International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume3, Issue 4 (April '2017)

# A MEDICAL INFORMATION SECURITY USING CRYPTOSYSTEM FOR WIRELESS SENSOR NETWORKS

**Dr .C.K.Gomathy,**
Assistant Professor,
Department of Computer Science Engineering,
SCSVMV University,
India.

**V.Geetha,**
Assistant Professor,
Department of Computer Science Engineering,
SCSVMV University,
India.

**T.Jayanthi,**
Assistant Professor,
Department of Computer Science Engineering,
SCSVMV University,
India.

**M.Bhargavi**
UG Scholar,
Department of Computer Science Engineering,
SCSVMV University,
India.

**P.Sai haritha,**
UG Scholar
Department of Computer Science Engineering,
SCSVMV University,
India.

**ABSTRACT:** In these days cryptography is widely used in many areas to protect data from threat and by using wireless sensor networks can also make the data more protected and by these networks in which these provide replaying action against many issues ,also can access the data from anywhere to anywhere by these wireless sensor networks and it will protect the medical data from threat by storing the data in three servers in this by using some cryptographic algorithms and can protect the data from inside also from attacks not only from outside also. By this only the authorized people only can access the data but not the others so data will be safe from attacks.

***Keywords: Wireless medical sensor network, patient data privacy, Paillier encryption, and ElGamal encryption***

## I.INTRODUCTION

To monitor the environment conditions in the wireless sensor networks use a large number of sensors and by this pass the information to the main location and this wireless sensor networks are mainly motivated by military applications and this sensor networks became very famous today and also used in many consumer and industrial areas, and now a days the promising fields like healthcare applications are maintained very well by these wireless sensor networks. now a days Wireless medical sensor networks certainly improve quality-of-care. Typical security threats to healthcare applications are Evas dropping and impersonation.

The main basic need of this project is now a days data has been undergoing attacks and also number of attackers and also the attacking techniques have been improvised and also medical information is more than 10 times useful than credit card details on black market. Attackers discovers more methods so health care becoming a target because it contains personal data like number, address etc. so there is a need of privacy protection for that patient data so in this project protecting the patient data not only from outside but also from inside

## II.PROBLEM STATEMENT

Wireless Sensor Networks (WSN) is an emerging technology that has the potential to transform the way of human life. Healthcare 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.

## III.RELATED WORK

**A k-anonymity privacy-preserving approach in wireless medical monitoring environments**

With the proliferation of wireless sensor networks and mobile technologies in general, it is possible to provide improved medical services and also to reduce costs as well as to manage the shortage of specialized personnel. Monitoring a person's health condition using sensors provides a lot of benefits but also exposes personal sensitive information to a number of privacy threats. By recording user-related data, it is often feasible for a malicious or negligent data provider to expose these data to an unauthorized user. One solution is to protect the patient's privacy by making difficult a linkage between specific measurements with a patient's identity. The presented algorithm is resource aware, as it minimizes energy consumption with respect to other more costly, cryptography-based approaches.

 

**A novel and lightweight system to secure wireless medical sensor networks**

Wireless medical sensor networks (MSNs) are a key enabling technology in e-healthcare that allows the data of a 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. And this 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.

**Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications**

Wireless sensor networks (WSN) in healthcare applications is growing in a fast pace. Numerous applications such as heart rate monitor, blood pressure monitor and endoscopic capsule are already in use. To address the growing use of sensor technology in this area, a new field known as wireless body area networks (WBAN or simply BAN) has emerged. As most devices and their applications are wireless in nature, security and privacy concerns are among major areas of concern. Due to direct involvement of humans also increases the sensitivity. Whether the data gathered from patients or individuals are obtained with the consent of the person or without it due to the need by the system, misuse or privacy concerns may restrict people from taking advantage of the full benefits from the system. People may not see these devices safe for daily use. There may also possibility of serious social unrest due to the fear that such devices may be used for monitoring and tracking individuals by government agencies or other private organizations.

**An Efficient Mutual Authentication and Access Control Scheme for Wireless Sensor Networks in Healthcare**

Wireless sensor networks (WSNs) will play an active role in the 21th Century Healthcare IT to reduce the healthcare cost and improve the quality of care. The protection of data confidentiality and patient privacy are the most critical requirements for the ubiquitous use of WSNs in healthcare environments. This requires a secure and lightweight user authentication and access control. Symmetric key - based access control is not suitable for WSNs in healthcare due to dynamic network topology, mobility, and stringent resource constraints. This is to ensure that medical data is not exposed to an unauthorized person. On the other hand, it ensures that medical data sent to healthcare professionals did not originate from a malicious node.

