International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Wireless Medical Sensor Data Patronage

M. Akshay Goud[1], K. S.S.V. Siddhartha[2], B. Saritha[3], G. Sravani[4], D. Priyanka[5]
[3]*Assistant Professor,* [1, 2, 4, 5] *B. Tech, Department of Computer Science and Engineering, St. Martin's Engineering College, Hyderabad, Telangana, India*

Abstract: ***Nowadays, Wireless Sensor Network is used on a large scale. Moreover, various applications of the Wireless sensor network are hospitals, home patient monitoring, area monitoring, environmental or earth sensing, industrial monitoring, Hardware and software monitoring. These networks are eavesdropping, middleman attacks, impersonation, replaying attacks compared to the wired networks. Previously many trials were done in order to protect the wireless sensor network. The existing system of wireless networks provides a solution to the data protection and it is limited during transmission notwithstanding the insider attacks. So, taking into consideration the previous policies, we propose a new policy to prevent these attacks by using data segregation, encryption with authentication mechanisms. The main motive of this paper is to safely distribute the patient to a remote location by deploying multiple servers in the form of the cryptosystem. Accordingly cryptosystem employed for this policy is the Paillier and Elgamal Cryptosystem. It is used to provide demographic analysis without compromising on the patient's data security.***

Keywords: Paillier and Elgamal Cryptosystem, Eavesdropping, Data integrity, Data Storage, Data Analyzation, Data Authorization, Impersonation, sharemind, Encryption, Decryption, Access, sensor, server, security.

I. INTRODUCTION

WSN is a wireless network that consists of base stations and numbers of nodes (wireless sensors).These networks are used to monitor physical or environmental conditions like sound, pressure, temperature and co-operatively pass data through the network to the main location. Moreover, initiation of wireless sensor networks is for the military purpose such as tracking and environment monitoring surveillance, enemy tracking, security detections are also performed by using these networks. Accordingly, extended their usage into various other fields such as the monitoring of traffic, dynamic routing management, monitoring of parking lots, rapid emergency response, industrial process monitoring, automated building climate control, ecosystem and habitat monitoring, civil structural health monitoring, etc. Nevertheless, health applications, such as Tracking and monitoring of patients and doctors use these networks. Ordinarily, networks are now the most propitious system for the healthcare applications. The health conditions of the patient can be monitored from anywhere and the data can be transferred to the remote location by these medical sensors. The sensors are deployed into the human body and the victim body conditions will transfer to the remote location in the form of the data with the help of the user interfaces and back-end systems.

The various types of wireless sensor networks are

1) Terrestrial WSN's
2) Underground WSNs
3) Under Water WSNs
4) Multimedia WSNs.
5) Mobile WSNs.

The WSN's used for health monitoring purpose is known as the mobile body networks. The mobile wireless sensor networks are much more versatile than the static sensor networks. They consist of a collection of sensor nodes that can be moved on their own and can be interacted with the physical environment. The mobile nodes have the ability to compute sense and communicate. The network topology plays an important role in MWSNs to transfer the data onto the mobile sensor nodes to the sink/base station. Then, the sink and the remote user/server are connected by the network. The effectiveness of large-scale mobile wireless sensor networks purely to depend on the data collection or topology management scheme. Therefore, the topology provides a guaranteed reliable network and better QoS in terms of mobility, traffic, end-to-end connection, etc. Lifeguard, AID-N, CareNet, ASNET, WiMoCa, SAPHIRE, THE-MUSS are some of the examples of the healthcare applications. Thus, healthcare systems are the most beneficial applications using wireless medical sensor technology that can perform patient care in homes, hospitals, clinics, disaster sites and the open environment.

