# Securing WMSN using SHAREMIND

**Prof. Dhanshri Patil[1], Priyanka Kanse[2], Priyanka Kakade[3],**

**Ketaki Sortur [4], Akshata Nalawade[5]**

*[1, 2,3,4,5] UG Student Department of Computer Engineering,*
*PCET's Nutan Maharashtra Institute of Engineering and Technology,*
*Talegaon Dabhade, Maharashtra (India)*

## ABSTRACT

*Healthcare applications are considered as promising fields for wireless sensor networks, where patients can be monitored using wireless medical sensor networks (WMSNs). Current WMSN healthcare research trends focus on patient reliable communication, patient mobility, and energy-efficient routing, as a few examples. However, deploying new technologies in healthcare applications without considering security makes patient privacy vulnerable. Moreover, the physiological data of an individual are highly sensitive. Therefore, security is a paramount requirement of healthcare applications, especially in the case of patient privacy, if the patient has an embarrassing disease. This project discusses the security and privacy issues in healthcare application using WMSNs. We highlight some popular healthcare projects using wireless medical sensor networks, and discuss their security the existing systems solutions can simply protect the patient data during transmission, but cannot protect the inside attack where the administrator of the patient database reveals the sensitive patient data. So we are proposing a approach to prevent the inside attack by using multiple data servers to store patient data. The main contribution of this paper is to distribute patients data securely in multiple data servers and performing the Paillier cryptosystems to perform statistical analysis on the patient data without compromising the patients privacy.*

***Keywords: Wireless medical sensor network, patient data privacy, Paillier encryption, AES.***

## I INTRODUCTION

A wireless sensor network is a network to monitor physical or environmental conditions such as temperature, sound, pressure, etc. The development of wireless sensor networks was motivated by air pollution monitoring, water quality monitoring, land side detection, forest fire detection, habitat monitoring and so on. Though there are many applications in wireless sensor network domain, human healthcare applications takes the major role. In human healthcare, sensors are used to monitor the patients' health status such as temperature level, sugar level, heart beat rate, blood pressure. For instance, if the patients sugar level is monitored 10 times per day then the data is up-dated in the database which is present in the local server. Likewise the values for blood pressure, heart beat, and temperature are also noted at regular intervals. There are many security issues such as data stealing, stealing and updating, storing the wrong values. Suppose if the intruder is trying to hack the patient details, there are many chances for the misuse of data which may lead to severe consequences. The data can also be modified by the hackers due to lack of security. The treatment prescribed by the doctors can be hacked which may even lead to death of the patients. Patients are the victims because of the above issues. To prevent these issues, the intrusion detection system is proposed. An intrusion detection system is a system used to check the ma-vicious activities and produces electronic reports to a management station. It consists of Paillier algorithm key cryptosystems. The algorithm is used to encrypt the patient details before storing it in the database and perform decryption when needed by the physician.

