FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Einsatz von KI-Methoden in der IT-Sicherheit

Nodari Papava

IT Forensik
FH Aachen

Zielsetzung der Bachelorarbeit

- Erkennung von Anomalien in HTTP Anfragen

```
GET /api/posts?author=mallory&category='%20or%20'1'%20=%20'
```

```
GET /api/posts?author=alice&category=sports
```

- Durchführung eines Experiments

Warum maschinelles Lernen ?

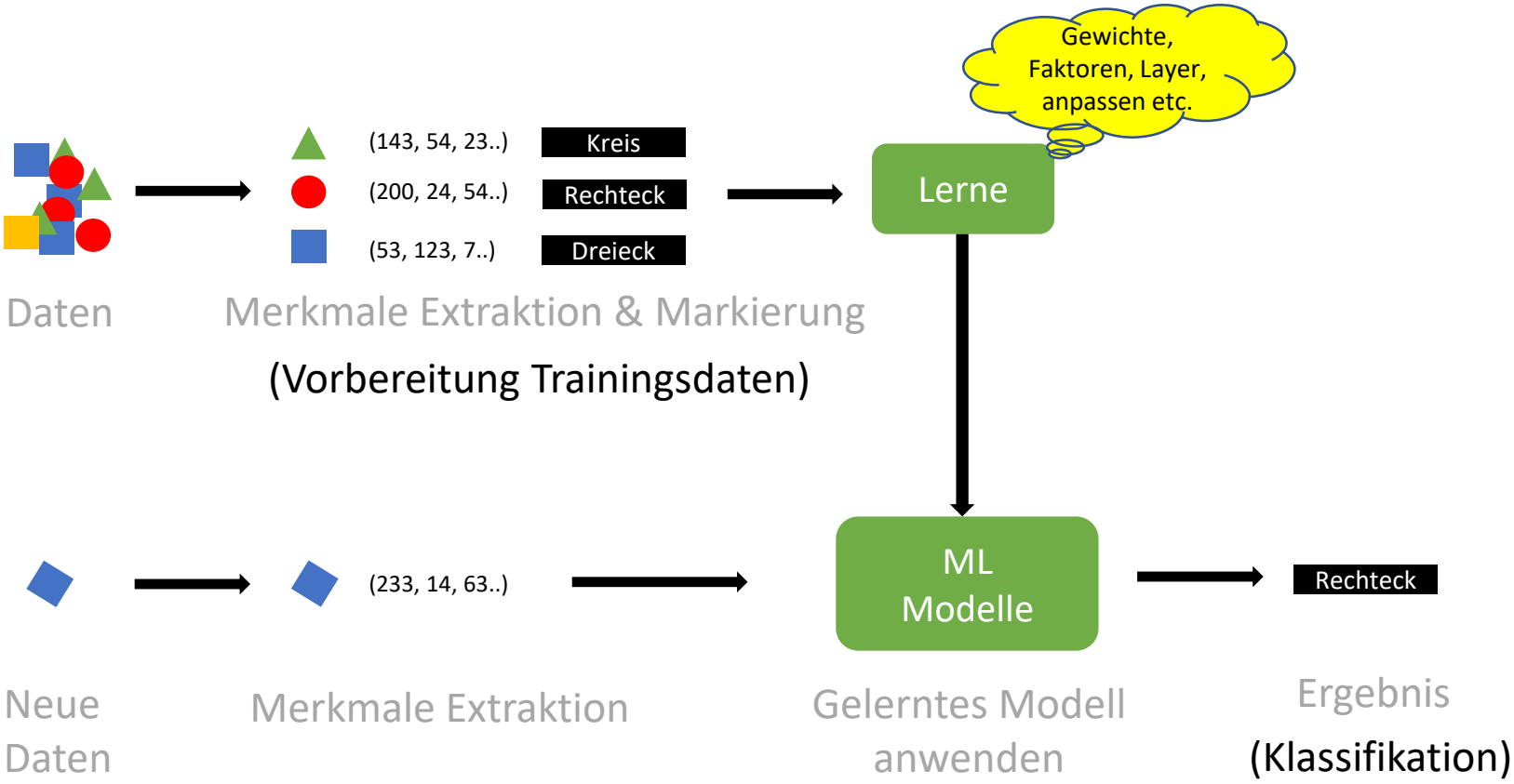
- Bearbeitung enormer Datenmengen in Echtzeit
- Schnelle Identifizierung von Angriffen
- Abdeckung des Mangels an IT-Sec. Experten
- Mögliche Erkennung von Zero-Day-Angriffen

Warum maschinelles Lernen ?

