Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 5, May-2018

Private and Secured Medical Data Transmission and Analysis for Wireless Healthcare System

Iram Nakade[1], Nikhil Gaikwad[2], Farazuddin Shaikh[3], Aniket Bhatkar[4], Prof. N.D.Sonawane[5]

PDEA's *College of Engineering, Manjari* (Bk.), Hadapsar, Pune, Maharashtra- 412307

Department of Computer, PDEA's College of Engineering

eramn22@gmail.com

nikhilgaikwad6007@gmail.com

farazshaikh261996@gmail.com

aniketbhatkar12@gmail.com

2nayna@gmail.com

Abstract — Healthcare applications square measure thought-about as promising fields for wireless sensing element networks, wherever patients will be monitored mistreatment wireless medical sensing element networks (WMSNs). Current WMSN attention analysis trends specialize in patient reliable communication, patient quality, and energy-efficient routing, as a number of examples. However, deploying new technologies in attention applications while not considering security makes patient privacy vulnerable. Moreover, the physiological information of a private square measure sensitive. Therefore, security could be a predominate demand of attention applications, particularly within the case of patient privacy, if the patient has AN embarrassing illness. This project discusses the protection and privacy problems in attention application mistreatment WMSNs. we tend to highlight some common attention comes mistreatment wireless medical sensing element networks, and discuss their security the present systems solutions will merely shield the patient information throughout transmission, however cannot shield the within attack wherever the administrator of the patient info reveals the sensitive patient information. thus we tend to square measure proposing a approach to forestall the within attack by mistreatment multiple information servers to store patient information. the most contribution of this paper is to distribute patient's information firmly in multiple information servers and performing arts the Paillier cryptosystems to perform applied mathematics analysis on the patient information while not compromising the patient's privacy.

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

I. INTRODUCTION

A wireless device network could be a network to observe physical or environmental conditions like temperature, sound, pressure, etc. the event of wireless device networks was intended by pollution observance, water quality observance, land facet detection, fire detection, and home ground observance then on. Although there square measure several applications in wireless device network domain, human tending applications takes the main role. In human tending, sensors square measure accustomed monitor the patients' health standing like temperature level, sugar level, heart beat rate, vital sign. For example, if the patient's sugar level is monitored ten times per day then the information is updated within the info that is gift within the native server. Likewise the values for vital sign, heartbeat, and temperature are noted at regular intervals. There square measure several security problems like knowledge stealing, stealing and change, storing the incorrect values. Suppose if the unwelcome person is making an attempt to hack the patient details, there square measure several probabilities for the misuse of information which can result in severe consequences. The information may also be changed by the hackers because of lack of security. The treatment prescribed by the doctors are often hacked which can even result in death of the patients. Patients square measure the victims thanks to the higher than problems. to forestall these problems, the intrusion detection system is projected. Associate degree intrusion detection system could be a system accustomed check the malicious activities and produces electronic reports to a management station. It consists of Paillier algorithmic rule key cryptosystems. The algorithmic rule is employed to cipher the patient details before storing it within the info and perform decoding once required by the medico.

II. LITERATURE REVIEW

1. Sharemind: a framework for fast privacy-preserving Computations (2008).
Authors: Dan Bogdanov, Sven Laur1, and Jan Willemson
Description:

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. 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.

2. Real-Time and Secure Wireless Health Monitoring
Authors: S. Dagtas, G. Pekhteryev, Z. S¸ahinoglu, H. Cam, and N. Challa
Description:

We present a framework for a wireless health monitoring system using wireless 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. The processed data as well as the analysis results are then transmitted to the service provider center for diagnostic reviews as well as storage. The main advantages 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 Zig Beenet work 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.

3. A Novel and Lightweight System to SecureWireless Medical Sensor Networks
Authors: Daojing He, Sammy Chanand Shaohua Tang.
Description:
Wireless medical sensor networks (MSNs) are a key enabling technology in e-healthcare that allows the data of patient's 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. The system employs hash-chain based key updating mechanism and proxy-protected signature technique to achieve efficient secure transmission and fine-grained data access control. Furthermore, we extend the system to provide backward secrecy and privacy preservation. Our system only requires symmetric-key encryption/decryption and hash operations and is thus suitable for the low-power sensor nodes. This paper also reports the experimental results of the proposed system in a network of resource-limited motes and laptop PCs, which show its efficiency in practice. To the best of our knowledge, this is the first secure data transmission and access control system for MSNs until now.

