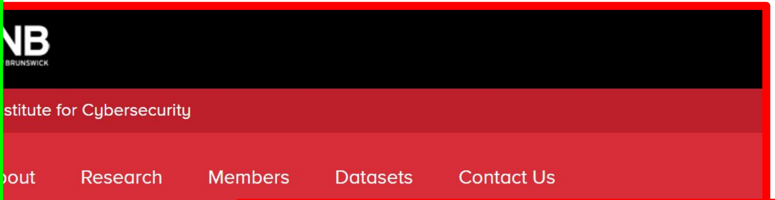
ML design cycle



Dataset Selection



[4]



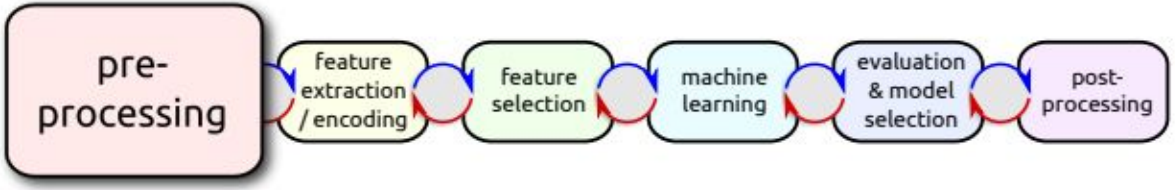
[2]

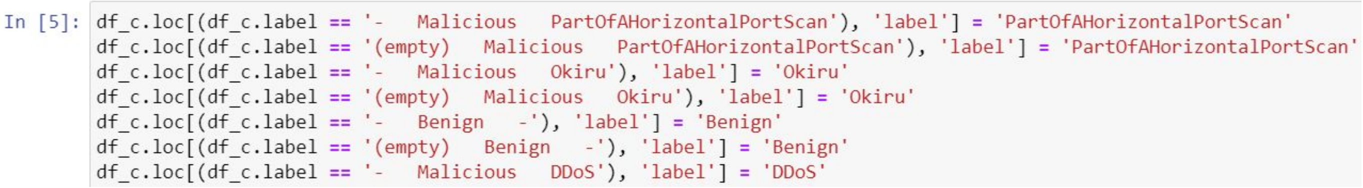
IoT Traffic Generation Patterns Dataset

Traffic Generation Patterns of 10000 IoT devices (incl. Attributes of Devices)

[3]

