ETH zürich

# Building Foundations for Systems Security: From Trust to Verification

**Dr. Prof. Shweta Shinde**
Secure & Trustworthy Systems Group

# Devices make our life comfortable

# Software makes our devices useful


By 2025

Humanity's collective data will reach 175 zettabytes

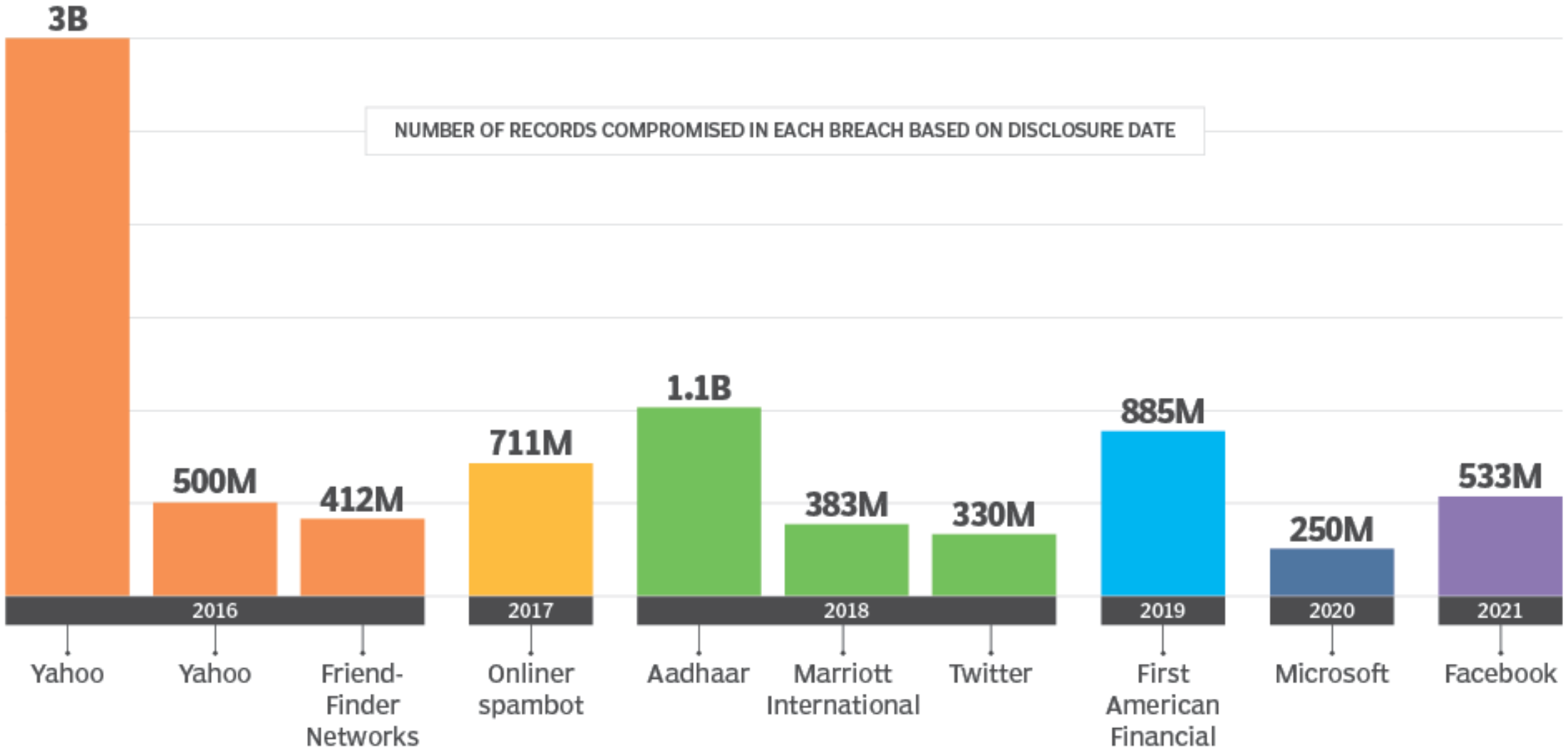
The number 175 followed by 21 zeros



https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020

# But, software also puts our data at risk

# 10 of the biggest data breaches in history



# Cyber-crime is growing exponentially

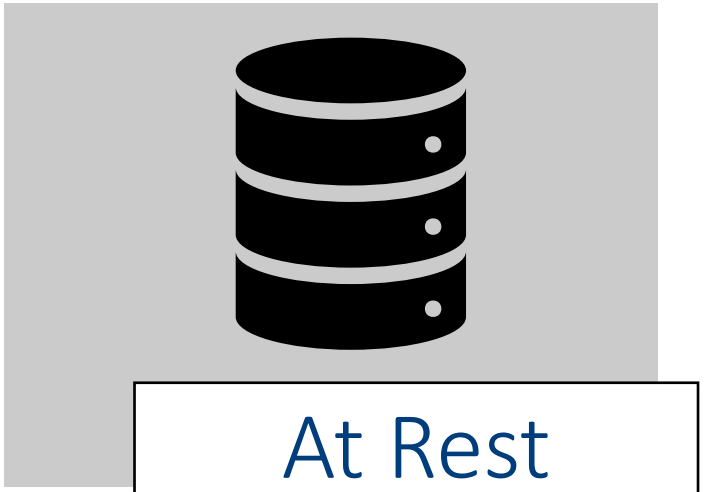
Cost of cybercrime is predicted to hit $8 trillion in 2023

