

Seminar course

# Confidential Cloud Computing

(aka “c3-seminar”)

Preliminary meeting

<https://dse.in.tum.de/>

Dimitrios Stavrakakis, Dr. Masanori Misono, Patrick Sabanic,  
Prof. Pramod Bhatotia



Welcome to the c3 seminar!

## Chair of Distributed Systems & Operating Systems

<https://dse.in.tum.de/team/>



**Dimitrios Stavrakakis**

PhD student



**Dr. Masanori Misono**

Postdoc



**Patrick Sabanic**

PhD student

# Confidential cloud computing (c3): Seminar info



**Communication:**

Join us with TUM email address (@tum.de)

[ls1-courses-tum.slack.com](https://ls1-courses-tum.slack.com)

[#ws-24-c3-seminar](#)

<https://github.com/TUM-DSE/seminars/>

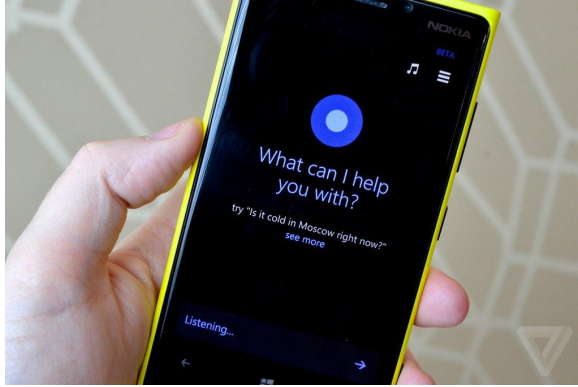
# Motivation & Context

# Cloud & data centers

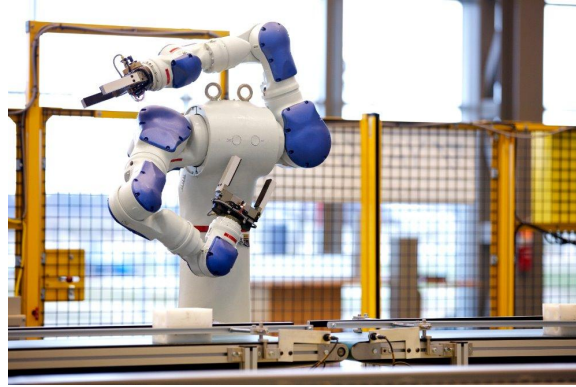


Scalable, flexible, and fault-tolerant computing substrate

# Process and store sensitive data



Consumer devices



Manufacturing



Healthcare

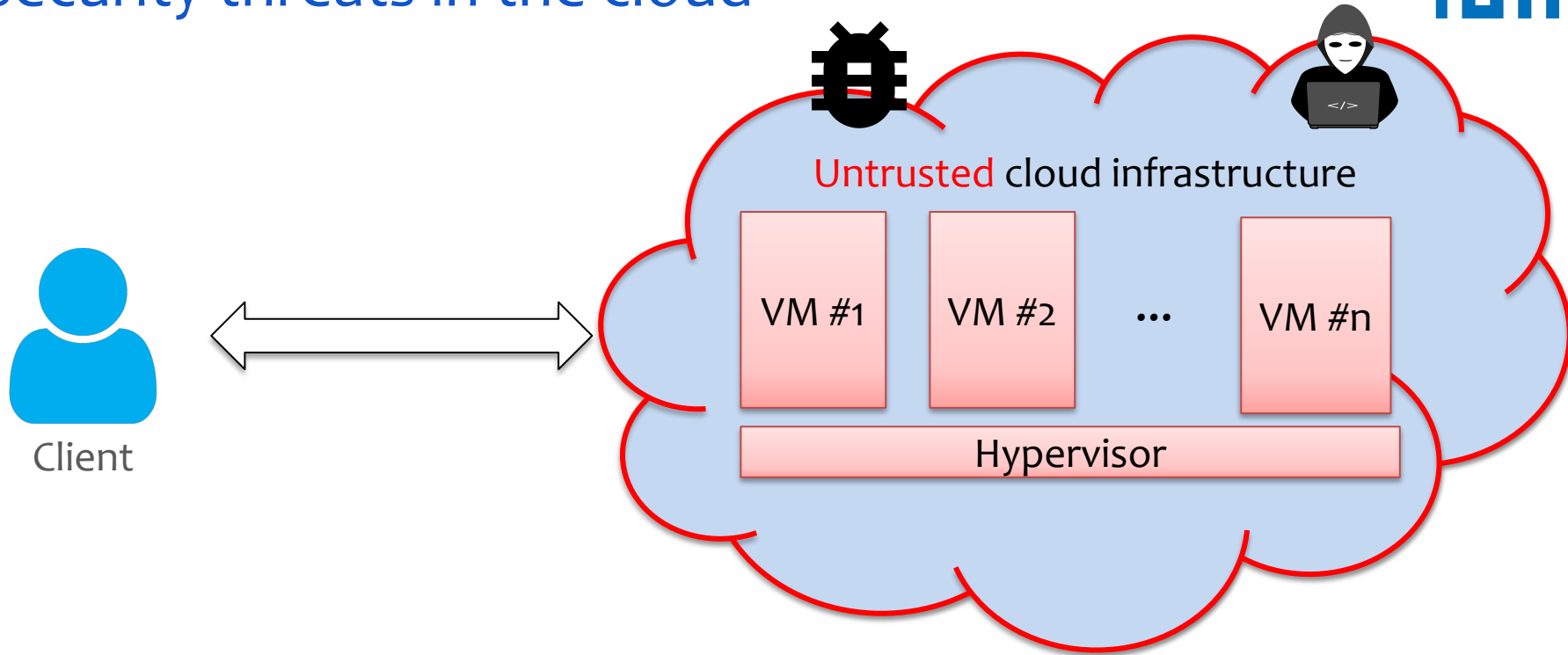


Transportation



Defense