4. Pervasive, Secure Access to a Hierarchical Sensor-based Healthcare Monitoring Architecture in Wireless Heterogeneous Networks
Authors: Y.M. Huang, M.Y. Hsieh, H.C. Chao, S.H. Hung, and J.H. Park.
Description:
This study presents a healthcare monitoring architecture coupled with wearable sensor systems and an environmental sensor network for monitoring elderly or chronic patients in their residence. The wearable sensor system, built into a fabric belt, consists of various medical sensors that collect a timely set of physiological health indicators transmitted via low energy wireless communication to mobile computing devices. Three application scenarios are implemented using the proposed network architecture. The group-based data collection and data transmission using the ad hoc mode promote outpatient health care services for only one medical staff member assigned to a set of patients. Adaptive security issues for data transmission are performed based on different wireless capabilities. This study also presents a monitoring application prototype for capturing sensor data from wireless sensor nodes. The implemented schemes were verified as performing efficiently and rapidly in the proposed network architecture.

5. Design and Implementation of a Secure Wireless Mote-Based Medical Sensor Network

Authors: KriangsiriMalasri and LanWang.

Description:

A *medical sensor network* can wirelessly monitor vital signs of humans, making it useful for long-term health care without sacrificing patient comfort and mobility. For such a network to be viable, its design must protect data privacy and authenticity given that medical data are highly sensitive. We identify the unique security challenges of such a sensor network and propose a set of resource-efficient mechanisms to address these challenges. Our solution includes (1) a novel two-tier scheme for verifying the authenticity of patient data,(2) a secure key agreement protocol to set up shared keys between sensor nodes and base stations, and (3) symmetric encryption/decryption for protecting data confidentiality and integrity. We have implemented the proposed mechanisms on a wireless mote platform, and our results confirm their feasibility.

III. SURVEY OF PROPOSED SYSTEM

WSNs deployed at an oversized scale in a very distributed manner, and their knowledge rates differs supported their applications, wherever the Wireless Medical detector Networks have direct human involvement square measure deployed on a tiny low scale should support quality (a patient will carry the devices), and WMSNs needs high knowledge rates with reliable communication. Physiological conditions of patients square measure closely monitored by deploying Wireless medical detector motes. These medical sensors square measure accustomed sense the patient's very important body parameters and transmit the perceived knowledge in a very timely fashion to some remote location while not human involvement. Mistreatment these medical detector readings the doctor will get the main points of a patient's health standing. The patient's very important body parameters embody heart beats, temperature, pressure level, sugar level, pulse rate. WMSNs carry the standard of care across wide range of aid applications. Additionally, different applications that conjointly have the benefit of WMSNs embody sports-person health standing observation and patient's self-care. Many analysis teams and comes have begun to develop health observation mistreatment wireless detector networks. Wireless Medical aid application offers variety of challenges, like, reliable transmission of information, secured knowledge transmission, nodes quality, detection of event delivery of information in time, power management, etc. Deploying new technologies in aid applications while not considering security usually makes patient privacy vulnerable. as an example, the patient's physiological very important signals square measure terribly sensitive therefore the run of the patient's pathologic knowledge may makes the patient embarrassed. Typically revealing malady data will build it not possible for them to get insurance protection and conjointly lead to an individual losing their job. to stop the patient knowledge from the within attacks, we tend to propose a brand new knowledge assortment protocol, wherever a detector splits the sensitive patient knowledge into 3 parts in keeping with a random variety generator supported hash operate and sends them to 3 servers, respective, via secure channels. To stay the privacy of the patient knowledge in knowledge access, we tend to propose a brand new knowledge access protocol on the premise of the Paillier cryptosystem. The protocol permits the user (e.g. physician) to access the patient knowledge while not revealing it to any knowledge server. To preserve the privacy of the patient knowledge in applied mathematics analysis, we tend to propose some new privacy-preserving applied mathematics analysis protocol on the premise of the Paillier cryptosystems. These protocols permit the user (e.g., medical researcher) to perform applied mathematics analysis on the patient knowledge while not compromising the patient knowledge privacy.

IV. Mathematical Model

Let W be the whole system which consists:

W= {IP, PRO, OP}

Where,

IP is the input of the system.

