IOT Security Gateway

Intrusion Detection In IOT Nets

Sakshi Kulkarni **Vishal Sivakumar**

Supervisor - Prof. Dr.-Ing. Axel Sikora

Intelligent Embedded Systems Lab

universität freiburg

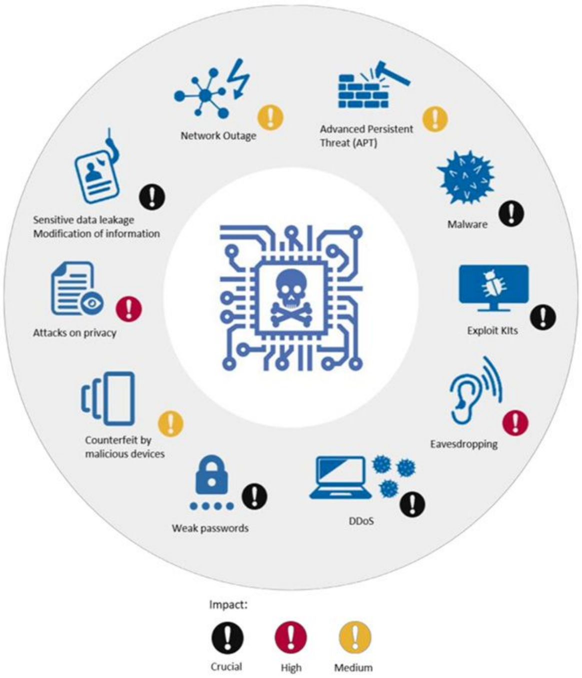
How detection is done?

Methods and Models

Results

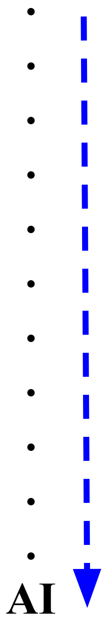
References

How detection is done?



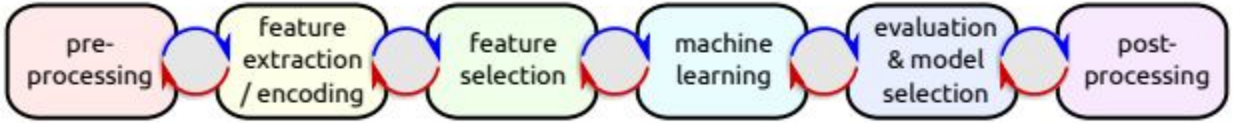
[1]

- Heuristic Analysis
- Signature-Based Detection



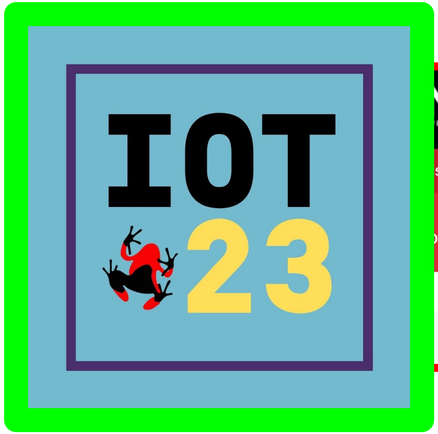
AI

ML design cycle

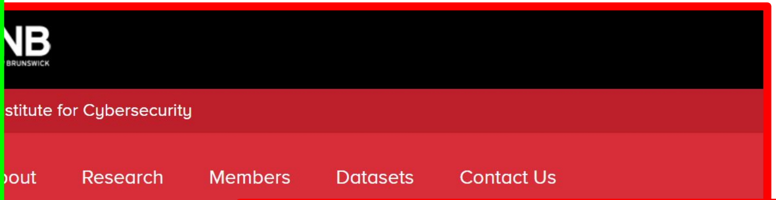


[7]

Dataset Selection



[4]



stitute for Cybersecurity

out Research Members Datasets Contact Us

[2]

