Privacy-Preserving Data Transmission Protocol For Wireless Medical Sensor Data

A.GAJENDER
M.TECH Student
CNIS, SNIST

M.NAGARAJU
Assistant Professor
Dept of IT, SNIST

Abstract: **Wireless Sensor Networks (WSN) has fascinated to great extent significance in the last decade. It opened a new series of applications such as monitoring including environmental monitoring large area, exploration of wildlife, and real-time patient medical data which is collected by wireless sensors. The WSN provides the options of flexibilities and costs saving for patients and healthcare enterprises. At the same time, there is a viable concern about the hospitals' ability to provide adequate care during emergency events. Tools that automate patient monitoring have likely to improve efficiency and quality of health care significantly. In hospitals, medical information sensors which monitor patients produce an increasingly large amount of real-time data. The delivery of this data through wireless networks in a hospital becomes a critical problem because the pathological information of an individual is highly sensitive. It must be kept private and secure. In this article, we propose a realistic approach to preventing the inside attack by ensuring secure data transmission. The main contribution of this article is securely distributing the patient data by implementing Privacy-Preserving Data Transmission Protocol and employing the Paillier and ElGamal cryptosystems to perform statistic analysis on the patient data without compromising the patients' privacy. We enhance this protocol to reduce the overhead by implementing secure data aggregation method.**

Keywords: **Privacy Protection; Paillier Cryptosystem; Patient Data Privacy;**

I. INTRODUCTION

Wireless Sensor Network (WSN) is a self-organized network of sensor nodes, where the nodes can interact with themselves using radio signals and these sensor nodes can function, monitor and understand the physical environment. It consists of spatially disposed sensors to observe natural or environmental conditions and to pass the data through the network to a target location. The modern bi-directional systems enable to control the activity of the sensors. The evolution of the wireless sensor networks was driven by military utilization such as battlefield surveillance and is also used in many mechanical and consumer applications like industrial process monitoring and control, machine health monitoring, etc. [3]. The WSN built with "nodes," where one or more sensor is connected to each node. Each sensor node consists of several parts, like a microcontroller, radio transceiver with an internal antenna to an external antenna, an electronic circuit for interfacing with the sensors and an energy source like a battery.

WSNs deployed at a large scale in an ordered manner, and their data rates differ based on their utilization. Where the Wireless Medical Networks have direct human involvement is deployed on a small scale must maintain mobility (a patient can carry the devices), and this medical network requires high data rates with reliable communication. Physiological stipulations of patients can monitor nearly by deploying medical sensor motes [11].

Medical sensors used to sense the patient's vital body parameters and transmit the sensation data in a timely order to some remote location without personal involvement. Using medical sensor readings the doctor can check patient's health status. The patient's operating body parameters include heart beats, body temperature, blood pressure, sugar level, pulse rate [1]. WMSNs carry the quality of care across the broad range of healthcare applications. Also, other applications that benefit from WMSNs include sports-person health status monitoring and patients self-care. Several research groups and projects have started to develop health monitoring using wireless sensor networks. Wireless Medical healthcare application offers some challenges, like the 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 [7]. For instance, the patient's physiological vital signals are very sensitive so the leakage of the patient's diseased data could make 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 [2]. Further, wireless medical sensor networks cover a broad range of healthcare applications, such as physiological data monitoring, activity monitoring in health-clubs, location tracking for the athlete are the broad range of healthcare applications. WMSNs share individual data with physicians and insurance

companies. Thus unauthorized collection and use of patient data by adversaries can cause life-threatening risks to the patient and make the patient's private matters publically available.

II. SYSTEM ARCHITECTURE

Data collection-Health care involves a variety of public and private data which includes health reviews, administrative enrollment, billing records, sensitive patient data which are used by the hospitals, doctors, physicians, etc. A data collection protocol is used where a sensor collects and splits the sensitive patient data into multiple components and sends them to multiple servers. In the wireless medical sensor network, each medical sensor sends the sensitive patient data to the distributed database system in a safe manner.

