Chapter 29
A Secure Remote User Authentication Protocol for Healthcare Monitoring Using Wireless Medical Sensor Networks

Preeti Chandrakar
National Institute of Technology (NIT), Raipur, Chhattisgarh, India

ABSTRACT

The wireless medical sensor networks WMSN play a crucial role in healthcare monitoring remotely. In remote healthcare monitoring, the sensor nodes are deployed in patient's body for collecting physiological data and transmit these data over an insecure channel. The patient's health information is highly sensitive and important. Any malicious modification in physiological data will make wrong diagnoses and harm the patient health. Therefore, privacy, data security, and user authentication are extremely important for accessing patient's real-time heath information over an insecure channel. In this regard, this article proposes a secure and robust two-factor based remote user authentication protocol for healthcare monitoring. The authentication proof has done with the help of BAN logic, which ensures that the proposed scheme provides mutual authentication and session key agreement securely. The informal security verification proves that the developed protocol is secure from various security attacks. The simulation of the proposed scheme has been done using AVISPA tool, whose simulation results confirm that the proposed scheme is secure from active and passive attacks. Performance evaluation shows that the proposed protocol is efficient in terms of security features, computation cost, communication cost, and execution time.

DOI: 10.4018/978-1-7998-8052-3.ch029

1. INTRODUCTION

Authentication Remote patient monitoring provides an efficient and convenient connection between patient at home and doctor at the clinic center. The doctor can get the status of the patient any place and any moment and the patient receives a proper treatment from the doctor over an insecure channel. If anyone acquires the patient's information illegally then the privacy of patient will be disclosed. User authentication is one of the most important security mechanism to protect the real time data from the unauthorized users; it provides both session key agreement and mutual authentication securely between participant entities (Wu, Xu, Kumari, & Li, 2017; Ibrahim, Kumari, Das, Wazid, & Odelu, 2016; Chandrakar & Om, 2015; Chandrakar & Om, 2016; Chandrakar & Om, 2017; Chandrakar & Om, 2017; Ali & Pal, 2017; Ali & Pal, 2017). In recent time only very few number of remote user authentication schemes developed by researchers for healthcare monitoring (Ali & Pal, 2017; Kumar, Lee, & Lee, 2012; Khan & Kumari, 2014; Wu, Xu, Kumari, & Li, 2015; He et al., 2015; Wu et al., 2017; Lu, Li, Peng, & Yang, 2016).

In 2012, Kumar et al. (2012) devised a user authentication scheme for monitoring the patient's health condition. They asserted that their scheme is fortified against several security threats. However, He et al. (2015) and Khan et al. (2014) showed that Kumar et al.'s (2012) protocol is not able to guard against some security threats. To remove those security weaknesses, He et al. and Khan et al. developed user authentication schemes. In 2015, Wu et al. (2015) and Li et al. (2016) demonstrate that He et al.'s scheme (2015) suffers from various security attacks. Wu et al. (2015) showed that He et al.'s scheme (2015) does not defend against sensor node capture attack, offline guessing threat, and user impersonation attack. Additionally, they introduced an extended scheme to solve the aforementioned weaknesses. However, Li et al. (2016) identified that the scheme (He et al., 2015) had various security pitfalls like incorrect authentication phase, denial of service attack and no wrong password detection mechanism. To address these security weaknesses, Li et al. (2016) introduced a biometric based authentication scheme for healthcare monitoring and claimed that their scheme improves the security and also holds the computation efficiency. But, Das et al. (2017) pointed out that Li et al. (2016) was insecure from insider attack and sensor node capture attack as well as they did not provide user anonymity and correct password change phase. In order to resolve the security flaws found in Li et al.'s protocol, they proposed a three-factor based authentication scheme for healthcare applications.

In 2016, Amin et al. (2016) designed a remote authentication scheme for health- care monitoring using wireless medical sensor networks and declared that their scheme is provably secure against several security threats. However, Jiang et al. (2017) showed that various security weaknesses in Amin et al. (2016) such as prone to sensor key exposure, stolen mobile device attack and de-synchronization attack. To overcome these security problems, they developed an enhanced authentication protocol using quadratic residues. In the same year, Jiang et al. (2016) developed three-factor based authentication scheme for e-health care applications and affirm that their proposed protocol can resistance to various known attacks and facilitates more security features. But, Irshad and Chaudhry (2017) showed that Jiang et al.'s scheme (2016) insecure against replay and denial-of-service attacks. To remove these security pitfalls, they designed an improved scheme. They proclaimed that their scheme can withstand replay and denial-of-service threats as well as efficient like as original Jiang et al.'s scheme. Very recently, Wu et al. (2017) designed a secure two-factor based remote authentication scheme for heath care monitoring using WMSN. They affirm that their scheme resistant to known security threats and more robust than existing relevant schemes.