Journal of Information Security and Applications 34 (2017) 255–270

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

A lightweight biometrics based remote user authentication scheme for IoT services

Parwinder Kaur Dhillon*, Sheetal Kalra

Department of Computer Science and Engineering, Guru Nanak Dev University, Regional Campus, Jalandhar, Punjab, 144001, India

ARTICLE INFO

Article history:
Available online 12 January 2017

Keywords:
Biometrics
IoT services
Key agreement
Remote user authentication
Security

ABSTRACT

User authentication is becoming crucial in the accelerating Internet of Things (IoT) environment. With IoT several applications and services have been emerging in the areas such as, surveillance, healthcare, security, etc. The services offered can be accessed through smart device applications by the user from anywhere, anytime and anyplace. This makes security and privacy critical to IoT. Moreover, security is paramount in IoT, to enable secure access to the services; multi-factor based authentication can provide high security. In this paper, a lightweight biometric based remote user authentication and key agreement scheme for secure access to IoT services has been proposed. The protocol makes use of lightweight hash operations and XOR operation. The security analysis proves that it is robust against multiple security attacks. The formal verification is performed using AVISPA tool, which confirms its security in the presence of a possible intruder.

1. Introduction

IoT envisions a future networking paradigm and service infrastructure in which spatially distributed physical objects will be widespread deployed to form information networks to facilitate advanced and intelligent services. This network of physical objects will include sensors, actuators, RFID tags or mobile devices, possessing the capability to sense, monitor and collect data about the user environment [1]. Using data collected by the devices, intelligent and ubiquitous services can be facilitated for the users such as surveillance, health care, security, traffic management, etc. IoT services enable interactions of the devices with the real world. Due to above scenarios, several applications for smart devices are being developed to access services offered by IoT networks. By combining IoT networks with smart devices, numerous suitable IoT services can be provided to users. For example, Lockitron can lock and unlock doors through Smartphone [2]. Likewise, most of the IoT services can be monitored and controlled through smart device applications. However, this brings with it adverse underlying effects such as invasion of privacy and information leakage. Moreover, due to the large number of applications in smart devices, these devices often store vital personal information about the user. As a result, attackers are expanding the scope of their attacks beyond the existing Internet environment into smart devices so as to extract the stored user information [3-6]. Furthermore, IoT services that are running in the background, track location based information about the user about which he/she may or may not be aware of. Such background applications might cause serious privacy issues in case if the user forgets to terminate them. On the other hand, some IoT services might record personal information about the user in the background, for example; the patient health monitoring service might track critical health factors without notifying its user. This, in turn, leads to several security problems to sensed data exchanged by *things* such as confidentiality, authenticity and integrity [7,8].

Fig. 1 shows the IoT environment, how remote users can access the different nodes of an IoT network through smart device applications. Remote users can access IoT services through smart device applications in order to connect to any node or sensing element in an unattended IoT environment. Once connected, the user can access desired information from specific nodes. This makes remote user authentication very crucial in IoT networks so that only legitimate users can access IoT nodes while using any service on his/her smart device [9,10]. Because nodes or sensors in IoT networks are resource constrained in terms of processing power, memory requirements, etc., adding resourceful gateway nodes that can support the constrained nodes or sensors, can provide quick on-demand delivery of data or information and take care of most of the processing.

Authentication has three different factors that symbolize user's identity, namely, *something user has* (ownership factor, e.g., smart cards, smart phones, tokens, etc.), *something user knows* (knowledge factor, e.g., passwords) and *something user is* (inherence factor

* Corresponding author.
E-mail address: parwindhillon@gmail.com (P.K. Dhillon).

http://dx.doi.org/10.1016/j.jisa.2017.01.003
2214-2126/

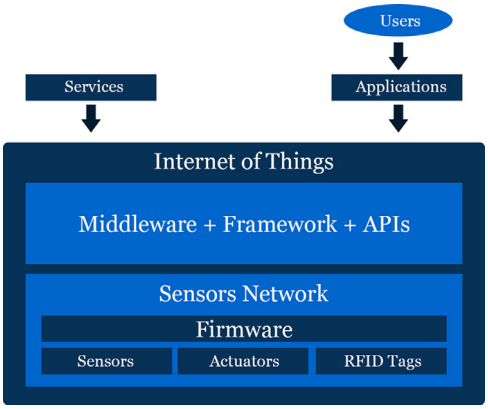

Fig. 1. Relationship between nodes and IoT.

e.g., fingerprint, iris scan, etc.) [11,13–16]. Traditional user authentication schemes are predominantly based on knowledge factor such as passwords. However, the last few years have witnessed that the Single Factor Authentication (SFA) approaches based on passwords alone are easy to breach and hence insufficient to guarantee security. Therefore, incorporating a second factor based on user's personal biometric traits can enable development of a stronger authentication scheme. Also, for user's ease and many security implications researchers have proposed several smart card based authentication protocols using biometric to provide increased security [17–19]. Adding biometrics offer several advantages such as hard to forge or distribute, cannot be lost or forgotten, difficult to copy, etc. Biometrics offers a scalable factor for strong user authentication that many organizations can use to keep them, and their users safe. Also, the speed with which "things" are getting connected to the Internet makes multi-factor authentication a viable solution for ensuring the security and privacy in IoT networks.

