Fully Homomorphic Encryption

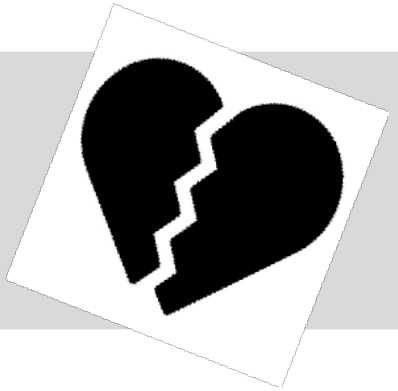
KI in der Cloud ohne Datenschutzbedenken

Jeder liebt die Cloud 

Vorteile:

- Kürzere Produkteinführungszeit
- Skalierbarkeit und Flexibilität
- Kosteneinsparungen
- *Bessere Zusammenarbeit*
- *Schutz vor Datenverlust*

Jeder liebt die Cloud



Vorteile:

- Kürzere Produkteinführungszeit
- Skalierbarkeit und Flexibilität
- Kosteneinsparungen
- *Bessere Zusammenarbeit*
- *Schutz vor Datenverlust*

Nachteile:

- Risiko der Anbieterabhängigkeit
- weniger Kontrolle über Cloud-Infrastruktur
- unvorhergesehene Kosten
- Integration in bestehende Systeme
- **Sicherheitsrisiken**

Aktuelle Sicherheit in der Cloud

3x

The number of data breaches **more than tripled** between 2013 and 2022.[21,22]

98%

98% of organizations have a relationship with a vendor that experienced a data breach within the last two years.[13]

Dramatic increase in sensitive data reported in the cloud.

75%

of respondents report that 40% or more of their data in the cloud is sensitive, up from 49% in 2021.

360 million

In the first eight months of 2023 alone, **over 360 million people were victims of corporate and institutional data breaches**.[25]

1 of 4

In the first three quarters of 2023, one in four people in the US had their health data exposed in a data breach.[26,27]

38%

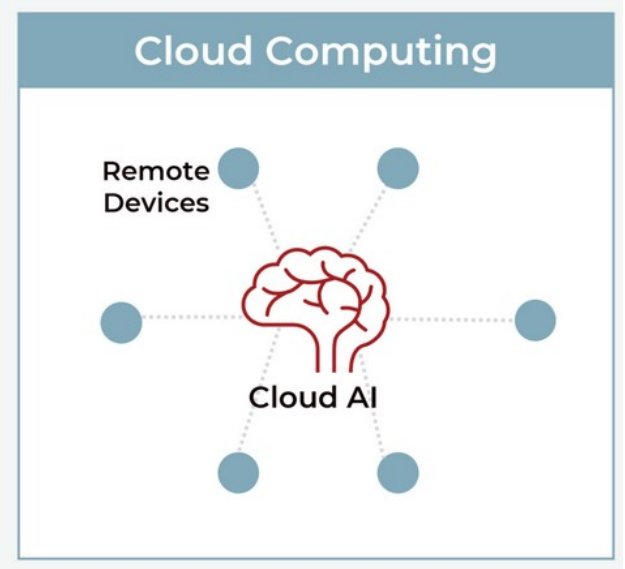
SaaS applications garnered the most votes as the leading targets for attackers (ranked first as a target by 38%), followed closely by cloud-based storage (ranked first as a target by 36%).

Ph.D. Madnick Stuart E. The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase. Tech. rep.
Accessed: 18.02.2024. Apple, Dec. 2023.