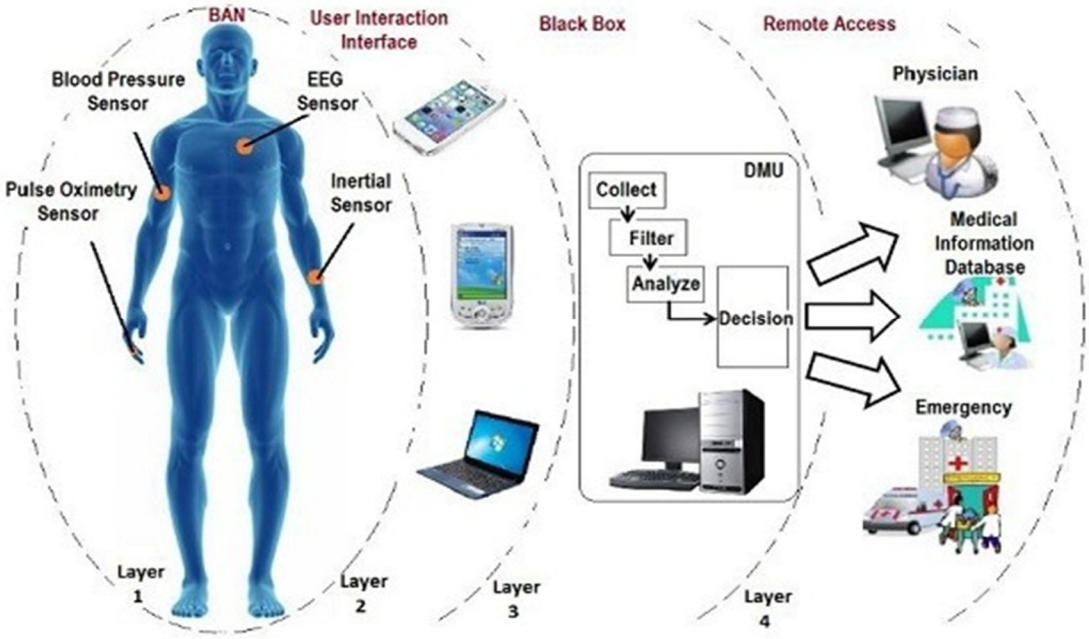

Fig: 1 Structure of Wireless Sensor Network

The data from the mobile sensors is stored in the backend for the long-term storage and detailed analysis of the patient data. The user interfaces are those which help to retrieve this data from the back end with the help of the query for any relevant user. Since the data is being transferred on the public channels and is stored on the back end they are vulnerable to the various attacks such as the clone attacks, eavesdropper attacks, and the man in the middle attacks. These attacks are the active attacks such as the network exploit in which a hacker attempts to make changes to data on the target or data en route to the target. The eavesdropping attack is a serious security threat to a wireless sensor network (WSN) since the eavesdropping attack is a prerequisite for other attacks. Conventional WSNs consist of wireless nodes equipped with Omni directional antennas, which broadcast radio signals in all directions and are consequently prone to the eavesdropping attacks. Passive Eavesdropping, in which the malicious nodes detect the information by listening to the message transmission in the broadcasting wireless medium; (ii) Active Eavesdropping, where the malicious nodes actively grab the information via sending queries to transmitters by disguising themselves as friendly nodes. These active eavesdropping attacks may result in the impersonation of the patient data which could be the serious threat to the patient privacy. There are even probabilities that the attacker might employ a rely on point when the data is being transmitted and this may result in the false alarms and the rescue team may start to protect the person who never existed. This may lead to the serious threat and completely destroy the wireless sensor network usage. The other two factors that are being exploited is the data integrity of the patient data. When the attacker modifies the data and when the altered data is given to the physician. The physician may give wrong treatment to the patient and this may be the serious threat to the life of the patient. Data breach is a confirmed incident in which sensitive, confidential or otherwise protected data accessed and/or disclosed in an unauthorized fashion. The attacker can use the malicious patient data for the personal benefit or the medical fraud. Conversely, to prevent these attacks various researchers have done many researchers. The k-anonymity is the technique used to differentiate one patient data from the other k-1 patient's data in the medical database. The Kumar and Lee conducted a survey on the paper that released in the year 2012 based on the literature. Conversely, the previous methods protected the transmission but not the data that is being transmitted. So the existing solutions can prevent the inside attacks but not the outside attacks. In this paper, we propose the policy in such a way the insider attacks as well. The design of the policy on the basis of the data integrity, the authentication and access.