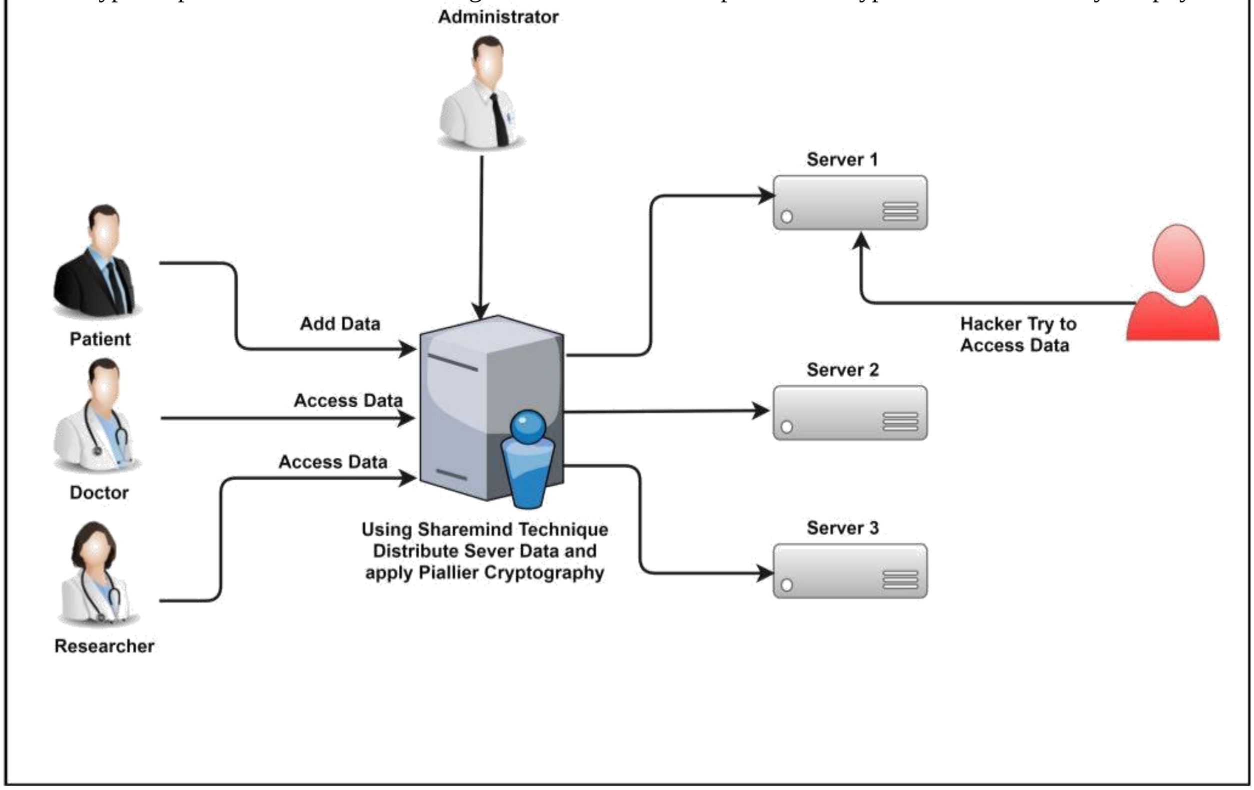

**Fig. 1: System Architecture of Proposed System**

## II LITERATURE REVIEW

- **Dan Bogdanov et.al.**Gathering and processing sensitive data is a difficult task. In fact, there is no common recipe for building the necessary information systems. In this paper, we present a provably secure and efficient general-purpose computation system to address this problem. Our solution SHAREMIND is a virtual machine for privacy-preserving data processing that relies on share computing techniques. This is a standard way for securely evaluating functions in a multi-party computation environment. The novelty of our solution is in the choice of the secret sharing scheme and the design of the protocol suite. We have made many practical decisions to make large-scale share computing feasible in practice.[1]

- **S. Dagtas, G. Pekhteryev et.al.** We present a framework for a wireless health monitoring system using wire-less networks such as ZigBee. Vital signals are collected and processed using a 3-tiered architecture. The first stage is the mobile device carried on the body that runs a number of wired and wireless probes. This device is also designed to perform some basic processing such as the heart rate and fatal failure detection. At the second stage, further processing is performed by a local server using the raw data transmitted by the mobile device continuously. The raw data is also stored at this server.[2]
- **Daojing He et.al.** Wireless medical sensor networks (MSNs) are a key enabling technology in e-healthcare that allows the data of patients vital body parameters to be collected by the wearable or implantable biosensors. However, the security and privacy protection of the collected data is a major unsolved issue, with challenges coming from the stringent resource constraints of MSN devices, and the high demand for both security/privacy and practicality. In this paper, we propose a lightweight and secure system for MSNs.[3]

## III MOTIVATION

In a wireless medical sensor network, the sensitive patient data is transmitted through the open air. It is more vulnerable to eavesdropping, spoofing, altering and replaying attacks, compared with the wired network. Some work has been done to secure the wireless medical sensor network using efficient symmetric key cryptosystem

## IV PROBLEM ANALYSIS

### Problem Statement:

Proposed system focus on the user accessibility and the retrieval compress server data.

User accessibility.

Retrieval of compromised data.

#### 4.1.1 Goals

- Protect the patient data during transmission.
- Stop the inside attack where the administrator of the patient database reveals the sensitive patient data of patients.

**4.1.2 Scope** Healthcare applications are considered promising fields for WMSNs, where patients can be monitored. Transmission in wireless environment needs safety and privacy of medical data. Retrieval of compromised data through proxy server . For data Security purpose, System gives permission to user regarding compromised data.

