netidee

STIPENDIEN

Trustworthy Context-Aware Access Control in IoT Environments based on the Fog Computing Paradigm

Endbericht | Call 15 | Stipendium ID 5294

Inhalt

1 Einleitung

The strongly increasing connectivity and interest in today's Information Technology (IT) infrastructure resulted in a huge amount of interconnected networks building the Internet of Things (IoT). Future development of IoT services strives to build **low-latency, reliable, highly distributed systems**, which cannot be fully satisfied through Cloud Computing capabilities. Compared to that, computing capabilities distribution paradigms, among others, Edge Computing (EC) and **Fog Computing (FC)**, aim to deploy computing and storage resources at the IoT networks' edge.

Furthermore, the central point for establishing IoT services is deploying computationally constrained IoT devices (sensors, actuators), which fail to offer adequate security mechanisms and protect transmitted information. As IoT devices are dominantly deployed at the IoT networks' edge, securing them using FC or EC would significantly improve IoT solutions' overall safety and acceptance.

2 Allgemeines

This dissertation aims at developing distributed security mechanisms for IoT systems based on the FC paradigm. The main goal is to bridge the security services provisioning between resource-limited Things and computationally rich remotely deployed Cloud Computing servers. A further goal is to enable the automation of the security services using context information in the IoT environment. To achieve these goals, research goals aim at enabling the following features in IoT systems:

- **Secure deployment** of FC-based services;
- Establishing FC-based **Identity and Trust Management** for IoT;
- **Access Control (AC)** distribution and its extension through **Context-Awareness (C-A)**.

Based on these goals, the key research questions have been defined:

1. **RQ 1** - How can decentralized management of access control be achieved in a Fog computing environment?
2. **RQ 2** - How can Fog computing be used for improving Identity management and authentication in IoT systems?
3. **RQ 3 -** How can context-awareness be incorporated in access control of a Fog computing based IoT system?

Since RQ1 focuses on AC mechanisms in IoT, answering it involved analyzing the distribution of security policies management for IoT use-cases, with a special focus on **AC schema modeling** and enabling **fine-granularity and extensibility for C-A factors**. Since the traditional solutions for AC distribution (LDAP, OAuth2, Shibboleth) fail to comply with FC requirements for the operability of FC service in “offline” scenarios, that is, when Cloud Server is unreachable, rethinking of AC

distribution practices was necessary. Moreover, numerous IoT services provided through a variety of IoT devices dictate seeking a generic AC model that offers extensibility for future IoT services. For that purpose, mainstream AC models like RBAC and IBAC are compared against the novel model models (e.g., CAPBAC, ABAC, LATBAC), resulting in the choice of ABAC as a promising solution for building the FC-based AC system.

RQ 2 examines research challenges in (1) Identity Management (IdM) and (2) mutual authentication, leading to trust establishment and maintenance in IoT systems. Enabling mutual authentication in IoT requires analysis of models for building and managing trust (PKI, Web of Trust, Kerberos). Thereby, the critical topic is the application of encryption algorithms and **Key Management Protocols (KMP)**, primarily due to the Things' resource constraints and the scale of IoT networks. Therefore, analysis of the state-of-the-art trust management approaches focused on their applicability in IoT networks concerning introduced computational and networking overhead and the possibilities to shift computationally demanding operations from IoT to Fog Node devices and allow better network scalability.

Since AC mechanisms are the central point for configuring and applying security policies, their integration with content analysis and enabling adaptable**, "smartified" security policy management** is researched in RQ 3. To achieve this, various C-A sources are examined concerning the context information they are analyzing and integration points with established AC models. Firstly, context quantification and management approaches have been examined. This involves the identification of context sources and context information collection, processing, and distribution procedures. Secondly, strategies for building C-A AC systems have been evaluated, leading to the design requirements for developing the C-A AC solution, i.e., scalability, extensibility, rich and comprehensive modeling, and automatic context lifecycle management.

3 Ergebnisse

The contributions of my dissertation revolve around the research questions outlined in the previous section, with the significant goal of advancing the state-of-the-art in creating trustworthy security services at the edge of IoT networks through the proposed messaging and data models. The main thesis contributions are categorized into three major research areas: FC, trust management, and Context-Aware Access Control (C-A AC).