II. LITERATURE SURVEY

Wireless Sensor Networks (WSN) is an emerging technology that has the potential to transform the way of human life. The Health applications are considered promising fields for Wireless Medical Sensor Network, where patient's health can be monitored using Medical Sensors. Wireless Medical Sensor Networks (WMSNs) are the key enabling technology in healthcare applications that allows the data of a patient's vital body parameters to be collected by wearable biosensors. Current WMSN healthcare research

trends focus on patient reliable communication, patient mobility and energy-efficient routing. Security and Privacy protection of the collected data is a major unsolved issue. We propose a practical approach to prevent the inside attack by using multiple data servers to store patient data. The main influence of this paper is securely distributing the patient data in multiple data servers and employing the Paillier and ElGamal cryptosystems to perform statistic analysis on the patient data without compromising the patient's confidentiality.

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. The designed solution Share mind 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. The protocols of SHAREMIND are information-theoretically secure in the honest-but-curious model with three computing participants. Although the honest-but-curious model does not tolerate malicious participants, it still provides significantly increased privacy preservation when compared to standard centralized databases.

Accordingly, we present a framework for a wireless health monitoring system using wireless networks such as ZigBee. Consequently, 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. It 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 on this server. The processed data, as well as the analysis results, are then transmitted to the service provider centre for diagnostic reviews as well as storage. The main advantage of the proposed framework are: (1) the ability to detect signals wirelessly within a Body Sensor Network (BSN), (2) low-power and reliable data transmission through ZigBee network nodes, (3) secure transmission of medical data over BSN, (4) efficient channel allocation for medical data transmission over wireless networks, and (5) optimized analysis of data using an adaptive architecture that maximizes the utility of processing and computational capacity at each platform.

A. Existing System

The use of the wireless sensor networks to improve the quality of care patient's treatment. Since the data is being transmitted through the network channels and these are vulnerable to the security attacks. The attacks such as the Eavesdropping, the middleman attacks. Moreover, eavesdropping attack is a serious security threat to a wireless sensor network (WSN) since the eavesdropping attack is a prerequisite for other attacks. Conventional WSNs consist of wireless nodes equipped with omnidirectional antennas, which broadcast radio signals in all directions and are consequently prone to the eavesdropping attacks. Passive Eavesdropping, in which the malicious nodes detect the information by listening to the message transmission in the broadcasting wireless medium; (ii) Active Eavesdropping, where the malicious nodes actively grab the information via sending queries to transmitters by disguising themselves as friendly nodes. Accordingly, active eavesdropping attacks may result in an impersonation of the patient data which could be the serious threat to the patient privacy. There are even probabilities that the attacker might employ a rely on point when the data is being transmitted and this may result in the false alarms and the rescue team may start to protect the not- existed person. Conversely may lead to the serious threat and completely destroy the wireless sensor network usage. The other two factors that are being exploited is the data integrity of the patient data. When the attacker modifies the data and when the physician takes the altered data. The physician may give wrong treatment to the patient and this may be the serious threat to the life of the patient. Data breach is a confirmed incident in which sensitive, confidential or otherwise protected data accessed and/or disclosed in an unauthorized fashion. The attacker can use the malicious patient data for the personal benefit or the medical fraud.

B. Disadvantages

1) Less secure because hackers can enter the access point and obtain all the information.
2) There are solutions which can prevent the outside attacks but not the inside data transmitted from the sensors to the remote location. The data that is being transmitted is vulnerable to the eavesdropping and the other attacks.

