# INTRODUCING DATA COLLECTION PROTOCOL FOR PROTECTING PATIENT DATA FROM INSIDE ATTACKS

**[1]PUNNA SHILPA, [2] N. NAVEEN KUMAR**

[1]M. Tech Student, Department of CSE, School of Information Technology (JNTUH), Village KPHB, Mandal Kukatpally, District Medchal, Telangana, India

[2]Assistant Professor, Department of CSE, School of Information Technology (JNTUH), Village KPHB, Mandal Kukatpally, District Medchal, Telangana, India

**ABSTRACT—** ***At present, the healthcare information is a significant to the wireless sensor networks, wherein sufferers can be monitored in hospitals or even at domestic the use of wireless medical sensor networks (WMSNs). In current years, many healthcare applications the use of WSNs had been evolved. The conventional solutions can protect the patient data at some point of transmission, however cannot prevent the inside assault where the administrator of the affected person database well-known shows the touchy affected person information. Hence, on this paper we propose an efficient data collection protocol to defend wireless clinical sensor information from the inside attackers. The proposed protocol will splits the sensitive patient data into three components according to a random number generator based on hash function and sends them to three servers, respective, via secure channels.***

***Keywords: Wireless Sensor Networks, inside attackers, Secure Channels***

## 1. INTRODUCTION

A significant proportion of the human population suffers from various medical conditions, including chronic ailments and medical emergencies due to sudden injuries. In absence of continuous medical care, many chronic ailments prove to be fatal. On the other hand in various medical emergency scenarios, timeliness of medical attention is even more important. In many such cases, e.g., cardiac arrest, the risk to a patient's life can be considerably minimized by improving the quality and timeliness of medical care in the "golden time window" immediately following the injury. Wireless Sensor Network (WSN) has paved the way for advancements in various aspects of sensing. These advancements have been possible with arrival of smart sensing techniques, smaller transceiver and sensing modules as well as stronger processing units. Applications of WSNs range from military applications to global climate monitoring applications and from applications in underwater networks to applications in structural health monitoring and beyond. An essential factor of WSN has been the design of fitness monitoring structures centering on wearable sensor modules for patients. With the growing older populace around the sector, research into fitness

tracking software has received prominence over the latest years. Authors of point out use of microprocessor based programs to compute the records from sensors to research a patient. This statistics changed into transmitted over telephonic networks just like the facsimile systems. Since the computational strength of the devices was susceptible, the applications had been confined to measuring simple parameters. With further research and stronger processors and communications systems multiple parameters could be monitored at once and data could be relayed over the internet.

The sensor devices have the capability of sensing, processing and transmitting vital physiological signals using wireless technology.

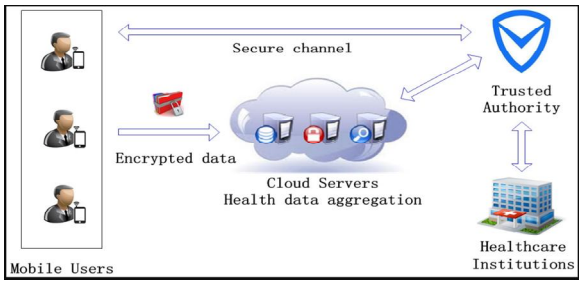



**Fig1. Example for HealthCare System Security**

Contrary to the traditional sensor networks that are carefully planned and deployed in the predetermined positions, WSNs can be deployed in an ad-hoc manner which make them robust, fault tolerance, and increase in spatial coverage. They can significantly be used to screen and track conditions of sufferers in both cities and rural regions the usage of an intranet or internet thereby decreasing the strain and strain of healthcare carriers, cast off medical mistakes, reduce workload, growth efficiency of clinic group of workers, reduce long term cost of healthcare offerings, and improve the consolation of the patients. Also, those structures provide beneficial methods to remotely acquire and monitor the physiological alerts without the want of interruption of the patient's everyday lifestyles, therefore improving lifestyles quality. Sensor nodes can be strategically positioned at the human frame to create a cluster this is known as wireless Body Area Network (WBAN) that can be used to gather affected person's vital symptoms. It is really worth noting that sensor nodes are being operated by batteries, their electricity consumption at some point of transmission ought to be minimum for reliable records transmission among WBAN and personal server. Using sensor nodes with conversation technology consisting of cell telephones i.e. PDA, General Packet Radio Service (GPRS), 3G, and the net, the sensor network can keep patient, caregivers, and medical doctor informed whilst also establishing traits and detecting versions in fitness. This paper, proposes a networking answer in which Sensor (Medical Super Sensor (MSS) is used to acquire multiple physiological symptoms sensed by way of each of the frame sensors in WBAN as well as forward them to the private server. An Intelligent Personal Digital Assistant (IPDA) is utilized as a private server; it has the potential to gather patient's essential signs and symptoms and prioritizes the records transmission based on affected person's modern circumstance as well as records content.