Konventionelle Erkennungssysteme	Erkennungssysteme mit lernender/ KI-Komponente
Software (SW) ist nicht lernfähig	SW lernt laufend hinzu
SW setzt Signaturen und Korrelationen gegen verschiedene Arten von Daten ein	SW lernt komplexe Muster aus einer großen Menge von Daten
Aktualisierung der SW erfolgt durch gesteuertes Update	SW befindet sich selbstständig im Updateprozess

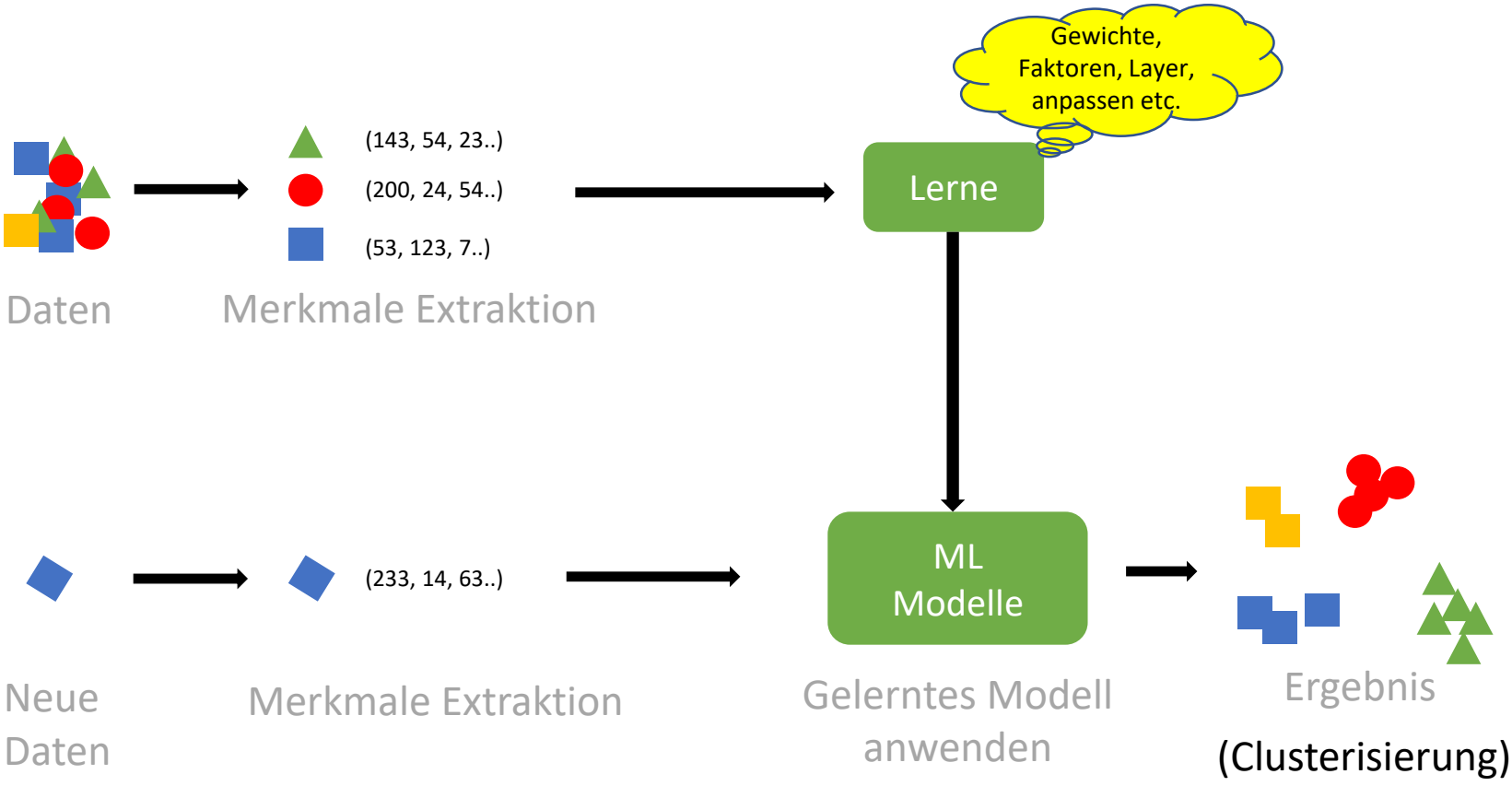
Grundidee des maschinellen Lernens

Was ist überwachtes Lernen?



