DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4223

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

WMSD: TOWARDS A NEW FRAMEWORK APPROACH TO PRIVACY-PRESERVING DESIGNED FOR APPROACH IN MEDICAL PATIENT DATA

Mrs. Rehana Tabassum
PG Student
Department . of Computer Science and Engineering
Malla Reddy Engineering College(A), Maisammaguda,
Dulapally road, Hyderabad, Telangana

Mr. Vijay Kumar Burugari
Associate Professor
Department . of Computer Science and Engineering
Malla Reddy Engineering College(A), Maisammaguda,
Dulapally road, Hyderabad, Telangana

Abstract: In present days' medical healthcare applications extensively uses wireless sensor networks (WSN).For example, clinic and home patient checking. Remote therapeutic sensor systems are more powerless against listening stealthily, adjustment, pantomime and replaying assaults than the wired systems. A considerable measure of work has been done to secure remote medicinal sensor systems. The current arrangements can ensure the patient information amid transmission, yet can't stop within assault where the director of the patient database uncovers the delicate patient information. In this paper, we propose a handy way to deal with keep within assault by utilizing numerous information servers to store persistent information. The primary commitment of this paper is safely circulating the patient information in different information servers and utilizing the Paillier and ElGamal cryptosystems to perform measurement examination on the patient information without bargaining the patients' security.

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

.

I.INTRODUCTION

A Wireless sensor network (WSN)comprises of spatially conveyed independent sensors to screen physical or natural conditions, for example, temperature, sound, weight, and so forth and to agreeably go their information through the system to a fundamental area. The advancement of remote sensor systems was roused by military applications such as combat zone reconnaissance; today such systems are utilized as a part of numerous mechanical and shopper applications, for example, modern process observing and control, machine health monitoring, and so on.

Social insurance applications are considered as promising fields for remote sensor systems, where patients can be observed in doctor's facilities and even at home utilizing remote therapeutic sensor systems (WMSNs)[4]. Lately, numerous medicinal services applications utilizing WSNs have been created, for example, CodeBlue[8].

A normal case of human services applications with WSNs is Alarm-Net created in University of Virginia for helped living and private checking. As shown in above the architecture of Alarm-Net is appeared in Fig. 1.Alert Net is made out of portable body organize, emplaced sensor arrange, AlarmGate applications, back-end frameworks, and UI's as takes after:

- ✓ Mobile body arrange has remote sensor gadgets worn by a patient which give physiological detecting.
- ✓ Information from the versatile body system is transmitted through the emplaced sensors to UIs or back-end frameworks.
- ✓ Emplaced sensor arrange has gadgets conveyed in the living space to detect natural quality or conditions, for
- ✓ example, temperature, clean, movement, and light. Emplaced sensors keep up associations with versatile body arranges as they travel through the living space.
- ✓ Alarm Gate applications fill in as application level passages between the remote sensor systems and IP systems. These hubs permit UIs and an association with a back-end database for long haul stockpiling of information.
- ✓ Back-end frameworks give online examination of sensor information and long haul stockpiling of information.
- ✓ User interfaces permit any genuine client of the framework to inquiry sensor information.

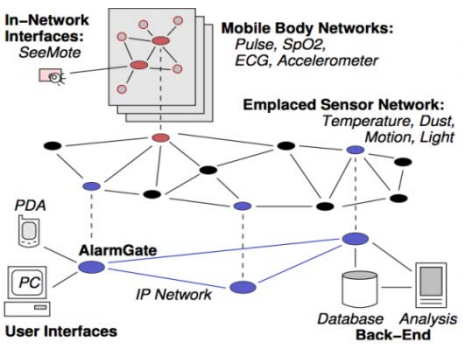

Fig 1:Alarm-Net Architecture

Pantomime is a security risk to the patient information validness. In a home care application, an assailant may imitate a remote depend point while persistent information is transmitting to the remote area. This may prompt false cautions to remote locales and a crisis group could begin a safeguard operation for a non-existent individual. This can even invalidate the point of remote human services.

Adjustment is a security danger to the patient information respectability. While the patient information is transmitted to the doctor, an enemy may catch the physiological information from the remote channels and change the physiological information. After the assaulted information (i.e., modified information) is sent to the doctor, it could imperil the patient. Information rupture is a security risk to the patient information protection.