THALES, 2023 CLOUD SECURITY STUDY - The Challenges of Data Security and Sovereignty in a Multicloud World, 2023
Accessed: 18.02.2024, THALES, June 2023

KI und die Cloud

ChatGPT – Wikipedia
https://de.wikipedia.org/wiki/ChatGPT
Accessed: 18.02.2024, Wikipedia



https://www.cardinalpeak.com/blog/at-the-edge-vs-in-the-cloud-artificial-intelligence-and-machine-learning
Accessed: 18.02.2024, CardinalPeak

Sicherheit in der Cloud

You

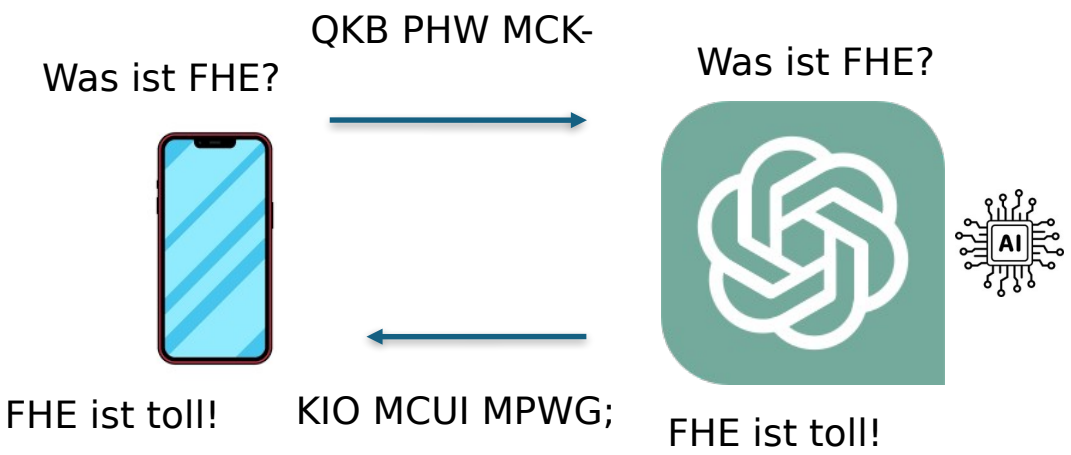
Wenn ich eine Anfrage an ChatGPT sende, wird diese verschlüsselt übertragen? Muss meine Anfrage auf den Servern bei OpenAI im Klartext vorliegen, um verarbeitet werden zu können?

Consensus

Ja, Anfragen an ChatGPT werden in der Regel verschlüsselt übertragen, typischerweise unter Verwendung von HTTPS, um die Sicherheit und Privatsphäre der Daten während der Übertragung zu gewährleisten. Damit ChatGPT die Anfrage verarbeiten kann, muss diese auf den Servern von OpenAI in einer Form vorliegen, die eine Analyse und Verarbeitung ermöglicht. In den meisten Fällen bedeutet das, dass die Anfrage in eine lesbare Form umgewandelt werden muss, die der Algorithmus verstehen kann, was oft als "Klartext" betrachtet wird. Dies ist notwendig, damit ChatGPT die Anfrage interpretieren und eine passende Antwort generieren kann.

