## Abstract

Digitalization is nowadays part of every industry and the amount of data that needs processing is steadily increasing every year with technologies such as the Internet of Things (IoT) and process automation in production environments. However, it is often not feasible for every individual company to host their own custom infrastructure, nor is it efficient as their demands are often heavily fluctuating. Therefore, in the last few years, an increasing amount of applications and processing in several domains have moved to the so-called cloud. This trend can be seen in the market size of cloud services which has quadrupled from 2017 to 2024 [1].

Yet, moving data to the cloud opens up vulnerabilities such as phishing attacks which leads to the data being stolen. Data breaches have increased in the last few years in both severity and associated costs [2]. Therefore, security demands have risen in the cloud computing field as well. This lead to a research topic intended to increase general general data security in the cloud, called *Confidential Computing*: With this, data is not only protected while *in transit* from one endpoint to another or stored on an encrypted hard-drive (i.e., *at rest*) but also while it is actively processed (i.e, *in use*) [3].

A company that has made notable effort in this field is AMD who have first released their *Secure Encrypted Virtualization* (SEV) technology in their servers in 2017 [4]. Their approach leverages RAM encryption to protect virtual machines running in the cloud. Over the last few years, their technology has advanced to also encrypt the corresponding CPU registers with *Secure Encrypted Virtualization - Encrypted State* (SEV-ES) [5] and keep encrypted memory consistent with *Secure Encrypted Virtualization - Secure Nested Pages* (SEV-SNP) [6].

Another topic relating to cloud computing are Unikernels. There, the operating system kernel is linked against its application during compile-time, leaving only functionalities that are necessary for this application integrated. Additionally, the isolation between individual users in the cloud is increased since each user has their own virtual machine separating them. This makes unikernels with their small footprint interesting in a field where resources are shared among many entities.

This talk is about combining SEV capabilities and the Hermit unikernel that is developed at RWTH Aachen Univeristy to increase its security.

## Bibliography

[1] “Public cloud computing market size 2025.” [Online]. Available: https://www.statista.com/statistics/273818/global-revenue-generated-with-cloud-computing-since-2009/

[2] IBM, “Cost of a Data Breach Report 2024,” 2024.

[3] T. L. Foundation, “Confidential Computing Consortium - Defining and Enabling Confidential Computing.” [Online]. Available: https://confidentialcomputing.io/wp-content/uploads/sites/10/2023/03/CCC_Overview.pdf

[4] D. Kaplan, J. Powell, and T. Woller, “AMD Memory Encryption,” Oct. 2021. [Online]. Available: https://www.amd.com/content/dam/amd/en/documents/epyc-business-docs/white-papers/memory-encryption-white-paper.pdf

[5] D. Kaplan, “Protecting VM Register State with SEV-ES,” Feb. 2017. [Online]. Available: https://www.amd.com/content/dam/amd/en/documents/epyc-business-docs/white-papers/Protecting-VM-Register-State-with-SEV-ES.pdf

[6] AMD, “AMD SEV-SNP: Strengthening VM Isolation with Integrity Protection and More,” Jan. 2020. [Online]. Available: https://www.amd.com/content/dam/amd/en/documents/epyc-business-docs/solution-briefs/amd-secure-encrypted-virtualization-solution-brief.pdf