# Security threats in the cloud



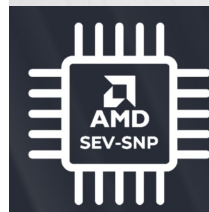
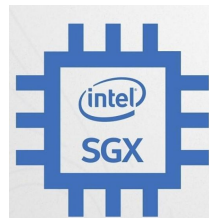
How can we provide **security** guarantees for workloads deployed on **untrusted** cloud infrastructures?



- Confidentiality
  - Unauthorized entities cannot “see” the computation/data
- Integrity
  - Unauthorized changes to the computation/data can be detected
- Freshness
  - Stateful computations are prone to rollback attacks (e.g., databases, storage)
- Authenticity
  - Remotely verify the authenticity of the remote party

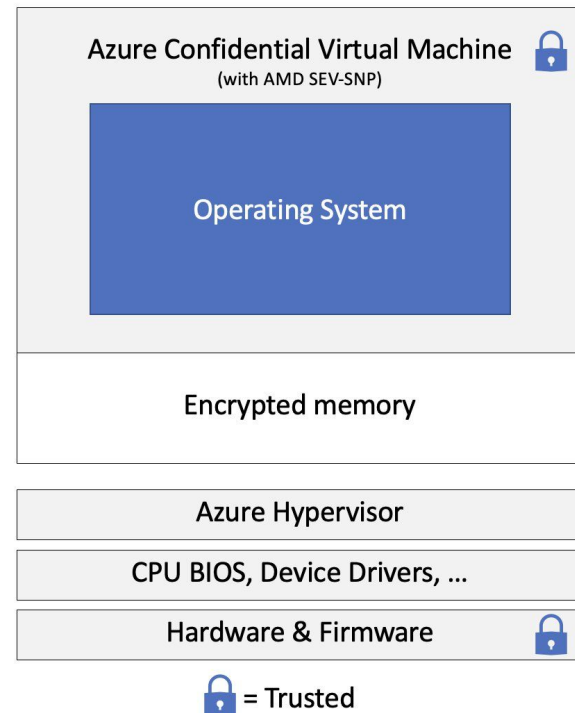
# Confidential computing

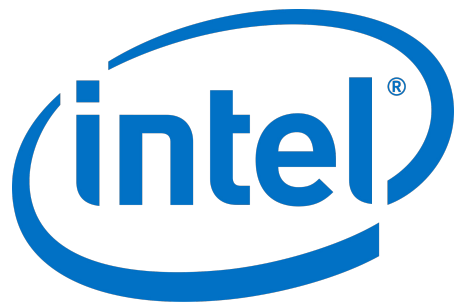
- **Confidential computing**
  - Cloud computing technology
  - Isolates sensitive data in a protected CPU “enclave” during processing
  - Even the cloud providers is out of the trusted computing base (Hypervisor)
- **Hardware assisted trusted computing**
  - Hardware extensions
  - Transparently encrypt/decrypt data in-use
- **Process based & VM-based deployments**



