Chapter 4
Examining of Data Security, Privacy, and Reliability for Cloud and Internet of Things Integration

Marcus Tanque
Independent Researcher, USA

ABSTRACT

Converging Cloud computing with Internet of Things transformed organizations' traditional technologies. This chapter examines the intersection of cloud computing and internet of things in consort with how these solutions often interact on the internet. Vendors develop CloudIoT capabilities to support organizations' day-to-day operations. IoT is a combined platform encompassing physical and virtual nodes. IoT objects comprise device-to-device data sharing, machine-to-machine provisioning, sensors, actuators, and processors. These systems may be deployed as hardware components and applications software. This chapter also emphasizes data security, reliability, resource provisioning, service-level agreement, quality of service, IoT, privacy, and device integration. This chapter also highlights operational benefits and/or security issues affecting CC and IoT technologies.

1. INTRODUCTION

This chapter evaluates benefits or challenges organizations continue to deal with. The study also calls attention to security, privacy and reliability problems affecting the integration of Cloud Computing (CC) and Internet of Things (IoT). CC and IoT have

DOI: 10.4018/978-1-5225-3445-7.ch004

altered how vendors and enterprises adopted and deployed these technologies on the global-scale. CC is a delivery platform involving services and deployment models. Such services range from Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), Public Cloud (PC), Private Cloud (PC), Hybrid Cloud (HC) and Community Cloud (CC). Government senior leaders and corporate decision makers rely on these services to make organizational informed decisions. IoT is a technology, which integrates smart objects i.e.: machines, wired and wireless sensory network devices, actuators, computer processors, aggregators, e-utilities, and thermostats. These devices or systems stem from robotic solutions, decision trigger and resource sharing (Abdelwahab, Hamdaoui, Guizani, & Rayes, 2014; Qusay, 2011). Such systems deliver unlimited interoperability solutions with minimum human involvement (Aazam & Huh, 2014; Akyildiz, Su, Sankarasubramaniam, & Cayirci, 2002; Alamri, Ansari, Hassan, Hossain, Alelaiwi, Hossain, 2013). This chapter also strengthens the merging of CC and IoT capabilities, once systems are deployed (Abdelwahab, Hamdaoui, Guizani, & Rayes, 2014; Qusay, 2011). This includes building on CC and IoT technologies' multi-layered vertical barriers and opportunities, for instance Machine-to-Machine (M2M), Device-to-Device (D2D), Man-to-Man (M2M), Machine-to-Man (M2M), System-to-System, Solution-to-Solution, and Physical-to-Virtual nodes (Aazam & Huh, 2014; Akyildiz et al., 2002; Atzori et al., 2010). Additional technology trends involving CC and IoT are also discussed in this chapter (Akyildiz et al., 2002; Ballon et al., 2011; Badger et al., 2011). Merging smart objects into IoT technology networks is essential for organizations' business continuity operations. While the merger of CC, big data, robotic systems, actuators, aggregators, and sensor systems validates an organization's applied capabilities e.g., CloudIoT smart devices and/or autonomous systems (Polsonetti, 2014). CloudIoT is an infrastructure solution that delivers operational IoT architecture and framework capabilities (Alamri et al., 2013; Ballon et al., 2011). In the next decades, the adoption of IoT objects will increase significantly (Ashton, 2009). Consumers and industries are excited with such evolutions, which will influence the economies of scale (Polsonetti, 2014; Akyildiz et al., 2002; Alamri, Ansari, Hassan, Hossain, Alelaiwi, Hossain, 2013). These security solutions also expand organizational business continuity and infrastructure capabilities and/or consumers' requirements. Today, IoT devices/systems comprises a billion of interconnected smart objects. These solutions offer concerted capabilities for centralized and distributed information sharing or real-time data-provisioning (Ashton, 2009). Modern smart systems have a dual interoperability and capability functions e.g., access of deployed control devices (Polsonetti, 2014; Atzori e al., 2010; Ballon et al., 2011; Ashton, 2009; RCRWireless, 2016).

In 1985 Peter T. Lewis initially discussed the term IoT at the "U.S. Congressional Black Caucus 15th Legislative Weekend Conference". Peter defines "Internet of Things