An information rupture is an occurrence in which delicate, secured or secret patient information has conceivably been seen, stolen or utilized by an individual unapproved to do as such. For instance, a malevolent patient database director may utilize the patient information, (for example, quiet character) for their own advantage, for example, for restorative misrepresentation, deceitful protection claims, and now and then this may even stance life-undermining dangers.

To secure the remote therapeutic sensor systems against different assaults, a great deal of work has been finished. In 2012 , an overview on the as of late distributed writing on secure human services observing utilizing remote sensor systems. Current arrangements are based on either mystery key encryption or open key encryption as takes after:

- Secret-key based arrangements expect that the mystery keys for encryption and confirmation are sent in the medicinal sensors and the servers ahead of time. A mystery key cryptosystem, for example, AES [1], These arrangements are normally productive. Nonetheless, the circulation of the secret-keys is less effective than the general public-key based arrangements.
- Public-key based arrangements accept that an open key cryptosystem, for example, DiffieHellman key trade convention [8] , is utilized to build up a mystery key for encryption on the premise of people in general keys. Run of the mill cases of open key based arrangements incorporate [11]. These arrangements encourage key dissemination and refresh. Be that as it may, they are normally wasteful and not straightforwardly pertinent to the remote restorative sensor systems, where the sensors have constrained calculation and correspondence abilities.

II. PRIVACY-PRESERVING WIRELESS MEDICAL SENSOR NETWORK

Like the clear majority of human services applications with remote therapeutic sensor arrange, our design has four frameworks as takes after.

- ✓ A remote restorative sensor organizes which detects the patient's body and transmits the patient information to a patient database framework;
- ✓ A patient database framework which stores the patient information from restorative sensors and gives questioning administrations to clients (e.g., doctors and therapeutic experts) [11];
- ✓ A patient information get to control framework which is utilized by the client (e.g., doctor) to get to the patient information and screen the patient;
- ✓ A patient information examination framework which is utilized by the client (e.g., medicinal analyst) to question the patient database framework and break down the patient information factually [12].

There might be a middleware between the remote therapeutic sensor arrange and the patient database framework. If this is true, the part of the middleware is just sending the scrambled patient information to the database framework.

In our model, the patient database framework is made from numerous database servers. We expect that all information servers are semi-legitimate, regularly called "genuine however inquisitive". That is, all information servers run our convention precisely as determined, however may attempt to learn

however much as could be expected about the patient information from their perspectives of the convention. Also, we expect that no less than one information server is not traded off by assailants. For straightforwardness [9], we accept that the quantity of information servers is three. Truth be told, it can be any number more than three. The engineering of our model with three information servers can be appeared in Fig. 2.

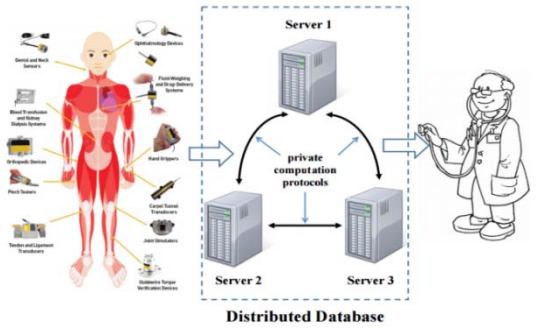

Fig. 2. Our Model

The security necessities for our model include:

- ✓ Data accumulation security: In the remote therapeutic sensor arrange, every medicinal sensor can safely send the patient information to the dispersed database framework.
- ✓ Data store security: In the dispersed patient database framework, the patient information can't be uncovered regardless of the possibility that two of three information servers are bargained by within assailants.
- ✓ Data get to security: In the patient get to control framework, just the approved client can access the patient information [7]. The patient information can't be uncovered to any information server amid the get to.
- ✓ Data examination security: In the patient information investigation framework, the approved client can get the factual investigation comes about as it were. The patient information can't be revealed to any information server

and even to the client amid the measurable investigation.

Our model considers two sorts of assaults, the outside assault and within assault. The outside assailant does not know any mystery enter in our framework, but rather endeavors to take in the patient information from the perspectives of our convention, or change the patient information [3], or mimic a medicinal sensor. Within aggressor is a noxious information server or a coalition of two vindictive information servers who know some mystery enters in our framework and endeavor to take in the patient information.

