# Unüberwachte Erkennung von Anomalien im Netzwerkverkehr mit Deep Learning

Ivaylo Krumov
University of Luxembourg
Email: ivaylo.krumov.001@student.uni.lu

**Dieser Bericht wurde unter der Aufsicht von:**
Salima Lamsiyah
University of Luxembourg
Email: salima.lamsiyah@uni.lu

## 1. Einleitung

In der heutigen vernetzten Welt haben die Bedrohungen für die Cybersicherheit aufgrund des schnellen Informationsaustauschs über das Internet zugenommen. Mit dem technologischen Fortschritt setzen Cyberkriminelle immer ausgefeiltere Techniken ein, um Schwachstellen im Netz auszunutzen. Die Erkennung von Anomalien in Netzwerkdaten, die auf potenzielle Sicherheitsverletzungen oder böswillige Aktivitäten hinweisen, ist eine große Herausforderung. Herkömmliche Erkennungsmethoden haben sich als unzureichend erwiesen, um den sich weiterentwickelnden Taktiken zu begegnen, so dass fortschrittliche Ansätze mit maschinellem Lernen und Deep Learning erforderlich sind.

Dieses Projekt untersucht die Anwendung von unbeaufsichtigten Deep-Learning-Modellen bei der Erkennung von Anomalien im Netzwerkverkehr. Es konzentriert sich auf neuronale Netzwerkarchitekturen, die große Datenmengen nutzen, um Muster zu erlernen und ungewöhnliche Verhaltensweisen ohne vordefinierte Muster zu erkennen, und erforscht ihr Potenzial zur Verbesserung von Cybersicherheitsanwendungen.

## 2. Wissenschaftliches Ergebnis

### 2.1. Anforderungen

Die wissenschaftliche Arbeit zielt darauf ab, die Frage zu beantworten: Wie können Deep-Learning-Modelle eingesetzt werden, um Anomalien im Netzwerkverkehr zu erkennen?“ Es enthält Erläuterungen zu relevanten Konzepten wie der Datenvorverarbeitung, der Feinabstimmung von Deep-Learning-Modellen und der Bewertung der Modellleistung. Das Papier stützt sich auf einschlägige akademische und wissenschaftliche Quellen, um einen Überblick über Cybersicherheit und die Erkennung von Netzwerkeinbrüchen zu geben, und erörtert maschinelles Lernen, die Architektur von Deep-Learning-Modellen und spezifische Merkmale von Modellen zur Erkennung von Anomalien wie Autocoder, Variationsautocoder und generative adversarische Netzwerke.

### 2.2. Gestaltung

Der wissenschaftliche Beitrag ist ein Text, der den technischen Beitrag ergänzt, indem er den Kontext zu dessen Ideen, Methoden und Umsetzung liefert. Er befasst sich mit Themen, die für die Beantwortung der wissenschaftlichen Frage relevant sind, und schafft den notwendigen Hintergrund für das Verständnis der technischen Arbeit. Die Recherche stützt sich auf mehrere wissenschaftliche Quellen, um Genauigkeit und Zuverlässigkeit zu gewährleisten. Nach der Darstellung der erforderlichen Definitionen und Erklärungen fasst der Text diese Informationen zusammen, um eine fundierte Antwort auf die wissenschaftliche Frage nach der Verwendung von Deep-Learning-Modellen für die Erkennung von Anomalien im Netzwerkverkehr zu formulieren.

### 2.3. Produktion

Um herauszufinden, wie Deep-Learning-Modelle für die Erkennung von Anomalien im Netzwerkverkehr eingesetzt werden können, ist es wichtig, die Grundlagen von Deep Learning und unüberwachtem Lernen zu verstehen. Deep Learning umfasst neuronale Netze mit mehreren Schichten, die automatisch komplexe Datenmuster lernen, was für die Erkennung von Anomalien von Vorteil ist, bei denen herkömmliche Methoden Schwierigkeiten haben können. Diese Modelle, die in der Lage sind, Abweichungen von gelernten Mustern zu erkennen, sind besonders nützlich für die Erkennung seltener und ungewöhnlicher Datenpunkte, die auf Probleme wie Systemausfälle oder Sicherheitsbedrohungen hinweisen könnten.