**Privacy-Preserving Wireless Medical Sensor Network**

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 cryptosystems. The efforts can protect the patient data during transmission, but cannot stop the inside attack where the administrator of the patient database reveals the sensitive patient data. To prevent from the inside attack, more advanced cryptographic techniques, such as attribute-based encryption, may be used. However, it is too expensive to implement the techniques in the wireless sensor networks with low-power and low-cost sensor nodes. Another contribution is employing Share mind system to protect patient data privacy and support medical research.

## IV.METHODOLOGIES

The architecture of distributed data base model contains with three data servers. They are illustrated as:

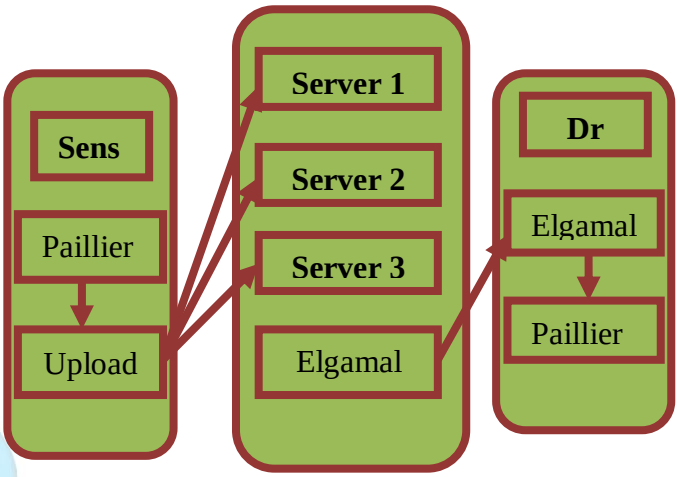


**Figure1: Distributed Server Model**

This is an initial deployment phase between each medical sensor and each data server. For each medical sensor, three secret keys are pre-deployed and pre-shared with three data servers, respectively. Each secret key is used to create a secure channel between the sensor and one data server. the distributed server model generate wireless medical sensor network. It contains n sensor nodes, 3 servers and one doctor node. These sensor nodes worn by a patient which provide physiological sensing to 3 servers. Then doctor can access these sensed data from servers.

In distributed server model , first sensor nodes and servers are connect with doctors. At the connection time, doctor generate the Paillier and Elgamal Public & Private Keys. Then send the Paillier Public Key to nodes for Paillier Encryption and send the Elgamal Public Key to Servers for Elgamal Encryption. and Sensor nodes sense physiological data.

Then split these data to 3 blocks for 3 servers .Then it encrypts these blocks based on Paillier Public Key. Followed by, it forward these encrypted blocks to 3 servers respectively.

To protect uploaded data against inside attacks, servers can encrypt once. Here servers apply Elgamal encryption using Elgamal Public Key.So these uploaded sensed data have more security against inside attacks.

In this module, doctor wants to access these uploaded sensed data. So he downloads all sensed data from all 3 servers. First he decrypts the sensed data based on Elgamal decryption using Elgamal Private Key. After Elgamal Decryption, doctor decrypts the sensed data based on Paillier Decryption using Paillier Private Key. Finally he gets the original sensed data. In this project we are mainly using cryptosystems like Elgamal and paillier this can be

shown as El_Gamal is a public-key cryptosystem technique was designed by Dr. Taher Elgamal El_Gamal depends on the one way function, means that the encryption and decryption are done in separate functions. The encryption process requires two modular exponentiations (extra time).

**Key generation**

- Generate a large random prime number (p)
- Choose a generator number (a)
- Choose an integer (x) less than (p-2) ,as secret number.
- Compute (d) where
  - $d= a^x \bmod p$
- Determine the public key (p, a, d), and the private key (x)

**Encryption**

- Obtain the public key (p , a , d ) from
- the receiver A.
- Choose an integer k such that :
  - $1 < k < p-2$
- Represent the plaintext as an integer m where $0 < m < p-1$
- compute (y) as follows :
  - $y = a^k \bmod p$
- compute (z) as follows :
  - $z = (d^k * m) \bmod p$
- Find the ciphertext (C) as follows :
  - $C= ( y , z )$
- The sender B send C to The receiver A .

