# Verifiable Security and Privacy Provisioning Protocol for High Reliability in Smart Healthcare Communication Environment

2022 4th Global Power, Energy and Communication Conference (GPECOM) | 978-1-6654-6925-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/GPECOM55404.2022.9815685

Vincent Omollo Nyangaresi
*Faculty of Biological & Physical Sciences*
*Tom Mboya University College*
Homabay, 40300, Kenya.
vnyangaresi@tmuc.ac.ke

Zaid Ameen Abduljabbar
*College of Education for Pure Sciences*
*University of Basrah*
Basrah, 61004, Iraq
zaid.ameen@uobasrah.edu.iq

Junchao Ma
*College of Big Data and Internet*
*Shenzhen Technology University*
Shenzhen, 518118, China
Corresponding author: majunchao@sztu.edu.cn

Mustafa A. Al Sibahee
*College of Big Data and Internet*
*Shenzhen Technology University*
Shenzhen, 518118, China
mustafa@sztu.edu.cn

***Abstract*—Critical patient data collected by body sensor units and transmitted over public wireless communication channels is exposed to numerous privacy and security attacks. As such, there is need for deployment of robust security solutions to uphold integrity, confidentiality and availability. In addition, the resource constrained nature of sensor nodes require efficient authentication protocols in terms of computation power, energy, bandwidth and storage requirements. To this end, many protocols based on public key infrastructure, blockchain and bilinear pairings are unsuitable for deployment in these sensor networks. Apart from efficiency shortfalls, most of the conventional security protocols cannot withstand majority of the typical wireless body area networks attacks. To this effect, a verifiable security and privacy provisioning protocol based on elliptic curve is presented in this paper. The reliability of the proposed is demonstrated via its robustness under Dolev–Yao (D-Y) and Canetti-Krawczyk (CK) threat models. On the other hand, its lightweight and efficient nature is investigated using execution time and bandwidth requirements, which are shown to be the least when compared with other schemes.**

***Keywords*—Authentication, ECC, reliability, privacy, protocol, security, verifiability.**

## I. Introduction

Wireless Body Area Networks (WBANs) deploy wearable sensors to offer remote monitoring as well as collection of patient bio-medical data. In this scenario, the bio-sensors serve to perceive patients' critical signs, process them and transmit the same to the hospital medical servers. As pointed out in [1], the deployment of these wireless sensors is on the rise for remote healthcare management. This increase is attributed to the recent advancement in sensor technology that collects data from diverse environments, process and forwards it to other nodes in the network. According to [2], bio-sensors observe patient health status and generate an alarm when the condition becomes critical. Ideally, these sensors can be implantable, placed on the patient's body or in the vicinity of the patient. The observed parameters may include heart rate, electro cardio gram (ECG), blood glucose levels, body movement, electroencephalogram (EEG), blood pressure and temperature among others. The overall goal of WBAN is to boost efficacy and quality of the conventional healthcare systems [3].

In spite of the numerous positive contributions of the WBANs, the communication of sensitive and private data over the public channels [4] inadvertently exposes these messages to many threats. Therefore, perfect privacy and security have emerged as significant challenges that may inadvertently hinder the deployment of WBANs. As explained in [5], security offers a healthy and secure communication environment between the bio-sensors and hospital servers. On the other hand, privacy protection ensures that only legitimate and authorized parties can access and view the sensed data. Due to proliferation of side-channel attacks against wireless sensors, the data in memory or in storage in the servers must be accorded proper protection. Other attacks, vulnerabilities and threats in this environment include tampering, Denial of Service (DoS) and jamming. For example, an adversary can capture and alter the information exchanged over the wireless channels. This can effectively lead to wrong diagnosis and inappropriate response from the medical staff, which can endanger patient life. Although strong encryption protocols that can be applied to protect these networks exist, the resource constrained nature of the sensor nodes hinder their deployments. Consequently, only lightweight cryptosystems are appropriate in these networks.

As discussed in [6], the WBAN communication process should satisfy non-repudiation, confidentiality, anonymity, authenticity, integrity and availability. However, authors in [7] and [8] identify Quality of Service (QoS) metrics such as low packet losses, transmission latencies, fault tolerance, availability and efficient energy and bandwidth usage as being significant in wireless networks. In addition, there is need to execute proper authentication and authorization before any access can be granted. The main contributions acclaimed in this article include the following:

- An elliptic curve cryptography based verifiable security and privacy provisioning protocol is developed to offer shorter key sizes and hence minimize bandwidth requirements.

978-1-6654-6925-8/22/$31.00 ©2022 IEEE