Kuo et al. [12] pointed following five characteristics of Biometrics:

- *Universal*: Biometrics is a universal trait possessed by every individual.
- *Distinctive*: Each individual possess distinct biometric features.
- *Persistent*: Biometric features never vary over time.
- *Collectable*: Biometric features can be measured or acquired easily using available devices, such as, fingerprint recognizer, etc.
- *Unique*: Biometric features are distinctive to each individual.

Several key requirements for developing an effective remote user authentication scheme for IoT networks include:

- *Lightweight security solution*: The nodes in the IoT networks are resource constrained in terms of processing power, battery backup, memory, speed, etc. Hence, a lightweight security solution is needed.
- *Key agreement*: A secure shared session key needs to be established between sensor nodes and the user outside the IoT network.
- *Mutual authentication*: For a secure authentication scheme both the communication parties need to be sure of the legitimacy of each other.
- *Multi-factor authentication*: Single factor schemes based only on passwords are easier to break, therefore, adding a second factor based on personal biometric can increase the security of the scheme.

The remaining paper is organized as follows. Section 2 gives an overview of the related work. Section 3 presents IoT security issues for better understanding of the topic. The proposed protocol, multi-factor biometric based mutual authentication and key agreement scheme for secure access of IoT services between the users and nodes is presented in Section 4, which is followed by the security and performance evaluation in Section 5. Section 6 concludes the paper.

2. Related work

2.1. IoT security protocols

Several studies and surveys have been conducted by several researchers relevant to the security in the IoT. Atzori et al. [3] performed a study on authentication, data integrity and privacy issues in the IoT, mostly in RFID systems and sensor networks. An ARM compliant framework for handling security and privacy in IoT-enabled smart buildings has been proposed by Hernández-Ramos et al. [6]. In order to achieve a high level of security in smart buildings, the authors have presented authentication and authorization mechanisms to access offered services. Gigli and Koo in [11] categorized IoT services on the basis of application of service into four types viz. Identity-Related Services, Information Aggregation Services, Collaborative-Aware Services and Ubiquitous Services. Li and Zhou [21] have presented various security issues for IoT. They have proposed a security architecture in which IoT security is analyzed from three dimensions, i.e., the security services, network layer and security domain. In [22], Ma et al. has discussed three main goals of IoT. Based on these goals he presented main challenges and key scientific problems that occur during IoT deployment. Thoma et al. in [23] performed a survey on usage for different IoT services and IoT service oriented architecture. In the survey they found the lack of a rational definition and categorized of IoT services, and presented a formal definition of IoT services and also gave a classification of IoT services on how a physical entity relates to its life cycle. Singh et al. [24] discussed different internet applications, services and also, proposed a model for IoT using the Semantic Fusion Model. In the proposed architecture, the authors introduced how smart semantic framework can help gathering information from sensor networks and encapsulating it for further processing. Zanella et al. [25] discussed a reference framework for urban IoT and presented a survey of technologies and protocols necessary for acceptance of urban IoT by local governments. Weber et al. [26] has highlighted the privacy risks associated with the use and access of data in IoT. They also suggested key elements that must be considered while formulating new rules and regulatory policies for ensuring security and privacy of data. A survey of several already existing IP-based Internet security protocols in wireless sensor networks that are suitable for use in IoT environments have been conducted by Nguyen et al. [27]. Ren et al. [28] studied several lightweight and attack-resistant security solutions for WSNs and IoT. These protocols have been analyzed to identify various IoT security requirements and challenges. They also classified the studied protocols based on the key bootstrapping approach. Wang et al. [29] conducted a thorough survey of different security and privacy issues of wireless sensor networks, which are relevant to IoT scenarios. The study identifies different constraints and requirements against IoT networks at different layers. They also proposed key management systems in WSN using cryptographic primitives. Kumar and Patel [30] gave a general description of diverse security threats and privacy issues encountered during processing, storage and transmission of data and information.

All these studies and surveys generally focus on identification of several challenges in IoT security and different security threats present in the IoT environments. However, since the advent of the IoT, researchers have proposed several solutions and protocols for handling security and privacy in IoT environments.