Chapter 50
Protecting Data Confidentiality in the Cloud of Things

Bashar Alohali
Liverpool John Moores University, UK

Vassilios G. Vassilakis
University of York, UK

ABSTRACT

Following the rapid development of the Internet of Things (IoT) technology worldwide, the integration of the IoT to the cloud, referred to as the Cloud of Things (CoT), has become essential for easy access and management of remote resources. However, security and malicious intrusions must be seriously considered to ensure network reliability and data confidentiality. In this paper, the authors analyze the security implications of CoT and propose a solution for data confidentiality. They prove that the proposed solution can effectively protect against a number of security attacks.

INTRODUCTION

Internet of Things (IoT) refers to a network of devices, appliances, buildings, vehicles and other elements that contain digital chips, software and sensors, and are connected with each other through the Internet, enabling them to collect, analyse and share data with each other. Typically, IoT relies on the process of assigning the objects an identity (ID) number, (e.g., the IP address) and controlling them via the Internet. The IoT involves connecting all devices that we use to the Internet via special receivers, and gathering information without the need for human intervention.

The common denominator between cloud computing and the IoT is the Internet and networking. The Internet is used to deliver services for cloud computing and to connect devices to the central servers in the IoT. Recently, global investment in cloud computing and storage in the cloud has increased. This effectively requires connecting devices to the Internet and access to their data clouds.

Researchers are working towards the creation of smart cities that will be controlled via the Internet and will generate and store large volumes of data. Towards this goal, the development of secure and efficient Cloud of Things (CoT) technologies is a very important and challenging task. The CoT control

DOI: 10.4018/978-1-5225-9866-4.ch050

will be used in hospitals, factories, power plants, cars, trains, airplanes, and even electrical appliances inside the house, e.g., to adjust the lights, TV, and other home devices.

The security of the CoT with regard to storing and retrieving information is controversial. Some people believe that information is not safe when the internal network is managed, while others believe that IoT clouds can provide the necessary security to ensure the conservation and integrity of information.

Information security problems in the IoT clouds come from the server and client provider, but the greatest responsibility is always that of the service provider. It is mandatory to provide a secure infrastructure and tools and storage depots that are safe. In this paper, we propose a security solution for ensuring data confidentiality in CoT. We use the Scyther tool in order to prove that the solution is secure against different types of attacks, including replay attacks.

BACKGROUND

Overview of CoT

IoT on which CoT is based, is a new IT paradigm that describes an imagined reality of trillions of things connected to each other. IoT enables transmitting valuable data that is stored, processed and analyzed by computers to control and adjust all sorts of human activities, such as healthcare, road traffic control, emergency management, retail, crime prevention, lighting, energy and power and/or transportation. IoT is closely linked with the concepts of "smart city", "ubiquitous computing" (Vasseur & Dunkels, 2010), and other paradigms that describe new technological reality in which sensors and microcontrollers are embedded in various things and integrated into human living. This results in increased comfort and security. IoT unites several individual technologies, including machine-to-machine (M2M) communication, supervisory control and data acquisition (SCADA) systems designed for industrial remote control of equipment, wireless sensor networks (WSN), and radio-frequency identification (RFID). All these systems and technologies have diverse and complex functionalities that include monitoring, sensing, tracking, locating, alerting, scheduling, controlling, protecting, logging, auditing, planning, maintenance, upgrading, data mining, trending, reporting, decision support, back office applications, and others (Gubbi, Buyya, Marusic, & Palaniswami, 2013).

One of the main differences of the IoT paradigm from the M2M technologies is remote sensing (McGrath & Scanaill, 2013). IoT's significance is on prospective creation of complex and all-embracing network architecture with its unique protocols, storage capacities, software applications and users is similar to the Internet.

The main idea behind cloud computing is a shared access of multiple users to physical computing infrastructure and software offered by cloud providers. Cloud computing formed into three different service scopes, including IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service) (Kifayat, Merabti, & Shi, 2010). These models may be deployed as a private, public, community, or hybrid clouds. From the technological viewpoint, the key characteristics of cloud technologies, such as on-demand service, broadband network access, resource pooling, rapid elasticity, and measured service are enabled by the virtualization process. Through virtualization single system images may be created from cluster machine infrastructure, which provides a unified user interface and efficient utilization of resources. Virtualization of cloud services is typically enabled by a middleware. Given their huge storage, computing and sharing capabilities, IT clouds may be regarded a key tech-