Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

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

Volume 4, Issue 10, October-2017

Secure Healthcare System Using Pailliar Cryptography

[1]*Prof. Raviraj Kasture,* [2]*Ashwini Jagtap,* [3]*Rakshanda Palekar,* [4]*Manasi Dhoble*

[1] *Department of Computer Engineering, ICEM, Pune*

[2] *Department of Computer Engineering, ICEM, Pune*

[3] *Department of Computer Engineering, ICEM, Pune*

[4] *Department of Computer Engineering, ICEM, Pune*

Abstract--- Healthcare applications square measure thought of as promising fields for wireless networks, wherever patients may be monitored exploitation wireless medical networks (WMNs). Current WMN tending analysis trends specialize in patient reliable communication, patient quality, and energy-efficient routing, as a number of examples. However, deploying new technologies in tending applications while not considering security makes patient privacy vulnerable. Moreover, the physiological knowledge of a private square measure sensitive. Therefore, security may be a overriding demand of tending applications, particularly within the case of patient privacy, if the patient has an embarrassing illness. This project discusses the protection and privacy problems in tending application exploitation WMNs. we have a tendency to highlight some in style tending comes exploitation wireless medical networks, and discuss their security the prevailing systems solutions will merely defend the patient knowledge throughout transmission, however cannot defend the within attack wherever the administrator of the patient information reveals the sensitive patient knowledge thus we have a tendency to square measure proposing an approach to stop the within attack by exploitation multiple knowledge servers to store patient knowledge. The most contribution of this paper is to distribute patient's knowledge firmly in multiple knowledge servers and acting the Paillier cryptosystems to perform applied math analysis on the patient knowledge while not compromising the patient's privacy.

Keywords --- Paillier cryptosystems, Wireless Medical Network, Patient Data Privacy.

I. INTRODUCTION

A wireless network could be a network to observe physical or environmental conditions like temperature, sound, pressure, etc. the event of wireless networks was motivated by pollution watching, water quality watching, land aspect detection, fire detection, home ground watching and then on. There square measure several applications in wireless network domain, human care applications take the key role. In human care, square measure won't to monitor the patients' health standing like temperature level, sugar level, heart beat rate, pressure level. For example, if the patient's sugar level is monitored ten times per day then the info is updated within the info that is gift within the native server. Likewise the values for pressure level, heartbeat, and temperature also are noted at regular intervals.

There square measure several security problems like information stealing, stealing and change, storing the incorrect values. Suppose if the persona non grata is making an attempt to hack the patient details, there square measure several probabilities for the misuse of knowledge which can cause severe consequences. The info may also be changed by the hacker's thanks to lack of security. The treatment prescribed by the doctors is hacked which can even cause death of the patients. Patients square measure the victims thanks to the higher than problems. To stop these problems, the intrusion detection system is planned. An intrusion detection system could be a system wont to check the malicious activities and produces electronic reports to a management station. It consists of Paillier algorithmic program key cryptosystems. The algorithmic program is employed to write in code the patient details before storing it within the info and perform secret writing once required by the documents.

II. EXISTING SYSTEM

The 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 WMNs. We highlight some popular healthcare projects using wireless medical 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.

2.1 Disadvantages of Existing System

1. Less secure.
2. Cannot protect inside attacker.
3. If any hacker get data from one DB server then whole data will be get to hacker.

III. PROPOSED SYSTEM

WSNs deployed at a large scale in a distributed manner, and their data rates differs based on their applications, where the Wireless Medical Networks have direct human involvement are deployed on a small scale must support mobility (a patient can carry the devices), and WMSNs requires high data rates with reliable communication. Physiological conditions of patients are closely monitored by deploying Wireless medical motes. These medical are used to sense the patient's vital body parameters and transmit the sensed data in a timely fashion to some remote location without human involvement. Using these medical readings the doctor can get the details of a patient's health status. The patient's vital body parameters include heart beats, body temperature, blood pressure, sugar level, pulse rate. WMSNs carry the quality of care across wide variety of healthcare applications. In addition, other applications that also benefit from WMNs include sports-person health status monitoring and patients self-care. Several research groups and projects have started to develop health monitoring using wireless networks. Wireless Medical healthcare application offers a number of challenges, like, reliable transmission of data, secured data transmission, nodes mobility, detection of event delivery of data in time, power management, etc. Deploying new technologies in healthcare applications without considering security often makes patient privacy vulnerable. For instance, the patient's physiological vital signals are very sensitive so the leakage of the patient's diseased data could makes the patient embarrassed. Sometimes revealing disease information can make it impossible for them to obtain insurance protection and also result in a person losing their job.