Data store security-The patient database system consists of multiple database servers. Assuming that all data servers are semi-honest, often called honest but curious". That is, all data servers run protocol exactly as specified, but try to learn as much as possible about the patient data. Also, assuming that the inside attackers do not compromise at least one data server [6].Data Access security-In the patient access control system, only the person who are authorized, can get access to the sensitive patient data. The patient data cannot be disclosed to any data server during the access. Paillier Public-Key Cryptosystem is used by the user (e.g., Doctor) to access the patient data and monitor the patient's health condition. The user sends the request including the patient's identity, an attribute of the data, the signature of the user on the query, and the certificate of the user to the three data servers through secure channels. The secure channels are used for the user to place his queries because the patient's personal details in the queries need to protect against outside attackers [5]. If the user's request passes the signature verification and meets the access control policies, then the servers can identify the shares of the data according to the patient's identity and the attribute of the data. AES are symmetric-key algorithms that use the same cryptographic keys for both encryptions of plaintext and decryption of cipher text [10].

AES is more secure than its predecessors such as DES and 3DES, as the algorithm is stronger and uses longer key lengths. AES is built for three key sizes 128,192,256 bits. The communication between the user and each data server is through a secure channel. The three data servers and the user's computing device are usually much more powerful in computation and communication. By using AES, we can achieve data confidentiality, authenticity, and integrity between the user and each data server. The sensitive patient data which stored in the database is encrypted using AES algorithm, and it stored on multiple servers. Paillier Public-Key Cryptosystem the Paillier encryption scheme invented by Pascal Paillier in 1999 is public key encryption algorithm.

It is consists of key generation, encryption, and decryption algorithms as follows: Key generation.

The key generation algorithm works as follows:

1.Choose any two large prime numbers p and q such that they are independent of each other $\gcd(pq,(p-1)(q-1)) = 1$

2.Compute $N = pq$, $\alpha = \text{lcm}(p-1, q-1)$ Where lcm stands for the Least Common Multiple.

3.Select random integer g where $g \in Z_N^*$ and ensure N divides the order of g by checking the existence of the following modular multiplicative inverse:

$\mu = (L(g \pmod{N^2}))^{-1} \pmod N$

Where function L is defined as $L(u) = u - 1/N$. The notation a/b does not denote the modular multiplication of time the modular multiplicative the inverse of b but rather it denotes the quotient of a divided by b.

The public (encryption) key pk is (N,g).

The private (decryption) key sk is (α,μ).

If using p,q of equivalent length, then

$g = N + 1, \propto = \emptyset(N), \mu = \emptyset(N)^{-1} \pmod N$

Where $N = pq$ and $\emptyset(N) = (p-1)(q-1)$.

a) Encryption

The encryption algorithm involves the following steps:

1. Let m be a message to encrypt, where $m \in Z N$.

2. Select a random r such that $r \in Z^*N$.

3. The ciphertext is computed as:

$$\mathbf{c = g^m.r^N \pmod{N^2}}$$

b) Decryption

The decryption algorithm involves the following steps: 1. Let c be the ciphertext to decrypt, where the ciphertext $c \in Z_N^{*2}$

Compute the plaintext message as:

$m = L(c^{\rho} \pmod{N^2}) \bullet \mu \pmod N$.

Homomorphic Properties

A remarkable feature of the Paillier cryptosystem is its homomorphic properties. Given two Ciphertexts $E(m_1, p_k) = g^{m1} r_1^N \pmod{N^2}$, $E(m_2, p_k) = g^{m2} r_2^N \pmod{N^2}$

Where r1, r2 are randomly chosen for Z_N^{*2}. The product of two ciphertexts will decrypt to sum of their corresponding plaintexts,D (E (m_1 ,pk_1).E

$(m_2 ,pk_2))= m_1 + m_2 \pmod N$.The product of a ciphertext with a plaintext raising g will decrypt to the sum of the corresponding plaintexts,D $(E (m_1 ,pk_1).g^{m2})= m_1 + m_2 \pmod N$.An encrypted plaintext raised to a constant k will decrypt to the product of the plaintext and the constant, 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.