**Decryption**

- Obtain the ciphertext (C) from B .
- compute (r) as follows :
  - $r = y^{p-1-x} \bmod p$
- Recover the plaintext as follows:
  - $m = ( r * z ) \bmod p$

## V.SECURITY AND PRIVACY ANALYSIS

The communication between each medical sensor and each data server is through a secure channel, which is implemented by a secret-key cryptosystem. The patient data over the secure channel is encrypted with the secret key pre-shared between the sensor and the data server. Without the secret key, the attacker cannot eaves-drop the patient data.

**Data Collection Protocol**

There is an initial deployment phase between each medical sensor and each data server. For each medical sensor, three secret keys are pre-deployed and pre-shared with three data servers, respectively. Each secret key is used to create a secure channel between the sensor and one data server. In addition, one more secret key is pre-deployed in each sensor in order to generate random numbers. Note that different medical sensors are deployed with different secret keys.

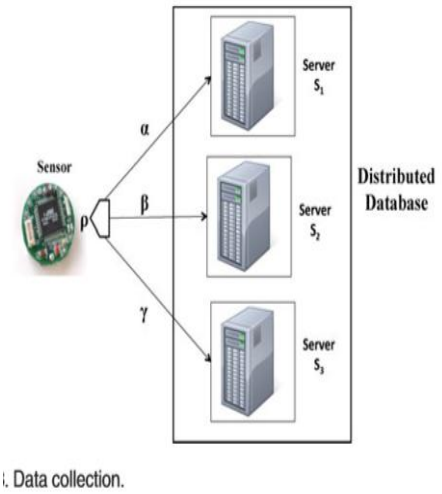


**Figure2: Distributed Database**

**Access control protocol**

In addition it assumes that the user establishes three channels with three data servers, respectively. To get access to the patient data, the user sends a request including the patient's identity, the data attribute, the signature of the user on the query, and the certificate of the user to the three data servers through the three secure channels, respectively.

**Statistical Analysis Protocols**

In Privacy protection system supports not only access control to the patient data but also privacy-preserving statistical analysis on the patient data for medical research, where the three data servers cooperate to help the medical researcher analyze the patient data without revealing the patient privacy.

## VI.RESULTS

The creation of doctor node and to this the sensor and server nodes are connected and the Elgamal key generation is done and uploading of files and splitting and encryption is done and the doctor node will decrypt and download the files the can be shown in below sample screens