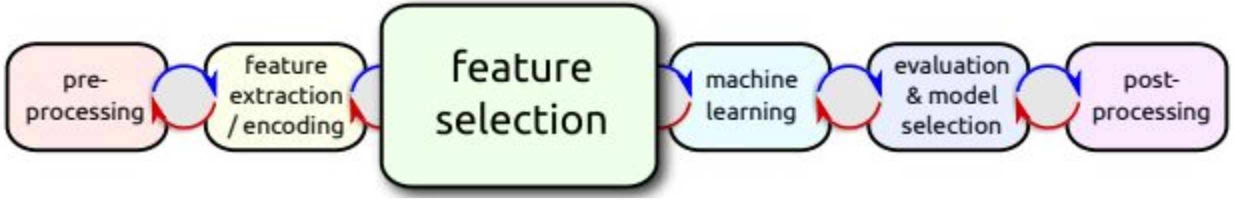
Pre-processing

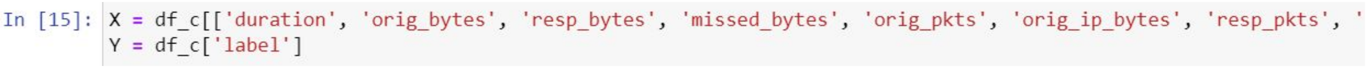




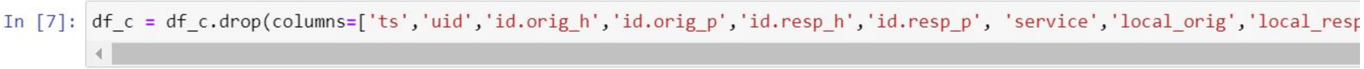
```
In [5]: df_c.loc[(df_c.label == '-   Malicious   PartOfAHorizontalPortScan'), 'label'] = 'PartOfAHorizontalPortScan'
        df_c.loc[(df_c.label == '(empty)   Malicious   PartOfAHorizontalPortScan'), 'label'] = 'PartOfAHorizontalPortScan'
        df_c.loc[(df_c.label == '-   Malicious   Okiru'), 'label'] = 'Okiru'
        df_c.loc[(df_c.label == '(empty)   Malicious   Okiru'), 'label'] = 'Okiru'
        df_c.loc[(df_c.label == '-   Benign   -'), 'label'] = 'Benign'
        df_c.loc[(df_c.label == '(empty)   Benign   -'), 'label'] = 'Benign'
        df_c.loc[(df_c.label == '-   Malicious   DDoS'), 'label'] = 'DDoS'
```

Feature selection



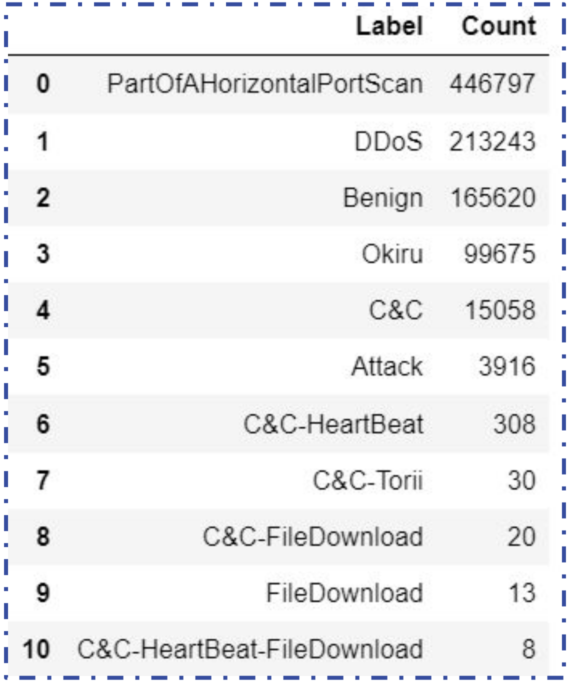


```
In [15]: X = df_c[['duration', 'orig_bytes', 'resp_bytes', 'missed_bytes', 'orig_pkts', 'orig_ip_bytes', 'resp_pkts', '
         Y = df_c['label']
```



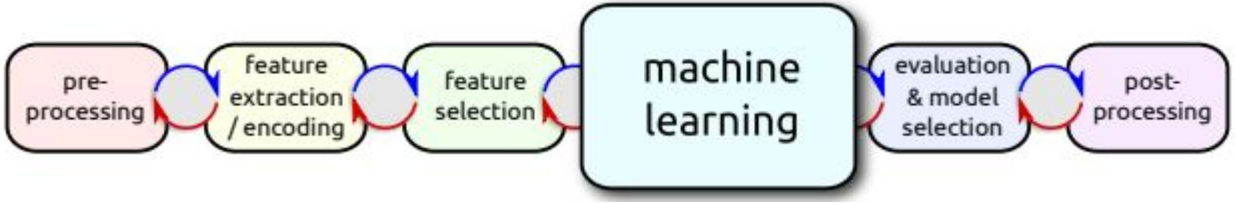
```
In [7]: df_c = df_c.drop(columns=['ts','uid','id.orig_h','id.orig_p','id.resp_h','id.resp_p', 'service','local_orig','local_resp
```