To prevent the patient data from the inside attacks, we propose a new data collection protocol, where system 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.

To keep the privacy of the patient data in data access, we propose a new data access protocol on the basis of the Paillier cryptosystem. The protocol allows the user (e.g. physician) to access the patient data without revealing it to any data server.

To preserve the privacy of the patient data in statistical analysis, we propose some new privacy-preserving statistical analysis protocol on the basis of the Paillier cryptosystems. These protocols allow the user (e.g., medical researcher) to perform statistical analysis on the patient data without compromising the patient data privacy.

IV. 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.

V. SYSTEM ARCHITECTURE

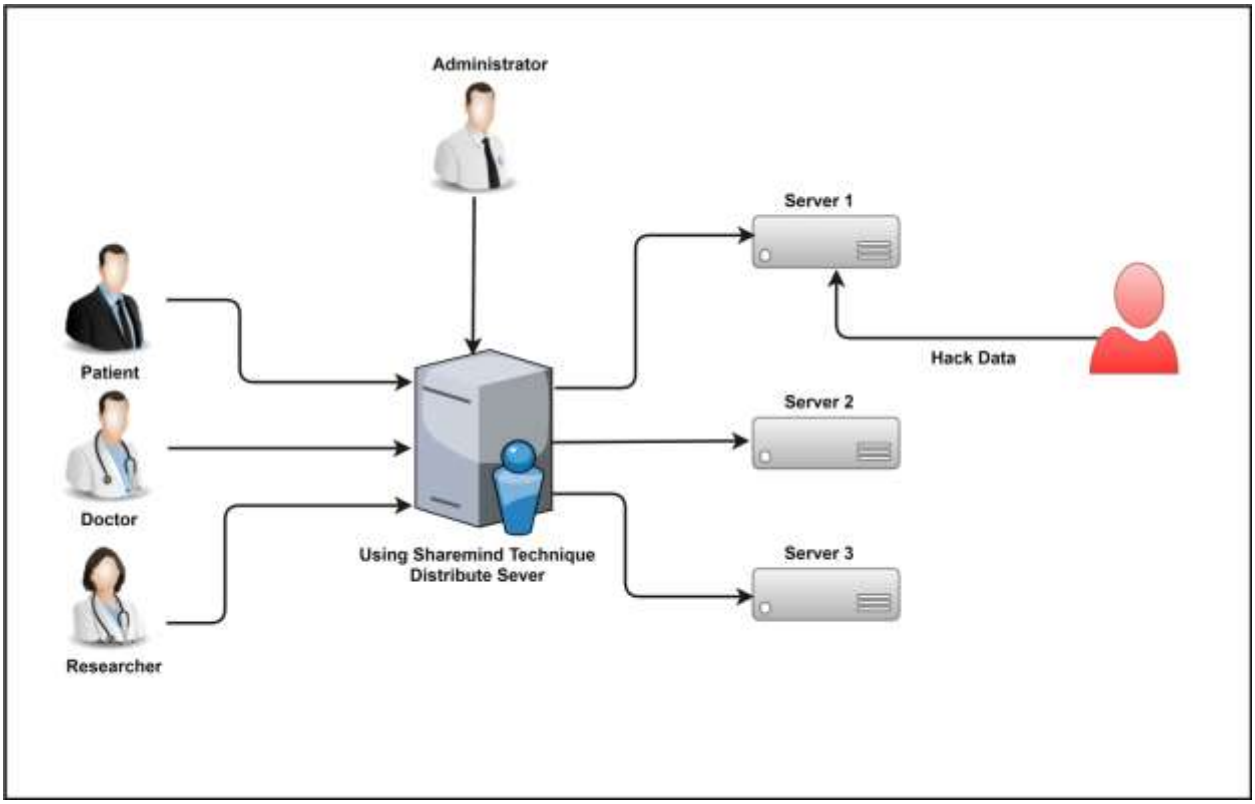

Figure 1. System Architecture of Proposed System

VI. CONCLUSION

In this paper, we have a tendency to thought-in regards to the matter of resource allocation in wireless Networks wherever sources have counsel to become transmitted for their corresponding destinations with the expertise of intermediate nodes with time-varying transmission channels. All intermediate nodes are believed-about as internal eavesdroppers from that this council must be protected. To provide confidentiality in this setting, we have a tendency to propose coding the message over long blocks of information which might be transmitted over completely different methods.

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 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 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 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 Loga-rithms. 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.