C. Proposed system

Let us consider the wireless networks consist of the medical sensors, the servers, and the end users. When the sensor stimulation starts and the data from the various sensors are being transferred to the servers and the queries would process to provide the

statistical analysis of the patient data. The data that is being transferred to three servers is a prediction of Yi et al in the concept of share mind. Accordingly, we suggest a new cryptosystem in order to improve the security of the system. The Paillier and Elgamal Cryptosystem used to prevent the insider attacks. The data after stimulation mobilized to the three servers and when the data is being transferred in the encryption form and stored on these servers. When the user at the other end authenticates and the when all the three servers compromise then only the data in decryption form and the access provided to the user. Even if two servers get compromised and one negotiates even then the data is safe and the integrity of patient is secure. The AES 256 bit encryption algorithm used in order to encrypt the data. With these policies, the data the integrity of patient is secure.

D. Advantages

1) The data integrity of the patient is safe
2) The protection of the data from insider attacks during the transmission
3) The patient would be secure further safe from any attacks
4) The vulnerability of this network overcame to some extent.

III. OVERVIEW

A. Modules Description

1) Data integrity: In this network, each and every sensor can transfer the data without any security violations with the help of the distributed database.
2) Data Storage: In this environment of the distributed database, even if two servers comprise, even then the third one remains. In this way, the data can't retrieve.
3) Data authorization: The authorized person will be given access to patient data. The disclosures of patient data cannot be done to any server while the accessing of the data.
4) Data analysation: The patient data when an authorized person accesses it is in the form of Statistical analysis. The data during the analysis is not disclosed to any server and even the user.

B. System architecture:

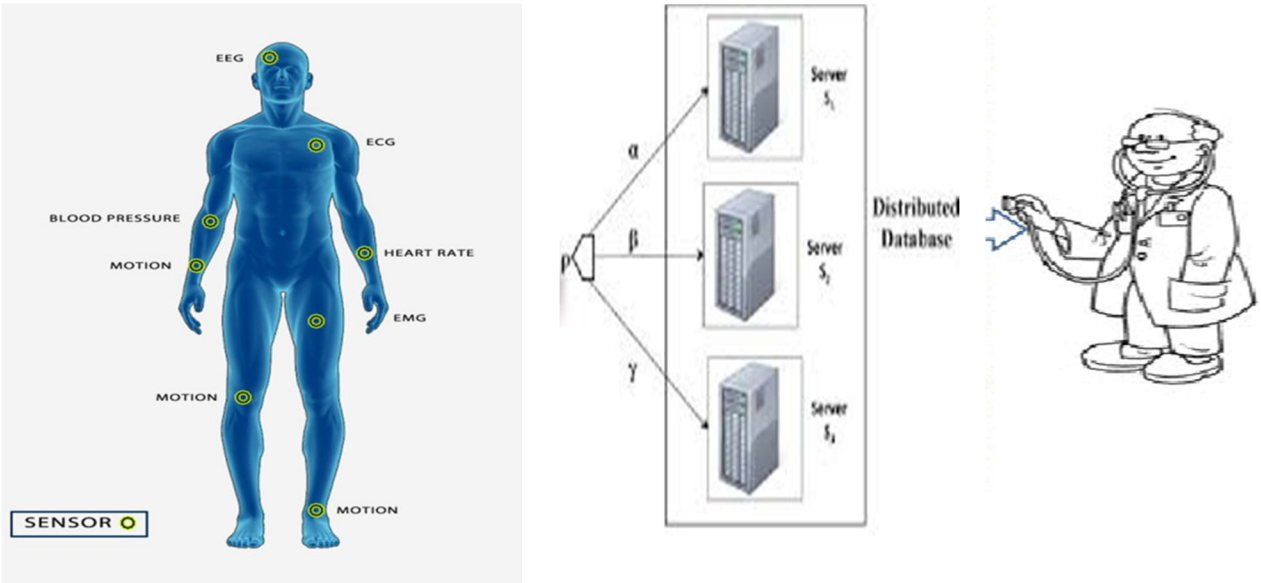

Fig: 2 System Architecture

IV. METHODOLOGY

The proposed framework consist of two algorithms

A. ElGamal Cryptosystem

In the cryptographic analysis, the ElGamal encryption is an asymmetric key encryption algorithm based on the public-key cryptography that is based on the Diffie–Hellman key exchange. Conversely, system provides an additional layer of security by asymmetrically encrypting keys which are previously used for the symmetric message encryption. Taher Elgamal described it in