## V METHODOLOGIES OF PROBLEM SOLVING AND EFFICIENCY ISSUES

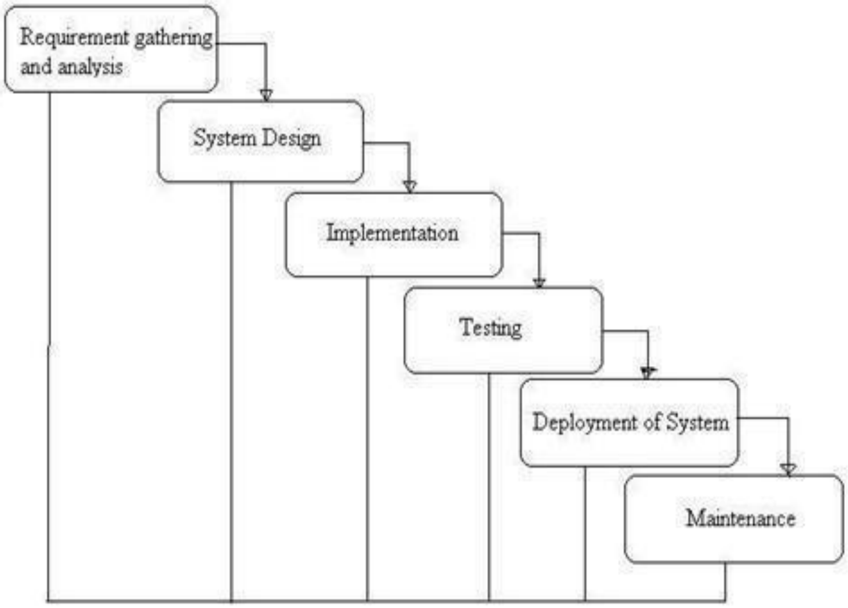

**Fig. 2: Waterfall model**

**1. Requirement gathering and analysis:**

In this step of waterfall we identify what are various requirements are need for our project such are software and hardware required, database, and interfaces.

**2. System Design:**

In this system design phase we design the system which is easily understood for end user i.e. user friendly. We design some UML diagrams and data flow diagram to understand the system flow and system module and sequence of execution.

**3. Implementation:**

In implementation phase of our project we have implemented various module required of successfully getting expected outcome at the different module levels. With inputs from system design, the system is first developed in small programs called units, which are integrated in the next phase. Each unit is developed and tested for its functionality which is referred to as Unit Testing.

**4. Testing:**

The different test cases are performed to test whether the project module are giving expected outcome in assumed time. All the units developed in the implementation phase are integrated into a system after testing of each unit.

**5. Deployment of System:**

Once the functional and non-functional testing is done, the product is deployed in the customer environment or released into the market.

**6. Maintenance:**

There are some issues which come up in the client environment. To fix those issues patches are released. Also to enhance the product some better versions are released. Maintenance is done to deliver these changes in the customer environment.

### 5.1 Application

In healthcare applications.

For providing security to patients sensitive data.

### 5.2 Advantages

- Practical approach to prevent the inside attack by securely distributing the patient data in multiple data servers.
- Employing the Paillier cryptosystems to perform statistical analysis on the patient data without compromising the patient’s privacy.
- In Proposed system, Due to secured distributed database architecture we can achieve data storage and data analysis security.
- Proposed data retrieval technique allow to retrieve the data compromised server(s).