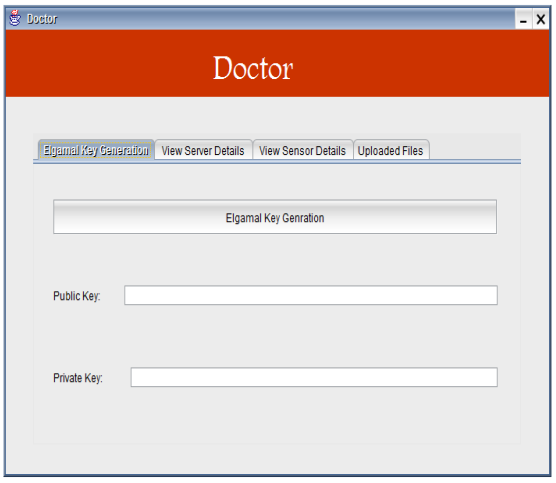


**Figure3: Doctor Node**

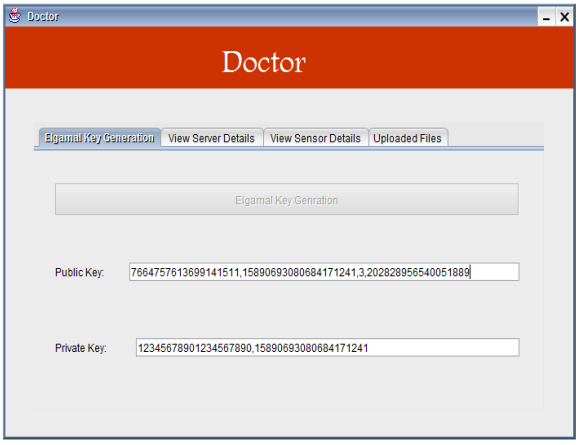


**Figure4: Key Generations**

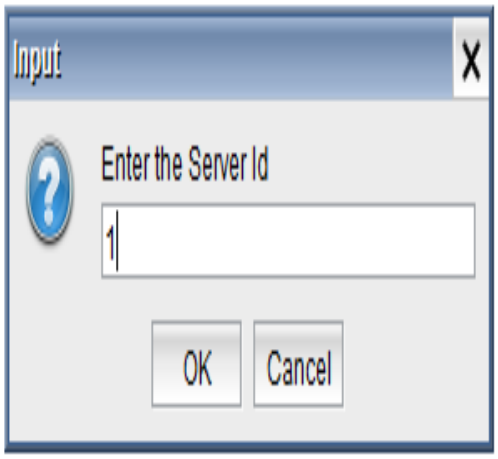


**Figure5: Distributed Server 1**

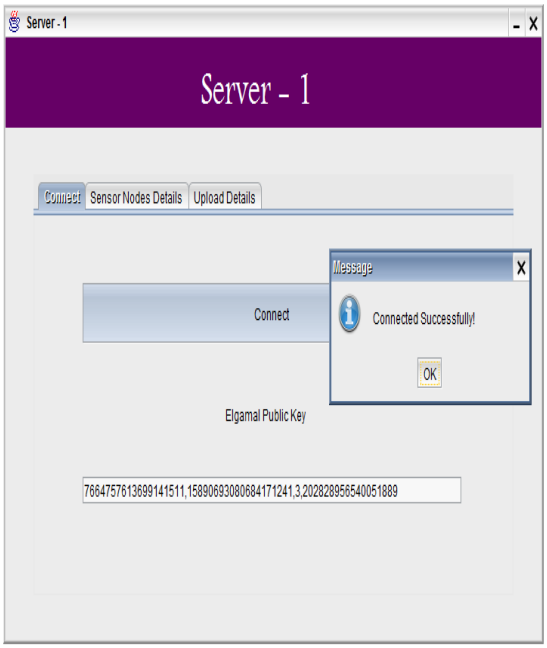


**Figure6: Server Node**

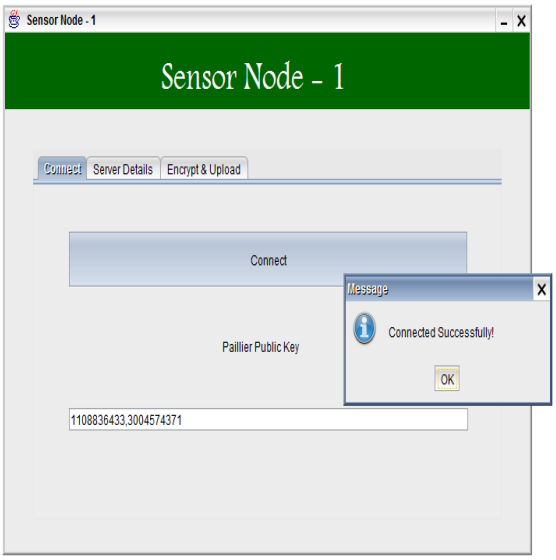


**Figure7: Sensor Node**


**Figure8: Elgamal Decryption**

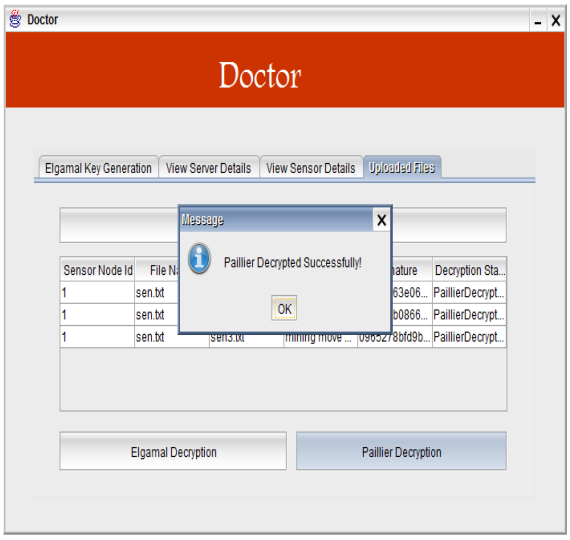


**Figure9: Pallier Decryption**

## VIII.FUTURE WORK

In privacy protection system focused in, the communication between each medical sensor and each data server is through a secure channel, which is implemented by a secret-key cryptosystem. The patient data over the secure channel is encrypted with the secret key pre-shared between the sensor and the data server. Without the secret key, the attacker cannot eaves- drop the patient data.

By AES and DSS, this can achieve data confidentiality, authenticity and integrity between the user and each data server. In our solution, the communications among three data servers can be also through secure channels. Like the secure communication between the user and the data servers, any two of the three data servers can establish a secret key with a public key cryptosystem. Then the communication between the two data servers can be encrypted with AES based on the secret key.