A) IP= {P, SD, SN, PD, U}

- P is the number of patients in the system.

- SN is the set of number of sensing nodes in the system.
- SD is the sensing data sensed from the medical SD.
- PD is the patient's database system which consists of number of databases.
- U is the set of number of user in the systems that are accessing the data from patient's database server.

B) PRO is the procedure of our proposed system:

Step 1: At first the wireless medical network which senses the patient's body and transmits the patient data to a patient database system.

Step 2: A patient database system which stores the patient data from medical and provides querying services to users (e.g., physicians and medical professionals).

Step 3: A patient data access control system which is used by the user (e.g., physician) to access the patient data and monitor the patient.

Step 4: A patient data analysis system which is used by the user (e.g., medical researcher) to query the patient database system and analyze the patient data statistically.

OP is the output of the system:

The system provides the privacy to the patient's sensible data available on the patient's database system in the sense of inside attacks.

V. SYSTEM ARCHITECTURE

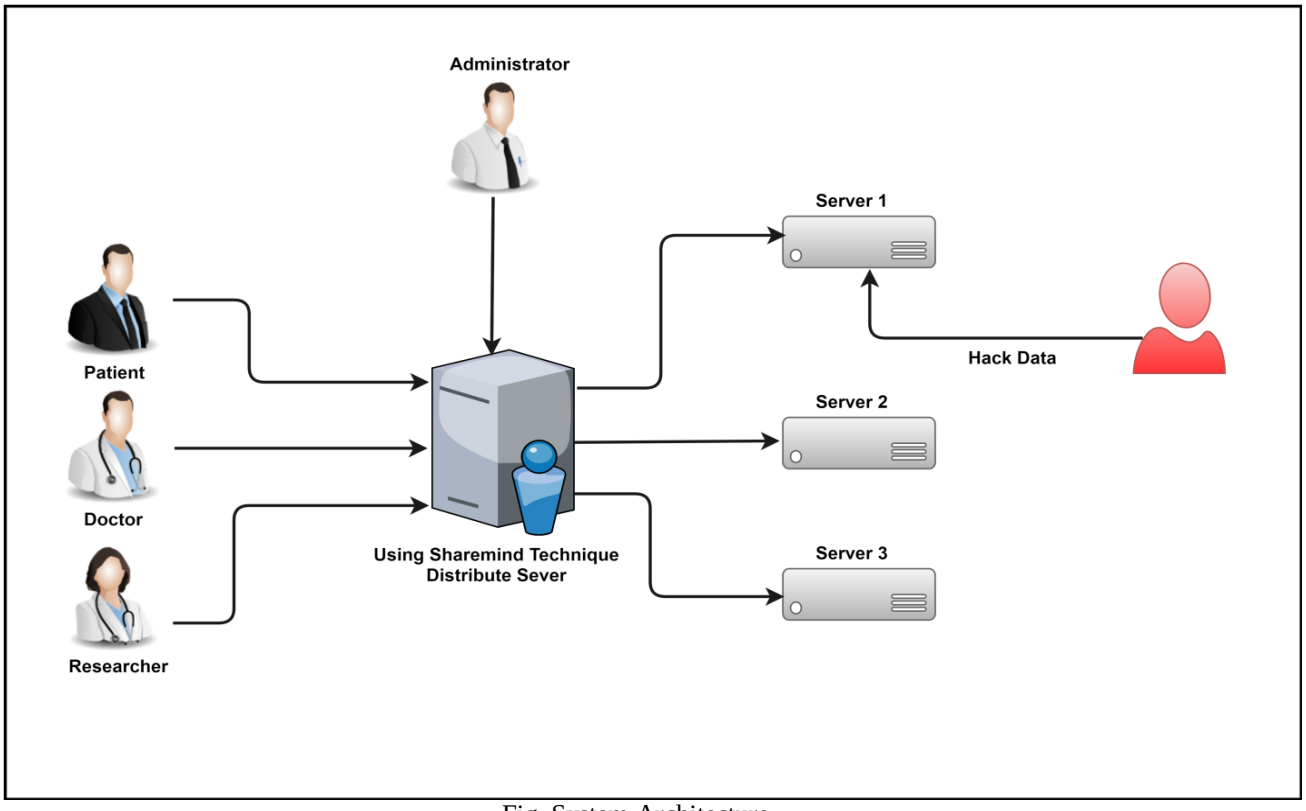

Fig. System Architecture

VI.ALGORITHM

A) Paillier Public-Key Cryptosystem:

It is composed of key generation, encryption and decryption algorithms as follows.