Contributions to all given research areas are represented through protocols, data models, simulations, and IoT services deployment strategies. To evaluate them, the smart home IoT framework called COSYLab (https://github.com/nemanja-ignjatov) is implemented in the scope of my dissertation. This framework offers implemented Cloud and Fog services for trust management and C-A AC in FC-based IoT, as presented in Figure 1. COSYLab services overviewFigure 1.

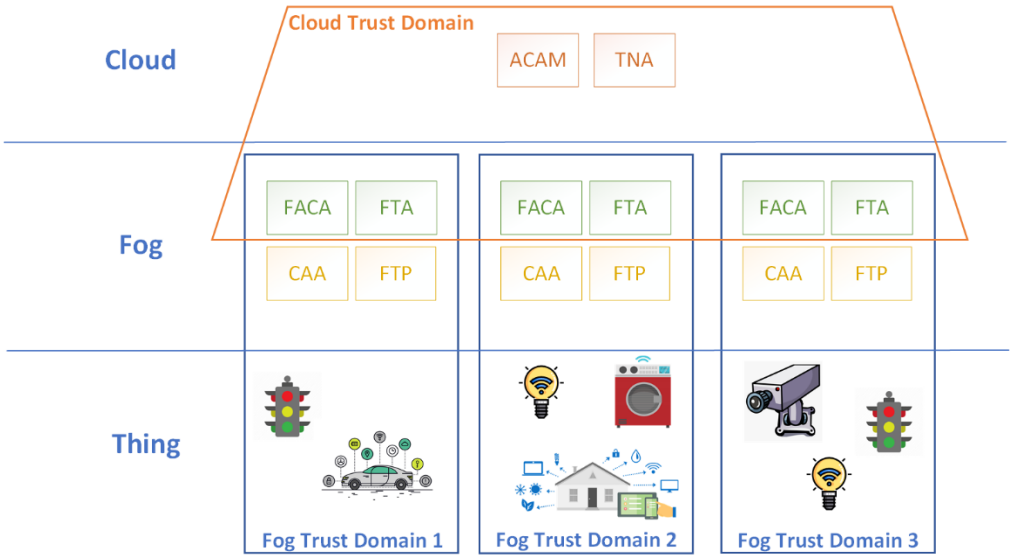

Figure 1. COSYLab services overview

Contributions in the trust management area are achieved through the developed FC-based trust management framework, establishing the trustworthiness of Things, FC-based IoT services, and IoT users. Achieving the dynamicity and scalability of trust management in IoT networks required low latency, distributed trust establishment mechanisms, and KMPs. For this reason, trust models such as direct trust and Web-of-Trust were not applicable, and a hierarchical trust model based on Public-Key Infrastructure (PKI) has been selected.

Since public-key cryptography enforces computationally demanding operations, its feasibility on resource-constrained IoT devices has been examined through simulations. For that purpose, a simulation engine for performance evaluation of various aspects of hierarchical trust management models is designed and implemented. Simulation results enabled the comparison of encryption schemes (RSA and EC) and key exchange protocols (Diffie-Hellman and Qu-Vanstone) concerning CPU, memory consumption, and introduced latency. Based on the simulation results, EC encryption with Diffie-Hellman key exchange has been chosen for building trust management services in COSYLab.

The implemented trust management services (1) Trustworthy Network Trust Anchor (TNTA), (2) Fog Trust Anchor, and (3) Fog Trust Provider are presented in Figure 1. These services are deployed in different trust domains – Cloud and Fog. Through this separation, each trust domain ensures operability in “offline” FC scenarios, ensuring the robustness of the implemented solution independent of the network quality.

Finally, the developed trust management system is extended through security profiles to support identity and key management procedures for the Things that are not capable of supporting digital certificates. This enables End-to-End identity and trust management mechanisms in IoT through FTP services hosted on Fog Nodes.

Distribution of AC mechanisms is achieved through Access Control Agents Management (ACAM) and Fog Access Control Agent (FACA), which enable AC support for Cloud and Fog domains, respectively. The developed AC distribution model enables mutual authentication between Fog and Cloud AC components using the above-mentioned trust management solution. Moreover, AC distribution allows security policies enforcement close to the IoT devices, reducing processing and data transmission latency.