In distributed server model, the three data servers are assumed to be semi-honest. Otherwise, the user can never obtain correct patient data and statistical analysis results. To ensure data authenticity and integrity in the communications among the three data servers

## VIII.DESCRIPTION

The generation of wireless medical sensor network as contains n sensor nodes, 3 servers and one doctor node. In sensor nodes worn by patients which provide by physiological in sensing to 3 servers. Then doctor can access these sensed data from servers. In this, first sensor nodes and servers are connecting with doctors. At the connection time, doctor generates the Paillier and Elgamal Public & Private Keys. Then send the Paillier Public Key to nodes for Paillier Encryption and send the Elgamal Public Key to Servers for Elgamal Encryption. Sensor nodes sense physiological data. Then split these data to 3 blocks for 3 servers. Then it encrypts these blocks based on Paillier Public Key.

Followed by, it forward these encrypt blocks to 3 servers respectively

To protect uploaded data against inside attacks, servers can encrypt once. Here servers apply Elgamal encryption using Elgamal Public Key. So these uploaded sensed data have more security against inside attacks. The doctor wants to access these uploaded sensed data. So he downloads all sensed data from all 3 servers.First he decrypts the sensed data based on Elgamal decryption using Elgamal Private Key.After Elgamal Decryption, doctor decrypts the sensed data based on Paillier Decryption using Paillier Private Key.Finally he gets the original sensed data.

## IX.CONCLUSION

In this thesis, investigation is done to security and privacy issues in the medical sensor data collection, storage and queries and presented a complete solution for privacy preserving medical sensor network. To secure the communication between medical sensors and data servers, use of the lightweight encryption scheme and MAC generation scheme based on SHA-3 proposed. To keep the privacy of the patient data, 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, an access control protocol, where three data servers cooperate to provide the user with the patient data, but do not know what it is. For the legitimate user (e.g., medical researcher) to perform statistical analysis on the patient data, proposed some new protocols for average, correlation, variance and regression analysis, where the three data servers cooperate to process the patient data without disclosing the patient privacy and then provide the user with the statistical analysis results. Security and privacy analysis has shown that our protocols are secure against both outside and inside attacks as long as one data server is not compromised. Performance analysis has shown that our protocols are practical as well. Unlike, our solution can preserve the patient data privacy as long as one of three data server is not compromised

## X .REFERENCES

[1]. S. Dagtas, G. Pekhteryev, Z. Sahinoglu, H. Cam, and N. Challa, "Real-Time and secure wireless health monitoring," Int.

[2]. J. Telemed. Appl., pp. 1–10, Jan. 2008. W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theory, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[3]. Sugumar, N. and C.K. Gomathy, 2014. Smart LCM for energy-efficient mechanism using CTX in wireless sensor network. Int. J. Adv. Found. Res. Comput., 1: 47-56.

[4]. (2013, Jul.). Digital signature standard (DSS). FIPS PUB 186-4 [Online]. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/ NIST.FIPS.186-4.pdf

[5]. T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Inf. Theory, vol. IT-31, no. 4, pp. 469–472, Jul. 1985.

[6]. Advanced encryption standard (AES). (2001, Nov. 26). FIPS PUB 197 [Online]. Available: http://csrc.nist.gov/publications/fips/ fips197/fips-197.pdf [2] P. Belsis and G. Pantziou.

[7]. Gomathy, C.K. and S. Rajalakshmi, 2014. A software ability link for service-oriented architectures. Global J. Manage. Bus. Res., 14: 11-14.

[8]. "A k-anonymity privacy-preserving approach in wireless medical monitoring environments," J. Per-sonal Ubiquitous Comput., vol. 18, no. 1, pp. 61–74, 2014. [3]

[9]. D. Bogdanov, S. Laur, and J. Willemson, "Sharemind: A frame- work for fast privacy-preserving computations," in Proc. 13th Eur. Symp. Res. Comput. Security, 2008, pp. 192–206. [4] R. Chakravorty,

[10]. "A programmable service architecture for mobile medical care," in Proc. 4th Annu. IEEE Int. Conf. Pervasive Comput. Commun. Workshop, Pisa, Italy, Mar. 13–17, 2006, pp. 532–536. [5] Crypto++ 5.6.0 Benchmarks [Online]. Available: http://www. cryptopp.com/benchmarks.html, 2009.