OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG

Design and Implementation of an Intelligent and Model-based Intrusion Detection System for IoT Networks

Laboratory for IT-Security and Compliance
Faculty of Computer Science and Mathematics
OTH Regensburg
University of Applied Sciences Regensburg

FAST-CSP

Peter Vogl
peter.vogl@oth-regensburg.de

Agenda

- About the Speaker
- Motivation
- Architecture of the iIDS
- Data Insights of Network Traffic
- Snorkel
- AI-based Network Data Analysis
- Conclusion and Future Work

Agenda

- About the Speaker
- Motivation
- Architecture of the iIDS
- Data Insights of Network Traffic
- Snorkel
- AI-based Network Data Analysis
- Conclusion and Future Work

About the Speaker

- September 2018 – July 2021
  Business Informatics B.Sc.
  University of Applied Sciences Regensburg

- Since September 2021
  Master of Applied Research (M.Sc.)
  - IoT, IT-Security & Compliance, AI
  University of Applied Sciences Regensburg

Agenda

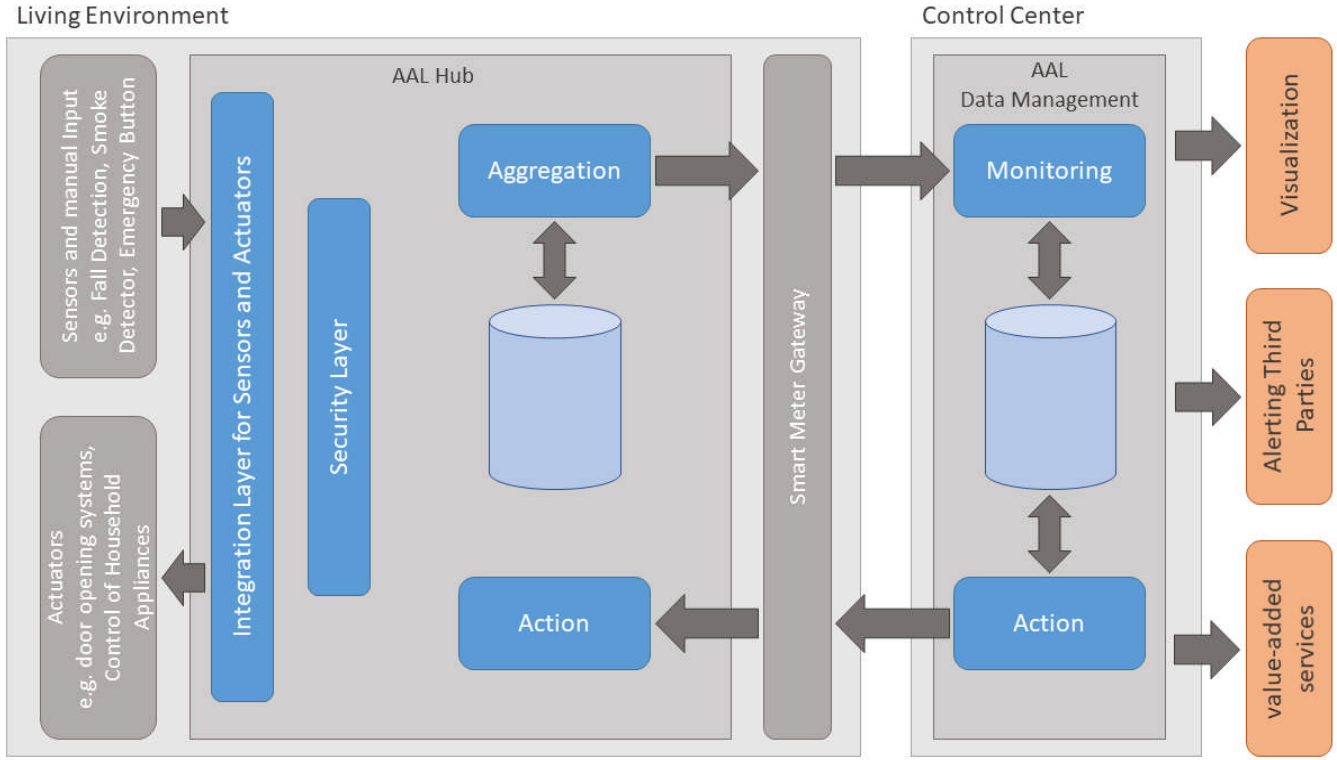
- About the Speaker
- Motivation
- Architecture of the iIDS
- Data Insights of Network Traffic
- Snorkel
- AI-based Network Data Analysis
- Conclusion and Future Work

