

ALMA MATER STUDIORUM · UNIVERSITÀ DI BOLOGNA

SCUOLA DI INGEGNERIA E ARCHITETTURA
DIPARTIMENTO DI INFORMATICA-SCIENZA E INGEGNERIA (DISI)
Corso di Laurea Magistrale in Ingegneria Informatica

**TITOLO
DELLA
TESI**

Candidato:
Angelo Feraudo

Relatore:
Prof. Paolo Bellavista

Correlatore:
Prof. Jon Crowcroft

Anno Accademico 2018/2019
Session III

Ringraziamenti

Abstract

Contents

Introduction	6
1 Technical background	7
1.1 Manufacturer Usage Description	7
1.2 Firewall	7
1.3 Federated learning	7
1.4 Network traffic	7
2 Existing technologies	8
2.1 MUD: MUD manager implementations	8
2.1.1 Security challenges	8
2.2 Federated Learning: setups and frameworks	8
2.2.1 Basic setup	8
2.2.2 DIoT	8
2.2.3 Tensor Flow Federated	8
2.2.4 PySyft	8
3 System design	9
3.1 MUD capable network	9
3.1.1 General description	9
3.1.2 Open Source MUD Manager	9
3.1.3 User Policy Server	9

3.2	Federated anomaly detection system	9
3.2.1	Federated Learning Architecture	9
3.2.1.1	Implementation	9
3.2.1.2	Model	9
3.2.1.3	Deployment	9
4	Evaluations	10
5	Related work	11
6	Future work	12
	Conclusion	12
	Bibliography	14

Introduction

Chapter 1

Technical background

1.1 Manufacturer Usage Description

1.2 Firewall

1.3 Federated learning

1.4 Network traffic

Chapter 2

Existing technologies

2.1 MUD: MUD manager implementations

2.1.1 Security challenges

2.2 Federated Learning: setups and frameworks

2.2.1 Basic setup

2.2.2 DīoT

2.2.3 Tensor Flow Federated

2.2.4 PySyft

Chapter 3

System design

3.1 MUD capable network

3.1.1 General description

3.1.2 Open Source MUD Manager

3.1.3 User Policy Server

3.2 Federated anomaly detection system

3.2.1 Federated Learning Architecture

3.2.1.1 Implementation

3.2.1.2 Model

3.2.1.3 Deployment

Chapter 4

Evaluations

Chapter 5

Related work

Chapter 6

Future work

Conclusion

Bibliography