Motivation für FHE

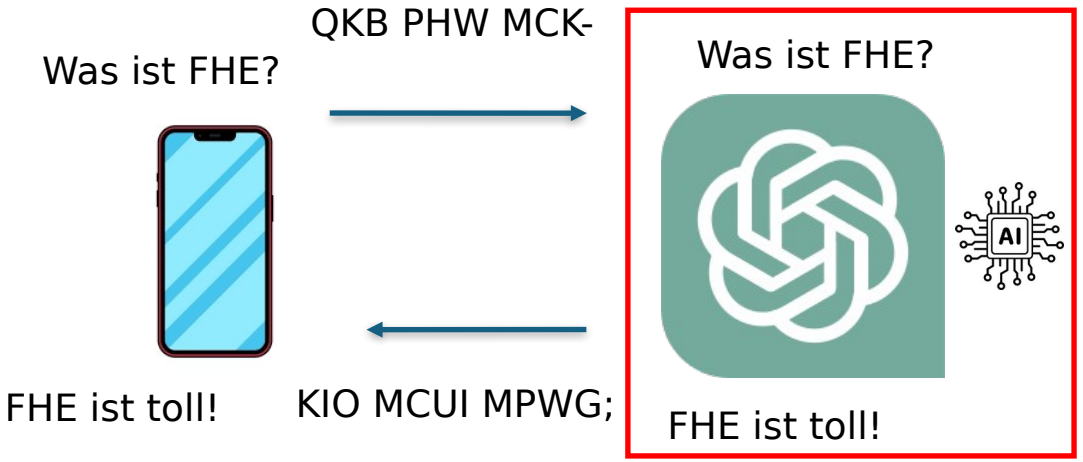
Ohne FHE



Daten werden entschlüsselt

Motivation für FHE

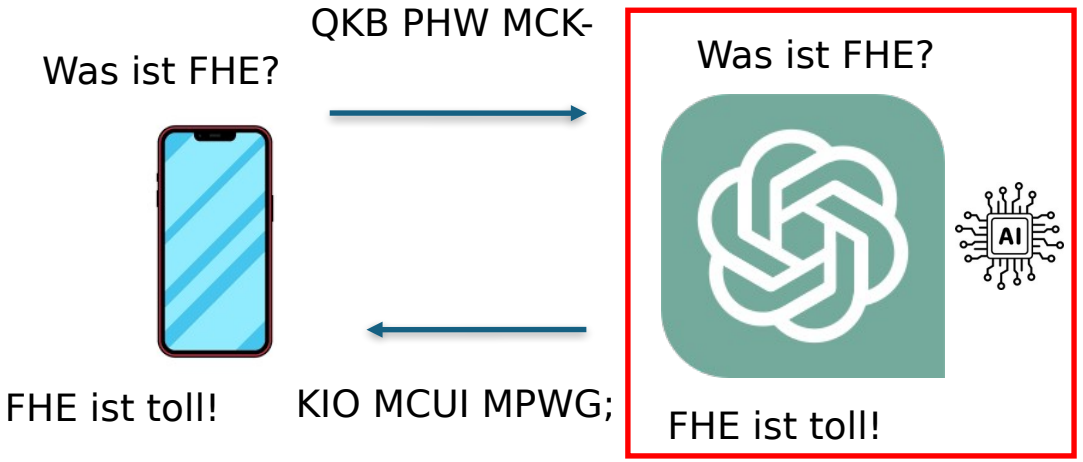
Ohne FHE



Daten werden entschlüsselt

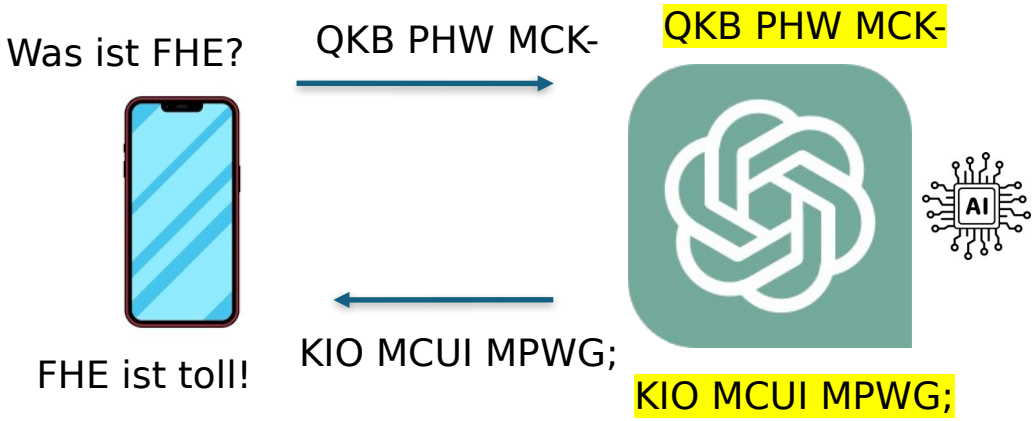
Motivation für FHE

Ohne FHE



Daten werden entschlüsselt

Mit FHE

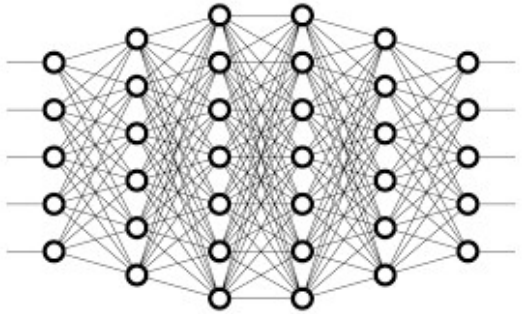


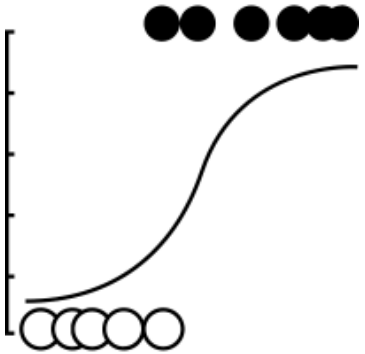
Daten sind immer verschlüsselt

Definition von Fully Homomorphic Encryption

Definition (FHE):

FHE erlaubt es uns *beliebige* Berechnungen auf verschlüsselten Daten durchzuführen!

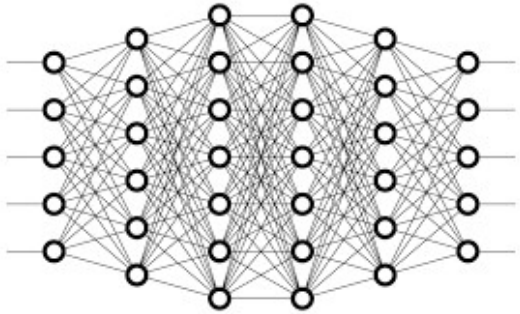


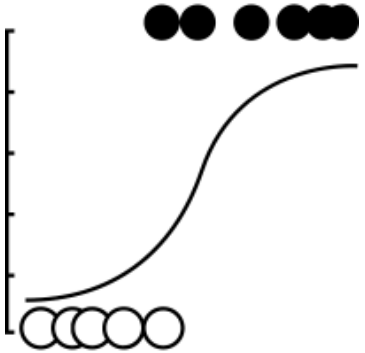


Definition von Fully Homomorphic Encryption

Definition (FHE):

FHE erlaubt es uns *beliebige* Berechnungen auf verschlüsselten Daten durchzuführen!





Definition (Levelled Homomorphic Encryption):

