Fachhochschule Aachen

Campus Jülich

Fachbereich: Medizintechnik und Technomathematik

Studiengang: Technomathematik

Secure Multi-Party Computation for Decentralized Distributed Systems

Masterarbeit von Frederic Klein

Diese Arbeit wurde betreut von:

1. Prüfer: Prof. Dr. rer. nat. Alexander Voß
2. Prüfer: Dr. Stephan Jonas

Aachen, Dezember, 2016

Diese Arbeit ist von mir selbständig angefertigt und verfasst. Es sind keine anderen als die angegebenen Quellen und Hilfsmittel benutzt worden.

Frederic Klein .....
Unterschrift

Abstract

1 page

Contents

List of Figures

List of Tables

List of Acronyms

LAN local area network.

SMPC secure multi-party computation.

SPAN smart phone ad hoc network.

Chapter 1

Introduction

In the last couple of years gamification has found it's way into many areas of our daily life. In regard to our personal life, companies like Amazon or Runtastic can base their gamification approach on publicly sharing personal achievements and statistics to improve user commitment. Gamification concerning our work life on the other hand can have much higher privacy demands. Since comparison is a key component for the gamification approach, privacy protecting computations of system wide statistical values (for example minimum and maximum) are needed. The solution comes in the form of secure multi-party computation (SMPC), a subfield of cryptography.

Existing frameworks for SMPC utilize the Internet protocol, though access to the Internet or even a local area network (LAN) cannot be provided in all environments. Especially many hospitals tend to avoid Wi-Fi to reduce the risk of electromagnetic interference with medical devices.

To be able to utilize SMPC in environments with Wi-Fi restrictions, this thesis studies the characteristics of mesh-networks and proposes describes the design of a SMPC framework for mesh-networks.

Context

Restatement of the problem

Restatement of the response

Roadmap

Chapter 2

Foundation

2.1 Case Study: "The Hygiene Games"

Gamification

Wireless Networks in Hospitals

2.2 Secure Multi-Party Computation

Secure Addition Protocol

Secure Comparison Protocol

Differential Privacy

Existing Frameworks

2.3 Mobile Ad Hoc Networks

- continuously self-configuring
- self-forming
- self-healing
- infrastructure-less
- peer-to-peer

- Difference to mesh: mobility of nodes

Smart Phone Ad Hoc Network

Example: firechat

Comparison to Wi-Fi Direct

- SPAN support multi-hop relays
- Wi-Fi Direct since Android 4.0
- Wi-Fi Direct: Soft AP

Wi-Fi Based smart phone ad hoc network (SPAN)

Bluetooth Based SPAN

2.4 Distributed Computing

Coordinator Election

Chapter 3

Methodology and Implementation

Chapter 4

Evaluation

Chapter 5

Conclusion

Appendix A

Some name

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.