# Confidential computing in the cloud

- **Hardware-assisted “secure enclaves”**
  - Keep the data encrypted in DRAM
  - Special memory encryption engine for cache line data
  - Caches are in the protection boundaries
- **Confidential VMs**
  - Full VM encryption technology
  - Isolates from the untrusted cloud provider
  - No trust in the cloud infrastructure or hypervisor
- **Commercially offered by cloud providers**
  - Google Cloud, Microsoft Azure, Alibaba Cloud





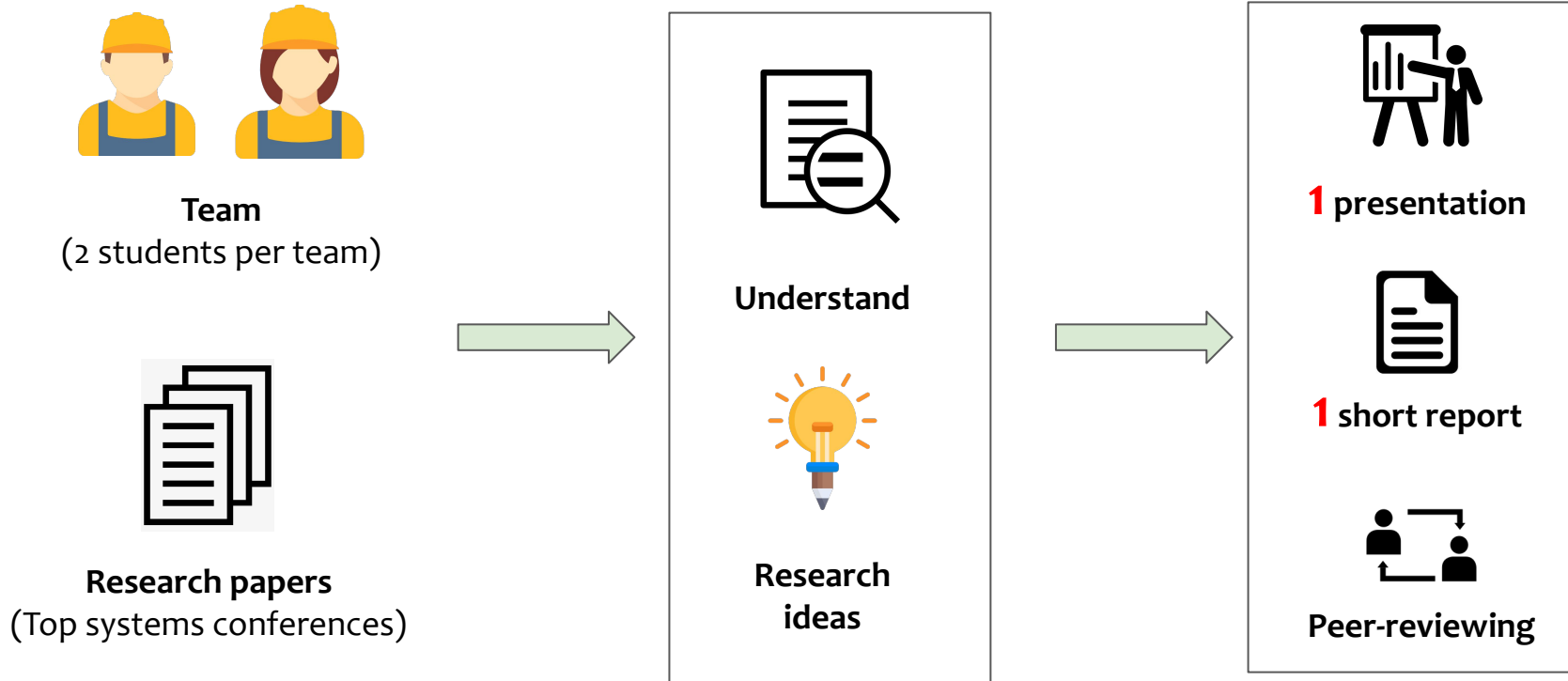
Process-based	Intel SGX	-	Arm Trustzone
VM-based	Intel TDX	AMD SEV	Arm CCA

