Hardware based Authentication and Trusted Platform Module functions (HAT) for IoTs

Florida Institute of Technology
High Tech with a Human Touch ™

Challenge:

- This project addresses the need for hardware-oriented capabilities and mechanisms for protecting our increasingly vulnerable microelectronic systems and devices.
- The increased integration and reliance on remote and mobile devices for personal, commercial and growing industrial systems in internet of things (IoTs) is driving the need for improved security and trust in these cyber-physical systems at the hardware level that cannot be dealt at software level only.

Scientific Impact:

- Development of on-chip security and trust primitives (STP) that are designed to serve security-related roles including encryption of storage, and trust-related roles including authentication, and pre-boot authentication for trusted platform modules (TPM).
- Design a hardware based authentication framework for security and safety critical applications
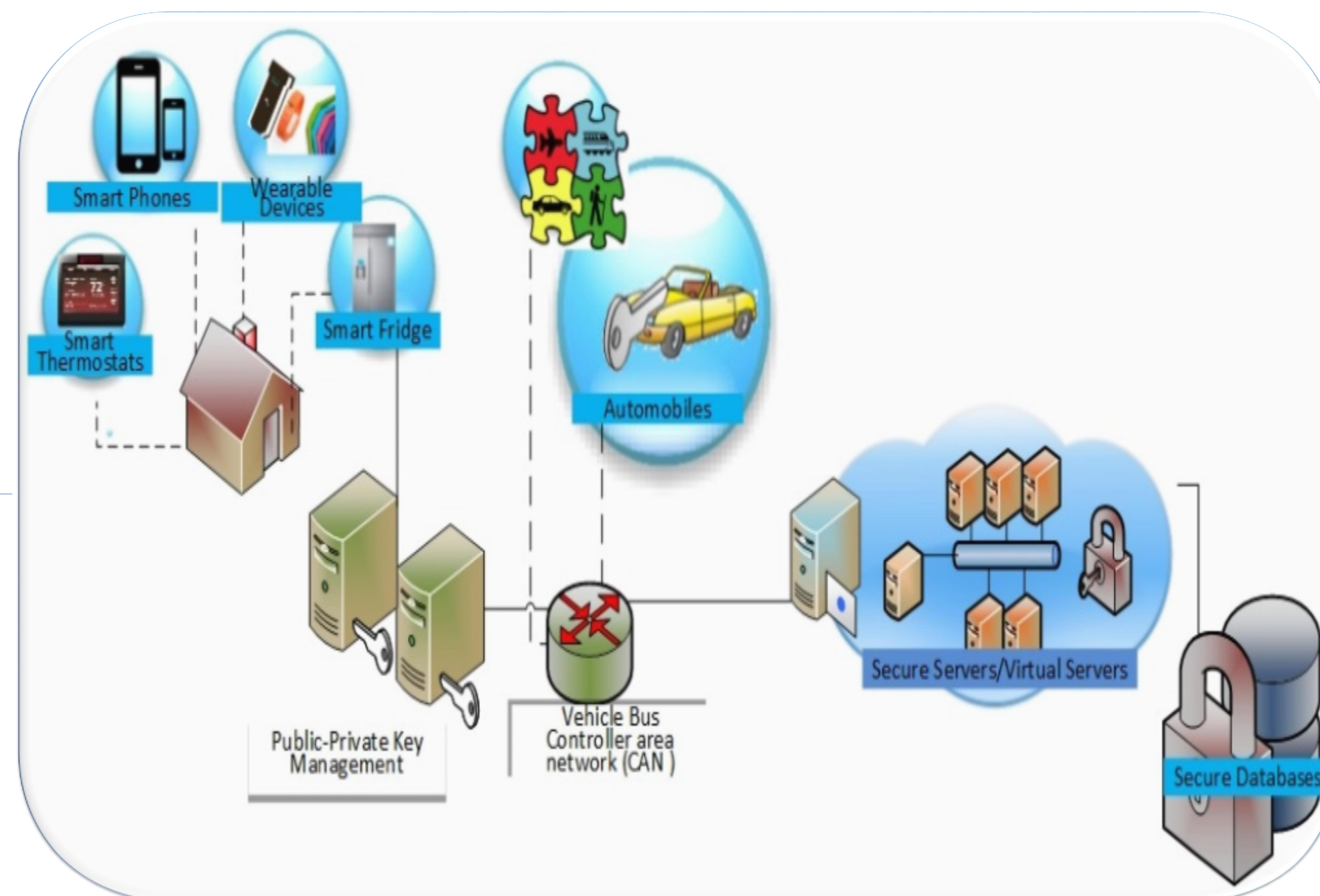
Solution:

- Delineating the threat model and evaluation of security and trust requirements at the device level,
- Evaluation of existing cryptographic primitives and their shortcomings,
- Development and evaluation of hardware based primitives for security and trust related roles.

- Design a hardware-based authentication framework using physical unclonable function (PUF), and
- Investigating PUF capabilities to extend features of trusted platform module (TPM)

Smart Phones · Wearable Devices · Smart Thermostats · Smart Fridge · Automobiles · Public-Private Key Management · Vehicle Bus Controller area network (CAN) · Secure Servers/Virtual Servers · Secure Databases

Broader Impact:

- This project is of interest to manufacturers of IoT devices and their users, including US government agencies as the project addresses the security challenges and offers counter measures to attacks by adversaries.
- Benefits to society: Trustworthy security and privacy protection in the use of IoT devices and applications.
- Dissemination of results are done via publications, tutorials, seminars, workshops and curriculum development for undergraduate and graduates.