Public Abstract
First Name:Bidyut
Middle Name:
Last Name:Mukherjee
Adviser's First Name:Prasad
Adviser's Last Name:Calyam
Co-Adviser's First Name:
Co-Adviser's Last Name:
Graduation Term:SP 2017
Department:Computer Science
Degree:MS
Title:**Lightweight IoT Security Middleware for End-to-End Cloud-Fog Communication**

IoT (Internet of Things) based smart devices such as sensors and wearables have been on the rise for the past decade. Being intrusive in nature, it is extremely important to ensure security and confidentiality in the data being transferred through such devices. The cloud servers situated close to the users, called 'fogs', are often used to provide critical data during scenarios ranging from e.g., disaster response to in-home healthcare. Since these devices typically operate in limited-resource environments close to the data source, security has to flexible and energy-efficient for data exchange with cloud platforms. In this thesis, we present the design and implementation of a lightweight IoT security middleware, i.e., a software system in between existing network systems, for end-to-end cloud-fog communications involving smart devices and cloud-hosted applications. The novelty of our middleware is in its ability to cope with intermittent network connectivity as well as device constraints in terms of computational power, memory and network bandwidth. To provide security during unreliable network conditions, we use a Session Resumption concept in order to reuse encrypted sessions from recent past, if a recently disconnected device wants to quickly reconnect after an interruption. The primary design goal is to not only secure IoT device communications, but also to maintain security compatibility with existing core cloud infrastructures. Experiment results show how our middleware implementation provides fast and resource-aware security by using static pre-shared keys (PSKs) for a variety of IoT-based application requirements. Thus, our work lays a foundation for promoting increased adoption of static properties such as Static PSKs that can be highly suitable for handling the trade-offs in high security or faster data transfer requirements within IoT-based applications.