Unüberwachtes Lernen, das ohne markierte Daten arbeitet, ergänzt das Deep Learning, indem es sich auf die Erkennung inhärenter Strukturen in den Daten konzentriert. Techniken wie Clustering, Dimensionalitätsreduktion und Dichteschätzung werden eingesetzt, um Anomalien zu erkennen. Die Kombination dieser Methoden mit Deep-Learning-Ansätzen wie Autoencodern, Variationalen Autoencodern (VAEs) und generativen adversen Netzwerken (GANs) verbessert die Erkennung von Anomalien. Autoencoder nutzen Rekonstruktionsfehler, um Anomalien zu erkennen, VAEs modellieren Daten-

verteilungen probabilistisch, und GANs nutzen adversariales Training, um Daten zu identifizieren, die von gelernten Mustern abweichen. Die Wirksamkeit dieser Modelle wird durch reale Anwendungen untermauert, die zeigen, dass sie in der Lage sind, Anomalien in verschiedenen Bereichen wie der industriellen Überwachung, der Erkennung von Finanzbetrug und der Netzwerksicherheit genau zu erkennen.

### 2.4. Bewertung

Der wissenschaftliche Beitrag bietet eine gründliche Untersuchung des unüberwachten Deep Learning, der Datenaufbereitung und der Modellbewertung und schafft damit eine solide Grundlage für das Verständnis von Anomalieerkennungssystemen. Er wendet diese Konzepte auf reale Szenarien an und demonstriert die Verwendung von Autoencodern, Variations-Autoencodern und GANs für die Erkennung von Anomalien in verschiedenen Bereichen. Die Arbeit ist gut organisiert und integriert wissenschaftliche Referenzen auf effektive Weise und bietet einen umfassenden Überblick, der die zentrale wissenschaftliche Frage des Projekts beantwortet. Er schlägt erfolgreich eine Brücke zwischen theoretischem Wissen und praktischen Anwendungen und schafft damit die Grundlage für die nachfolgenden technischen Ergebnisse.

## 3. Technisches Ergebnis

### 3.1. Anforderungen

Die technische Leistung erfordert die Implementierung und das Training von mindestens zwei verschiedenen Deep-Learning-Modellen für die Erkennung von Anomalien auf einem detaillierten Netzwerkverkehrsdatensatz, wobei Techniken verwendet werden, die sich zwischen den Modellen unterscheiden. Dazu gehört die Vorverarbeitung der Daten mit Tools wie Pandas und Numpy, die Bewertung der Modelle mit Leistungsmetriken und die Visualisierung der Ergebnisse mit Matplotlib. Die Modelle müssen eine hohe Genauigkeit und Effizienz aufweisen, große Datensätze effektiv verwalten und skalierbar, gut dokumentiert und benutzerfreundlich sein, insbesondere in Jupyter-Notebooks. Außerdem sollte der Code anpassbar sein, um verschiedene Hyperparameter zur Optimierung der Erkennungsleistung zu testen.

### 3.2. Gestaltung

Das Ergebnis besteht aus drei Jupyter-Notebooks, die jeweils eine bestimmte Phase des Lebenszyklus des Anomalieerkennungsmodells behandeln: Vorverarbeitung, Training und Test. Unter Verwendung eines Autoencoders, eines Variations-Autoencoders und eines generativen adversen Netzwerks aus PyOD bewerten diese Notebooks die Leistung des Modells durch iterative Verfeinerungen und Abstimmung der Hyperparameter über drei Wochen. Jedes Notebook ist so strukturiert, dass es die Vorverarbeitung der Daten, das Training des Modells und die Leistungsbewertung umfasst, wobei Metriken wie Genauigkeit, F1-Score und ROC-Kurve in Diagrammen visualisiert werden. Die Notebooks arbeiten unabhängig voneinander und ermöglichen flexible Experimente, ohne dass gemeinsam genutzte Dateien verändert werden müssen.