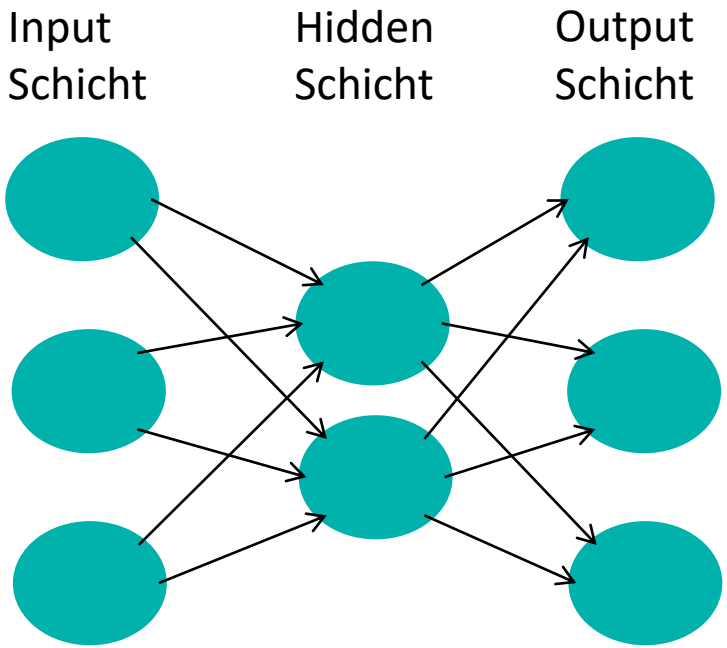
Grundidee des maschinellen Lernens

Was ist unüberwachtes Lernen?



Neuronales Netz Autoencoder

- Besteht aus Neuronen und Gewichten
- Gewichte übertragen die Signale
- Neuronen leiten die Signale weiter
- Eingaben werden komprimiert und wiederhergestellt



Neuronales Netz Autoencoder

Normale Anfragen

GET /normal/request=1

GET /normal/request=2

⋮

GET /normal/request=N

Abnormale Anfragen

GET /anomaly/request=1’

GET /anomaly/request=2’