Will grow to $10.5 trillion by 2025

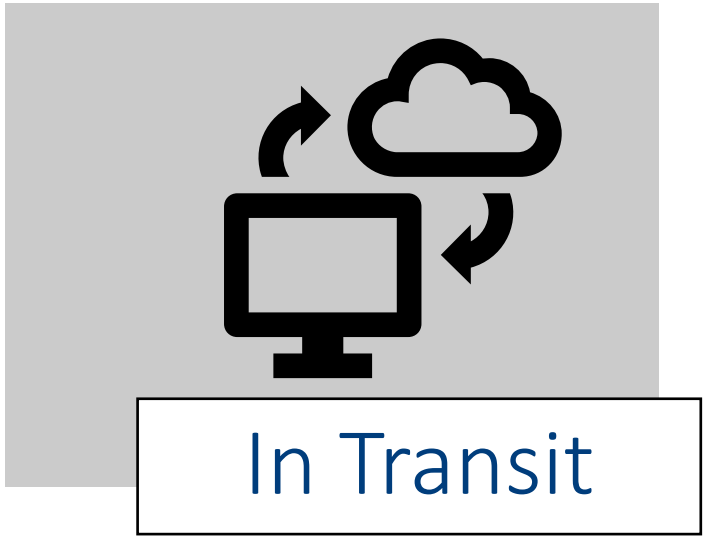


https://www.esentire.com/resources/library/2022-official-cybercrime-report

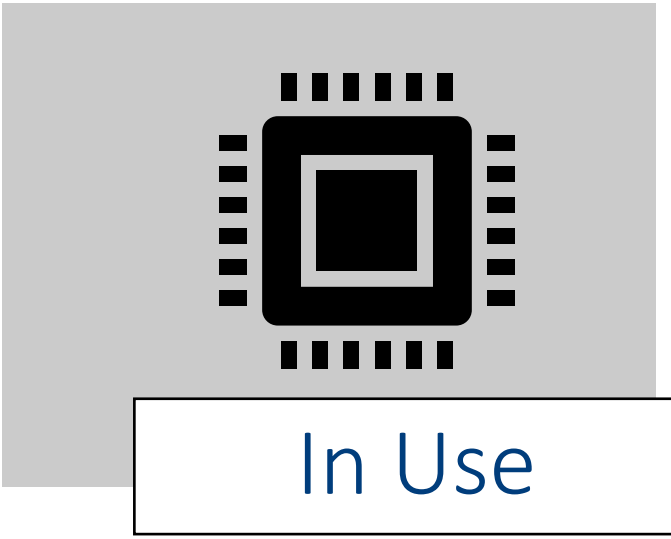
# Attack Surface for Confidential Data



At Rest

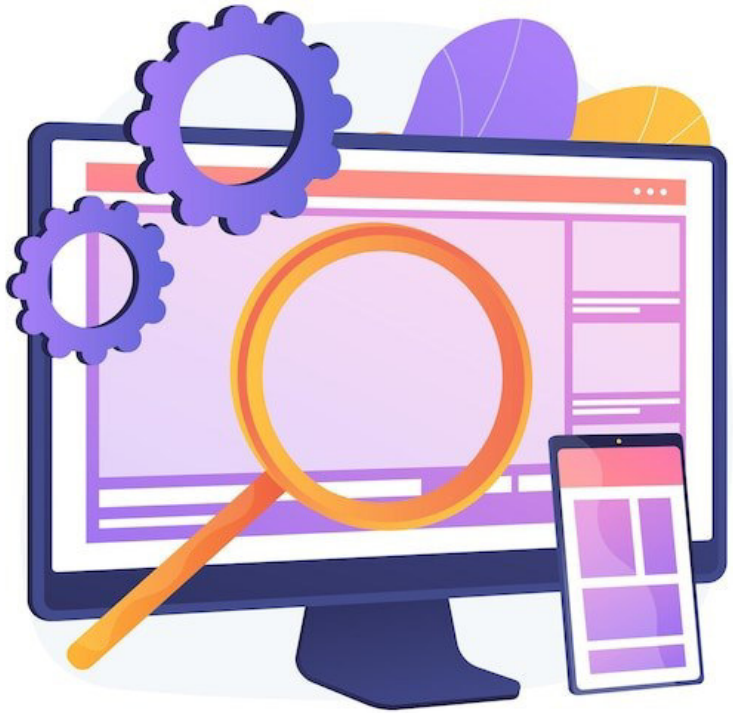


In Transit



In Use