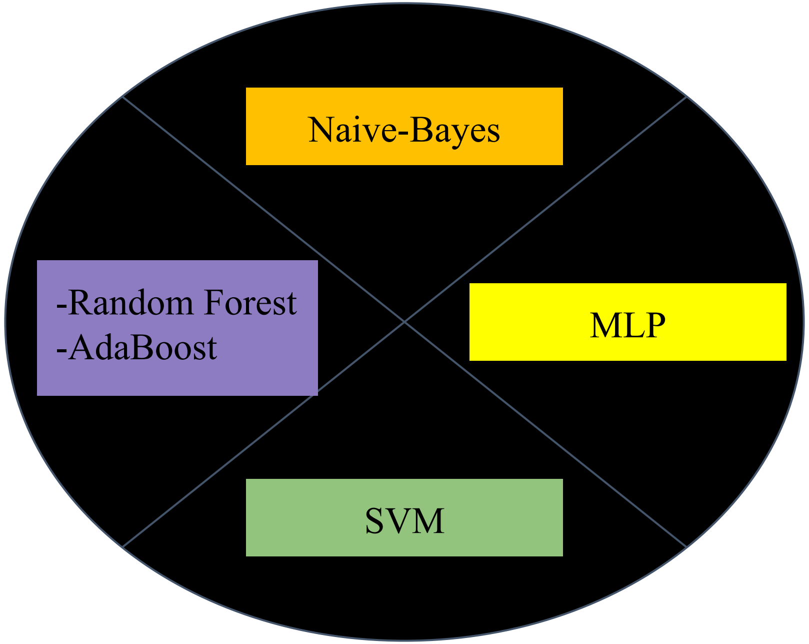
Label overview



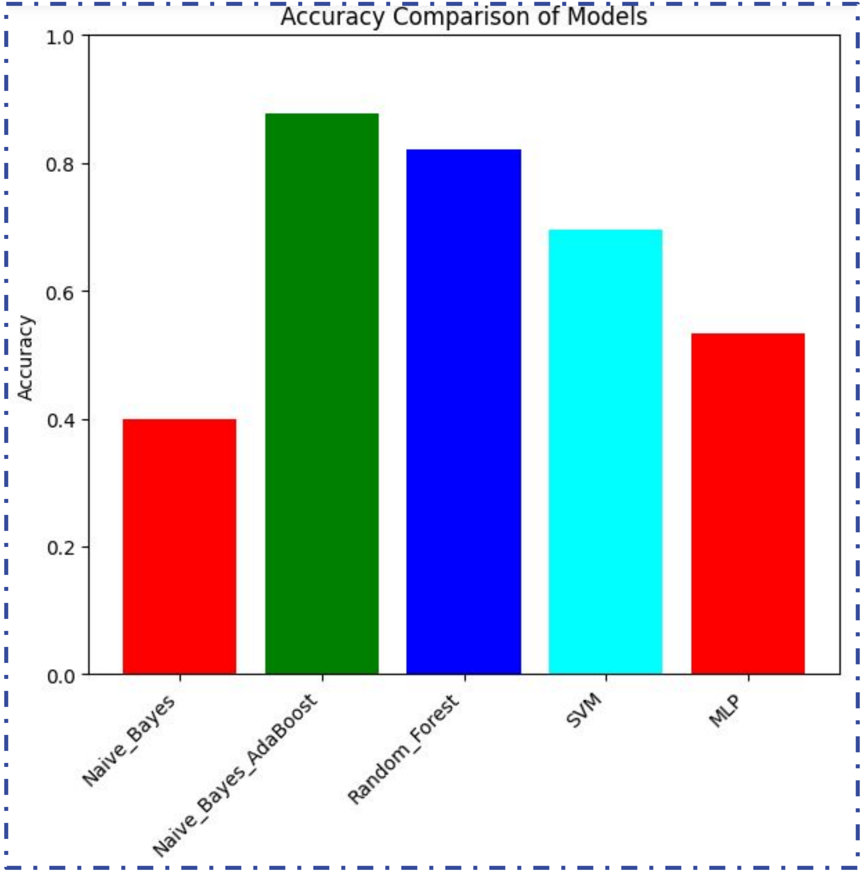
	Label	Count
0	PartOfAHorizontalPortScan	446797
1	DDoS	213243
2	Benign	165620
3	Okiru	99675
4	C&C	15058
5	Attack	3916
6	C&C-HeartBeat	308
7	C&C-Torii	30
8	C&C-FileDownload	20
9	FileDownload	13
10	C&C-HeartBeat-FileDownload	8