Previous Work

Architecture of an intelligent Intrusion Detection System for Smart Home

Julian Graf, Katrin Neubauer, Sebastian Fischer, Rudolf Hackenberg
IEEE International Conference on Pervasive Computing and Communications Workshops
23-27 March 2020

Secure Gateway for Ambient Assisted Living (SEGAL)

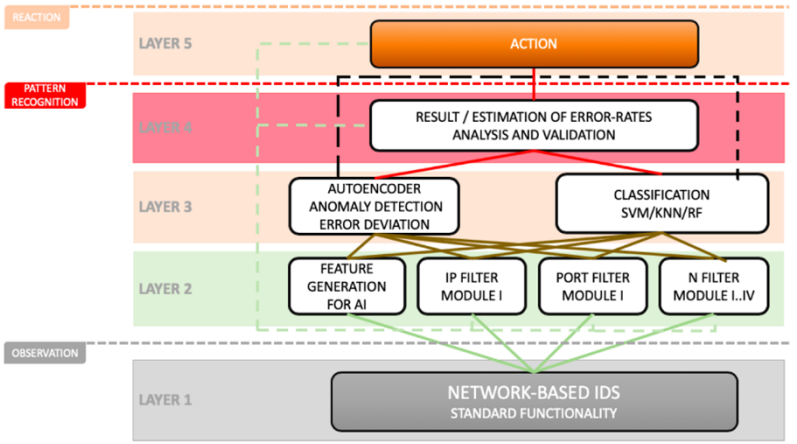


Agenda

- About the Speaker
- Motivation
- Architecture of the iIDS
- Data Insights of Network Traffic
- Snorkel
- AI-based Network Data Analysis
- Conclusion and Future Work

Architecture of the iIDS

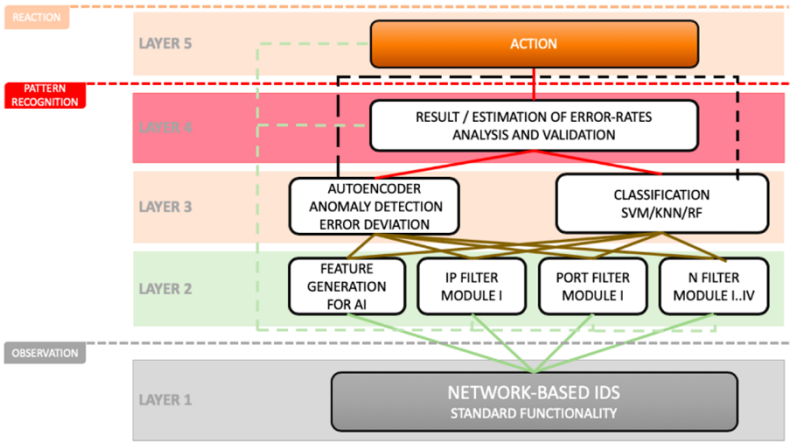
- **Layer 1**
  Packet capturing of WLAN and Bluetooth data with Libpcap / Pcap4J
- **Layer 2**
  Rule-based modules to analyze port and address information and data preparation for the upcoming AI modules
- **Layer 3**
  AI-based modules for anomaly detection and intrusion classification



Architecture of the iIDS

- Layer 4
  Analysis of the return values from the rule-based and AI-based modules to calculate the probability of an intrusion

- Layer 5
  Deployment of countermeasures to prevent or limit damage to the system



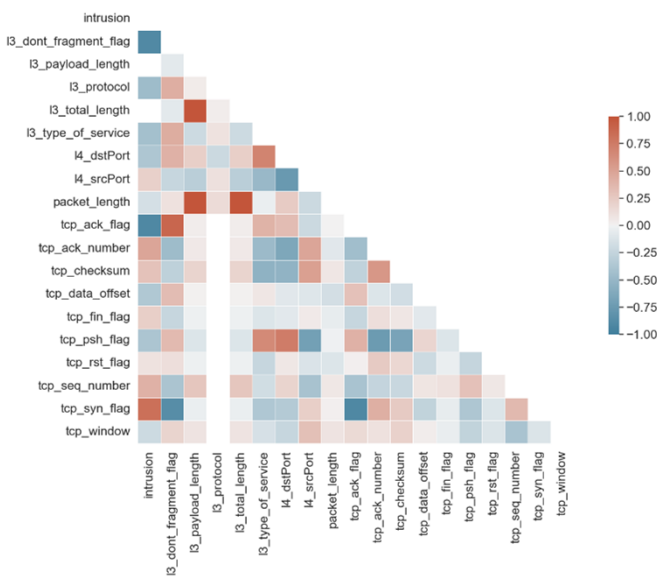
Agenda

- About the Speaker
- Motivation
- Architecture of the iIDS
- Data Insights of Network Traffic
- Snorkel
- AI-based Network Data Analysis
- Conclusion and Future Work

Data Insights

- 52 different header information are collected from the protocols of Layers 2, 3 and 4 of the ISO/OSI model.