Besides the trust management AC distribution aspect, local AC provisioning through the FACA deployment on Fog Node requires maintaining consistency of security policies between Cloud Server and Fog Node. Security policy consistency is ensured between FACA and ACAM through the synchronization protocols that enable/disable IoT services in ACAM and the distribution of security policy configuration to all FACA services. Based on the ACAM configuration FACA adapts its security policies and allows the prompt intervention of system administrators in case of an attack on IoT services, minimizing the damage that can occur on users' IoT devices.

Extending AC mechanisms with context information utilized the results from the analysis of context information quantification techniques along with collection and aggregation strategies and building a data model for integrating context information into security policies. Based on the results, three C-A agents (CAA) (cf. Figure 2) have been designed and developed, representing different C-A factors that can occur in a smart home environment: (1) Location (LCAA), (2) user behavior (BCAA) and (3) connectivity (CCAA).

Implemented CAAs are integrated with security policies provided by FACA through generic C-A AC API, which abstracts context information through security policy attributes and offers IoT users to use context information once assigning access rights in a smart home. Moreover, developed protocols enable simple registration of the further CAAs, enabling automatic context lifecycle management in local IoT networks.

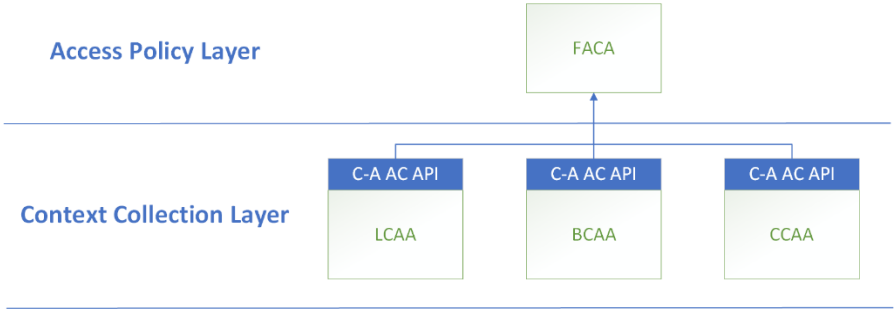

Figure 2. C-A AC services architecture

Primary contributions of the developed C-A AC solution involve (i) defining the interface and message exchanges for integration of context information into security policies, (ii) defining a common C-A AC data model, and (iii) extending AC services with capabilities to apply context information during authorization procedures. Finally, the implemented C-A AC solution has been evaluated in the Smart Home environment, providing results on functional and performance implications of C-A AC services in the IoT environment.

Finally, COSYLab has been deployed and evaluated against the devices available on the market: Raspberry Pi 4, Raspberry Pi 3, and Raspberry Zero. The evaluation consisted of measuring CPU usage, memory consumption, as well as COSYLab components processing and networking latency during components startup and execution of the designed protocols. Performed evaluation and analysis of the results prove the feasibility of IoT services deployment on Fog Node devices in local IoT networks. This conclusion allows further research of FC-based IoT solutions and their enrichment through novel services.

4 Geplante weiterführende Aktivitäten

Since I have submitted my dissertation at the University of Vienna, I am currently waiting for the reviews and approval of my thesis defense, which is expected to occur in autumn this year. Until then, I am planning on publishing my research results through conference papers this summer and preparing myself for the upcoming defense presentation.

After completing my Ph.D. studies, I plan to continue researching IoT security in the FC-based IoT landscape and additionally developing COSYLab, with a focus on scalability and services deployment. The future goal is to enable COSYLab to be used in larger IoT networks like Smart Building or Smart City.

5 Anregungen für Weiterführung durch Dritte

IoT security research involves numerous challenges, especially concerning the computational resources of the IoT devices and the scale of the IoT networks. For that reason, the introduction of lightweight security protocols and rethinking the existing ones significantly impact the adoption of IoT. The most important reason for this is the overall safety and security of users and their private information in IoT environments.

Moreover, FC is established just a couple of years ago and is in its infancy. For that reason, the establishment of future FC-based IoT services allows seamless possibilities for research and establishment of novel IoT services in the upcoming years. This leads to the creation of more intelligent and self-managed IoT environments, improving the overall quality of life for IoT users.