# Attack Surface: Rest, Transit, Use

# Protecting Data at Rest

1. Data encryption

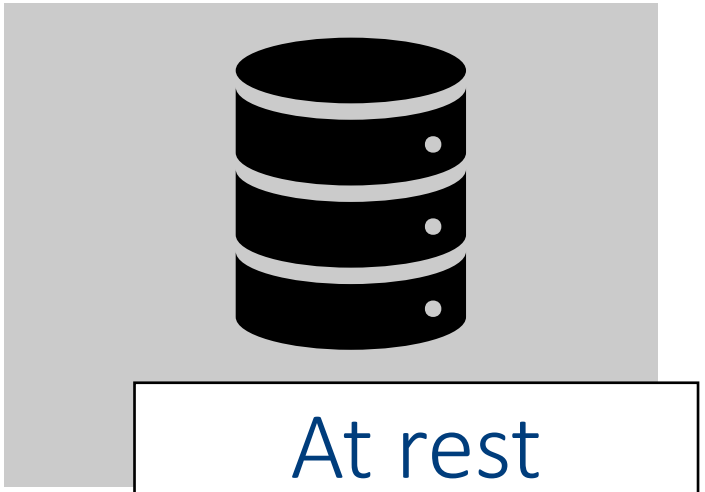
2. Policy implementation
   - limit access to certain records (e.g., health information)
   - encrypt file types before saving (e.g., spreadsheets)

# Protecting Data at Transit

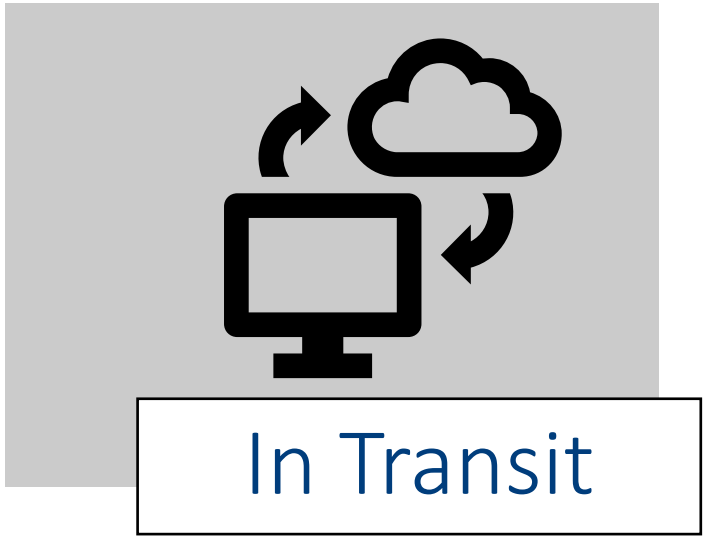
1. encryption
   - stop data interception