## VI DATA MODEL AND DESCRIPTION

### 6.1 Data objects and Relationships

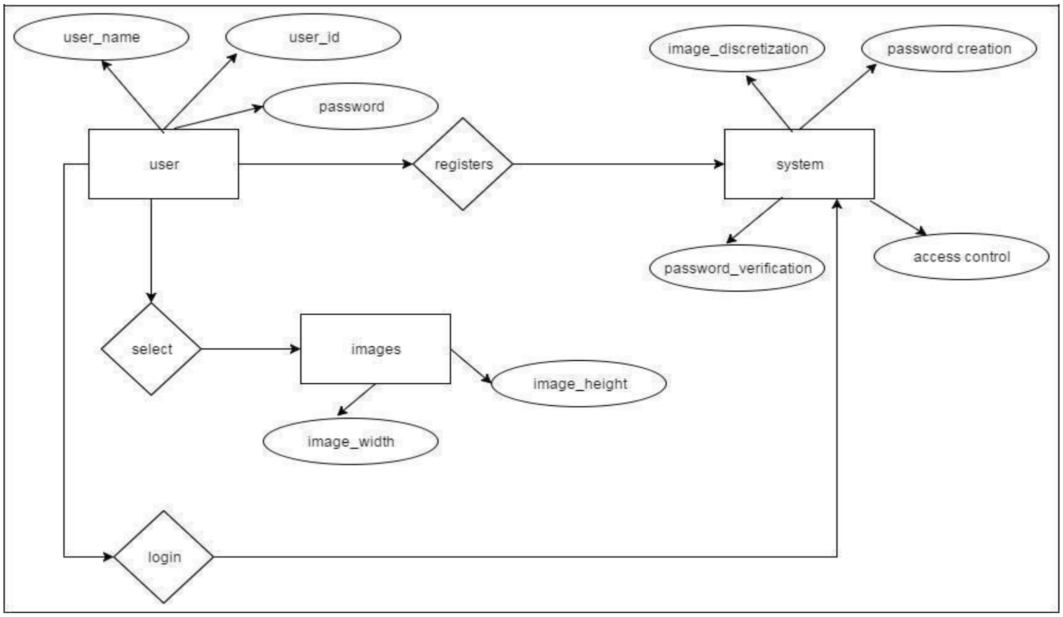

Fig 3: ER diagram

## VII. FUNCTIONAL MODEL AND DESCRIPTION

### 7.1 Data Flow Diagram

### 7.1.1 Level 0 Data Flow Diagram

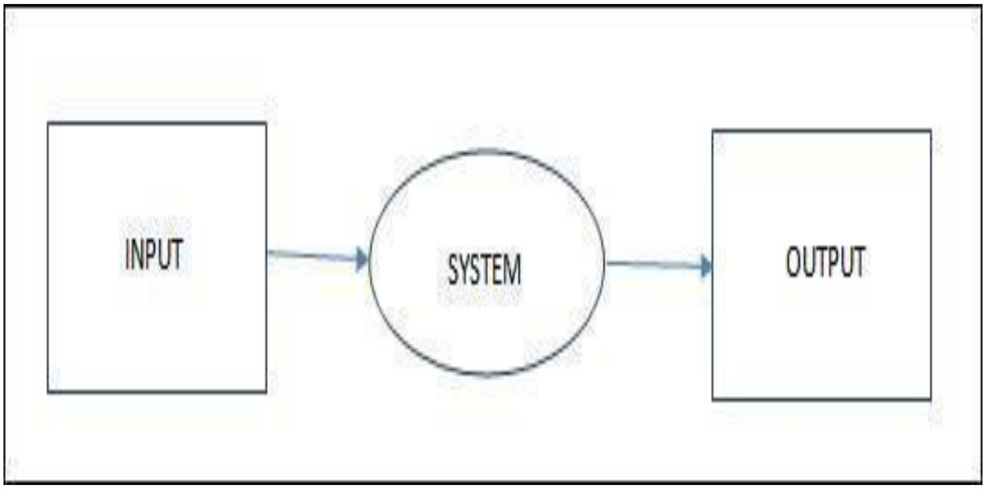

Fig. 7.1.1: DFD-0

### 7.1.2 Level 1 Data Flow Diagram

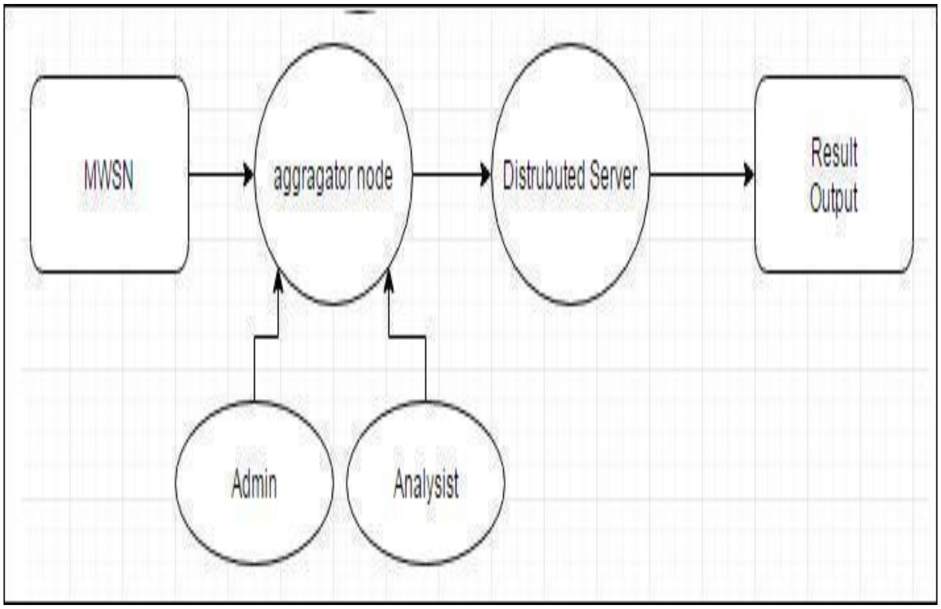

Fig.7.1.2DFD-1

### 7.1.3Level 2 Data Flow Diagram

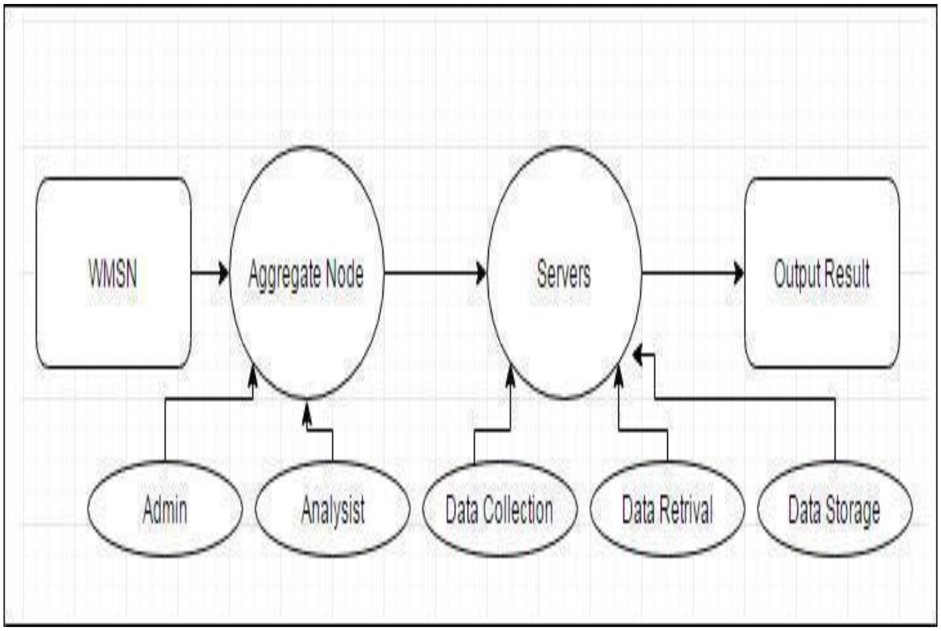

**Fig.7.1.3DFD-2**

## VIII CONCLUSION

We have investigated the security and privacy issues in the medical sensor data collection storage and queries and presented a complete solution for privacy-preserving medical sensor net-work through the ad-hoc network. To keep the privacy of the patient data, we proposed a new data collection protocol which splits the patient data into three numbers and stores them in three data servers, respectively. As long as one data server is not compromised, the privacy of the patient data can be preserved. For the legitimate user e.g. physician to access the patient data, we proposed an access control protocol, where three data servers cooperate to provide the user with the patient data, but do not know what it is. In case any two of three servers are compromised the proposed system provides a proxy based data retrieval system.