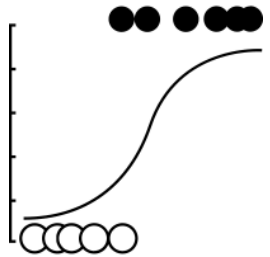
LHE erlaubt es uns Berechnungen bis zu einer *bestimmten Komplexität* auf verschlüsselten Daten durchzuführen.

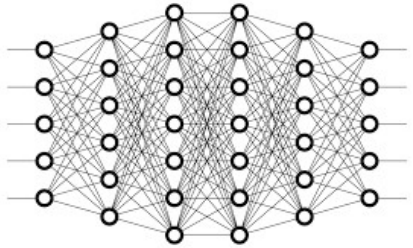
FHE ist sicher

Verschlüsselung ist sicher

- Gleiche Daten werden unterschiedlich verschlüsselt
- FHE ist nicht ordnungserhaltend

Leakt keine Infos über Berechnungen





Quantensicher

Probieren geht über Studieren!

HElayers benutzen:

Downloade das Docker Image und spiele mit den Tutorials rum!
https://ibm.github.io/helayers/user/installation.html

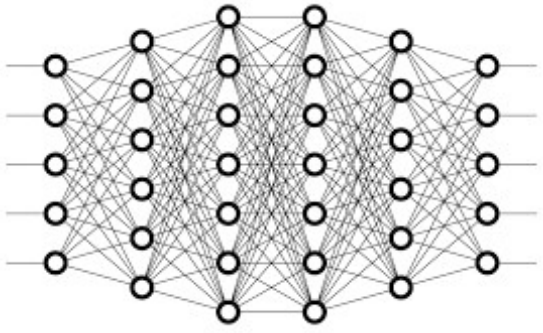
docker pull icr.io/helayers/helayers-pylab-x86_64:latest
docker images
docker run -p 8888:8888 -d --rm --name helayers-lab icr.io/helayers/helayers-pylab-x86_64:latest
http://127.0.0.1:8888/lab/?token=demo-experience-with-fhe-and-python

Probieren geht über Studieren!