TUBITAK1001-118E277 AND 1 COLLABORATOR · UPDATED 2 YEARS AGO

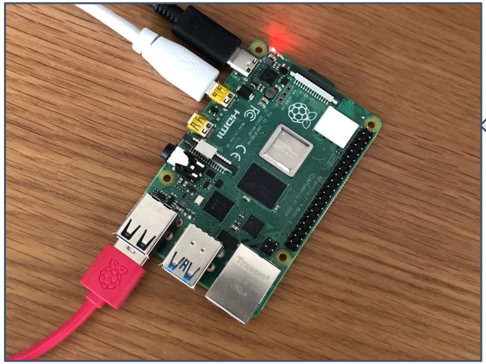
IoT Traffic Generation Patterns Dataset

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

Data Card Code (1) Discussion (0)

[3]

Real and Infected IOT Devices



[6]

[6]

3 Real IOT Devices : [4]

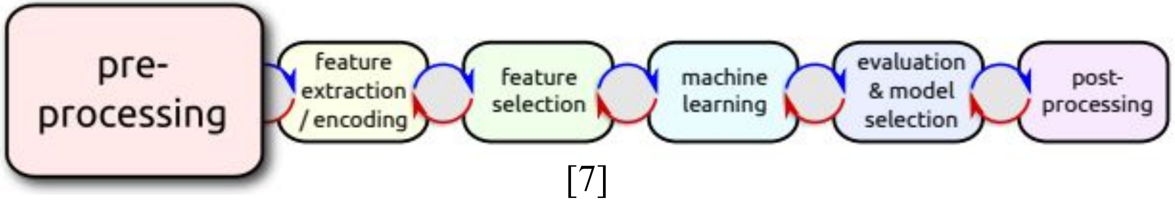
- Philips HUE smart LED lamp
- Amazon Echo home intelligent personal assistant
- Somfy smart doorlock

[4]

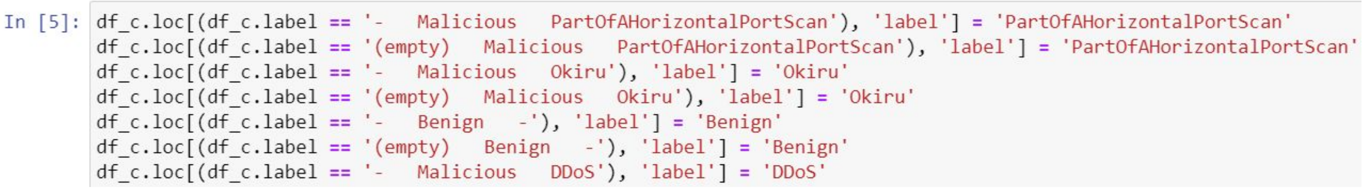
[4]

[4]

