Confidential Cloud Services

Neele Peter
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 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.

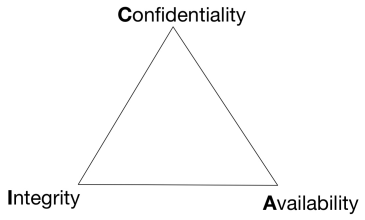

Figure 1: Graphic of the CIA triad

2 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 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 COMPARISON

4.1 Rollback Attacks

4.2 Reconfiguration

4.3 Desaster

4.4 Usecase

5 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.