Confidential and Privacy-Preserving Computing in Distributed Systems

Bachelor's Thesis of

Wenzhe Vincent Cui

at the Department of Informatics
KASTEL – Institute of Information Security and Dependability

Reviewer:	Prof. A
Second reviewer:	Prof. B
Advisor:	M.Sc. C
Second advisor:	M.Sc. D

xx. Month 20XX – xx. Month 20XX

Karlsruher Institut für Technologie
Fakultät für Informatik
Postfach 6980
76128 Karlsruhe

I declare that I have developed and written the enclosed thesis completely by myself. I have submitted neither parts of nor the complete thesis as an examination elsewhere. I have not used any other than the aids that I have mentioned. I have marked all parts of the thesis that I have included from referenced literature, either in their original wording or paraphrasing their contents. This also applies to figures, sketches, images and similar depictions, as well as sources from the internet.

PLACE, DATE

. . . . . .

(Wenzhe Vincent Cui)

Abstract

English abstract.

Zusammenfassung

Deutsche Zusammenfassung

Contents

List of Figures

List of Tables

1. Introduction

1.1. Motivation

1.2. Research Methodology

2. Confidential Computing

2.1. Trusted Execution Environments (TEEs)

Defined by Confidential Computing Consortium.

2.1.1. Properties

- Data confidentiality
- Data integrity
- Code integrity

Depending on the specific TEE, it may also provide:

- Code confidentiality
- Authenticated Launch
- Programmability
- Attestation
- Recoverability

2.1.2. Confidential Computing Environments (CCEs)

Defined by Edgeless Systems. Trusted Execution Environment with specific capabilities:

- Runtime encryption (Data confidentiality/integrity)
- Isolation
- Remote attestation

2.2. TEE Flavors

2.2.1. Virtual-Machine-based TEE

AMD SEV, Intel TDX, IBM Secure Execution and PEF, ...

2.2.2. Process-based TEE

Intel SGX, ...
Application Splitting:

- Enclave
- Host

3. Privacy-Preserving Computing

3.1. Secure Multi-Party Computation

3.2. Homomorphic Encryption

4. Case Studies

4.1. Confidential Containers

4.2. Marble Run

4.3. Constellation Kubernetes

4.4. Sharemind

4.5. Veracruz

5. Evaluation

6. Conclusion

…

A. Appendix

A.1. First Appendix Section

Figure A.1.: A figure

...