Pre-processing

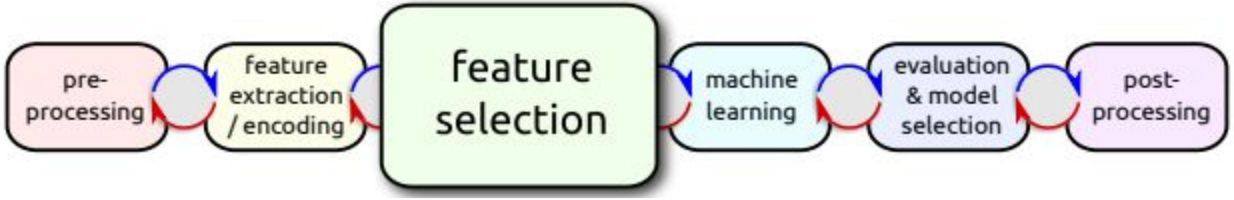


[7]



```
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



pre-processing

feature extraction / encoding

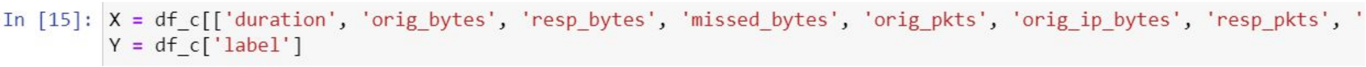
feature selection

machine learning

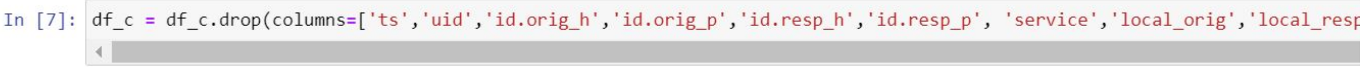
evaluation & model selection

post-processing

[7]

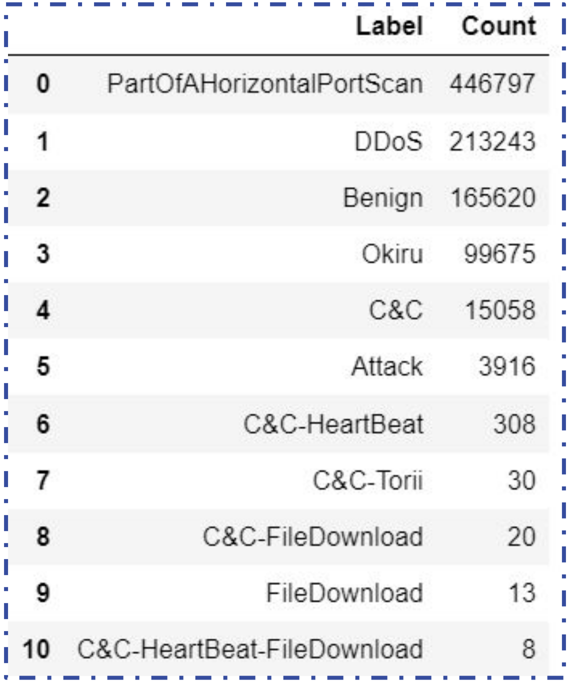