1) Key generation

The key generation algorithm works as follows.

- Choose two large prime numbers p and q randomly and independently of each other such that

$$\gcd\big(pq,(p-1)(q-1)\big)=1$$

- Compute

$$N=pq,\lambda=lcm(p-1,q-1)$$

Where lcm stands for the least common multiple.

- Select random integer g where g $\in\mathbb{Z}^*_{N^2}$ and ensure N divides the order of g by checking the existence of the following modular multiplicative inverse:

$$\mu=\left(L\left(g^{\lambda}(mod N^2)\right)\right)^{-1}(mod\ N)$$

where function L is defined as

$$L(u)=\frac{u-1}{N}$$

Note that the notation a/b does not denote the modular multiplication of a times the modular multiplicative inverse of b but rather the quotient of a divided by b.

The public (encryption) key pk is (N,g).
The private (decryption) key sk is (λ,μ).

If using p,q of equivalent length, one can simply choose

$$g=N+1,\lambda=\varphi(N)^{-1}(mod\ N)$$

where N = pq and $\varphi(N)=(P-1)(q-1)$

2) Encryption:

The encryption algorithm works as follows.

- Let m be a message to encrypt, where m $\in\mathbb{Z}_N$
- Select random r where r $\in\mathbb{Z}^*_N$
- Compute ciphertext as:

$$C=g^m.r^N(mod\ N^2)$$

3) Decryption:

The decryption algorithm works as follows.

- Let c be the ciphertext to decrypt, where the ciphertext c$\in\mathbb{Z}^*_{N^2}$.
- Compute the plaintext message as:

$$m = \left(c^{\lambda}(mod\ N^2)\right).\mu(mod\ N)$$

4) Homomorphic Properties

A notable feature of the Paillier cryptosystem is its homomorphic properties. Given two ciphertexts
$E(m_1, pk) = g^{m1} r_1^N (mod\ N^2)$
$E(m_2, pk) = g^{m2} r_2^N (mod\ N^2)$
where r1,r2 are randomly chosen for$\mathbb{Z}_N^*$,we have
the following homomorphic properties.

$$D\left(E(m_1, pk_1).E(m_2, pk_2)\right) = m_1 + m_2 (mod\ N)$$

The product of a ciphertext with a plaintext raising g will decrypt to the sum of the corresponding plaintexts,

$$D(E(m_1, pk_1).g^{m2}) = m_1 + m_2 (mod\ N)$$

An encrypted plaintext raised to a constant k will decrypt to the product of the plaintext and the constant,

$$D(E(m_1, pk_1)^k) = km_1 (mod\ N)$$

However, given the Paillier encryptions of two messages, there is no known way to compute an encryption of the product of these messages without knowing the private key.

VII.CONCLUSION

We have investigated the protection and privacy problems within the medical device knowledge assortment storage and queries and given an entire answer for privacy-preserving medical device net-work through the ad-hoc network. to stay the privacy of the patient knowledge, we have a tendency to planned a replacement knowledge assortment protocol that splits the patient knowledge into 3 numbers and stores them in 3 knowledge servers, severally. As long in concert knowledge server isn't compromised, the privacy of the patient knowledge will be preserved. For the legitimate user e.g. Dr. to access the patient knowledge, we have a tendency to planned AN access management protocol, wherever 3 knowledge servers work to supply the user with the patient knowledge, however don't recognize what it's. Just in case any 2 of 3 server's area unit compromised the planned system provides a proxy primarily based knowledge retrieval system.

VIII.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 Network. In Proc. TrustCom13, pages 118-125, 2013.

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

[4] Y. M. Huang, M. Y. Hsieh, H. C. Hung, J. H. Park. Pervasive, Secure Access to a Hierarchical 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 wireless medical monitoring environments. Journal Personal and Ubiquitous Computing, 18(1): 61-74, 2014.

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

[8] P. Paillier. Public-key Cryptosystems Based on Composite Degree Residuosity Classes. In Proc. EUROCRYPT99, pages 223-238, 1999.