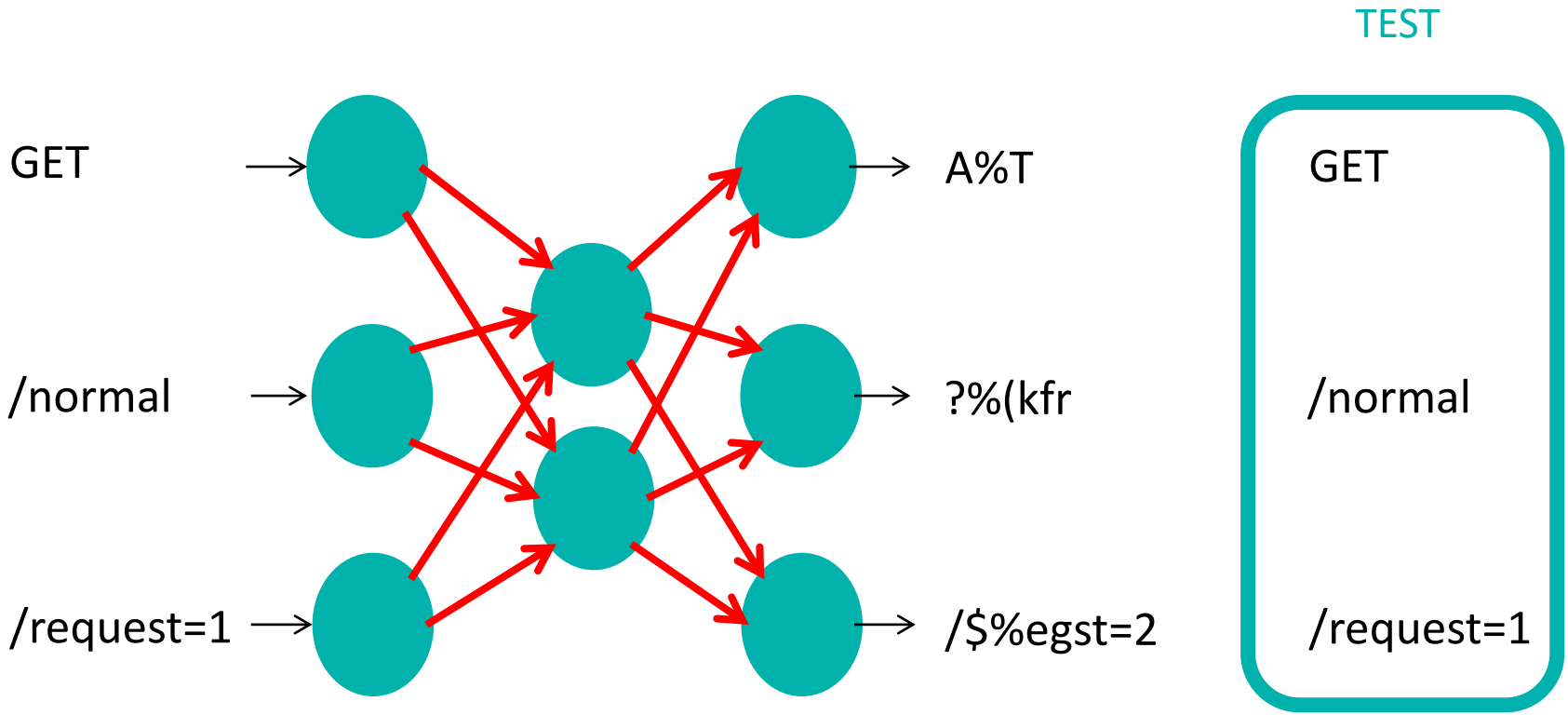
⋮

GET /anomaly/request=N’