2. authentication
   - stop impersonation

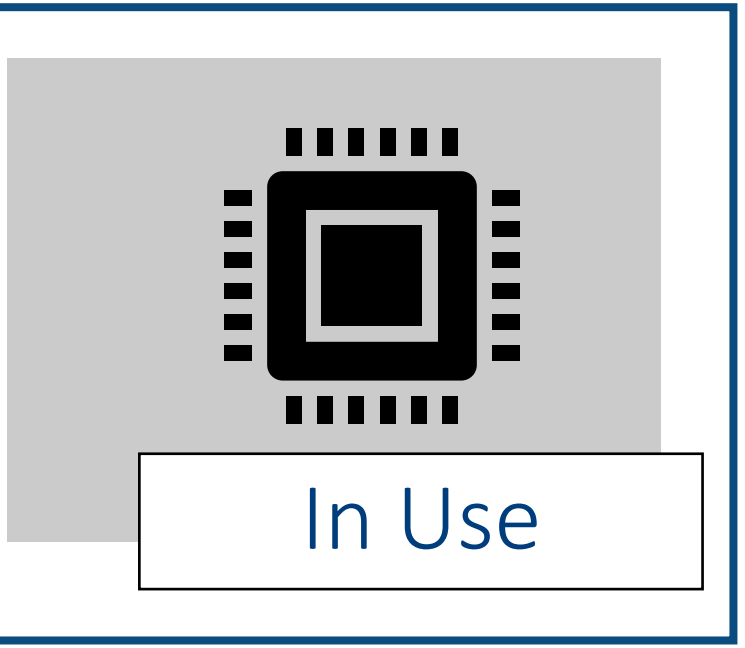
# Attack Surface for Confidential Data



At rest



In Transit

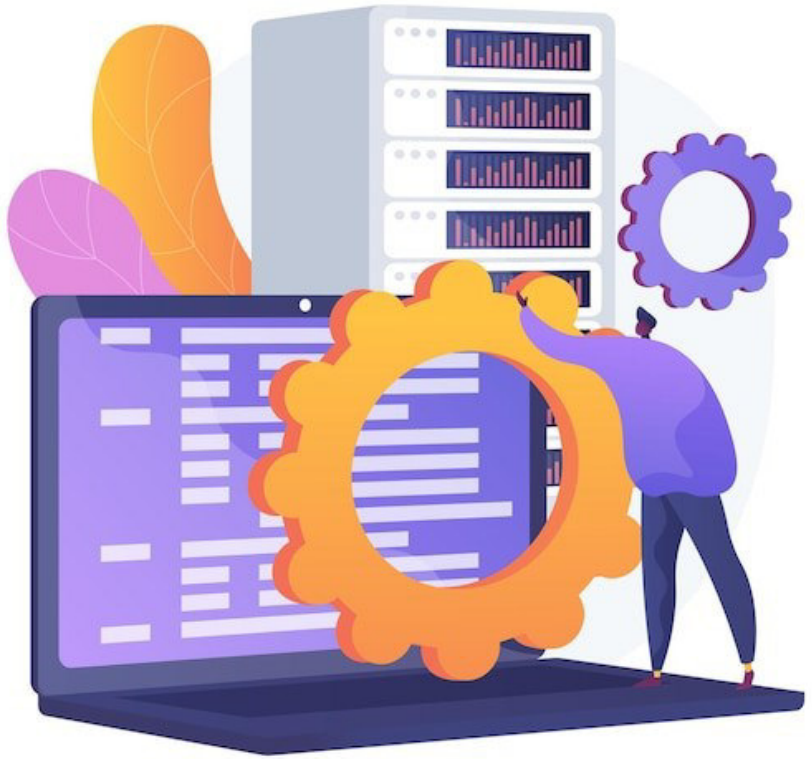


In Use

# Attack Surface: Data in-use

- Software
  - May have bugs

- Physical Access
  - Malicious operators
  - Legal obligation



# Protecting Data in-use

1. Homomorphic Encryption
   - Use data without ever decrypting it
   - Operate directly on encrypted data
   - Except encryption keys, no confidential data to leak!

2. Multi-party Computation
   - parties to jointly compute a function over their inputs
   - while keeping those inputs private

# Adoption of Multi-party computation

Market contribution (2021) 18-23%
Market growth (5-year) 145-150%

| Use case scenarios[1] | Description |
|---|---|
| Private data sharing | • Private or regulated data can be shared safely across enterprises with the guarantee of encryption across data storage, transmission, and processing. Such data sharing opens new avenues of collaboration and revenue generation for enterprises<br>• Examples include clinical trials, sharing of Real World Data (RWD) by healthcare providers, and Swiss banks sharing data outside of Switzerland |
| Multi-party analytics | • Enterprises can unlock new insights by collaboratively pooling and analyzing data across market participants. Confidential computing considerably reduces the risk of exposing sensitive data during analysis and enhances compliance to regulations<br>• Examples include fraud detection in BFSI, collaborative scientific research, conducting market studies, and customer data analysis across firms |
| Privacy-preserving AI/ML modeling | • Confidential computing helps keep the input data and output model secure throughout the training process<br>• Currently, the majority of modeling and simulations are conducted on data aggregated at a centralized location. MPC also enhances the value proposition for decentralized modeling techniques such as federated learning, wherein each node executes processes on a TEE |

clinical trials, sharing of Real World Data (RWD) by healthcare providers, and Swiss banks sharing data outside of Switzerland