## 2. RELATED WORK

D. Malan, T. F. Jones, M. Welsh, and S. Moulton had completed an initial design of CodeBlue and prototypes of several of the components described herein. The pulse oximetry mote has been completed and development of an ECG mote is currently underway. They explored the use of an adaptive

spanning-tree multi-hop routing algorithm, based on the TinyOS Surge protocol, and they incorporated dynamic transmission power scaling to minimize interference. A lightweight public key infrastructure based on elliptic curve cryptography is currently being tested. A sophisticated programming model the usage of summary regions for routing, information sharing, and aggregation has additionally been advanced.

Pardeep Kumar and Hoon-Jae Lee mentioned the security and privateness issues in healthcare packages the usage of scientific sensor networks. They have been shown that a well-planned security mechanism must be designed for the successful deployment of such a wireless application. In this respect, they found many important challenges in implementing a secure healthcare monitoring system using medical sensors, which reflects the fact that if a technology is safe, then people will trust it. Otherwise, its use will not be practical, and could even endanger the patient's life.

The objective of F. Hu, M. Jiang, M. Wagner, and D. C. Dong research was to take advantage of the modern low-cost low-power sensor and wireless communication technology to create a TSN for ECG monitoring purposes. F. Hu, M. Jiang, M. Wagner, and D. C. Dong TSN device has the potential to offer non-stop vital sign monitoring abilties without the exhaustion of any manpower. In fact, it is meant to give support to the present day healthcare environments and loose medical specialists for greater urgent features. By automating the critical signal monitoring system, the most up to date information for all patients is made to be had always. Based on wireless sensor community generation, wearable mobile structures are allotted to the patients of difficulty. These mobile platforms are chargeable for gathering patient important signal using a three-lead ECG tracking gadget. The gathered information is transmitted wirelessly over radio to the receiving station related to a computing device wherein the facts are processed. ECG function extraction or classification techniques are applied to the patient statistics, and the feature points of interests extracted. This information provides significant facts for the diagnosis of feasible cardiovascular illnesses.

## 3. FRAMEWORK

### A. System Overview

This paper proposes an approach that provides high end security for the patient's sensitive physiological information and assures most privacy for the patients. This approach deals with the protection of information by using a cryptography mechanism referred to as Paillier cryptosystem that includes a unique homomorphic property of manufacturing the total of plaintexts whereas encrypting the product of cipher texts. This mechanism is an important approach during this proposed system.

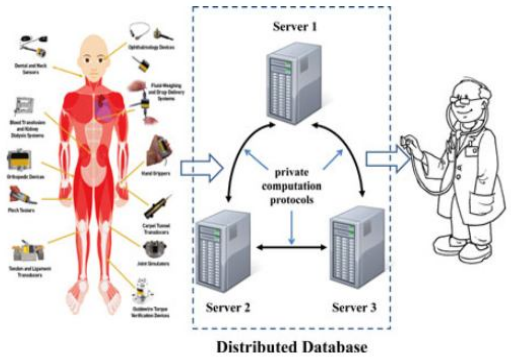



**Fig2. System Overview**

In our model, the patient database system is composed of multiple database servers. We assume

that all data servers are semi-honest, often called "honest but curious". That is, all data servers run our protocol exactly as specified, but may try to learn as much as possible about the patient data from their views of the protocol. In addition, we assume that at least one data server is not compromised by attackers. For simplicity, we assume that the number of data servers is three. In fact, it can be any number more than three.

