ERCIM "ALAIN BENSOUSSAN" FELLOWSHIP PROGRAMME

Scientific Report

First name / Family name	Pushpendu Kar
Nationality	Indian
Name of the *Host Organisation*	Norwegian University of science and Technology (NTNU)
First Name / family name of the *Scientific Coordinator*	Prof. Hao Wang
Period of the fellowship	01/02/2018 to 31/01/2019

I – SCIENTIFIC ACTIVITY DURING YOUR FELLOWSHIP

EZPlugIn: Universal **Plug**-n-Play Framework in a Heterogeneous IoT **In**frastructure

Internet of Things (IoT) integrates a very large scale of technologies in various fields and application areas (smart city to smart forming and smart-homes to smart factories). An IoT system comprises of a large number of smart devices and sensors connected together that are often nonintrusive, transparent, and invisible. Communication among these devices and sensors needs to happen anytime, anywhere for any related services. Generally, communication among them happens through wireless in automatic and ad hoc manner. Additionally, in an IoT system, services are more complex, mobile, and decentralize. Thus, data integration in an IoT system over different environments is more difficult. In such a situation, data integration needs to be done by modular interoperable components. Volumes of data from different sources need to combine to

extract relevant features through infrastructure solution. The process of data combining helps in interpreting data and devises and their relationships. This leads to statistical analysis for decision making. Further, since IoT is so vast that all the applications cannot run on single architecture. Thus, IoT systems are built on different heterogeneous architectures. These heterogeneous architectures should be open and follow some standards. As well as they should not restrict users to use end-to-end and fixed solutions. Therefore, an IoT system should be flexible enough to use in the cases such as identification, intelligent devices, and smart objects.

IoT application system should be global for serving different industries and fields. Here, information interoperability needs to take place between enterprises, industries, regions, or countries. Interoperability in an IoT system is essential for going through layers such as, physical, communication, functional, and application. Different languages and protocols contribute to build these levels. Domain transparent languages and protocols are required to develop the levels. A comprehensive approach is needed in addressing and solving the interoperability of IoT devices and services at several layers.

Considering the above-mentioned facts, we propose EZPlugIn, in which we tries to propose a universal plug-n-play framework, where users need not to bother about interoperability among devices in the IoT infrastructure. The proposed framework for plug-n-play of devices for an IoT network in smart home. In such an IoT system, users need not to bother about interoperability among devices. A new device can be connected with this system without thinking about their interoperability with existing hardware and software. To achieve such a unified IoT system we adopted Named Data Networking (NDN) communication paradigm to connect between devices. In the NDN communication model, a device accesses data and services from other device by the name itself rather that its physical location.

Universal Plug-n-Play infrastructure and abstraction of devices, services, and applications make the security solutions for IoT more complex. In this unified IoT architecture, it is essential to establish communication between devices and corresponding services and applications. In such platform, any entity has a chance to intentionally or unintentionally misrepresent itself. This will lead to the attacks like eavesdropping, spoofing, and phishing. Therefore, our aim is also to build a robust security solution for such a unified IoT architecture. In this context, we have implemented a security scheme that can be suitable for Service Oriented Architecture (SOA) based IoT network. The proposed scheme allows to transfer data in a network only if the public key (encrypted hop-count) received by the packet matches with the public key (decrypted hop-count) between the source and destination node stored in the routing table. Otherwise, the data are considered to be malicious and discarded from the network. A non-cooperative Stackelberg game based mathematical model is presented, which considers defenders as leaders and attackers as followers. We have simulated our proposed scheme and have compared it with the existing security and authentication scheme, UAKMP, in identical conditions. From the analysis of the results we evaluate that, SecureIoT has improved performance with reduced communication overheads.