# Protecting Data Security inSmart Internet-of-Things (IoT) Environments

Lan Wang lanwang@memphis.edu Department of Computer Science University of Memphis

December 16, 2016

## 1 Justification for Research: Security in Smart Environments

Internet of Things (IoT) are making our environment smarter. In an office building, tens of thou- sands of sensors may be installed to monitor electricity, lighting, temperature, humidity, and other environmental parameters (Figure 1). In an industrial facility, even more sensors and actuators may be used to monitor and control the equipment, processes and products. Furthermore, our homes and vehicles are relying on an increasing array of sensors and devices to make them more autonomous. The IoT devices in these environments collect an enormous amount of data that are transmitted to local servers, data centers and clouds for storage and processing. The data may be used in business and personal decisions as well as actions and controls on the environment. It can also be used to infer organizational and personal behavior. As such, it is critically important to protect the confidentiality, integrity, authenticity and availability of the data. However, various security problems with these smart systems have surfaced [1, 2, 3], which pose serious threats to the businesses and people who make use of the smart environments.

IoT security solutions in the current Internet have several major issues. First, the system designers expect that data will be safe within a secure perimeter, so the focus of data protection is to set up a firewall at the network border or a password on a website. However, if the perimeter fails for some reason, the data is exposed to the attacker. Second, the firmware in the smart devices may be modified maliciously during transport, installation and operation, but the devices do not authenticate the firmware adequately and simply execute it as if it is a valid firmware update. Third, the security setup for sensors and devices is cumbersome so the security measures, if any, are often side-stepped or ignored by people who install them in a smart environment.

The above issues are difficult to address in the current Internet architecture due to its focus on connection-based or container-based security. Instead, we need to fundamentally change our ap- proach from securing connections to securing data. The new data-centric Internet architecture NDN (Named Data Networking) offers us such a platform. In our recent work funded by FIT, we have been applying data-centric approaches to securing NDN-based smart home systems (Section 0.3). In this project, we plan to extend our research in two directions.

First, we will continue our research on smart home security to address more challenging design issues when we scale up the system and relax our assumptions. Second, we will examine a broader set of IoT environments, such as industrial facilities, warehouses and shipping containers, to com- pare their security issues with those in the smart home environment. For similar problems, we will apply the mechanisms developed in our smart home system to these environments. For new problems, we will articulate and analyze them in order to motivate new research proposals.

If the proposed project is successful, our research results can be used to secure a variety of smart IoT environments. The improved security will benefit residents and companies in our community who are interested in deploying these smart systems. Moreover, we expect that the methodology developed in this project will become the basis of our research proposals to NSF, DoD and DoE, all of which have been investing in programs to secure IoT systems. This research area is highly interdisciplinary, with collaboration opportunities with researchers in Electrical Engineering, Civil Engineering, as well as Business Information and Technology. Last but not the least, this research area has a good potential for commercialization, given the lack of secure IoT systems in the market. With one of her patents licensed by a company, the PI of this proposed project is both interested and experienced in technology transfer.