# Confidential Cloud Services

Neele Peter
neele.peter@fau.de
Friedrich-Alexander-Universität Erlangen-Nürnberg

## ABSTRACT

In this paper I am going to compare two confidential cloud services, the Confidential Consortium Framework (CCF) [4] and Nimble [2]. They both provide

## 1 INTRODUCTION

A Confidential Cloud Service is an additional service that can be applied on top of an existing cloud provider [3]. These confidential services are needed, if properties have requirements of safety, which cannot be guranteed by a normal cloud provider.
The CIA triade 1 explains three important requirements of information security [5] [1]. It contains data confidentiality, Integrity protection and high availability. Data confidentiality is keeping the data private, which is very important especially for cloud providers. Challenges are encrypting the data and protecting the keys. Integrity protection is introduced as a requirement for data confidentiality. It is the ensurance of complete and correct code that is not changed by a bad party. But these two characteristics are hard to implement although they are mandatory for cloud computing. This is, because in clod computing the trusted computing base (TCB) gets bigger, so applications in the field of finances, medicine or governmental issues cannot afford to trust this whole TCB. High availability is required by the fact the people rely on the systems thatare on the cloud. So they should work, even if failures occur.

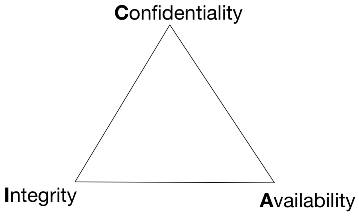

**Figure 1: Graphic of the CIA triade**

## 2 BACKGROUND

Before I start with an example of a confidential cloud service some definitions must be clear to understand the following parts.

### 2.1 Trusted Execution Environments

A Trusted Execution Environment (TEE) is a hardware based component where critical an be runned inside a part called Enclave. The code inside this Enclave is hard to modify by malicious parties and can thus be trusted more and is therefore often be used for confidential computing. But of course it is not impossible to change code inside a TEE, so this eventualities should also be ekpt in mind.

### 2.2 Rollback Attacks

There exist many different attacks for cloud services like forking attacks, side channel attacks or rollback attacks. These are all important attacks that should be protected by a confidential cloud service, but in this paper I will focus on rollback attacks.
In this attack malicious parties safe an older version of the system and apply this older version. So they "roll back" the state of the system. This can be useful for guessing encryption keys. For keys there often exist some limitations of guesses, so the key cannot get brute forced. The problem is with rolling back the state of the system a malicious member can go back to the state before the first try and try guessing again. So brute forcing the encryption key is still possible by using these attacks.

## 3 CCF

One example of service, that can be added on a cloud to make it confidential is the Confidential Consortium Framework (CCF) [4]. It wants to guarantee the CIA requirements (confidentiality, integrity and availability) on multiparty applications.

### 3.1 Idea

### 3.2 Confidentiality

### 3.3 Reconfiguration

### 3.4 Desaster Protocol

### 3.5 TCB

### 3.6 Challenges

As mentioned before CCF does not have a rollback detection, because it allows rollback attacks to happen, because it is not affecting the system. The problems are that they (1) make the assumption that the code inside the TEE cannot be changed and (2) that thy put their persistent storage outside the TEEs and is therefore not protected for a rollback attack.

# 4 COMPARISON WITH NIMBLE

Another example for such a service is Nimble [2]. It also tries to ensure the requirement of the CIA triad, but has the focus of preventing rollback attacks.

## 4.1 Idea

## 4.2 Confidentiality

## 4.3 Reconfiguration

## 4.4 Desaster Protocol

## 4.5 TCB

## 4.6 Challenges

# 5 RELATED WORK

# 6 CONCLUSION

# REFERENCES

[1] Michael Aminzade. Confidentiality, integrity and availability–finding a balanced it framework. *Network Security*, 2018(5):9–11, 2018.

[2] Sebastian Angel, Aditya Basu, Weidong Cui, Trent Jaeger, Stella Lau, Srinath Setty, and Sudheesh Singanamalla. Nimble: Rollback protection for confidential cloud services (extended version). Cryptology ePrint Archive, Paper 2023/761, 2023. https://eprint.iacr.org/2023/761.

[3] Sascha Fahl, Marian Harbach, Thomas Muders, and Matthew Smith. Confidentiality as a service–usable security for the cloud. In *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, pages 153–162. IEEE, 2012.

[4] Heidi Howard, Fritz Alder, Edward Ashton, Amaury Chamayou, Sylvan Clebsch, Manuel Costa, Antoine Delignat-Lavaud, Cedric Fournet, Andrew Jeffery, Matthew Kerner, Fotios Kounelis, Markus A. Kuppe, Julien Maffre, Mark Russinovich, and Christoph M. Wintersteiger. Confidential consortium framework: Secure multiparty applications with confidentiality, integrity, and high availability, 2023.

[5] Michael E Whitman, Herbert J Mattord, et al. *Principles of information security*. Thomson Course Technology Boston, MA, 2009.