htl3 rennweg

IT & MECHATRONIK

Informationstechnologie | Netzwerktechnik

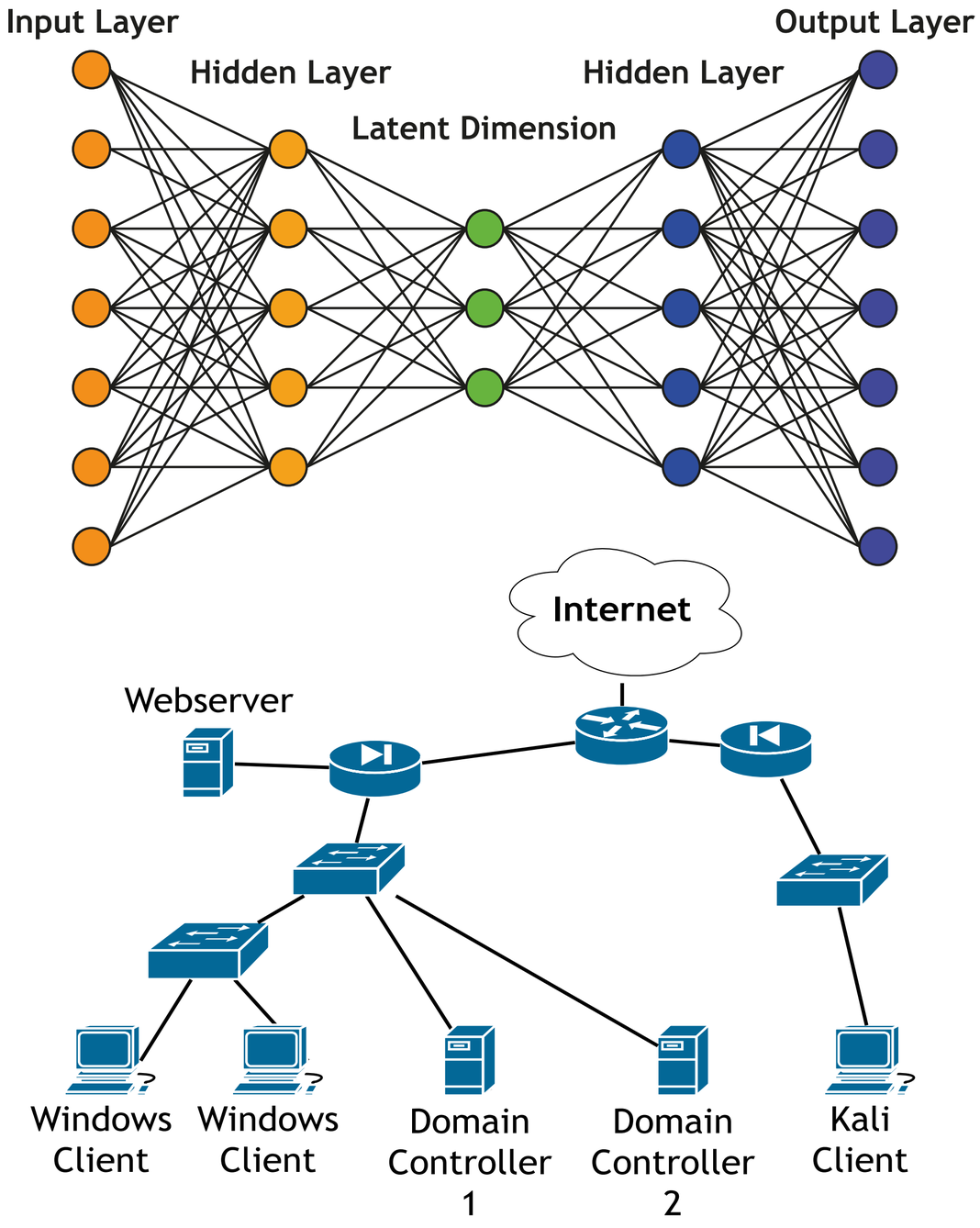
Sherlock

AI supported Network Intrusion Detection

Aufgabenstellung

Die Diplomarbeit „Sherlock -AI supported Network Intrusion Detection“ befasst sich mit dem Erkennen von Angriffen in einem Netzwerk mithilfe von Künstlicher Intelligenz. Im Rahmen der Arbeit wird ein neuronales Netzwerk geplant, trainiert und getestet. Das Projektteam erstellt ein simuliertes Firmennetzwerk „Spielwiese“, das der Aufzeichnung von Netzwerkdaten dient. Diese Daten werden zum Trainieren und Testen des neuronalen Netzes genutzt.

INFO	
Schuljahr	2023/24
Scrum Master	Luca Sautter
Product Owner	Nik Sauer
Developer	Maximilian Kniely
Developer	Martin Bierbaumer
Auftraggeber	Christian Schöndorfer
Stv. Auftraggeber	Harald Zainzinger
Gesamtstunden	720 Stunden



Technische Umsetzung

Zuerst zeichnen wir die zu untersuchenden Netzwerkdaten auf einem zentralen System auf und wandeln sie in einen Netflow um. Der Netflow besteht aus den wichtigsten Merkmalen für jede Kommunikation, wie zum Beispiel der Dauer der Übertragung, der Menge der übertragenen Bytes und mehr. Diese Merkmale dienen als Eingabe für unseren Autoencoder (KI-Modell, siehe Grafik). Im Autoencoder werden die Eingaben komprimiert (encodiert), diese encodierten Daten werden dann bestmöglich rekonstruiert. Unser Autoencoder ist trainiert, um Netzdaten ohne Angriffe möglichst genau rekonstruieren zu können. Um festzustellen, ob es sich bei der Kommunikation um einen Angriff handelt, berechnen wir den Unterschied zwischen den rekonstruierten und den originalen Daten (Reconstruction Loss). Wenn dieser Unterschied einen bestimmten Schwellenwert überschreitet, wird die Kommunikation als potenzieller Angriff gemeldet.

bds421 accelerating AI technology

easyname