INTERNATIONAL JOURNAL OF TECHNOLOGY AND COMPUTING (IJTC)
ISSN-2455-099X,
Volume 2, Issue 9 September 2016

Dual Layered Response for WBANs based upon Authentication and Authorization Layers

Abhishek Sinha[1], Dr. Raman Chadha[2], Chander Prabha[3]

[1]M.Tech Student, [2]Professor Head, [3]Associate Professor

[123]Department of Computer Science and Engineering, CGCTC, Jhanjeri, mohali

[1]abhi.blaze23@gmail.com, [2]dr.ramanchadha@gmail.com, [3]c.prabha.cgc@gmail.com

ABSTRACT-- The holter is the device used for the purpose of heart rate computation from the patient's body and deployed on the patient's body. The proposed model has been designed for the authentication level security between the cloud based healthcare record management service and the wearable body sensor deployed on the patient body (Also called holter). The proposed model uses the strong authentication keys encrypted using the double layered encryption architecture, which is specifically designed for the proposed model. The proposed model adds the two-level security for the transmission security, which uses the secure initial setup phase and key exchange model at the second level. The proposed model has been tested for the transmission delay added by the encryption, decryption and key exchange process. The proposed model adds the minimum possible delay in the time based periodic authentication mechanisms. The proposed model performance has been evaluated in details using the various performance parameters. The experimental results have proved the efficiency of the proposed model in protecting against the external threats.

KEYWORDS—Healthcare networks, Holter communications, Cloud platforms, Network security, WBAN security.

I. INTRODUCTION

The security of Wireless Bode Area Networks (WBAN) can be compromised in many ways. [23] A remote end user accessing base station information can be prevented from doing so in a variety of ways. Communication between the base station and sensor nodes can be blocked. This can be accomplished by analog jamming of signals or by digital jamming in the form of DoS (Denial of Service) attacks that flood the network, base stations or both. Targeted DoS attacks on strategic nodes in the WBAN can also block communication of large parts of the network with the base station. Communication between base stations and other sensor nodes can be prevented by setting up incorrect routing information so that traffic goes to the wrong destination or loops. One way to do this is to spoof the base station and deceive nodes into routing all packets to the spoofed base station instead of the real base station. [23, 24]

Another way of breaching security is to destroy the base station itself. This can be accomplished by monitoring the volume and direction of packet traffic toward the base station so that the location is eventually revealed. [7] Destruction can also be accomplished by listening to the RF signals to locate and triangulate the location of the base station. A third threat is eavesdropping. This is made easier by wireless hop-to-hop communication. Eavesdropping can be used to track and determine the location of the base station for destruction. There are many other methods to breach the WSN security. [18]

II. LITERATURE REVIEW

Hossain et al. [29]termed cloud computing through NIST as a model for pervasive, accessible, demand-driven network access to resources such as network bandwidth utilization, storage, software services etc. from shared pool of computing resources that can be easily available with nominal management attempt. Wang et al. [41] discussed that in traditional IT solutions, the IT services were hosted under complete physical and personnel controls whereas, cloud computing shifted the application and databases phase to large data centre servers on the Internet. This shift gave rise to many software and data security, recovery, and privacy related problems. The authors focused on security of data storage in cloud. Doukas et al. [12] discussed about the application of Cloud Computing in healthcare services to update and retrieve patient health information. The @HealthCloud application was developed for HTC G1 mobile phone running on Google's Android operating system. Fan et al. [14] proposed a "Data Capture and Auto Identification Reference" (DACAR) platform for developing eHealth applications equipped with authentication, integrity, confidentiality, authorisation, secure data transmission. It was a hardware and software suite to integrate, capture, store and consume sensitive medical data and supports large scale health services using Cloud infrastructure. Zarandi et al. [43] presented K2C (Key to Cloud) -a scalable and lazy revocation based protocol to share and store data securely in untrusted clouds also. Hierarchical Identity-Based Encryption and Key-Policy Attribute-Based Encryption were used for access control, key updation and authorisation. Fitch et al. [15] addressed the various concerns of Cloud such as data security, reliability, and availability and the threats such as network outage, data breaches, and exploitations. So the authors developed a novel security solution to cloud storage based on hierarchical colored Petri nets (CPN).

III. EXPERIMENTAL DESIGN

The heart rate is computed on the Patient Body Sensor (PBS) device and forwarded to the cloud healthcare records management server. The data communication between Patient Body Sensor (PBS) and cloud healthcare records management server must be secured to protect the privacy of the user data for any data forgery attacks. Such data forgery attacks can be used for the information falsification, which can affect the health service decision in the critical condition. If the hacker will update and forward the data as normal heart rate using the replay attack with information fabrication, when the original patient information is showing the critical level heartbeat, the cloud based healthcare record management service will not raise alarm for patient's critical situation. The following mechanism has