Papers from top systems conferences: OSDI, EuroSys, ASPLOS, USENIX Security, IEEE S&P, ACM CCS

Topics
Confidential Virtual Machines (CVMs)
Trusted computing in the cloud
Confidential computing primitives
Operating systems and hypervisors
Hardware-assisted memory safety & security
Microarchitectural & software-based attacks & mitigations
...

Format

# Bird's eyes view



## Phase I

Kick-off



## Phase II: Understand & explore

Understand



Presentation

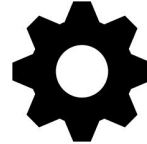


## Phase III: Research

Design



Implement  
( Bonus)



## Phase IV: Report & review

Report



Peer-review





# Phase I: Kick-off meeting



**Format and motivation**  
(all participants meeting)



**Team formation**  
(2 students per team)



**Paper selection**  
(Top systems conferences)



**The first week**

**NOTE**

1. A list of papers will be provided for FCFS bidding
2. Paper presentation guidelines will be provided for the next phase

# Phase II: Understand & explore



## Understand the paper(s)

### Focus

1. **Understand** the paper and related work
2. **Explore** a “laundry list” of research ideas/directions



## Paper presentation

### Focus

1. Explain the work/related work (“**why?**” and “**how?**”)
2. Explain and discuss all possible research directions
3. Pick a research direction



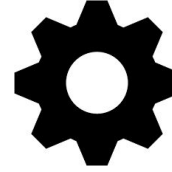
# Phase III: Research



## Research work

### **Focus:**

Indepth research work to nail-down the problem and detailed approach to solve it!