Paillier Public-Key Cryptosystem:

The Paillier encryption conspire [5], named after and created by Pascal Paillier in 1999, is a probabilistic open key encryption calculation. It is made from key era, encryption and unscrambling calculations as takes after.

III.KEY GENERATION

The key era calculation fills in as takes after.

- ✓ Choose two huge prime numbers p and q arbitrarily and autonomously of each other with the end goal that
$$\gcd(pq, (p-1)(q-1)) = 1$$
- ✓ Compute
$$N = pq, \lambda = lcm(p-1, q-1)$$

Encryption:

The encryption algorithm the whole thing as follows.

- ✓ Let m be a message to encode, where m ∈ZN .
- ✓ Select accidental r where r ∈ Z ∗N .
- ✓ Compute cryptogram text as:
$$c = g^m \cdot r^N (mod\ N^2)$$

Decryption:

The decryption algorithm the whole thing as follows.

- ✓ Let c be the cryptogram text to decrypt, where the cryptogram text c ∈ Z ∗ N2 .
- ✓ Compute the plain text message as:

$$m = L(c^\lambda (mod\ N^2)) \cdot \mu (mod\ N)$$

Data Collection Protocol:

There is an underlying arrangement stage between every restorative sensor and every information server. For every therapeutic sensor, three mystery keys are pre-conveyed and pre-imparted to three information servers, separately. Every mystery key is utilized to make a protected channel between the sensor and one information server [10]. Moreover, one more mystery key is pre-sent in every sensor keeping in mind the end goal to produce irregular numbers. Take note of that diverse restorative sensors are conveyed with various mystery keys.

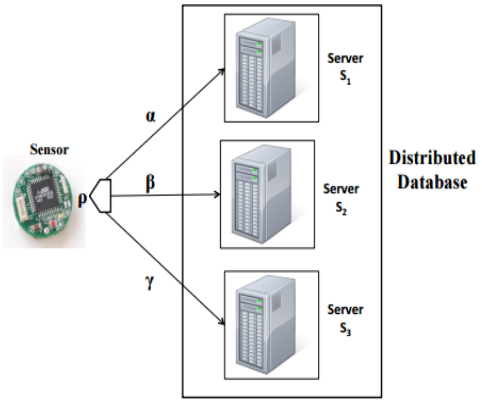

Fig. 3. Our three-server's modal

At the point when a therapeutic sensor sends a delicate numerical patient information ρ (e.g., temperature perusing) to the circulated tolerant database, to keep any information server from understanding the patient information and uncovering the patient security (within assault) [2], the medicinal sensor parts the patient information ρ (a whole number) into three whole numbers α, β, γ to such an extent that α+β+γ = ρ and sends them to the three information servers through three secure channels, separately, as appeared in Fig. 3.

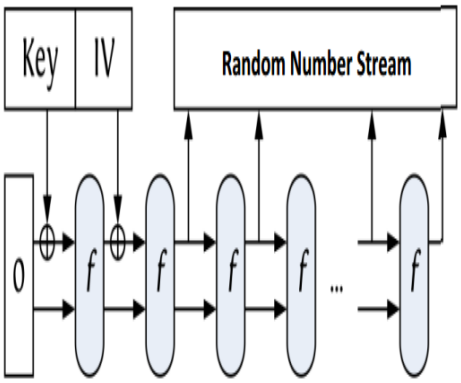

Fig. 4. Random Number Stream Generation

Access Switch Protocol:

There is an instatement stage before any client (doctor) can access the patient information. In this stage, the client creates an open and private key match (pk, sk) for the Paillier cryptosystem [2] as depicted in Section 2.1 and a mark check and marking key combine (pk∗ ,sk∗) for the Digital Signature Standard (DSS) [9]. For security reason, the measure of N in the Paillier cryptosystem is required to be more than 1024 bits. Accept that there exists a Public Key Infrastructure (PKI), where there exists a Certificate Authority (CA) which affirms people in general keys (pk, pk∗) for the client in an advanced testament. Also, we accept that the client sets up three secure channel with three information servers, separately. To access the patient information, the client sends a demand including the patient's personality, the informationproperty, the mark

of the client on the question, and the declaration of the client to the three information servers through the three secure channels, individually.

Comment: We utilize the safe channels for the client to present his inquiries on the grounds that the patient's close to home data in the questions should be secured against outside aggressors.