Notable adopters

CREDIT SUISSE LYNXCARE RBC swisscom UCSF

# Why isn’t everyone use these techniques?

Both suffer from common challenges:

1. Slows down performance
2. Needs new software
3. Cannot support all computation

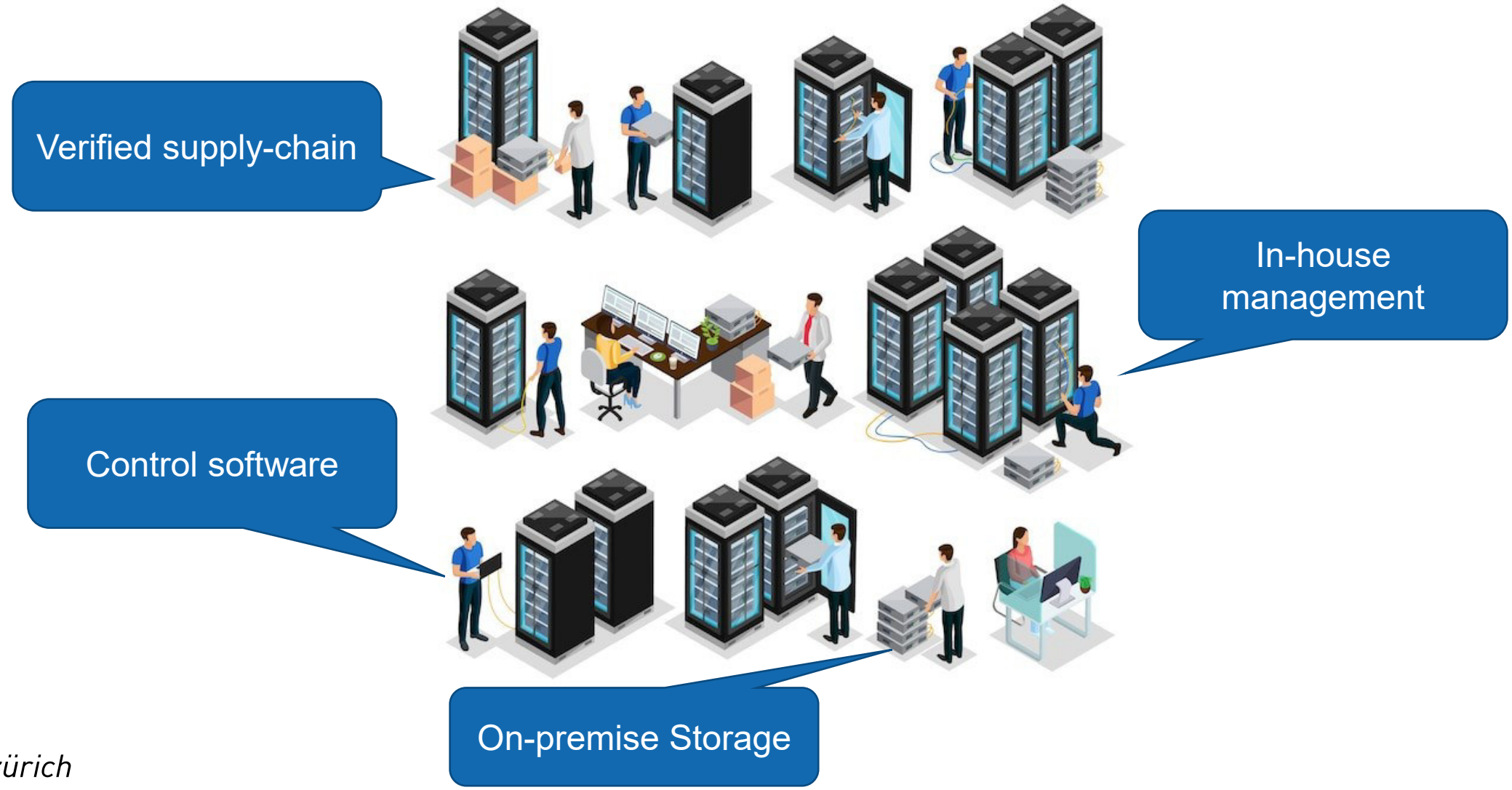
# What is the threat to data in use?