Paillier cryptosystem

Patient information access control protocol. The data access protocol is used to maintain privacy of the sensitive patient data during access by the physician without revealing to any servers

Input: α,β,γ,pk,sk

Output: ρ = α + β + γ

1. The data server S1 picks a random $r_1 \in Z_N^*$ and computes C1 = Encrypt (α,pk)= g r1 N (mod N2) And sends C1 to the server S2.
2. The data server S2 picks a random r2∈ Z* N and computes C2 = Encrypt (β,pk)= g r2 N (mod N2) and sends C1 C2 to the server S
3. The data server S3 picks a random r3 Z* N and computes C3 = Encrypt $\gamma = g^{\gamma}$ r3 N (mod N 2) and replies C1 C2 C3 to the user.
4. The user computes ρ = Decrypt(C1 C2 C3,sk).
5. Return ρ Because of the homomorphic properties of the Paillier Cryptosystem,C1 C2 C3` = E (α,pk) E (β,pk) E (γ,pk) = $(g^{\alpha}$ r1 N) $(g^{\beta}$ r2 N) $(g^{\gamma}$ r1 N) (mod N2) = Decrypt(C1 C2 C3 ; sk) = α+ β +γ.

Elliptic Curve Digital Signature Authentication (ECDSA)

Alice, with domain parameters D = (q, FR, a, b, G, n, h), public key Q and private key d, does the following steps to sign the message m

1. Selects a Random number k ϵ [1, n – 1]
2. Computes Point kG = (x, y) and r = x mod n, if r = 0 then goto Step 1
3. Compute t = k–1 mod n
4. Compute e = SHA-1(m), where SHA-1 denotes the 160 bit hash function
5. Compute s = k– 1 (e + d_a*r) mod n, if s = 0 goto Step 1
6. The signature of message m is the pair (r, s)
7. Alice sends Bob the message m and her signature (r, s).

To verify Alice's signature, Bob does the following (Note that Bob knows the domain parameters D and Alice's public key Q)

1. Verify r and s are integers in the range [1, n – 1]
2. Compute e = SHA-1(m)
3. Compute w = s–1 mod n
4. Compute u1 = e.w and u2 = r.w
5. Compute Point X = (x1, y1) = u1G + u2Q
6. If X = O, then reject the signature

   Else compute v = x1 mod n
7. Accept Alice's signature iff v = r.

An illustration of the above steps is represented below

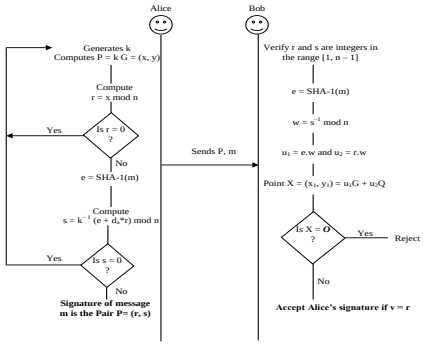

Fig 1:Illustration of Elliptic Curve Digital Signature Algorithm.

III. PRIVACYAND PERFORMANCE ANALYSIS

Inpatient information access control protocol, the sensitive patient data is always encrypted by the public key of the user. The attacker cannot access the patient data even if two of the three data servers are compromised by the inside attack without the private key of the user(eg: physician). Even if the user gets the encrypted data, he will not be able to decrypt without the cooperation of all the three servers. Inpatient information access control protocol which is based on the Pailliercryptosystem [12], the dominated computation is the modular exponentiation, i.e., ax (mod N2) where x ∈ Z* N. Each data server computes two modular exponentiations and exchange | N2 | = 2 | N | bits, where | N |is the length of N. The user calculates one modular exponentiation and transfers 2| N | bits.

