International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 1912-1917 www.ijaem.net

Secure Patient Data Transmission Using Wireless Sensor Network

[1]Vetrimanikumar.J, [2]Sabitha.D, [2]Sharmila.S, [2]Sowmiya.K, [2]Thenpandi.B

[1]*Assistant Professor,Department of Electronics and Communication Engineering,SSM Institute of Engineering and Technology*

[2]*UG Scholar,Department of Electronics and Communication Engineering,SSM Institute of Engineering and Technology*

Submitted: 15-06-2022 Revised: 20-06-2022 Accepted: 25-06-2022

ABSTRACT

Wireless Sensor Networks (WSN) based healthcare systems are increasing day by day to advise the health status and living environment habitat of peoples. However, WSN based healthcare application suffers from the issues related to privacy and security. Susceptible attacks and security consideration comes into WSN based healthcare applications as an interesting and challenging problem. One of the challenges in WSNs is to provide high-security requirements with constrained resources. The security requirements in WSNs are comprised of node authentication, data confidentiality, anti-compromise and resilience against traffic analysis.In this paper, wehave proposed a privacy preservation scheme for WSN based healthcare application utilizing the principles of multipath routing, secret sharing and hashing. The healthcare data collected from the wireless sensor network is splits into n components. Further, the hash value is computed for each component with the help of well-known hashing technique. The change in hash value is used to detect changes in the message. These n components are then transferred to n servers, with the help of multipath routing. This article provides extensive simulations to validate new approach. Results show that secret splitting along with multipath routing helps to attain privacy preservation in WSN based healthcare system."

KEYWORDS: Elliptic curve cryptography, User Authentication, Access control, Wireless Sensor Networks

I. INTRODUCTION

The security of wireless sensor networks is becoming increasingly important as they grow more ubiquitous. This is especially true for products like medical sensors, where confidentiality is critical.The WSNs sensors are used to measure, monitor and record the patient's data such as blood pressure, heart rate, temperature and other vital data. These devices frequently communicate sensitive data, necessitating the use of a cryptographic technique that ensures data confidentiality and integrity, as well as the legitimacy of people using the sensor network's devices. All of these are provided by public-key cryptography; but, owing of computational and battery power limits, the most prevalent public-key algorithm (RSA) cannot be used because it is too computationally expensive. Because it requires substantially smaller key sizes, Elliptic Curve Cryptography (ECC) presents an option that provides comparable security strength withsignificantly less computation. Data encryption, digital signatures, user authentication, and other applications have all made substantial use of public-key cryptography. In comparison to the widely used symmetric key cryptography in sensor networks, public-key cryptography offers a more flexible and straightforward interface that requires no key predistribution, pairwise key sharing, or a sophisticated one-way key chain mechanism. However, there is a widespread perception in the sensor network research community that public-key cryptography is not feasible since the required computational intensity is incompatible with sensors with limited processing power and energy budget. The preliminary investigation appears to debunk this myth. The Wireless Sensor Network (WSN) is a self-organizing network that consists of a collection of sensor nodes that collect environmental data and communicate it to a sink or base station. The information can be gathered from the base station for further assessment. Sinks in