Trust is good?

30 Million
Lines of Code
Without Proofs

# Potential Solution: Self-hosted Infrastructure

Not always a practical solution

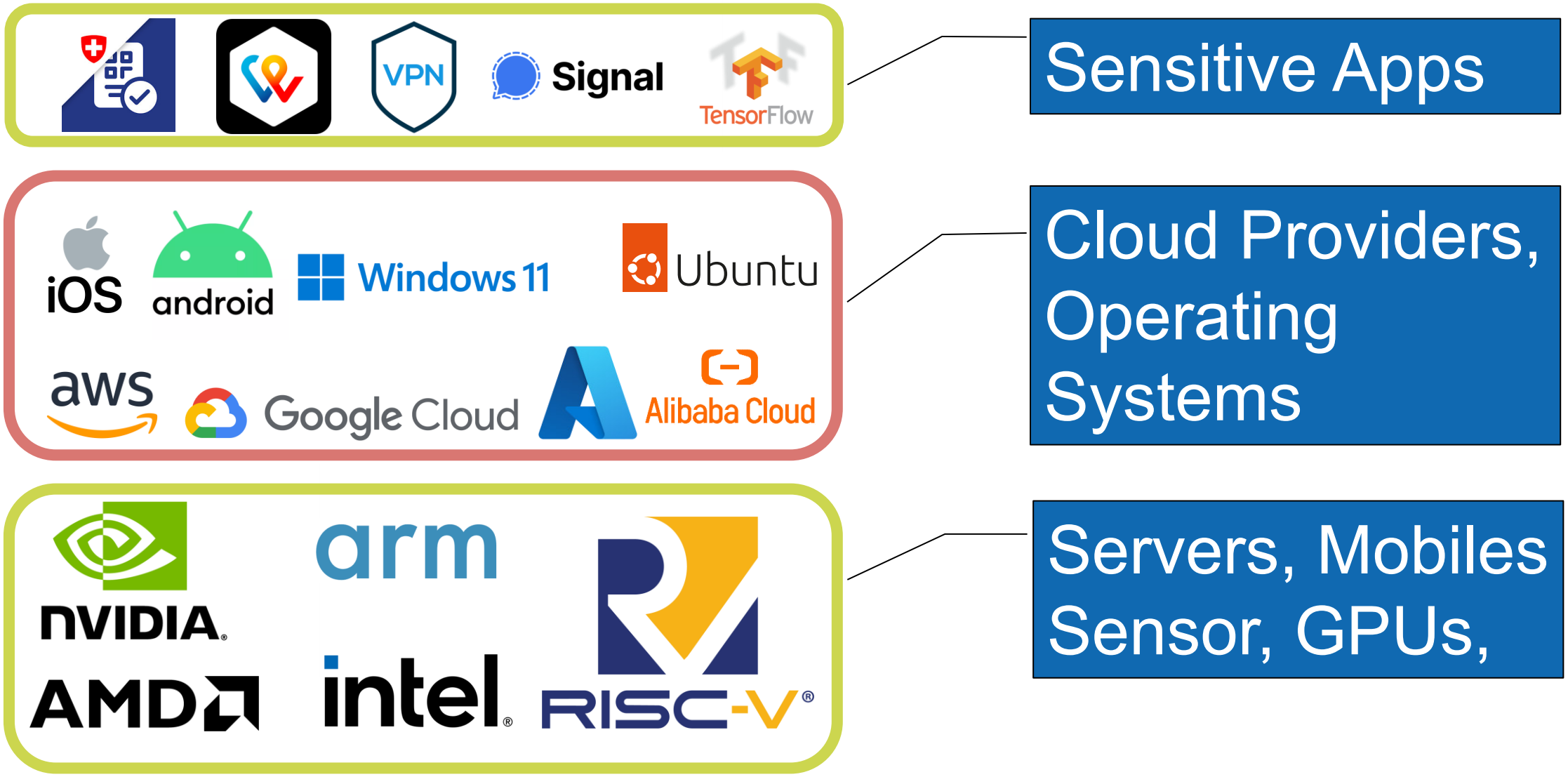


# Solution: Confidential Computing with Hardware-based Protection in the Cloud


Control is better!