```
In [15]: X = df_c[['duration', 'orig_bytes', 'resp_bytes', 'missed_bytes', 'orig_pkts', 'orig_ip_bytes', 'resp_pkts', '
         Y = df_c['label']
```



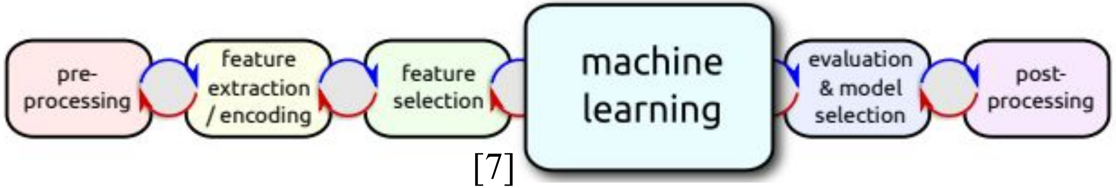
```
In [7]: df_c = df_c.drop(columns=['ts','uid','id.orig_h','id.orig_p','id.resp_h','id.resp_p', 'service','local_orig','local_resp
```

Label overview

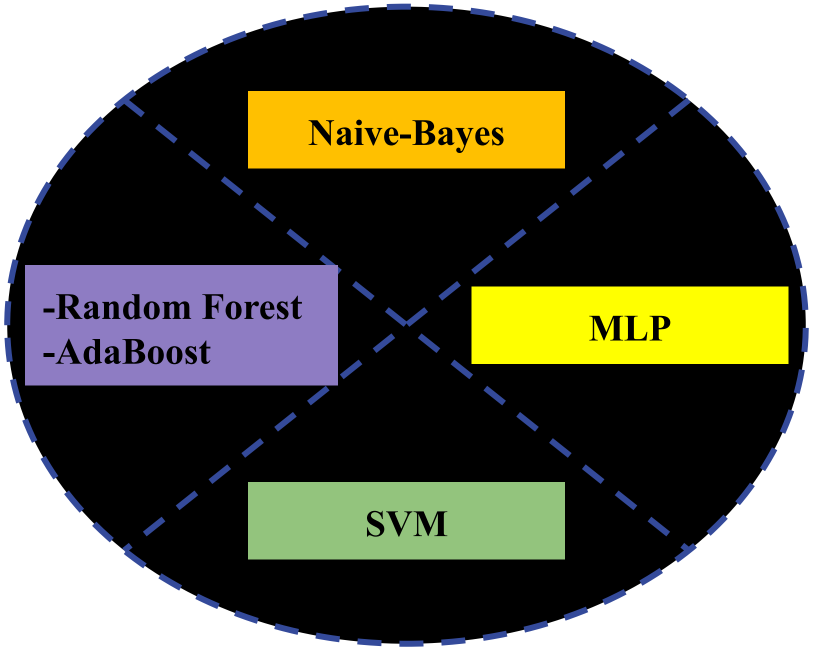


	Label	Count
0	PartOfAHorizontalPortScan	446797
1	DDoS	213243
2	Benign	165620
3	Okiru	99675
4	C&C	15058
5	Attack	3916
6	C&C-HeartBeat	308
7	C&C-Torii	30
8	C&C-FileDownload	20
9	FileDownload	13
10	C&C-HeartBeat-FileDownload	8

Models



[7]



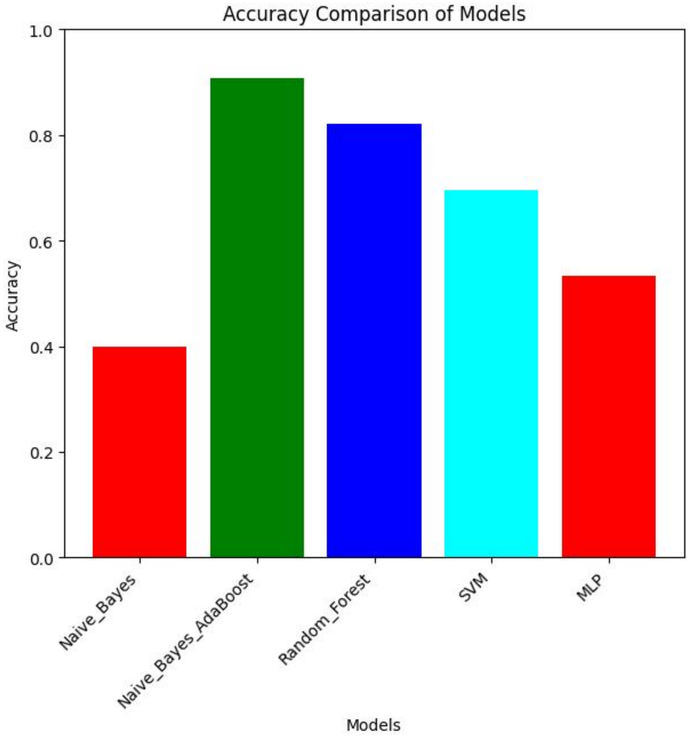
Naive-Bayes

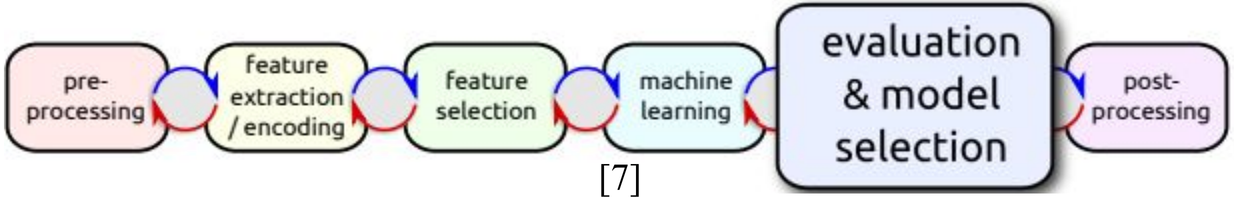
-Random Forest
-AdaBoost

MLP

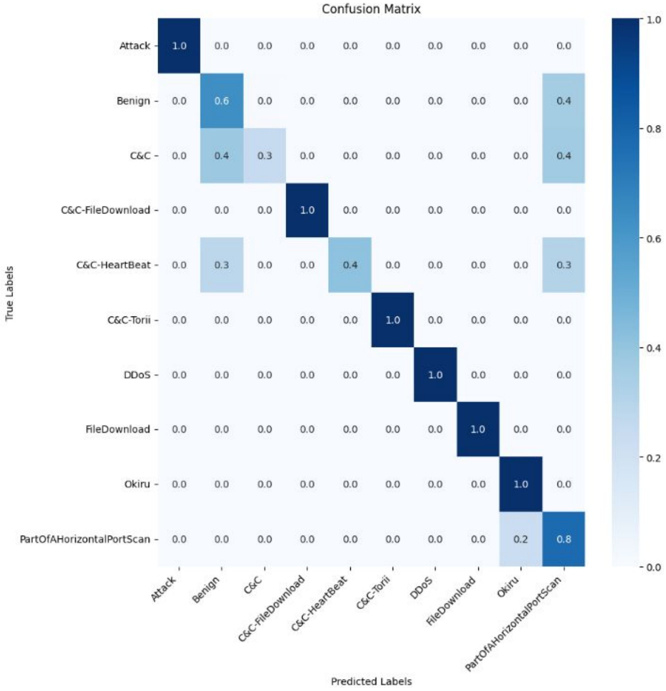
SVM

Accuracy and confusion matrix





[7]



	Attack	Benign	C&C	C&C-FileDownload	C&C-HeartBeat	C&C-Torii	DDoS	FileDownload	Okiru	PartOfAHorizontalPortScan
Attack	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Benign	0.0	0.6	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.4
C&C	0.0	0.4	0.3	0.0	0.0	0.0	0.0	0.0	0.0	0.4
C&C-FileDownload	0.0	0.0	0.0	1.0	0.0	0.0	0.0	0.0	0.0	0.0
C&C-HeartBeat	0.0	0.3	0.0	0.0	0.4	0.0	0.0	0.0	0.0	0.3
C&C-Torii	0.0	0.0	0.0	0.0	0.0	1.0	0.0	0.0	0.0	0.0
DDoS	0.0	0.0	0.0	0.0	0.0	0.0	1.0	0.0	0.0	0.0