- Most important features
  - TCP flags (e.g. Synchronization, Acknowledgment, Reset)
  - Port information (Source and Destination port number)
  - Packet and Payload lengths
  - Type of service (e.g. ICMP packets with a service type 8 for an Echo request)



Agenda

- About the Speaker
- Motivation
- Architecture of the iIDS
- Data Insights of Network Traffic
- Snorkel
- AI-based Network Data Analysis
- Conclusion and Future Work

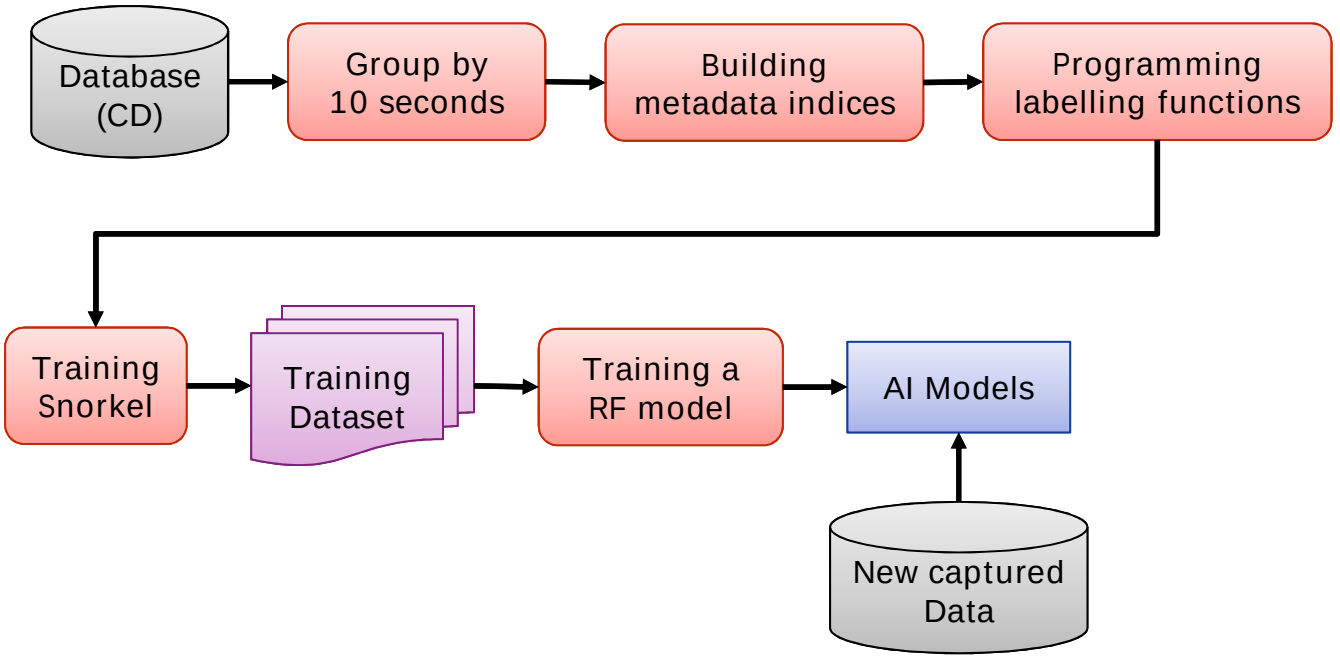
Snorkel

- Developed by Alex Ratner and colleges at the Stanford University since 2015
- Creates training data sets for other AI models
- Based on Tensorboard/Tensorflow 1.5
- Deprecated since late 2020