Autoencoder-Training

Gewichte: Schlecht

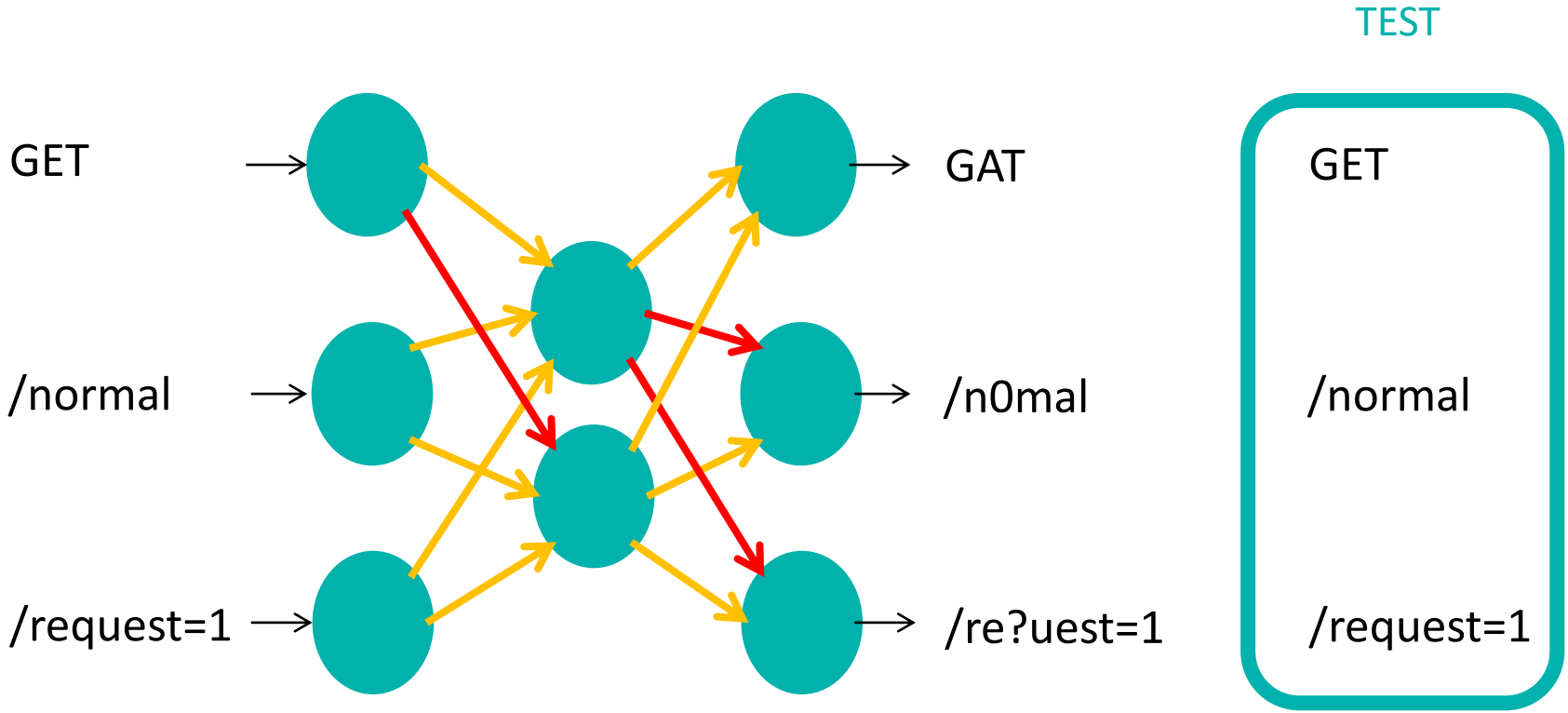
Fehler: Hoch



Autoencoder-Training

Gewichte: Besser

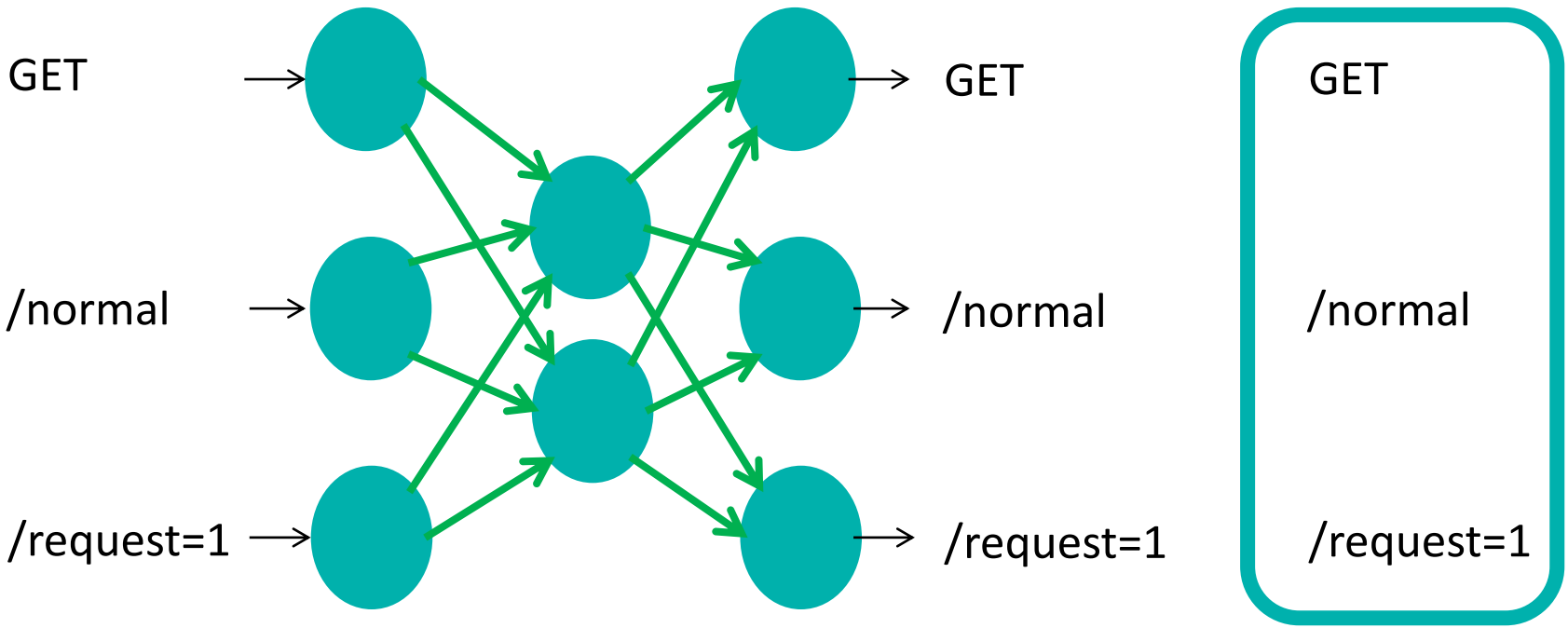
Fehler: Mittel



Autoencoder-Training

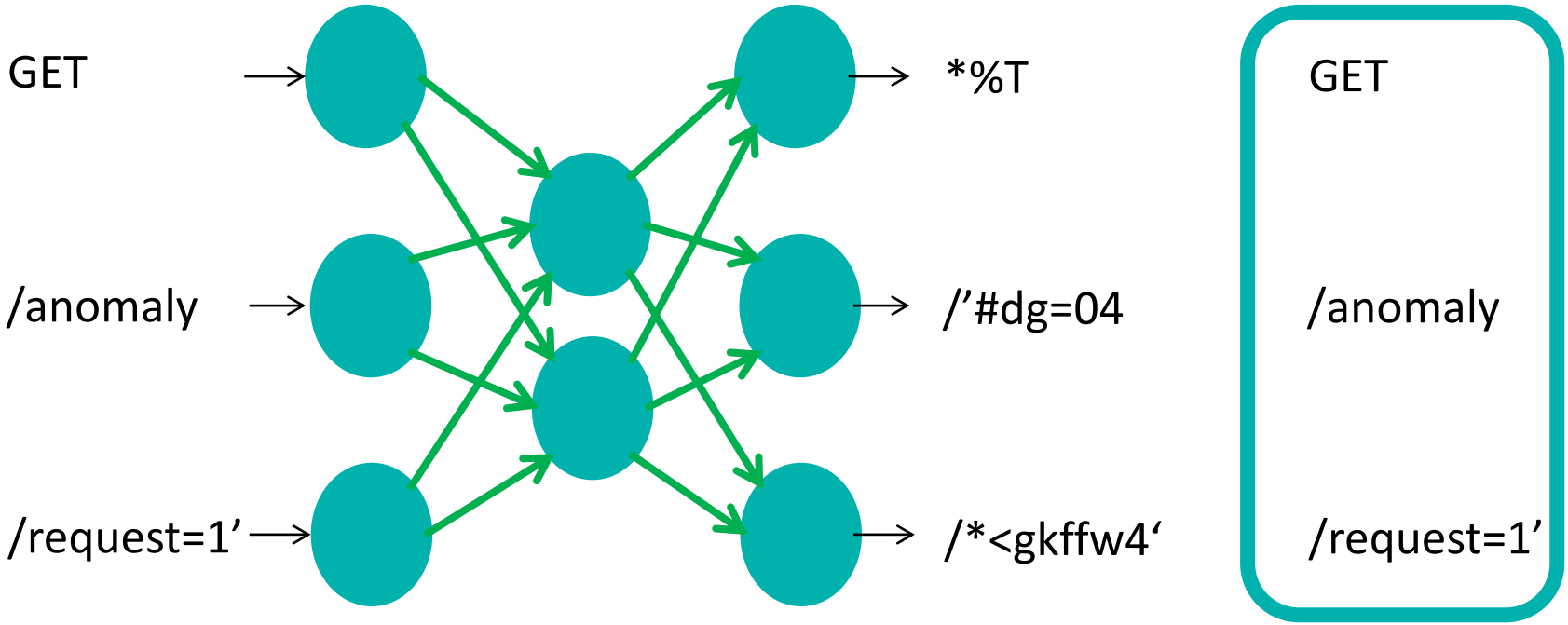
Gewichte: Gut

Fehler: Niedrig



Autoencoder-Test

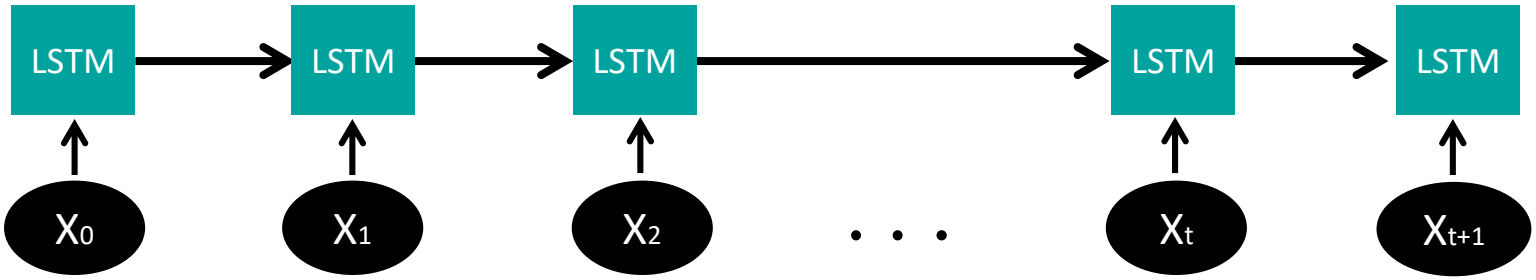
Fehler: Hoch