On the off chance that the client's demand passes the mark verifi-cation and meets the get to control arrangements, the three servers discover the offers of the information α, β, γ agreeing the patient's character and the trait of the information. At that point the three information servers and the client run Algorithm 1.

Comment: We require every information server to confirm the mark of the client and check the get to control approaches. The confirmation and check can be trusted because no less than one information server is not traded off

Algorithm 1 Patient Information Retrieval

Input: $\alpha, \beta, \gamma, pk, sk$

Output: $\rho = \alpha + \beta + \gamma$

1: The data server S_1 picks a random $r_1 \in \mathbb{Z}_N^*$ and computes

$$C_1 = Encrypt(\alpha, pk) = g^{\alpha} r_1^N (mod\ N^2)$$

and sends C_1 to the data server S_2.

2: The data server S_2 picks a random $r_2 \in \mathbb{Z}_N^*$ and computes

$$C_2 = Encrypt(\beta, pk) = g^{\beta} r_2^N (mod\ N^2)$$

and sends C_1C_2 to the data server S_3.

3: The data server S_3 picks a random $r_3 \in \mathbb{Z}_N^*$ and computes

$$C_3 = Encrypt(\gamma, pk) = g^{\gamma} r_3^N (mod\ N^2)$$

and replies $C_1C_2C_3$ to the user.

4: The user computes

$$\rho = Decrypt(C_1C_2C_3, sk)$$

5: **return** ρ

IV. CONCLUSION:

We have researched the security and assurance issues in the remedial sensor information aggregation, stockpiling and addresses and showed an aggregate response for insurance sparing therapeutic sensor arrange. To secure the correspondence between helpful sensors and information servers, we used the lightweight encryption plan and MAC time plot considering SHA-3 proposed.To keep the assurance of the patient information, we proposed another information gathering tradition which parts the patient information into three numbers and stores them in three information servers, separately the length of one information server is not exchanged off, the security of the patient information can be spared. For the bona fide customer (e.g., specialist) to get to the patient information, we proposed a get the chance to control tradition, where three information servers take part to outfit the customer with the patient information, yet don't understand what it is. For the honest to goodness customer (e.g., remedial examiner) to perform genuine examination on the patient information, we proposed some new traditions for ordinary, relationship, contrast and backslide examination, where the three information servers take an interest to deal with the patient information without uncovering the patient security and after that give the customer the true examination comes to fruition. Security and assurance examination has shown that our traditions are secure additions both outside and inside ambushes the length of one information server is not exchanged off. Execution examination has shown that our traditions are sensible.

V.REFERENCES

1) Advanced Encryption Standard (AES). FIPS PUB 197, Novem- ber 26, 2001. http://csrc.nist.gov/publications/fips/fips197/fips- 197.pdf
2) 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.
3) D. Bogdanov, S. Laur, J. Willemson. Sharemind: a Framework for Fast Privacy-Preserving Computations. In Proc. ESORICS'08, pages 192-206, 2008.
4) R. Chakravorty. A Programmable Service Architecture for Mobile Medical Care. In Proc. 4th Annual IEEE International Conference on Pervasive Computing and Communication Workshop (PERSOMW'06), Pisa, Italy, 13-17 March 2006.
5) Crypto++ 5.6.0 Benchmarks. http://www.cryptopp.com / benchmarks.html.
6) J. Daemen, G. Bertoni, M. Peeters, G. V. Assche, Permutation-based Encryption, Authentication and Authenticated Encryption, DIAC'12, Stockholm, 6 July 2012. Available at http://www.hyperelliptic.org/DIAC/slides /PermutationDIAC2012.pdf
7) W. Diffie and M. Hellman. New Directions in Cryptography. IEEE Transactions on Information Theory, 22 (6): 644-654, 1976.
8) Digital Signature Standard (DSS). FIPS PUB 186-4, July 2013, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
9) 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.
10) 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.
11) Chaudry, B., Wang, J., Wu, S., Maglione, M., Mojica, W., Roth, E., Morton, S.C., Shekelle, P.G.: Systematic review: Impact of health information technology on quality, efficiency, and costs of medical care. Annals of Internal Medicine 144(10), 742–752 (2006)
12) De Cristofaro, E., Kim, J., Tsudik, G.: Linear-complexity private set intersection protocols secure in malicious model. In: ASIACRYPT 2010, volume 6477 of LNCS, pages 213–231. Springer (2010)