Chapter 9
An Adaptive Security Framework for the Internet of Things Applications Based on the Contextual Information

Harsuminder Kaur Gill
Jaypee University of Information Technology, India

Anil Kumar Verma
Thapar University, India

Rajinder Sandhu
Jaypee University of Information Technology, India

ABSTRACT

With the growth of Internet of Things and user demand for personalized applications, context-aware applications are gaining popularity in current IT cyberspace. Personalized content, which can be a notification, recommendation, etc., are generated based on the contextual information such as location, temperature, and nearby objects. Furthermore, contextual information can also play an important role in security management of user or device in real time. When the context of a user or device changes, the security mechanisms should also be updated in real time for better performance and quality of service. Access to a specific resource may also be dependent upon user's/device's current context. In this chapter, the role of contextual information for IoT application security is discussed and a framework is provided which auto-updates security policy of the device based on its current context. Proposed framework makes use of machine learning algorithm to update the security policies based on the current context of the IoT device(s).

DOI: 10.4018/978-1-5225-5742-5.ch009

INTRODUCTION

With the advancements and successful adoption of network connecting technologies such as LTE, 3G, WiMax, etc., the Internet has become a necessity in a current era of living. Around 3.5 billion Internet users are available in the world which is around 40% of the total population ("Internet Live Stats," 2014). Due to such colossal connectivity, a new paradigm has evolved in which not only humans but other things such as fan, machine, car, etc., also connect to the Internet, share data and execute certain tasks with or without any human intervention. This novel paradigm is known as the Internet of Things (IoT). As the name suggests, it is the interconnection of things (sensors, RFID tags, smart devices, etc.) with each other using the Internet so that these things can share information and make some useful decisions (Sandhu and Sood, 2016). In 1998, IoT was first coined by Kevin Auston in his presentation on future of networks. Later, it has been introduced in the Oxford dictionary with the following definition: *"The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data."* IoT has multiple application areas such as smart healthcare, smart home, smart school, smart transport and many more. Out of the many challenges of IoT, effective decision making with relevance to the current context of the user or the thing is very important. Any decision made by IoT based application which is out of the current context of the user/thing affects the overall performance and accuracy of the system. However, with real-time data available through the IoT devices, smart context-aware applications can be developed. On the other hand, the IoT framework consists of billions of sensors deployed around the world where the analysis of the data generated by all connected sensors is not feasible. Integration of context awareness in the deployment and usage of IoT devices will provide a method in which only suitable sensors can be prompted to make any decision. This will yield the better performance and scalability of IoT based applications.

Context-aware IoT paradigm proves to be novel for application users. However, security remains the essential requirement in any application. Security mechanism in IoT applications is usually handled in a traditional way such as assigning a role to the application user, grant for resources, etc. These traditional methods are independent and proved to provide the desired security, but the consideration of context also plays an important role and can be very helpful. The security in IoT applications should be highly dependent upon the context of the device and security policies should be updated if the context of the IoT device changes. Consider a scenario when the context (location) of a user/device changes from a public Internet access area to private network. Based on the context, security policies can be updated so that overall QoS of application is optimized. This will make IoT based applications more secure and reliable.