Chapter 93
A Survey of Authentication Schemes in the Internet of Things

Yasmine Labiod
Networks and Systems Laboratory, Badji Mokhtar Annaba University, Annaba, Algeria

Abdelaziz Amara Korba
Networks and Systems Laboratory, Badji Mokhtar Annaba University, Annaba, Algeria

Nacira Ghoualmi-Zine
https://orcid.org/0000-0001-5271-5970
Networks and Systems Laboratory, Badji Mokhtar Annaba University, Annaba, Algeria

ABSTRACT

In the recent years, the Internet of Things (IoT) has been widely deployed in different daily life aspects such as home automation, electronic health, the electric grid, etc. Nevertheless, the IoT paradigm raises major security and privacy issues. To secure the IoT devices, many research works have been conducted to counter those issues and discover a better way to remove those risks, or at least reduce their effects on the user's privacy and security requirements. This article mainly focuses on a critical review of the recent authentication techniques for IoT devices. First, this research presents a taxonomy of the current cryptography-based authentication schemes for IoT. In addition, this is followed by a discussion of the limitations, advantages, objectives, and attacks supported of current cryptography-based authentication schemes. Finally, the authors make in-depth study on the most relevant authentication schemes for IoT in the context of users, devices, and architecture that are needed to secure IoT environments and that are needed for improving IoT security and items to be addressed in the future.

DOI: 10.4018/978-1-7998-5351-0.ch093

1. INTRODUCTION

The Internet of Things (IoT) was first invented by Kevin Ashton in 1999. Internet of Things is an integration of various objects with electronics, software, sensors, and actuators that can communicate directly with one another without human intervention via the Internet to collect and exchange data with each other. The main objectives of the IoT is to fulfill a task in various applications and to achieve a network infrastructure with communication protocols that able to exchange and use information and software to allow the connection and integration of sensors, personal, smart devices, and items, anytime and on any network (Yang et al., 2014). Therefore, we can find many applications of IoT in almost all fields. Internet of things is a smart network of different smart objects which can be identified, positioned, tracked, collected and managed remotely.

Security issues, such as authentication, privacy, authorization, integrity, confidentiality, Encryption, access control, and system configuration are the main challenges in any Internet of Things applications. IoT applications such as Cloud computing, sensor nodes, mobile devices, e-health system can provide a smart environment for global connectivity that facilitates life by being susceptible, adaptive, and reacting to human requirement. However, security is not guaranteed. The authentication is the main regard issue concerning the development of an Internet of Things application and one of the most important and critical requirements for IoT. Traditionally, authentication techniques rely on usernames and passwords, which can be easily compromised and the information on users may be leaked. The main objective of the authentication is to identify users and devices in networks to restrict access to authorized people and non-manipulated objects and to keep information on users protected when user signal is interrupted or intercepted. This issue should be addressed to eliminate the risk, or at least minimize their effects on the user's confidence of personal data and security requirements. Standardization organizations like IEEE and IETF are also working towards making IoT more secure by designing necessary communication technologies. These technologies are important in order to provide mutual authentication between the user and the server, reduce computation and communication overhead in IoT systems, and to make IoT more responsible and power efficient against any attackers.

There are many published surveys on IoT security issues and challenges. Yang et al. (2017) analyzed existing mechanisms and architectures for authentication, access control, and across-layer techniques whenever applicable. Alaba et al. (2017) presented a comparative study on IoT security scenario and vulnerabilities. They classified current IoT security in the context of its application, users, architecture, and communication. Therefore, this paper provides an analysis of the different authentication schemes proposed in the literature. Through an authentication schemes classification, it compares and analyses the existing authentication schemes in the contexts of users, architecture, and devices, and showing their advantages and limitations. After the introduction, the rest of the paper is organized as follows; section 2 provides the works that are related to cryptography-based authentication schemes for IoT. Section 3 provides a review of various authentication schemes in the contexts of users. Section 4 provides discussions to the authentication schemes in the contexts of smart devices. Section 6 provides a review of new technologies-based authentication for IoT. Finally, Section 5 concludes the study (Figure 1).