## Research prototype

### **Bonus: (Optional)**

**“Build the system to solve it!”** and show us the working idea and associated results



# Phase IV: Report & review



## Report

### Focus

Prepare a single “short & sweet” report summarizing

- (a) Paper
- (b) Research work



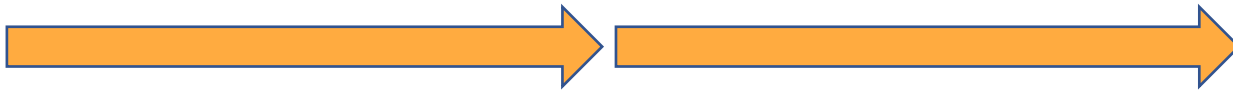
## Peer-review

### Focus

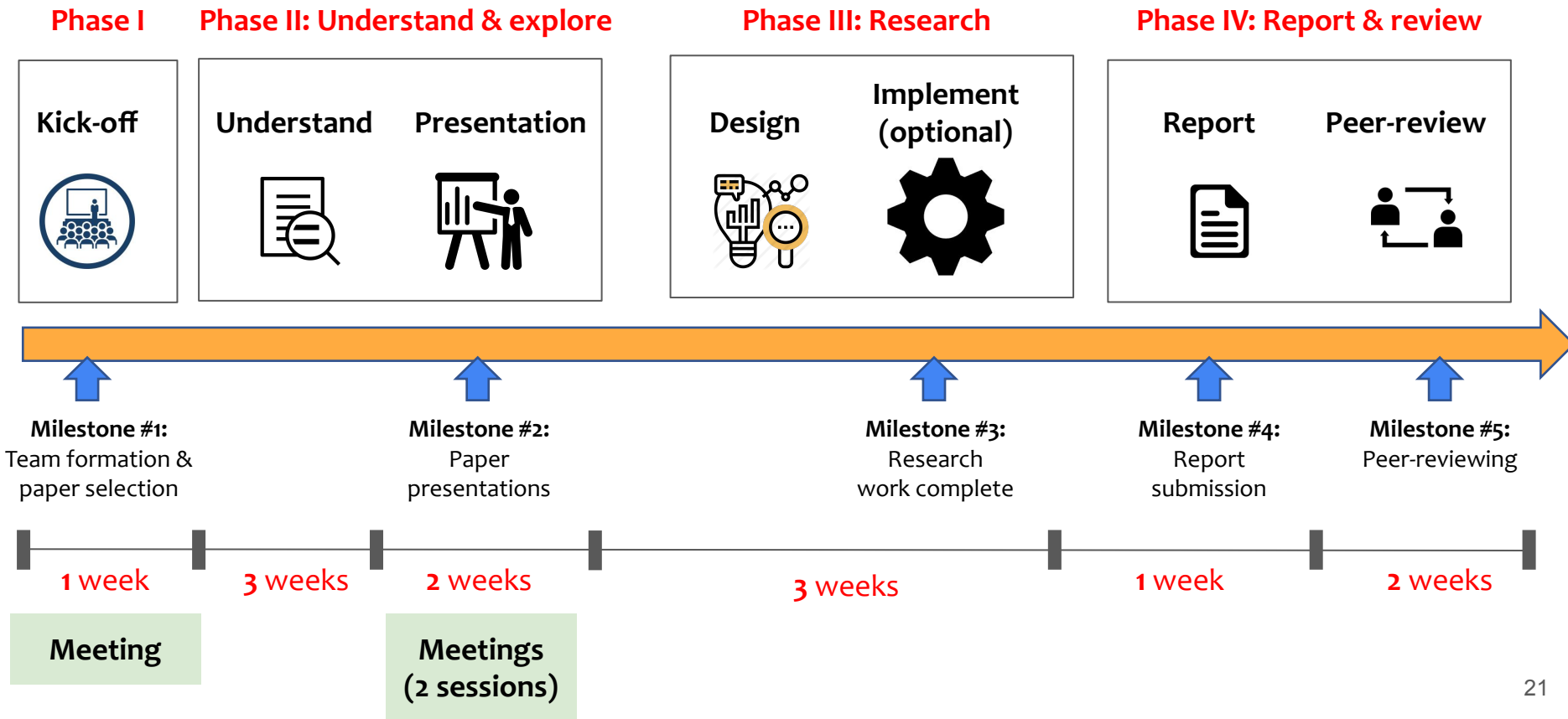
Give constructive (positive and critical) feedback for

- (a) Paper summary
- (b) Research work

# END.



# Overall timeline



- Format
  - Team-based seminar course (2 students per team)
- Communication
  - Slack for announcements and information sharing
  - Hotcrp for report submission and peer-reviewing
- Meetings (**in-person**, attendance is **compulsory**)
  - **Meeting #1:** Kick-off
  - **Meeting #2:** Paper presentation (Session 1)
  - **Meeting #3:** Paper presentation (Session 2)

# Learning goals

- Learn about the cutting-edge research in computer systems
- Promote critical thinking
- Cultivate an environment for innovation
  - To push the boundaries by advancing the state-of-the-art
- Improve scientific skills
  - Presentation
  - Writing
  - Communication: discussion and arguing
  - Mentorship: giving feedback and moderating discussion
- Encourage system building and evaluation
  - Learn by building, breaking, and benchmarking systems
- Importantly, to have fun!

- University plagiarism policy
  - <https://www.in.tum.de/en/current-students/administrative-matters/student-code-of-conduct/>
- Decorum
  - Promote freedom of thoughts and open exchange of ideas
  - Cultivate dignity, understanding and mutual respect, and embrace diversity
  - Racism and bullying will not be tolerated



# Interested?

## Matching platform

Welcome to the Matching platform [matching.in.tum.de/](https://matching.in.tum.de/)!

Dear students,

we changed the name of the course "Seminar: Recent advances in Computer Systems", for consistency reasons.  
The new name are "Seminar: Hot Topics in Computer Systems", now.

Login with your TUM identifier.

 TUM login

Login for exchange students  
(without TUM identifier)

 Exchange student login

Any questions? Visit the FAQs!

 FAQs

### Sign up on the TUM matching platform

# Contacts

- Dimitrios Stavrakakis
  - [dimitrios.stavrakakis@tum.de](mailto:dimitrios.stavrakakis@tum.de)
- **All seminar-related info:** <https://github.com/TUM-DSE/seminars>



**Workspace:** <http://ls1-courses-tum.slack.com/>

**Channel:** [#ws-24-c3-seminar](#)

Join us with TUM email address (@tum.de)