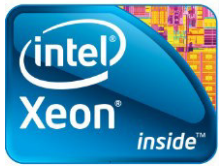
30 Thousand Lines of Code With Proofs

# Versatile Principle Applied to Real Systems



# Evolution of Confidential Computing


ARM TRUSTZONE






NVIDIA

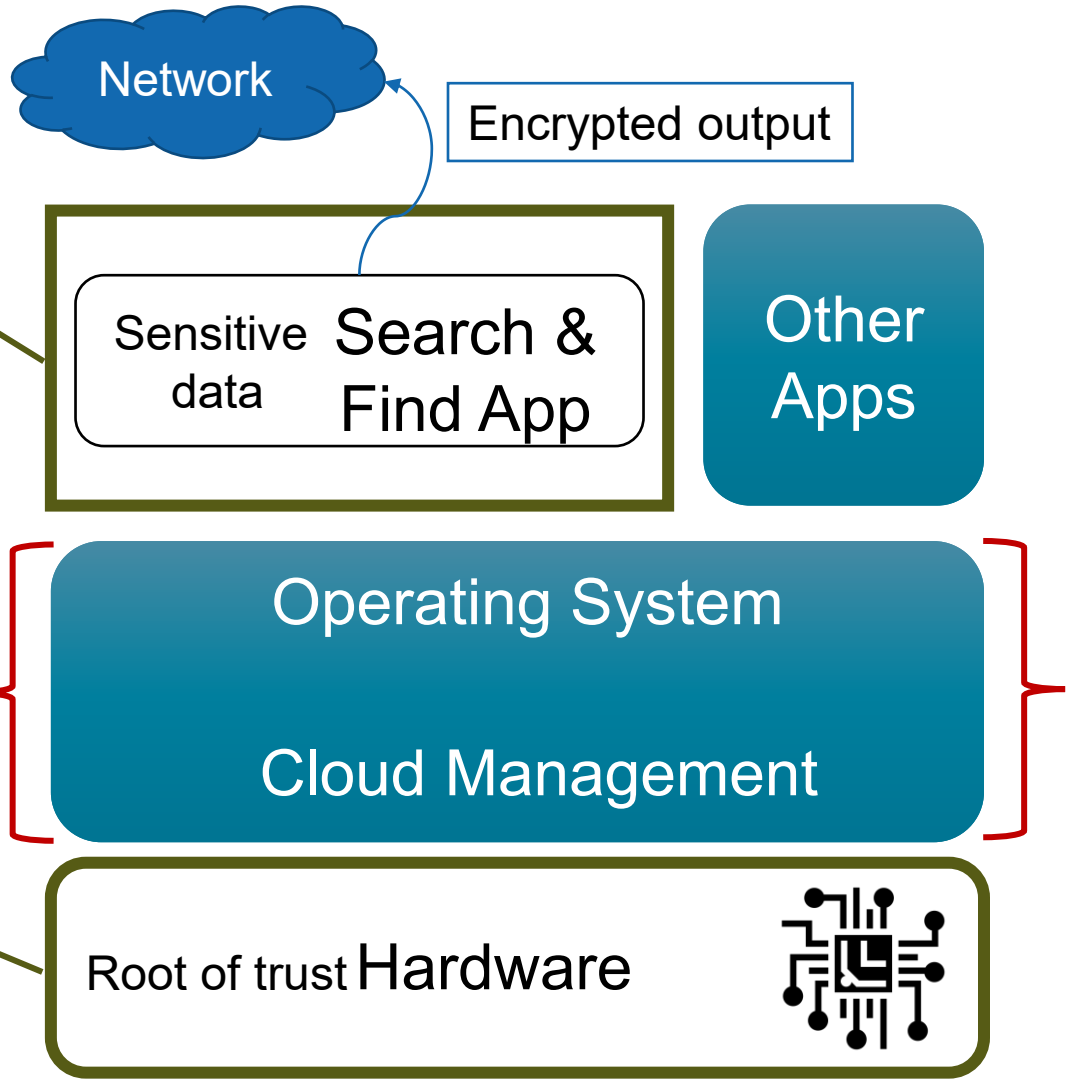
| 2004 | 2005 | 2006 | 2014 | 2015 | 2022 | 2023 |
|---|---|---|---|---|---|---|
| TPM 1.2 | ARM TrustZone | Intel TXT | TPM 2.0 | Intel SGX | NVIDIA CC | Intel TDX<br>ARM CCA |