### B. Medical Data Collection in Wireless Sensor Networks

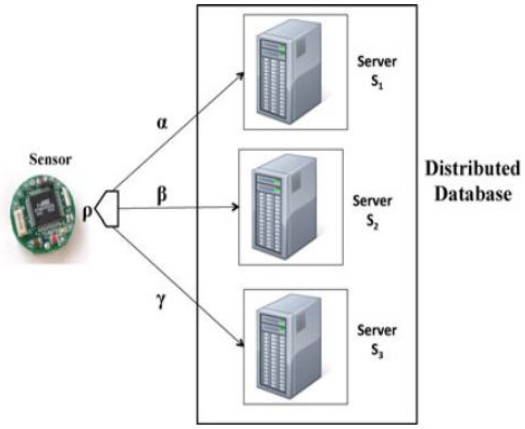



**Fig2. Collecting Data from Multiple Servers**

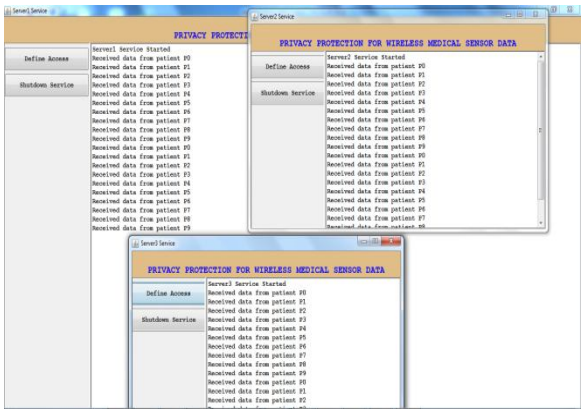
To collect medical sensor data from the sensors there is an initial deployment phase between each medical sensor and each data server. For each medical sensor, three secret keys are pre-deployed and pre-shared with three data servers, respectively. Each secret key is used to create a secure channel between the sensor and one data server.

The data collection will be done by data collection protocol. The protocol collects the data from multiple servers by using distributed database. This protocol can prevent the collected data from inside attackers.

## 4. EXPERIMENTAL RESULT

In this experiment, we took three servers to collect the patient data from medical sensors. In this we need to run all three servers. After started the servers, admin can define the access to the users in this system. Add the users of access type either Patient Information Retrieval (PIR) or Average Analysis Protocol (AAP). Here, the PIR will retrieve the specified patient information and AAP will average all the values for the patients.

To get the patient records we need to enter the patient sensor size. The records of the patients retrieved through the three servers.




In the above screen we can observe the three server communication while transferring patient data.

## 5. CONCLUSION

In this paper we conclude that, the main aim of this paper is to protect the medical sensor data from the inside attackers. To provide security to the medical sensor data in this paper we proposed data collection protocol and the authorized user to access data from the sensors, we proposed an access control protocol. From the experimental results, we observed the performance of these two proposed protocols.

## REFERENCES

[1] P. Belsis and G. Pantziou, "A k-anonymity privacy-preserving approach in wireless medical monitoring environments," J. Personal Ubiquitous Comput., vol. 18, no. 1, pp. 61–74, 2014.

[2] D. Bogdanov, S. Laur, and J. Willemson, "Sharemind: A framework for fast privacy-preserving computations," in Proc. 13th Eur. Symp. Res. Comput. Security, 2008, pp. 192–206.

[3] R. Chakravorty, "A programmable service architecture for mobile medical care," in Proc. 4th Annu. IEEE Int. Conf. Pervasive Comput. Commun. Workshop, Pisa, Italy, Mar. 13–17, 2006, pp. 532–536.

[4] J. Daemen, G. Bertoni, M. Peeters, and G. V. Assche. (2012, Jul. 6). Permutation-based encryption, authentication and authenticated encryption. Proc. Directions Authenticated Ciphers, Stockholm, Sweden [Online]. Available: http://www.hyperelliptic.org/DIAC/slides/PermutationDIAC2012.pdf

[5] S. Dagtas, G. Pekhteryev, Z. Sahinoglu, H. Cam, and N. Challa, "Real-Time and secure wireless health monitoring," Int. J. Telemed. Appl., pp. 1–10, Jan. 2008.

[6] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theory, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[7] (2013, Jul.). Digital signature standard (DSS). FIPS PUB 186-4 [Online]. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[8] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Inf. Theory, vol. IT-31, no. 4, pp. 469–472, Jul. 1985.

[9] D. He, S. Chan, and S. Tang, "A novel and lightweight system to secure wireless medical sensor networks," IEEE J. Biomed. Health Informat., vol. 18, no. 1, pp. 316–326, Jan. 2014.