## REFERENCES

[1] Yi, Xun, et al. Privacy Protection for Wireless Medical Sensor Data. IEEE Transactions on Dependable and Secure Computing 13.3 (2016): 369-380

[2] X. Yi, J. Willemson, F. Nat-Abdesselam. Privacy-Preserving Wireless Medical Sensor Net-work. In Proc. TrustCom13, pages 118-125, 2013.

[3] D. He, S. Chan and S. Tang. A Novel and Lightweight System to Secure Wire-less Medical Sensor Networks. IEEE Journal of Biomedical and Health Infor-matics, 18 (1): 316-326, 2014.

[4] Y. M. Huang, M. Y. Hsieh, H. C. Hung, J. H. Park. Pervasive, Secure Access to a Hierarchi-cal Sensor-Based Healthcare Monitoring Architecture in Wireless Heterogeneous Networks. IEEE J. Select. Areas Commun. 27: 400-411, 2009.

[5] K. Malasri, L. Wang. Design and Implementation of Secure Wireless Mote-Based Medical Sensor Network. Sensors 9: 6273-6297, 2009.

[6] P. Belsis and G. Pantziou. A k-anonymity privacy-preserving approach in wire-less medical monitoring environments. Journal Personal and Ubiquitous Com-puting, 18(1): 61-74, 2014.

[7] T. ElGamal. A Public-Key Cryptosystem and a Signature Scheme Based on Dis-crete Loga-rithms. IEEE Transactions on Information Theory, 31 (4): 469-472, 1985.