# A Concrete Example

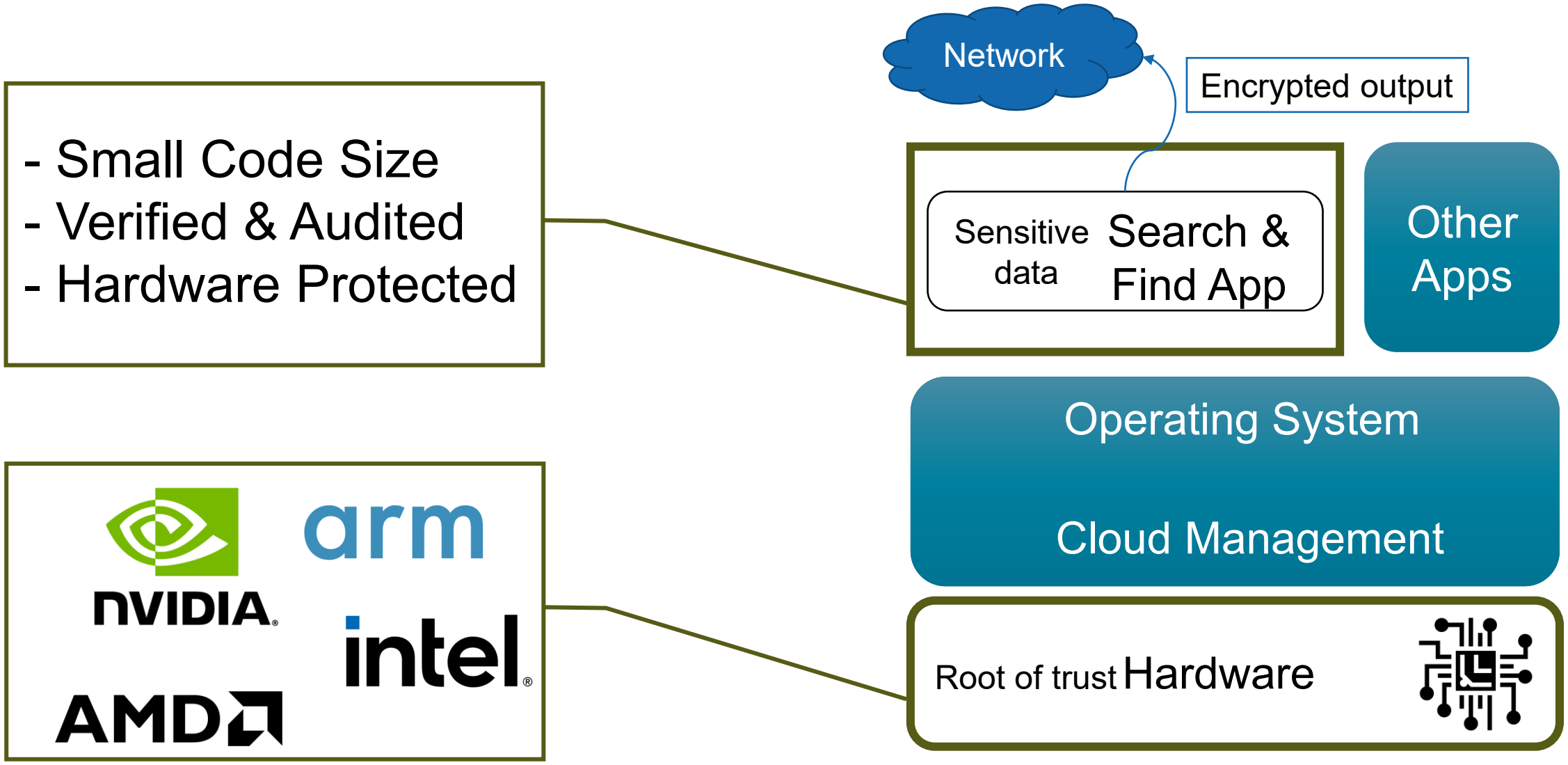
- Protect Sensitive Data
- Support Functionality (AI/ML)

- Nation State Adversaries
- Coercive Environment

- Trustworthy open alternatives
- Modularized trust design



# Confidential Computing for Software Security



# Solution: Confidential Computing with Hardware-based Protection on the Smartphone

# Summary

- Confidential data is at risk of attacks during
  - Rest
  - Transit
  - Use

- Protecting data in use is challenging at scale

- Using hardware-based confidential computing is a middle ground

# Thank you for your attention!

**Dr. Prof. Shweta Shinde**
shweta.shinde@inf.ethz.ch

ETH Zurich
Department of Computer Science
CAB F71.2
Universitätstrasse 6
8006 Zurich, Switzerland