

# Chapter 5

## Security Issues and Its Countermeasures in Examining the Cloud-Assisted IoT

**Govind P. Gupta**

*National Institute of Technology, India*

### **ABSTRACT**

*Internet of Things (IoT) offers the capability to connect and integrate both digital and physical objects to the internet and to enable machine-to-machine and machine-to-human communication or interactions services. The real-time adoptions and deployments of such systems for different applications such as smart cities, smart grids, smart homes, or smart environments require guaranteed security and privacy-enabled IoT services. This is due to fact that devices in the IoT generate, process, and exchange huge amounts of safety-critical data as well as privacy-sensitive information. In order to ensure secure and safe operation and to avoid cyber-attacks on such systems, it is crucial to incorporate security and privacy measures to countermeasure the different possible attacks. This chapter presents different security and privacy requirements and a taxonomy of security threats in the context of the IoT. In addition, the authors survey the most relevant defense strategies available in the literature related to IoT security with their merits and demerits.*

### **INTRODUCTION**

The Internet of Things (IoT) is characterized by a collection of heterogeneous, geographically distributed, smart devices that interact with each other on a collaborative basis to complete a particular task (Vermesan, 2011; Tsai, 2014;

DOI: 10.4018/978-1-5225-3445-7.ch005

Ning, 2012). The core objective of the IoT is to provide smart services in a variety of application domains such as Smart Homes, Smart Cities, Smart Grids and so on (Turner, 2011; Roman, 2011). In these application domains, security and privacy requirements of the IoT play a very important role which includes privacy and confidentiality of data exchanged among devices and controlling stations, access control within the IoT, and trust among connected devices and users.

Fundamental hurdles for pushing IoT and its services into the real-world applications are security, privacy and trust (Jing, 2014; Rodrigo, 2013; Sicari, 2015; Zheng, 2014). The main aim of the security services designed for the IoT is to provide secure interactions between the devices and the Internet host, and protecting the information and service provisioning of all relevant components of IoT. Generally, in a collaborative and information sharing system such as the IoT, different security and privacy services such as confidentiality, data integrity, access control, anonymity, and availability for users and smart things and trustworthiness among smart devices and users are required. These security services are very important to ensure secure communication among different entities of the IoT. Due to the heterogeneity and ad hoc nature of IoT components and the lack of computing resources such as processing power and storage, it is required to tailor existing security solutions to this new smart environment. Traditional security and privacy mechanisms cannot be directly applied to the IoT (Ning, 2012; Turner, 2011; Roman, 2011). This is due to fact that in the IoT, different communication stacks, standards and resource-constrained devices are involved. In addition, the IoT involves a high number of interconnected devices that arise the requirements of a scalable security and privacy mechanisms for this system.

This chapter presents an overview of the different security issues and threats in the context of the IoT. The author also analyzes the most relevant security strategies available in the literature related to the IoT security. The rest of this chapter is organized as follows. Section 2 provides a brief explanation on why security and privacy are required in the IoT. Following this, a brief description of the related research on privacy, authentication, data confidentiality, access control, trust and non-repudiation are discussed in Section 3. Next, a taxonomy of threats mitigation in different plane of IoT such as device plane, gateway plane and service plane are provided in Section 4. Then, Section 5 provides some security analyses of the standard IoT-related protocols. After that, research challenges and future works in the direction of IoT security are presented in Section 6. Finally, the chapter concludes.

23 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: [www.igi-global.com/chapter/security-issues-and-its-countermeasures-in-examining-the-cloud-assisted-iot/191834](http://www.igi-global.com/chapter/security-issues-and-its-countermeasures-in-examining-the-cloud-assisted-iot/191834)

## Related Content

---

### Recent Advances in Edge Computing Paradigms: Taxonomy Benchmarks and Standards for Unconventional Computing

Sana Sodanapalli, Hewan Shrestha, Chandramohan Dhasarathan, Puviyarasi T. and Sam Goundar (2021). *International Journal of Fog Computing* (pp. 37-51).

[www.irma-international.org/article/recent-advances-in-edge-computing-paradigms/284863](http://www.irma-international.org/article/recent-advances-in-edge-computing-paradigms/284863)

### Communication Infrastructures in Access Networks

Syed Ali Haider, M. Yasin Akhtar Raja and Khurram Kazi (2015). *Cloud Technology: Concepts, Methodologies, Tools, and Applications* (pp. 943-969).

[www.irma-international.org/chapter/communication-infrastructures-in-access-networks/119891](http://www.irma-international.org/chapter/communication-infrastructures-in-access-networks/119891)

### Designing Instruction and Professional Development to Support Augmented Reality Activities

Kelly M. Torres and Aubrey Statti (2021). *International Journal of Fog Computing* (pp. 18-36).

[www.irma-international.org/article/designing-instruction-and-professional-development-to-support-augmented-reality-activities/284862](http://www.irma-international.org/article/designing-instruction-and-professional-development-to-support-augmented-reality-activities/284862)

### Cloud Services for Healthcare: Insights from a Multidisciplinary Integration Project

Konstantinos Koumaditis, George Pittas, Marinos Themistocleous, George Vassilacopoulos, Andriana Prentza, Dimosthenis Kyriazis and Flora Malamateniou (2015). *Delivery and Adoption of Cloud Computing Services in Contemporary Organizations* (pp. 292-317).

[www.irma-international.org/chapter/cloud-services-for-healthcare/126860](http://www.irma-international.org/chapter/cloud-services-for-healthcare/126860)

### Applications of Virtualization Technology in Grid Systems and Cloud Servers

Mohammad Samadi Gharajeh (2018). *Design and Use of Virtualization Technology in Cloud Computing* (pp. 1-28).

[www.irma-international.org/chapter/applications-of-virtualization-technology-in-grid-systems-and-cloud-servers/188121](http://www.irma-international.org/chapter/applications-of-virtualization-technology-in-grid-systems-and-cloud-servers/188121)