Models


pre-processing
feature extraction / encoding
feature selection
machine learning
evaluation & model selection
post-processing

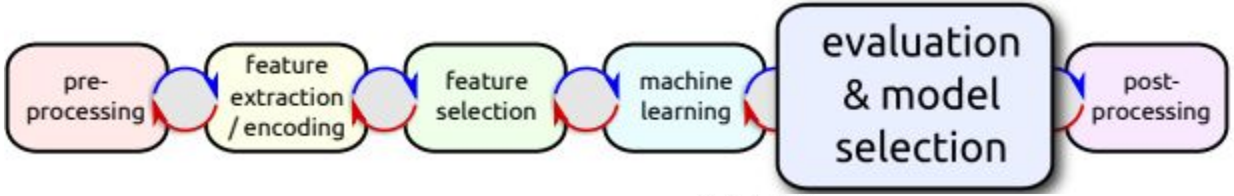

Naive-Bayes
-Random Forest
-AdaBoost
MLP
SVM

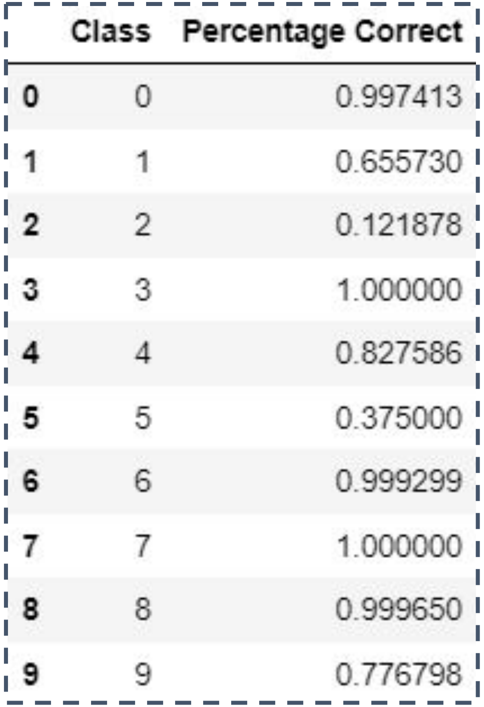
Accuracy and confusion matrix



universität freiburg

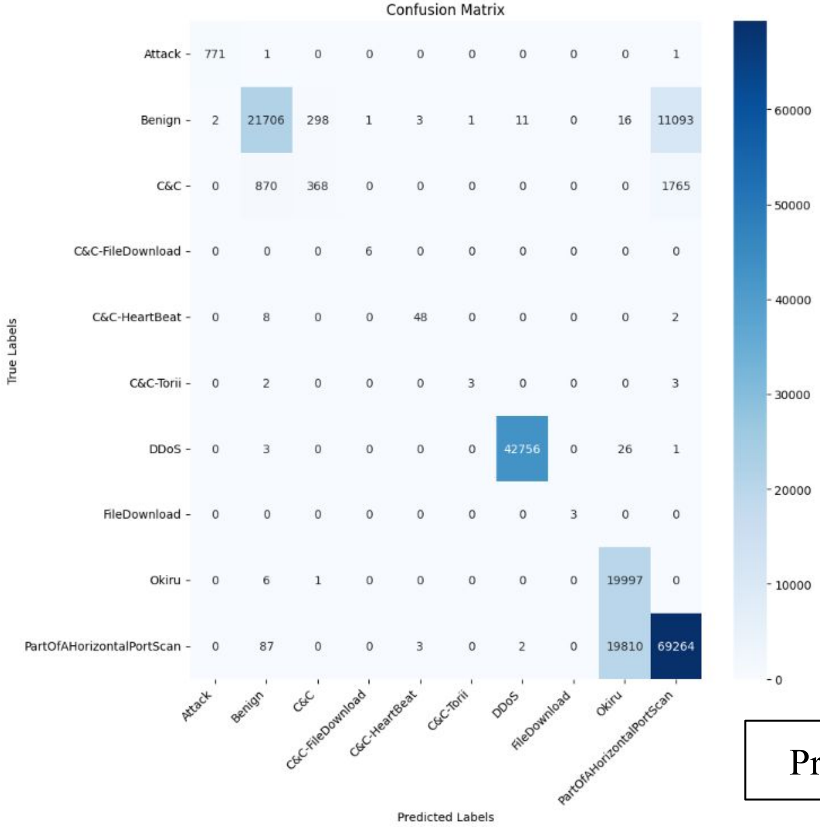
Intelligent Embedded Systems Lab





	Class	Percentage Correct
0	0	0.997413
1	1	0.655730
2	2	0.121878
3	3	1.000000
4	4	0.827586
5	5	0.375000
6	6	0.999299
7	7	1.000000
8	8	0.999650
9	9	0.776798

Random-Forest



Confusion Matrix

	Attack	Benign	C&C	C&C-FileDownload	C&C-HeartBeat	C&C-Torii	DDoS	FileDownload	Okiru	PartOfAHorizontalPortScan
Attack	771	1	0	0	0	0	0	0	0	1
Benign	2	21706	298	1	3	1	11	0	16	11093
C&C	0	870	368	0	0	0	0	0	0	1765
C&C-FileDownload	0	0	0	6	0	0	0	0	0	0
C&C-HeartBeat	0	8	0	0	48	0	0	0	0	2
C&C-Torii	0	2	0	0	0	3	0	0	0	3
DDoS	0	3	0	0	0	0	42756	0	26	1
FileDownload	0	0	0	0	0	0	0	3	0	0
Okiru	0	6	1	0	0	0	0	0	19997	0
PartOfAHorizontalPortScan	0	87	0	0	3	0	2	0	19810	69264

Prof. Dr. Josif Grabocka

References

1. HD Wallpaper: Codes On A Screen, artificial intelligence, developing, web design | Wallpaper Flare. (n.d.). Retrieved from https://www.wallpaperflare.com/codes-on-a-screen-artificial-intelligence-developing-web-design-wallpaper-aiwog