Sequence to Sequence Autoencoder

Seq2Seq

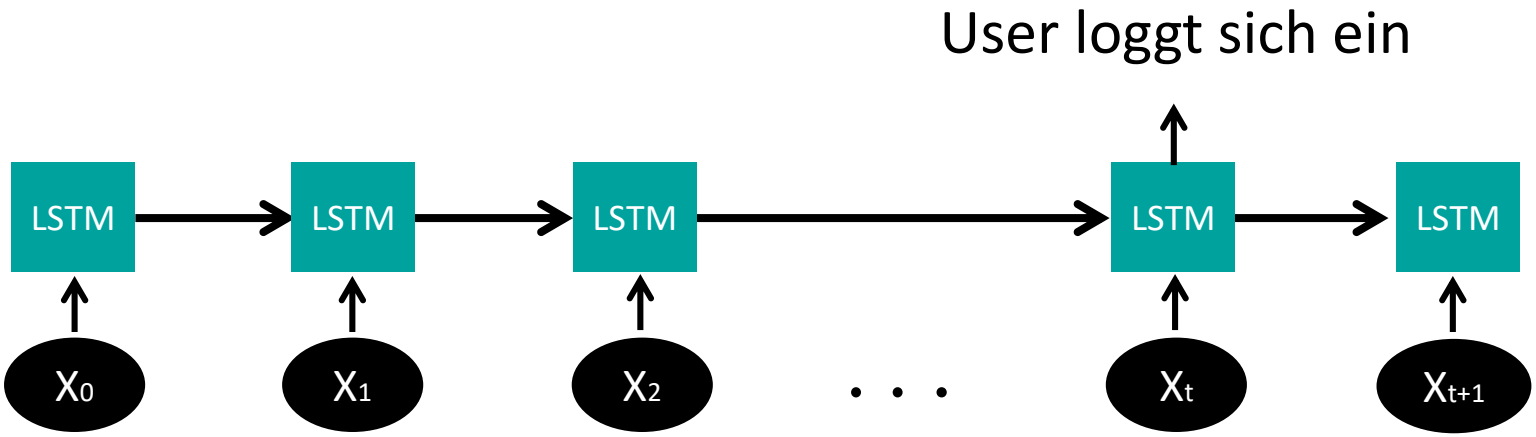
- Ähnliche Funktionalität wie bei Autoencoder
- Neuronen besitzen ein Gedächtnis
- Die kontextuelle Verbindungen bleiben erhalten



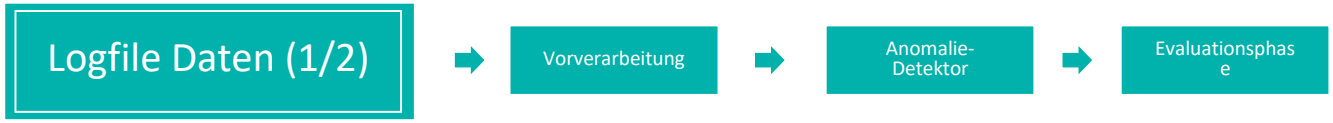
Sequence to Sequence Autoencoder

Seq2Seq

- Ähnliche Funktionalität wie bei Autoencoder
- Neuronen besitzen ein Gedächtnis
- Die kontextuelle Verbindungen bleiben erhalten



Umsetzung



HTTP dataset CSIC 2010 :

- 65 000 normale und abnormale Anfragen
- POST & GET Anfragen mit Header
- SQL & CRLF injection, XSS und u.a
- Angriffen generiert W3af

CSIC (Spanish Research National Council)
CRLF (Carriage Return Line Feed)
XSS (Cross-Site-Scripting)
W3af (Open Source Web Application Security Scanner)

