Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 113 (2017) 113–120

Procedia Computer Science

www.elsevier.com/locate/procedia

The 8th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2017)

An Improved Remote User Verification Scheme in Wireless Body Area Networks

Aakriti Arya[a], Chaitanya Reddy[a], Trupil Limbasiya[a,*]

[a]*NIIT University, Neemrana, Rajasthan - 301705, India*

Abstract

We mostly practice multiple kinds of facilities for different intentions, which help us in various ways to fulfill our wishes. However, the model checks the legitimacy of the resources client else the system user or the regularity may lose significant data with respect to the security. Hence, the concerned authority has to verify the user based on differently available credentials (identity, text-based password, smart card, biometric identity). The wireless body area network (WBAN) is a system t facilitate to customers for providing automatic health monitoring, which sends crucial health-related data to the doctors with the help of body sensors. A sender must identify the receiver before sending this kind of important data properly. Scientists advised several verification solutions in the wireless body area networks. However, different schemes cannot withstand against multiple attacks. We suggest a new authentication scheme, which is secured with respect to many attacks such as replay, fake server/sensor, plain text, stolen verifier, and internal.

Peer-review under responsibility of the Conference Program Chairs.

Keywords: Attack; Authentication; Modification; Privacy; Session key;

1. Introduction

With the rapid development of Internet technology, it has become an integral part of everyones life and thus, its services have been expanded in all sectors right from medical to communication. Since, it is practiced by a large number of people but one should make sure that the authorized person is only availing a particular service and not a malicious user. Thus, we need a proper authentication system, which can provide a precise level of security. Authentication is defined as a process in which a legitimate user puts in his or her credentials or something that ensures the identity and legitimacy of the user. There are different factors of authentication such as one factor, two factor and three factor, as we move up the scale, the authentication scheme gets better and secure.

Nowadays, authentication plays the utmost important role within the system and knowingly or unknowingly. We use it everywhere. Right from when you unlock your phone or laptop using a password to the online transactions that you make every day using OTP (one-time time password) authentication is employed mostly, and the reason is

* Corresponding author. Tel.: +91-9924827591.
E-mail address: limbasiyatrupil@gmail.com

1877-0509
Peer-review under responsibility of the Conference Program Chairs.
10.1016/j.procs.2017.08.324

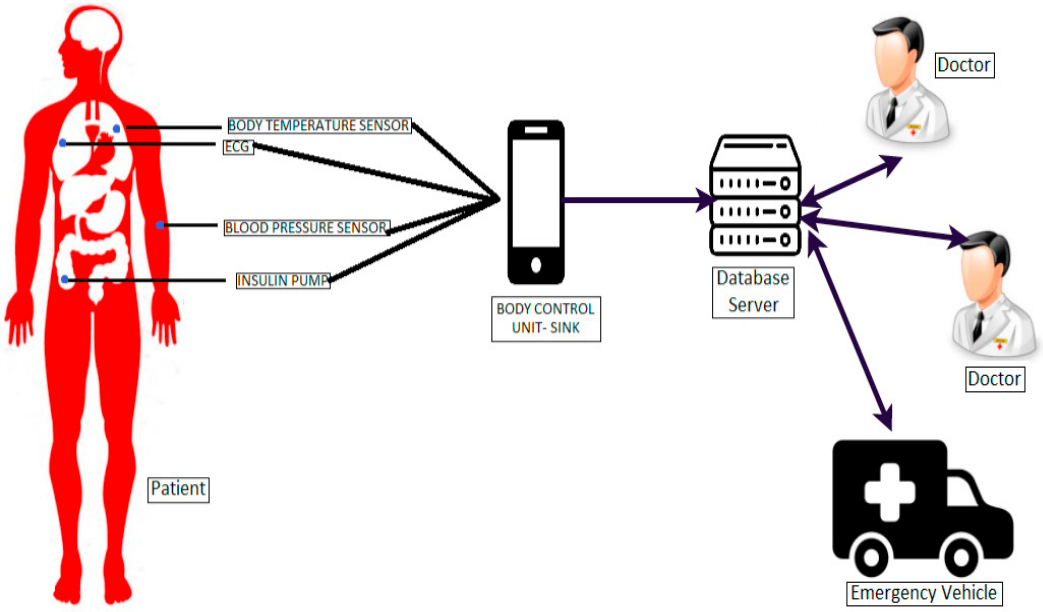

Fig. 1. The General Scenario of Wireless Body Area Networks

very obvious-security. Without a proper authentication model, we would have to face a menace that would lead to malicious and fraud users accessing your data impersonating being you. WBANs (Wireless body area networks) have an authentication system as their backbone because a lapse in such technologies could lead to the death to a person. Thus, there are numerous advantages applications of authentication. WBAN is a major application of authentication schemes. Because it includes a bunch of sensors deployed inside a human body in order to keep a tab related to health and improves it. It basically measures certain parameters such as blood pressure, insulin level and heart beating [1]. The application of WBAN is spread in various sectors such as military, fitness, medical, and so on [2]. Fig.1 explains the structure of WBAN, which is constituted using three basic components: the sensor nodes which are placed inside the body of a customer, the cellular phone, which basically acts as a sink for WBAN and the back-end server, which is connected to WBAN system via the Internet for transferring crucial data.

WBAN was launched to decrease the cost in the traditional healthcare cost and help people, who are unable to travel to healthcare centers every now [3] but with its advantages, there are major security concerns that come along. Since, WBAN has some unique characteristics, self-organized, limited storage as a large amount of medical data cannot be stored in the sensors deployed inside the human body, noised signals and highly consumed energy as the sensors work all day long securing this particular technology is a great challenge to solve. Thus, if there is a lack of authentication in WBAN, then it might lead to breach of patients privacy and may lead to hazardous results such as the patients death [4, 5].

Therefore, scientists recommend taking care of authentication as it is of utmost importance in order to make sure that data confidentiality, integrity and availability are maintained within the WBAN framework. There are many solutions [6, 7, 8] in order to obtain the security, but some schemes failed in providing a certain level of security during some circumstances. The public-key crypto-systems were also employed to ensure proper authentication and verification of the transmitted information are done [9]. The use of symmetric cryptography also came into the picture, where authors [10] advised a monitoring system, which was basically based on hardware and software-based cardiac patient health care monitoring protocol.

A scheme [11] introduced a biometric-based security for data authentication, which shows that dilemma by securing data communication, while reducing computational complexity. The biometric characteristics are represented by employing ECG characteristics. Lee et al. [12] employed an HMAC scheme to fulfill mutual authentication and thwart clone attacks, which was focused on the physical un-clonable function (PUF) circuit. And it was employed to derive secrets from physical characteristics of integrated circuits. Kanjee et al. [13] further proposed a two-tiered authentication