IV. RESULTS

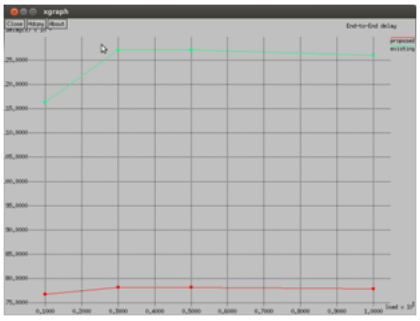

Fig 2: End-to-End Delay

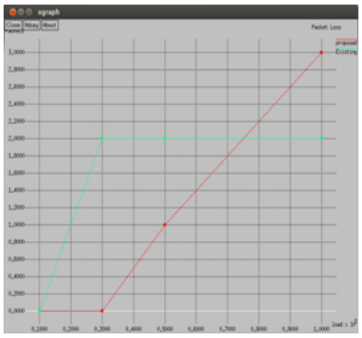

Fig 3: Packet loss

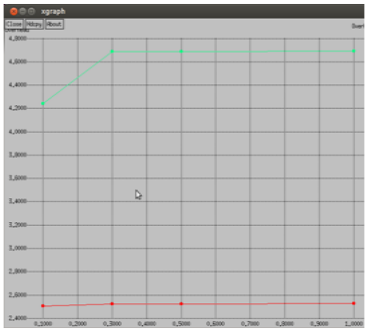

Fig 4: Overhead

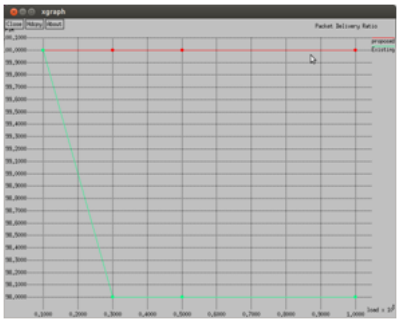

Fig 5: Packet Delivery Ratio

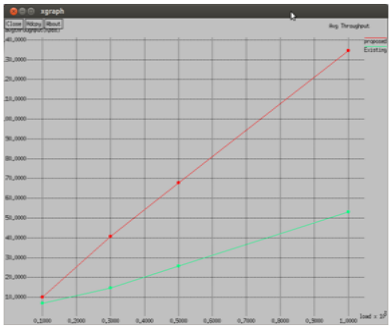

Fig 6: Avg Throughput

V. CONCLUSION

The different scheme has been prescribed to implement the Healthcare Architecture, but the security and privacy of the medical data are still a concern [4]. Maintenance of the server, upgrading the server, providing storage capacity updating the Software used and their licensing is also a big concern. Providing security and privacy of Medical data can be achieved by keeping the patient data in Cloud Servers where sensitive data is stored in encrypted format, and it is shared with authorized users only. To improve the privacy and security, Proxy Re-encryption technique is used where the intent is to transform the cipher data that the owner uploads into cipher text that the user of the data can decrypt using his or her private key. The queries forwarded by these users are evaluated on the encrypted data such that the cloud server does not learn any useful information other than the query output. The server is maintained by the cloud service provider itself. Storing the patient data in cloud servers can quicken and improve data transmission and enable remote data collection which can help the doctors to take a better decision in the case of emergency.

VI. REFERENCES

[1] M. Ahmed, X. Huang, and H. Cui, "Smart Decision Making for Internal Attacks in Wireless Sensor Network," International Journal of Computer Science and Network Security, vol. 12, no. 12, pp. 15–23, Dec. 2012.

[2] D. Bogdanov, S. Laur, J. Willemson. Sharemind: a Framework for Fast Privacy-Preserving Computations. In Proc. ESORICS'08, pages 192-206, 2008.

[3] Dan Baehr, Steve McKinney, Aaron Quirk, and Khaled Harfoush, "On the Practicality of Elliptic Curve Cryptography for Medical Sensor Networks," IEEE, 2013.

[4] X. Du and H.-H. Chen, "Security in wireless sensor networks," IEEE Wireless Communications, vol. 15, no. 4, pp. 60–66, 2008.

[5] H. Ghamgin, M. S. Akhgar, and M. T. Jafari, "Attacks in Wireless Sensor Network," vol. 5, no. 7, pp. 954–960, 2011.

[6] X. Huang, M. R. Ahmed, D. Sharma, and H. Cui, "Protecting wireless sensor networks from internal attacks based on uncertain decisions," in 2013IEEE Wireless Communications and Networking Conference (WCNC), pp. 1854–1859, 2013.

[7] P. Kumar and H. J. Lee. Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey. Sensors 12: 55-91, 2012.

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

[9] K. Lu, Y. Qian, and J. Hu, "A framework for distributed key management schemes in heterogeneous wireless sensor networks,"

IEEE Transactions on Wireless Communications, vol. 7, no. 2, pp. 639–647, Feb. 2008.

[10] Advanced Encryption Standard (AES). FIPS PUB 197, November 26, 2001. http://csrc.nist.gov/publications/fips/fips197/fips197.pdf

[11] Oliver N. and Flores F., "HealthGear: A RealTime Wearable System for Monitoring and Analyzing Physiological Signals," International Workshop on Wearable and Implantable Body Sensor Networks, pp. 3-5, 2006.

[12] P. Paillier. Public-key Cryptosystems Based on Composite Degree Residuosity Classes. In Proc. EUROCRYPT'99, pages 223-238, 1999.