1985. This encryption algorithm is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems. The Digital Signature Algorithm (DSA) is variant of ElGamal signature scheme

1) Key aspects

a) This is based on the Discrete Logarithm problem

b) It is used to implement Randomized encryption

2) Application

a) It can establish a secure channel for key sharing

b) It is used for Encrypting messages

3) Key Generation: The key generator works as follows

a) It generates an efficient description of a cyclic group G of order q with generator g. See below for a discussion on the required properties of this group.

b) It chooses an x randomly from {1… q-1}.

c) It computes h: $=g^x$.

d) It publishes h, along with the description of G, q, g, as her **public key**. It retains x as the private key, which must be kept secret.

4) Encryption Procedure: Participant B encrypts a message m to A

a) Obtain A's authentic public key (p, g, g^a).

b) Represent the message as integer's m in the range

c) Select a random integer k, $1 \leq k \leq p-2$.

d) Compute ¥ = g^k mod p and §= m * $(g^a)^k$.

e) Send cipher text c = (¥,§) to A

5) Decryption Procedure: Participant A receives encrypted message m from B

a) Use private key a to compute ($p1^a$) mod p. Note: $p1^a=a=a^{ak}$

b) Recover m by computing (m^a) mod p.

6) Features

a) Use of a random factor k for encryption

b) Variant of DH: shared secret is g^{ak}

B. AES Algorithm

The Advanced Encryption Standard is based on the concept of the symmetric block cipher. Accordingly, in order to provide protection to classified information and is implemented in software as well as hardware to encrypt sensitive data. Moreover, algorithm comprises of the three block ciphers: AES-128, AES-192 and AES-256. As the cipher encrypts and decrypts data in the blocks of 128 bits using cryptographic keys of 128, 192 and 256-bits, respectively. Certainly, AES encryption algorithm defines a varied number of transformations that are to be performed on data stored in an array. Nevertheless, the first step of the cipher is to insert the data into an array and the cipher transformations are repeated over in the form of encryption rounds. The number of rounds is determined by the help of key length, 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys respectively.

1) Steps

a) Rijndael's key is used to derive the round keys from the cipher key. It requires a 128-bit round key block for each round and adds one more.

b) The bitwise xor is used for a block of the round key as it is combined with each byte of the state.

c) According to a table where each byte is replaced with another substitution step in a non-linear manner.

d) A certain number of steps in a cyclic manner are shifted to the last three rows of the state by performing the transposition.

e) Combining the four bytes in each column. an operation is employed where it operates on the columns of the state by mixing it.

f) Finally, Add the Round-Key.

g) The final round consists of the same rounds that are mentioned above except the Mix-columns.