### 3.3. Produktion

Das endgültige Ergebnis besteht aus drei Jupyter-Notebooks, die jeweils eine bestimmte Phase des Deep-Learning-Modell-Lebenszyklus für die Erkennung von Anomalien unter Verwendung des UNSW-NB15-Datensatzes behandeln sollen. Der von der UNSW Canberra zur Verfügung gestellte Datensatz ist in einen Trainings- und einen Testdatensatz unterteilt und enthält detaillierte Netzwerkverkehrseinträge mit 42 Merkmalen und Kennzeichnungen, die normale oder anomale Anfragen anzeigen. Die Notebooks wenden konsistente Vorverarbeitungstechniken an, darunter das Laden der Daten, die Anpassung der Kontaminationsrate, die Codierung kategorischer Merkmale und die Aufteilung der Datensätze. Die Vorverarbeitung stellt sicher, dass die Daten einheitlich für die Modellschulung und -bewertung vorbereitet werden. Zu den wichtigsten Schritten gehören die Anpassung der Kontaminationsrate und die Umkehrung der Kennzeichnung aufgrund des inhärenten Ungleichgewichts des Datensatzes.

Die Modelle - ein Autoencoder, ein Variations-Autoencoder (VAE) und ein generatives adversariales Netzwerk (GAN) - werden jeweils mit diesen vorverarbeiteten Daten trainiert. Der Autoencoder wird nach empirischer Abstimmung mit spezifischen Hyperparametern eingerichtet und zeigt mit einem ROC-AUC-Wert von 0,7302 und angemessener Genauigkeit mäßigen Erfolg. Die VAE, die zwar ähnliche Schritte durchläuft, schneidet mit einem ROC-Wert von 0,6495 und einer geringeren Genauigkeit etwas schlechter ab. Das GAN-Modell zeigt trotz der Herausforderung, einen großen Datensatz zu verarbeiten, die beste Leistung mit einem ROC-Wert von 0,7997 und einer hohen Genauigkeit für normale Proben. Die Effektivität jedes Modells wird anhand von Metriken wie ROC-Kurven, Konfusionsmatrizen und Precision-Recall-Scores bewertet, wobei Visualisierungen die Leistungsunterschiede und die allgemeinen Fähigkeiten bei der Erkennung von Anomalien hervorheben.

### 3.4. Bewertung

Im Rahmen des Projekts wurden Deep-Learning-Modelle für die Erkennung von Netzwerkanomalien, einschließlich Autoencodern, VAEs und GANs, anhand des UNSW-NB15-Datensatzes erfolgreich evaluiert. Das GAN erreichte die höchste ROC-AUC-Punktzahl, wurde aber mit einem reduzierten Datensatz getestet, was sich möglicherweise auf seine Ergebnisse auswirkte. Der Autoencoder schnitt gut ab, während der VAE unterdurchschnittlich abschnitt, was darauf hindeutet, dass er weiter optimiert werden muss. Insgesamt

wurden die Ziele erreicht und Verbesserungsmöglichkeiten aufgezeigt, insbesondere bei der Modelloptimierung und Skalierbarkeit.

## 4. Schlussfolgerung

Die in diesem Bericht vorgestellte Forschung und Analyse hat die Durchführbarkeit und Effektivität von unbeaufsichtigten Deep-Learning-Modellen für die Erkennung von Anomalien im Netzwerkverkehr nachgewiesen. Die wissenschaftliche Analyse umfasste Schlüsselkonzepte, während die technische Komponente mehrere Deep-Learning-Modelle für die Erkennung von Anomalien implementierte und bewertete. Trotz zeitlicher Beschränkungen schnitten die Modelle relativ gut ab, was die Praxistauglichkeit des unüberwachten Deep Learning in diesem Bereich bestätigt. Das Projekt zeigt, dass die Kombination von theoretischem Wissen und praktischer Umsetzung sowie die richtige Anpassung und Optimierung diese Modelle in leistungsfähige Werkzeuge zur Erkennung von Anomalien und zur Minimierung potenzieller Risiken in der Netzwerksicherheit verwandeln können.