Umsetzung

- Entfernung der statischen Anfragen ohne Parameter

  GET /wp-content/themes/oldmusic/images/twitter-icon.jpg

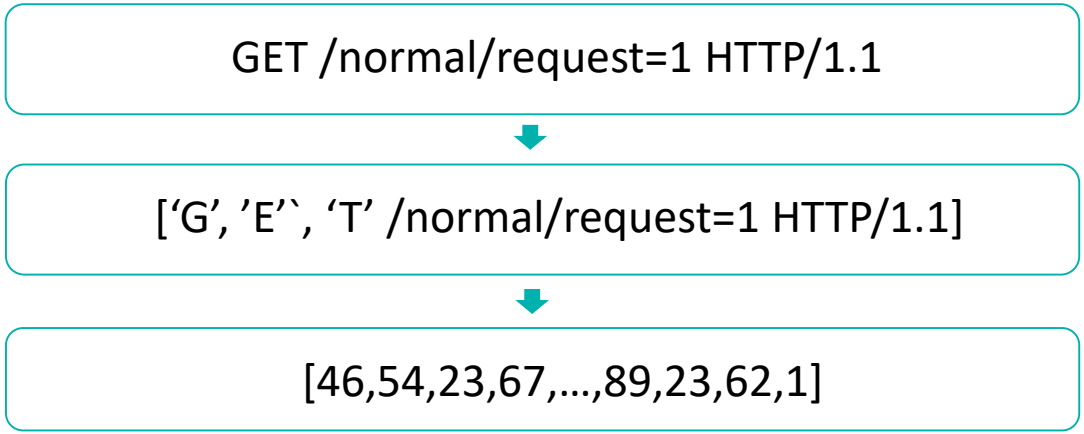
  GET /lg4-common-gp/js/global/global.main.d4fdde8a.js

  GET /lg4-common-gp/css/modules.b3306130.css

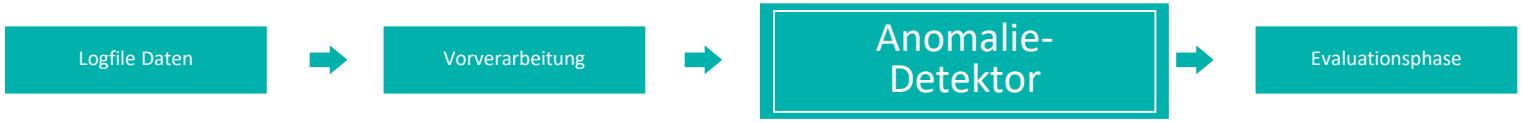
- Entfernung von Duplikaten

Umsetzung

- Worteinbettungen – (engl. Word embedding)



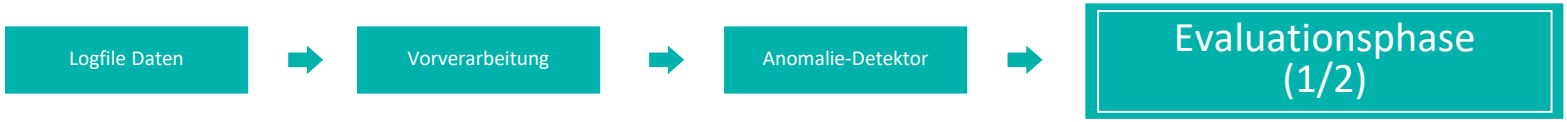
Umsetzung



Seq2Seq

- 64 LSTM-Zellen jeweils mit 64 Neuronen
- Trainingszeiten ca.5-8 Stunden

Umsetzung



Vorhersage

Aktuell	Normal	Angriff
Normal	True Negative (TN)	False Positive (FP)
Angriff	False Negative (FN)	True Positive (TP)

Umsetzung

Logfile Daten → Vorverarbeitung → Anomalie-Detektor → **Evaluationsphase (2/2)**

Vorhersage

Aktuell	Normal	Angriff
Normal 3000 Anfragen	True Negative (TN) 2991	False Positive (FP) 9
Angriff 1000 Anfragen	False Negative (FN) 19	True Positive (TP) 981

Zusammenfassung und Ausblick

Benutzt wurde:

- die Skriptsprache Python
- das Framework Tensorflow-GPU
- die Software-Bibliothek Scikit-learn, Keras

Ausführliche Auswertung der Ergebnisse

Vielen Dank für Ihre Aufmerksamkeit.

Fragen?