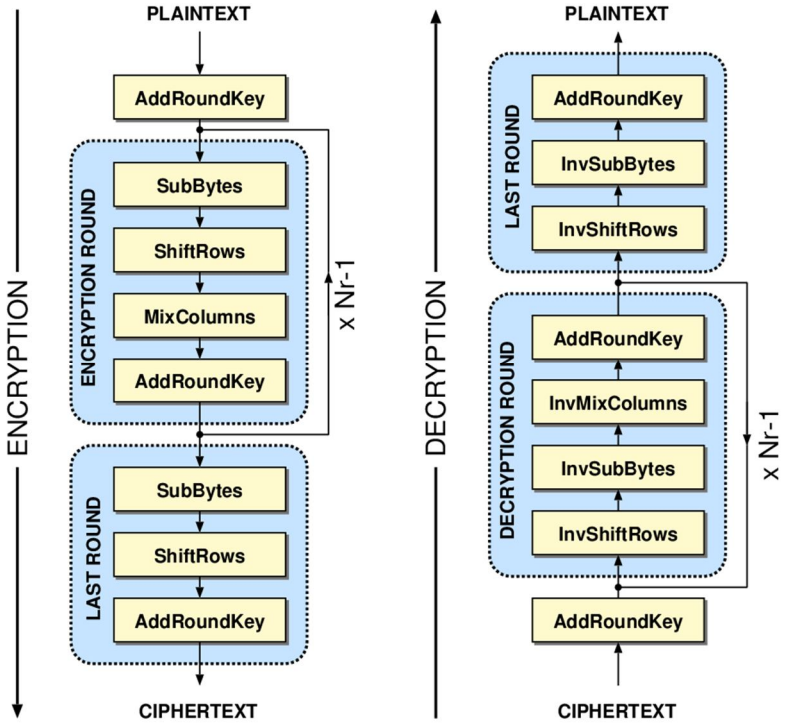

Fig: 3 Execution of AES Algorithm

V. RESULTS

Accordingly, define the user access to relevant users in the three servers. The stimulation of the patient starts and data transmission is initiated from sensors, it is stored in the servers with the help of distributed database. The authorized user gains access to the data with the help of his credentials. The data is retrieved in the form of the statistical analysis. The data during the analysis is not disclosed to any server and even the user. The data is in encrypted format during the transmission and it is decrypted when the user access it at the other end.

VI. CONCLUSION

After the clear analysis of the security and the privacy issues involved in the medical sensor data in various stages such as the collection, storage and the queries that are involved in the retrieval of the data in the form of the statistical analysis. The communication between the data servers and the medical sensors has been secured as we employed the AES 256bit for encryption and the Elgamal Cryptosystem for decryption. The data integrity of the patient data is preserved as the data is distributed among three servers and even if two servers are compromised still we are secure because the data can be accessed only if all the three servers are compromised. Each and every sensor can transfer the data without any security violations with the help of the distributed database. The patient data access can be provided only to the authorized person. The patient data
cannot be disclosed to any server while the accessing of the data. By this we are preserving the data authorization. The patient data which is provided to authorized person is in the form of Statistical analysis. The data during the analysis will not be disclosed to any server and even the user. The data analysation is performed. The protocols are secure against the inside and the outside attacks. The data is secure until all the three servers are not compromised.

BIBLIOGRAPHY

[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, programmable service architecture for mobile medical care,” in Proc.
a. 4th Annu. IEEE Int. Conf. Pervasive Comput. Commun. Workshop, Pisa, Italy, Mar. 13–17, 2006, pp. 532–536
[4] Crypto++ 5.6.0 Benchmarks [Online]. Available:
i. http://www.cryptopp.com/benchmarks.html, 2009.

[5] J. Daemen, G. Bertoni, M. Peeters, and G. V. Assche. (2012, Jul. 6).Permutation-based encryption, authentication and authenticated encryption. Proc. Directions Authenticated
[6] 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.
[7] W. Diffie and M. Hellman, "New directions in cryptography,"IEEE Trans. Inf. Theory, vol.
i. IT-22, no. 6, pp. 644–654, Nov. 1976.
[8] (2013, Jul.). Digital signature standard (DSS). FIPS PUB 186-4[Online]. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
[9] T. ElGamal, "A public-key cryptosystem and a signature schemebased on discrete logarithms," IEEE Trans. Inf. Theory, vol. IT-31,no. 4, pp. 469–472, Jul. 1985.
[10] D. He, S. Chan, and S. Tang, "A novel and lightweight system tosecure wireless medical sensor networks," IEEE J. Biomed. Health In format., vol. 18, no. 1, pp. 316–326, Jan. 2014
[11] Xun Yi, Athman Bouguettaya, Fellow, IEEE, Dimitrios Georgakopoulos, Andy Song, and Jan Willemson Dependable And Secure Computing, Vol. 13, No. 3, May/June 2016