Baue aus Low level Funktionen High Level Funktionen:

- Trainiere Modell ohne Verschlüsselung
- Evaluiere Modell aber auf verschlüsselten Daten

Link zu weiterem Tutorial



Grenzen von FHE

Hauptprobleme

- FHE ist langsam,
- nicht standardisiert
- und schwierig zu benutzen

Lösung

Laufzeit um 2 Bits homomorph zu multiplizieren

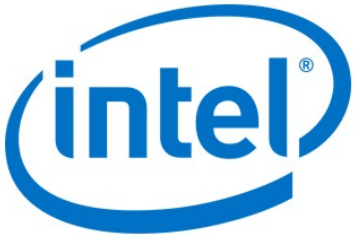
Year	runtime	speedup	speedup per year
2009	30 min	-	-
2014	2000 ns	$9 \cdot 10^8$	$18 \cdot 10^7$
2020	100 ns	20	3.33
	. . . Hardware Acceleration . . .		
2024	*0.1 ns*	*1000*	*250*

Grenzen von FHE

Hauptprobleme

- FHE ist langsam,
- nicht standardisiert
- und schwierig zu benutzen

Lösung

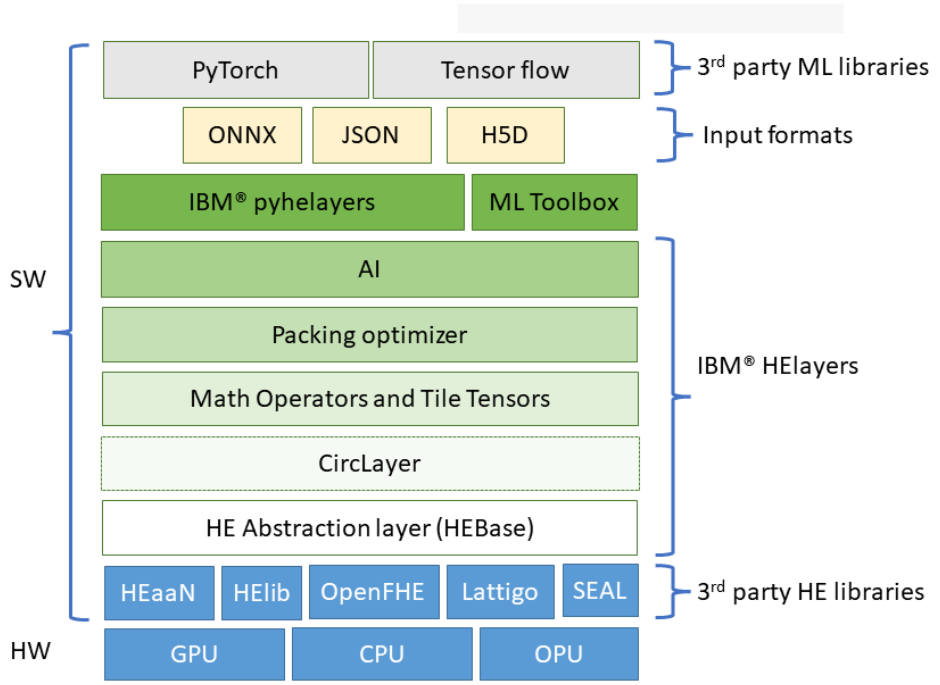


Grenzen von FHE

Hauptprobleme

- FHE ist langsam,
- nicht standardisiert
- und schwierig zu benutzen

Lösung



Meine Masterarbeit

ML Modell

Meine Masterarbeit

ML Modell

Datensatz

Portuguese Bank Marketing Data Set

Telemarketing campaign about term deposits

Meine Masterarbeit

ML Modell

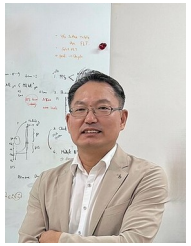
dmlc XGBoost

Datensatz

Portuguese Bank Marketing Data Set

Telemarketing campaign about term deposits

Verschlüsselungs-verfahren


C


K


K


S

Link zu den Slides