snorkel

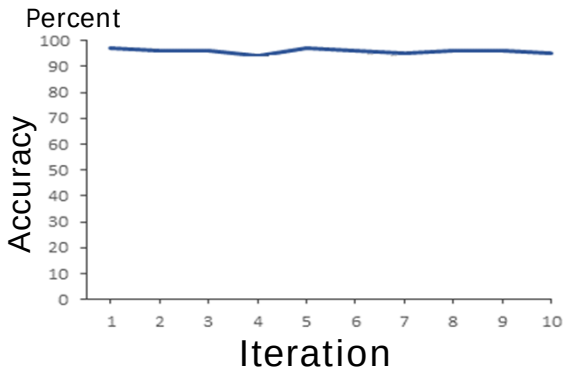
https://www.snorkel.org/

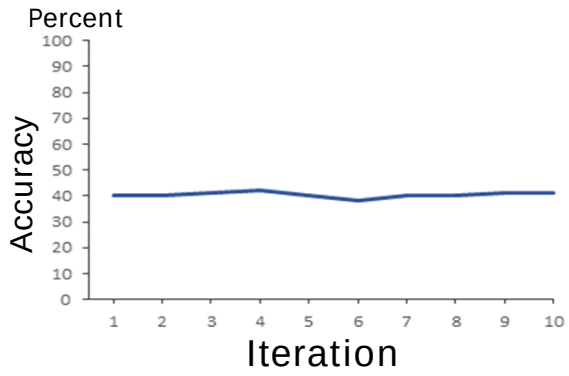
Approach Overview



Labeling Functions

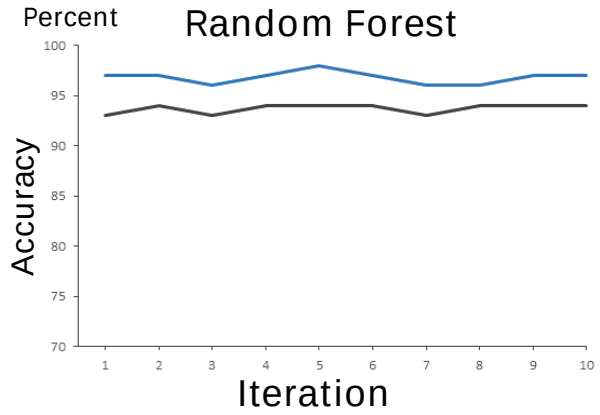
- For each category a separate labelling function is necessary
- Labelling functions have a large influence on the time performance

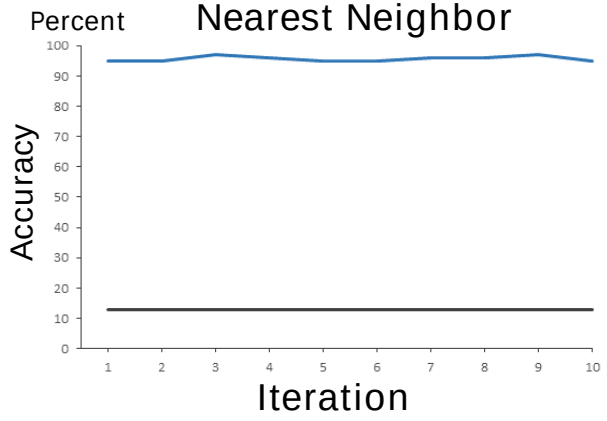




AI Model Training Results

- Snorkel data set is used to train the AI models
- The test of the trained AI models is done with ungrouped captured data
- 5 different AI models are tested
  - Nearest Neighbor
  - Support Vector Machine
  - Logistic Regression
  - Decision Tree
  - Random Forest
- Best Result: Random Forest

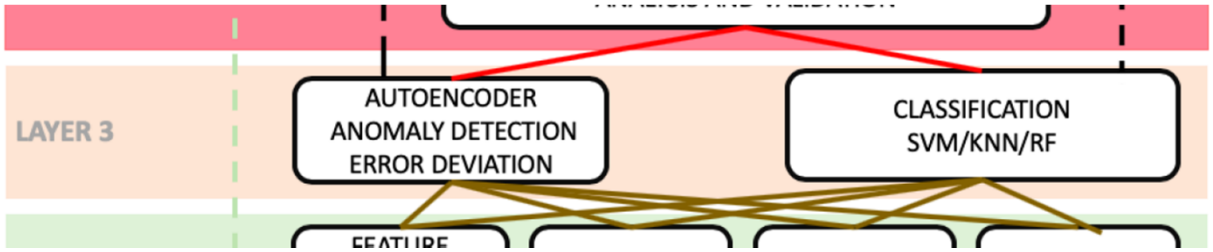




Agenda

- About the Speaker
- Motivation
- Architecture of the iIDS
- Data Insights of Network Traffic
- Snorkel
- AI-based Network Data Analysis
- Conclusion and Future Work

iIDS – Machine Learning Models



Anomaly Detection

Neuronal Network:
- AutoEncoder Algorithm

Binary Search Tree:
- Isolation Forest Algorithm

Attack Classification

Neuronal Network:
- CNN – VGG-19

Agenda

- About the Speaker
- Motivation
- Architecture of the iIDS
- Data Insights of Network Traffic
- Snorkel
- AI-based Network Data Analysis
- Conclusion and Future Work

Future Work

- Development of the 4th Layer – Calculation of the probability of an intrusion
- Generate new normal and attack data for training and testing of the AI-based modules
- Testing of the overall system with the additional data