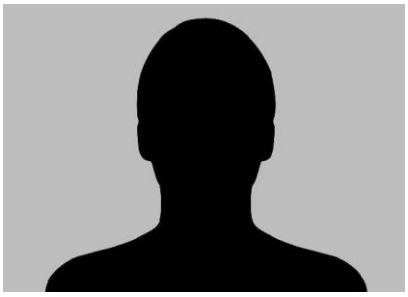
Zürcher Hochschule
für Angewandte Wissenschaften

School of Engineering

InIT Institut für angewandte Informationstechnologie

Paketebene-Analyse mit Deep Learning zur Erkennung von Netzwerkangriffen



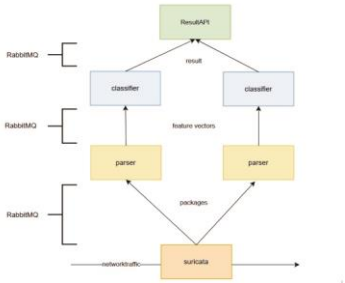
Diplomierende
Nathan Lepori
Nicola Stauffer

Dozierende
Bernhard Tellenbach
Gürkan Gür

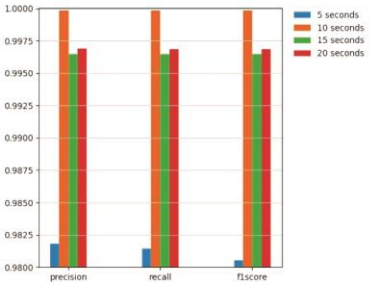
Cybersicherheit spielt eine entscheidende Rolle in modernen Netzwerkinfrastrukturen, wo eine erfolgreiche Attacke zu enormen Schäden, dem Verlust sensibler Daten und finanziellen Verlusten führen kann. Diese Herausforderung wird durch die kritischen und allgegenwärtigen Dienste der IKT-Infrastruktur, die in der heutigen menschlichen Zivilisation unentbehrlich geworden sind, noch verschärft. Dieses Phänomen wurde anhand der Abhängigkeit von digitalen Diensten, selbst bei alltäglichen Aktivitäten, in der gegenwärtigen COVID-19-Pandemie-Ära eindrücklich demonstriert. Darüber hinaus werden mit der Einführung zukünftiger Netzwerktechnologien in Form der 5G-Technologie noch mehr Geräte an Netzwerke angeschlossen werden, was die Herausforderungen in der Sicherheit noch erschwert und die Angriffsoberfläche drastisch erhöht. Denken wir nur an all die vernetzten IoT-Geräte, die ständig im Netzwerk exponiert sind und die aufgrund ihrer begrenzten Rechenleistung normalerweise keinen integrierten Schutz haben, nicht einmal vor den trivialsten Angriffen.

In dieser Arbeit untersuchen wir das Potential der Network Intrusion Detection, die auf Deep Learning basiert und in bestehende IDS-Technologien integriert wird. Das Hauptziel dieser Arbeit ist es, eine Lösung für die durch Machine Learning unterstützte Network Intrusion Detection für eine Reihe von spezifischen Netzwerkangriffen vorzustellen und zu analysieren. Die Architektur für die entwickelte Lösung wird dokumentiert, ebenso der Prozess des Trainings und Testens von zwei Deep Neural Networks, die zur Erkennung von Angriffen vom Typ DDoS mit einem hohen Grad an Generalisierung ausgelegt sind. Die Leistungsanalyse mittels zweier unterschiedlicher Datensätze zeigt die potentielle Leistung der beiden Deep Neural Networks und untersucht, ob ein verallgemeinerter, tiefgreifender lernbasierter Erkennungsansatz möglich ist.

Darüber hinaus bieten wir eine Erklärbarkeitsanalyse auf einem spezifischen Testfall an, um Erkenntnisse darüber zu gewinnen, wie die Eigenschaften des Netzwerks bei der Modellerstellung und den Ergebnissen eine Rolle spielen. Schlussendlich wird ein flexibles Open-Source-Framework für Deep Learning mit Intrusion Detection zur Verfügung gestellt, das es jedem ermöglicht, diese Technologie auf bequeme Weise zu nutzen und bei Bedarf um neue intelligente Detektionstechniken zu erweitern.



Architektur des Open Source Framework



Resultate für die Klassifikation von DDoS-Attacken mit Flow Features