Cloud Centric Authentication for Wearable Healthcare Monitoring System

ABSTRACT

Security and privacy are the major concerns in cloud computing as users have limited access on the stored data at the remote locations managed by different service providers. These become more challenging especially for the data generated from

the wearable devices as it is highly sensitive and heterogeneous in nature. Most of the existing techniques reported in the literature are having high computation and communication costs and are vulnerable to various known attacks, which reduce their importance for applicability in real-world environment. Hence, in this paper, we propose a new cloud based user authentication scheme for secure authentication of medical data. After successful mutual authentication between a user and wearable sensor node, both establish a secret session key that is used for future secure communications. The extensively-used Real-Or-Random (ROR) model based

formal security analysis and the broadly-accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool based formal security verification show that the proposed scheme provides the session-key security and protects active attacks. The proposed scheme is also informally analyzed to show its resilience against other known attacks. Moreover, we have done a detailed comparative analysis for the communication and computation costs along with security and functionality features which proves its efficiency in comparison to the other existing schemes of its category.

**EXISTING SYSTEM**

* Castiglione et al. [25] developed a Software-as-a-Service (SaaS)-based cloud architecture that allows heterogeneous devices to interact amongst themselves to provide secure and efficient access to healthcare resources regardless of network capabilities used by the end users.
* Xiao et al. [28] proposed a cloud-based RFID authentication protocol. Their protocol protects the data transmission between the reader and the cloud server without any help from a third party, and it also preserves tag privacy even if the tag does not update its identification.
* Surekha et al. [29] proposed a realistic lightweight authentication protocol for securing cloud-based RFID system. However, the location privacy of the reader in these two protocols is not protected.
* Li et al. [30] designed an authenticated key establishment mechanism for wearable devices which is lightweight. Later, He and Zeadally [31] proposed a novel authentication model (called Ambient Assisted Living (AAL)) that can be applied for monitoring the health related information of a patient and it supports the telehealthcare services too. Moreover, user anonymity and forward secrecy properties are preserved in the AAL.

**Disadvantages**

* + There is only Smart card based Health Care System.
  + There is no Dynamic Wearable Sensor Addition Phase.

**PROPOSED SYSTEM**

* In this paper, the system proposes a new cloud based user authentication scheme for secure authentication of medical data. After successful mutual authentication between a user and wearable sensor node, both establish a secret session key that is used for future secure communications.
* The extensively-used Real-Or-Random (ROR) model based formal security analysis and the broadly-accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool based formal security verification show that the proposed scheme provides the session-key security and protects active attacks. The proposed scheme is also informally analyzed to show its resilience against other known attacks.
* Moreover, we have done a detailed comparative analysis for the communication and computation costs along with security and functionality features which proves its efficiency in comparison to the other existing schemes of its category.

**Advantages**

* The system is uses smart wearable devices-based healthcare system which is more secure and dynamic.
* The system allows password change, smart card revocation and also new wearable sensor addition phases.

**SYSTEM REQUIREMENTS**

➢ **H/W System Configuration:-**

➢ Processor - Pentium –IV

➢ RAM - 4 GB (min)

➢ Hard Disk - 20 GB

➢ Key Board - Standard Windows Keyboard

➢ Mouse - Two or Three Button Mouse

➢ Monitor - SVGA

**Software Requirements:**

* Operating System - Windows XP
* Coding Language - Java/J2EE(JSP,Servlet)
* Front End - J2EE
* Back End - MySQL