MRI: Development of an Information Assurance and Performance Infrastructure for the Internet of Things

Project Summary

Keywords: information assurance, security, performance, elastic computing, Internet of Things

The goal of this development proposal is to develop a new infrastructure at Temple University: an Information Assurance and Performance (IAP) infrastructure for the Internet of Things (IoT). IoT, in which sensing and actuation is embedded in everyday objects connected via the Internet, has the potential to support an increased level of intelligent, dynamic decision making across a wide array of domains, such as smart cities, intelligent agriculture, and emergency response management. However, IoT systems are vulnerable to security threats, which limits their widespread adoption. In addition, in the future, systems will be challenged by the large amounts of IoT data communicated over the network and stored in cloud-based data centers.

The proposed infrastructure will enable a number of innovative research projects on **IoT security and performance**, as well as on the related supporting technologies, such as robust data storage schemes and elastic provisioning algorithms for cloud-based systems. The infrastructure consists of a range of mobile and embedded IoT devices, IoT edge-computing servers, Software Defined Networking (SDN) switches, high performance and reliable data storage, and software components that implement emerging research in secure communication protocols, elastic computing algorithms, and computational offloading in IoT systems.

Intellectual Merit: The research projects described in this proposal will result in the exploration of 1) novel scalable and trustworthy architectures and network protocols for IoT systems, 2) role-based behavioral threat detection approaches for IoT systems, 3) elastic provisioning algorithms for cloud-based systems, 4) data deduplication algorithms for high reliability and storage efficiency in erasure coded data centers, and 5) risk aware failure identification for expedited recovery. The exploration of these research projects is enabled by construction of the proposed testbed hardware, algorithms/protocols/schemes, and the corresponding software implementation.

The infrastructure developed in this project consists of: (a) the resulting IAP architecture and testbed hardware; (b) algorithms, protocols, and schemes; and (c) implementation of (b) as software components on the testbed hardware. Through the development of web-based software interfaces and resource reservation components, the IAP-IoT infrastructure will be made available to external researchers to support projects in IoT, cyber physical systems (CPS), cyber security, edge computing, pervasive computing, networking, and high performance computing communities.

Broader Impacts: The proposed infrastructure will enable new research in IoT security and performance, as well as the supporting technologies, such as reliable storage and elastic computing. Such systems have a wide range of applications, healthcare and life sciences, municipal infrastructure, smart home, retail, manufacturing, agriculture, education, automation, and entertainment. Hence, the proposed infrastructure and the supported research will have broader impacts in these applications that are of significant importance to society. This project will also support the development of a new graduate course in IoT security; the infrastructure will be used for lab sessions of the course to provide research training for the diverse student body at Temple University, which represents one of the most comprehensive and diverse learning environments in the nation. Finally, the infrastructure will be available to external researchers and educators, providing support for research and education projects across a wide range of computer science and electrical engineering subject areas.