# Einleitung;

Laut einer Prognose der renommierten Quelle wird der Verbrauchersektor bis zum Jahr 2030 mit weltweit fast 33 Milliarden angeschlossenen Geräten das *Internet of Things* (IoT) anführen. Gleichzeitig wird die zunehmende Verbreitung des IoT sowohl in Privathaushalten als auch in der Industrie die Zahl und Arten der Cyberangriffe auf Unternehmen erhöhen, was das Wachstum des IoT-Sicherheitsmarktes vorantreibt. (1)

Angesichts dieses Wachstums es ist von wesentlicher Bedeutung, ein System zur Erkennung dieser Angriffe zu schaffen und neue oder bisher unbekannte Angriffe auf Systeme oder Netze zu verhindern.

*Intrusion Detection Systems (IDS)* sind Software-Applikationen, die auf Endpunkten oder speziellen Hardwaregeräten installiert werden und diese Vorgänge verwalten. Es verwendet zwei Methoden, um jegliches bösartige Verhalten im Netzwerk zu erkennen und den Administrator zu benachrichtigen. Das *Signature-based detection system (SBDS)* die Signatur von *network flow* mit der Datenbank der Angriffssignaturen vergleicht. Bei einer Übereinstimmung wird die Bedrohung Flag eingesetzt. Die zweite Methode, *das Anamoly-based detection system (ABDS)*, basiert auf dem Prinzip des maschinellen Lernens (ML). Im Gegensatz zur vorherigen Methode kann es Zero-Day-Exploits abfangen - Angriffe, die Software-Schwachstellen ausnutzen, bevor der Software-Entwickler davon weiß oder Zeit hat, sie zu patchen. (2)

In dieser Arbeit für den Zweck der ABDS werden ML-Modelle mit herkömmlichen *Shallow-learning* Algorithmen entwickelt und ihr Ergebnis wird ausgewertet und ggf. optimiert. Für den Training , Testing und Validierung des Modells wird Datensätze aus IEEE-Plattform die neue IoT Netzwerkverkehr Datensatz Edge-IIoTset eingesetzt (später wäre auch mit CIDIDS Datensatz). Mit den Erkenntnisse aus dieser Arbeit kann als IDS mit Fähigkeit von ABDS auf eingebettete System entwickelt werden. Das dients dazu eine sichere Kommunikationssystem sowohl in Industrie als auch in Haushalt Netzwerk.

# Literaturübersicht;

Für die Literaturreferenz wurden Veröffentlichungen von mehreren vertrauenswürdigen Instituten herangezogen. Die erste stammt von der IEEE-Organisation, die technische Fachpublikationen aus der ganzen Welt bereitstellt und verwaltet. Die zweite stammt von ADbench, einer Kooperation zwischen Forschern der Shanghai University of Finance and Economics (SUFE) und der Carnegie Mellon University (CMU).

Zusätzlich zur Erstellung und Analyse des Edge-IIoT-Sets haben die Autoren in (3) die traditionellen Algorithmen des MLs mit dem Datensatz ausgewertet. Die experimentellen Ergebnisse des vorgeschlagenen Datensatzes verwenden eine zentralisierte Lernmethode, bei der Datensätze von Benutzern an verschiedenen Standorten gesammelt werden und mit Hilfe des Cloud Computing ein Model erstellt wird. Bei der Mehrklassen-Klassifikation (K = 15) liegt RF mit der höchsten Erkennungsrate vor KNN und der SVM. Bei der 6-Klassen-Klassifizierung führt SVM mit einer Erkennungsrate von 85,62 %, KNN und RF erreichen 83,39 % bzw. 82,90 %. Endlich, bei der binären Klassifizierung (K = 2) erzielten RF, SVM, KNN und DNN alle die höchste

Erkennungsrate von 99,99 %, während DT bei allen Klassifizierungsarten am wenigsten Ergebnisse aufweist.

Ashraf et al. (4) kombinierten verschiedene ML-Methoden zur Anomalie Erkennung (wie RF, DT, K-NN, XGBoost, SVM, and ANN) mit einer Vielzahl von Merkmalsreduktionsalgorithmen (wie RF, XGBoost, Chi-Square, PCA and Boruta), um zu ermitteln, welcher Ansatz die höchste Erkennungsrate erzielte. Beim Training und Testen mit dem Datensatz CICIDS 2017 zeigte sich, dass die Kombination von Boruta Merkmalsreduktion mit XGBoost und RF eine hohe Erkennungssrate aufweist. Die Anwendung von der Chi-Square mit dem DT eine Erkennungsrate von 99,85% erreicht, während (KNN) mit der (PCA) 99,12 %. SVM schnitten mit RF-Merkmalsreduktion gut ab. Diese Ergebnisse unterstreichen die signifikante Auswirkung der Merkmalsreduktionsarten auf die Erkennungsrate der ML-Methoden.

Mit demselben Datensatz [CICIDS 2017] trainierten und evaluiert Samir et al in (5) drei ML-Modelle (KNN, *similarity*-KNN, LOF) zur Erkennung von Anomalien, jedoch mit dem Unterschied, dass sie nur normale Datenpunkten (‚*Attack_label' gleich 0*) zum Trainieren des Modells verwendeten. Darüber hinaus wurde die Erkennungsrate jedes Modells mit und ohne die Anwendung der Dimensionsreduktionstechnik PCA verglichen. Im Durchschnitt übertraf LOF mit einer Erkennungssrate von 90,54 % sowohl die *similarity*-KNN als auch KNN. Durch das Training nur mit normalen Datenpunkten hat das Modell eine höhere Trefferquote bei der Erkennung *novel Attacks* als üblicher Methode. Obwohl die Anwendung von PCA zu nur einer leichten Steigerung der Erkennungsrate aller Methoden führte, war die damit einhergehende Zeitersparnis während des Trainings und der Tests enorm signifikant.

## Arbeitsverlauf;

Zum Trainieren der ML-Modelle wurde der Datensatz EdgeIIoTset-2018 benutzt. Bevor der Datensatz für das Training verwendet wird, sollte er auf redundante, nicht gültige Features untersucht und entfernt werden. Danach die Skalierung oder Normalisation für die angewendet, wo es benötigt wird. Letztlich wird der Datensatz in zwei Teile für Training und Testing unterteilt.

Für ML-Algorithmen SVM (supervised), LOF (unsupervised), similarity KNN (unsupervised), und RF (supervised) eingesetzt. Nach dem Training mit Training Datensatz wird jedes Modell anhand des Testing Datensatzes bewertet. Mit Hilfe von Auswertung Metriken (wie Erkennungsrate, Trefferquote) werden die Modelle individuell für jeden Angriff untersucht.

Schließlich werden verschiedene Dimensionsreduktionstechniken wie PCA, RF, SVD implementiert, um die Erkennungsrate und den Zeitverbrauch der Modale zu vergleichen.

Preprocessing:

- Ungültuige Feature Entfernen. (strings, variance=0, NaN)
- Angemessene Skalierung.
- Korrelationsmatrix erstellen. (Um abhängige Features zu erkennen)
- Datensätze für Training und Testing einteilen.

Training:

- Similarity/enhanced KNN, SVM, LOF, RF trainieren. (Nur mit Normal?)

Auswertung:

- Erkennungsrate, Trefferquote, Genauigkeit und F-maß (Im Allgemein oder für einzelne Attacks)
- Konfusionsmatrix
- Zeit Aufwand

Feature Reduktion:

- PCA, RF, SVD (noch nicht komplett)
- Auswertung wie oben.

Ensemble!!  Simulation!!