FileDownload	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.0	0.0	0.0
Okiru	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.0	0.0
PartOfAHorizontalPortScan	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.2	0.8

Random-Forest

Comparison with the Literature

Model (paper[8])	Accuracy	Model [ours]	Accuracy
Decision Trees	0.73		
Naive Bayes	0.30	Naive Bayes	0.40
SVM	0.69	SVM	0.70 (with reduced labels)
-	-	AdaBoost	0.91
-	-	Random Forest	0.82

Future works

- Having similar or extended features, capture dataset for more attack scenarios.
- Deploy for Real-time Anomaly detection(TinyML).
- Move to Deep Learning Architectures(TinyDL) (if required).

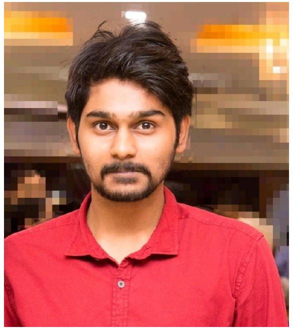
[9]

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
7. Prof. Dr. Josif Grabocka. Lecture, December 2021.
8. Y. Liang. (2021). Anomaly Detection in IoT-23 Dataset. [Online]. Available: https://github.com/yliang725/Anomaly-Detection-IoT23/blob/main/Research%20Paper/Research%20Paper.pdf
9. WorqIQ. (2018, September). Open to Think: Pure Thinking Power. [Online]. Available: https://worqiq.com/2018/09/open-to-think-pure-thinking-power/

Our Team

Prof. Dr. Axel Sikora
(Mentor)



Vishal Sivakumar
(5253589)

Sakshi Kulkarni
(5586550)

Questions

Thank YOU

Intelligent Embedded Systems Lab

universität freiburg