Abstract

Due to the emergence of internet of things (IoT), the number of devices connected to the IoT network has been increasing at an unprecedented rate. Concurrently, new IoT protocols and services are emerging day-by-day, which open up different security threats and attacks. The presence of heterogeneous devices and services makes it difficult to restrict unauthorized access to the IoT system. Further, the involvement of authorized entities in malicious activities brings another challenge for trustworthy service provisioning in IoT.

Toward building a trustworthy IoT service provisioning system, in the first part of the thesis, we design a *zero-trust* framework for securing the IoT system from unauthorized access. Along with zero-trust authentication, we also need to ensure that untrusted entities are not involved in IoT service provisioning. In this context, we propose different trustworthy service provisioning approaches, while considering some of the major and essential IoT services. We propose a trustworthy data collection approach that allows IoT applications to select only trustful data for sensitive data-driven services. The IoT devices are usually resource-limited and offload the computation-intensive tasks to nearby fog nodes. Considering the importance of the task offloading services in IoT, we propose a task offloading scheme that selects trustful fog nodes, while satisfying the trust requirements of the task, the dependency between subtasks, and user mobility.

Due to many task offloading requests, the overloaded fog nodes use unutilized storage and computational resources from the edge nodes. Although the edge nodes share the resources with fog nodes, the actual tasks are being processed at the edge nodes. Therefore, we propose a trustworthy edge computing approach that considers the resources from the trusted edge nodes, while maximizing the utilities of both edge and fog nodes. The edge or fog nodes involved in service provisioning may act maliciously. Therefore, we design a trustworthy and transparent service composition framework, where the nodes involved in the microservices cannot repudiate their involvement. Finally, we propose a service selection framework that allows IoT users to select trustworthy services from nearby available nodes.

Keywords: Internet of Things, Trustworthy services, Zero-trust, Authentication, Data collection, Task offloading, Edge computing, Service composition