2. IDS 2018 | Datasets | Research | Canadian Institute for Cybersecurity | UNB. (n.d.). Retrieved from https://www.unb.ca/cic/datasets/ids-2018.html
3. IoT Traffic Generation Patterns Dataset. (2021, November 11). Kaggle. Retrieved from https://www.kaggle.com/datasets/tubitak1001118e277/iot-traffic-generation-patterns
4. IoT-23 Dataset: A labeled dataset of Malware and Benign IoT Traffic. — Stratosphere IPS. (n.d.). Stratosphere IPS. Retrieved from https://www.stratosphereips.org/datasets-iot23
5. Security, H. N. (2017, November 21). Defining and securing the Internet of Things - Help Net Security. Help Net Security. Retrieved from https://www.helpnetsecurity.com/2017/11/22/defining-securing-iot/
6. TechCrunch is part of the Yahoo family of brands. (2019, June 23). Retrieved from https://techcrunch.com/2019/06/23/the-raspberry-pi-foundation-unveils-the-raspberry-pi-4/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAAgi8O8ROYuFBWx1jrJmfR91osTMSci87c-sA-1IU3uTHOYZuEHcwfmRoQUbY1CMkUsHRWHvEhFFmcFhn0LWmdACkBQ1bVLVTkPKvt9lAmI_6QRGNDOfsRRcLJCNR38juUvypqoxL1CmGCkga9Q2BpZwasZwgDxhqu5oFK4DYUEm

Questions

Thank YOU

Intelligent Embedded Systems Lab

universität freiburg