

Protecting Wireless Medical Sensor Data from Inside Attackers through Data Collection Protocol

N. Naveen Kumar¹, Punna Shilpa²

Assistant Professor, Department of CSE, School of Information Technology (JNTUH), Village KPHB, Mandal
Kukatpally, District Medchal, Telangana, India¹

M. Tech Student, Department of CSE, School of Information Technology (JNTUH), Village KPHB, Mandal
Kukatpally, District Medchal, Telangana, India²

ABSTRACT Recently, the utilization of Wireless sensor Network (WSN) in health care applications is growing quickly as a result of it's got many benefits over the standard wired systems like easy use, reduced risk of infections, reduced risk of failures, reduced user discomfort and it provides increased quality, however providing security and privacy could be a major concern. There are many solutions so as to guard the patient information throughout transmission, however it cannot stop the within attacker from revealing the patient sensitive information. The within attacker is a patient information administrator. the most aim of this paper is to stop the within attack by distributing the patient information firmly in multiple servers and to use the Paillier cryptosystem to carry out statistic analysis on the patient information while not compromising the privacy of the patient's information.

KEYWORDS: Wireless Sensor Network, Paillier Cryptosystem

I. INTRODUCTION

Wireless sensor Network (WSN) could be a self-configure network of little sensor nodes, wherever the sensor nodes will communicate among themselves exploitation radio signals, and these device nodes will sense, monitor and understand the physical surroundings. It consists of spatially distributed sensors to watch physical or environmental conditions and to pass the information through the network to a destination location; the bi-directional fashionable networks alter to regulate the activity of the sensors. The event of the wireless device networks was motivated by military applications like battlefield surveillance and is additionally utilized in several industrial and client applications like process monitoring and management, machine health monitoring, etc. The WSN is constructed of "nodes", wherever one or a lot of device is connected to every node. Every device node accommodates many components, like radio transceiver with an interior antenna to an external antenna, microcontroller, electronic circuit for interfacing with the sensors and an energy supply sort of a battery. WSNs deployed at a large scale in a very distributed manner, and their information rates differs supported their applications, wherever the Wireless Medical device Networks have direct human involvement are deployed on atiny low scale should support quality (a patient will carry the devices), and WMSNs needs high information rates with reliable communication. Physiological conditions of patients are closely monitored by deploying Wireless medical device motes. These medical sensors are used to sense the patient's important body parameters and transmit the detected information in a very timely fashion to some remote location while not human involvement. Exploitation these medical device readings the doctor will get the main points of a patient's health standing. The patient's important body parameters embody heart beats, blood heat, pressure level, sugar level, pulse rate. WMSNs carry the standard of care across big variety of care applications. Additionally, alternative applications that additionally enjoy WMSNs embody sports-person health status watching and patients self-care. Many analysis teams and comes have began to develop health monitoring victimization wireless device networks. Wireless Medical care application offers variety of challenges, like, reliable transmission of information, secured knowledge

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

transmission, nodes quality, detection of event delivery of information in time, power management, etc. Deploying new technologies in care applications while not considering security typically makes patient privacy vulnerable; as an example, the patient's physiological important signals are very sensitive that the leakage of the patient's diseased information may makes the patient embarrassed. Generally revealing disease data will create it not possible for them to get insurance protection and additionally lead to someone losing their job. Further, wireless medical device networks cover a broad varies of care applications, like physiological information monitoring, activity monitoring in health-clubs, location tracking for athlete are the broad vary of care applications. WMSNs share individual information with physicians and insurance corporations. So unauthorized collection and use of patient information by adversaries will cause grave risks to the patient and create the patient's personal matters in public available. As an example, an easy state of affairs, a patient's body sensors transmit the body information to a nurse; the patient's privacy is broken once some aggressor is overhang dropping. Later that attacker will post the patient information on social web site and create risks to the patient's privacy. so wireless care can give several benefits to patient monitoring, however the medical health information of a private are highly vulnerable to various threats, therefore security and privacy become a number of the big issues for care applications, once it involves adopting wireless technology. A healthcare supplier is subjected to strict civil and criminal penalties if insurance portability and responsibility Act rules don't seem to be followed properly. So the safety and privacy of the sensed information is that the major concern in care applications.

II. RELATED WORK

A survey on secure healthcare monitoring exploitation wireless sensor networks was done by Kumar and Lee wherever they create use of trusty server protocol for key management. Trusty server based mostly scheme give stronger security, however in real time surroundings; it may become one purpose for the whole network failure. trusty server isn't suited for essential applications as a result of there could occur issues like providing less cupboard space, poor quantifiability, bottleneck drawback etc. so as to resolve this issue, the information is distributed across multiple servers to realize high scalability, providing a lot of memory than one server will give, improved load equalization and helps in avoiding bottleneck issues. D. Bogdanov, S. Laur, J. Williamson planned a Share mind system, that could be a virtual machine for privacy-preserving processing that rely on the shared computing techniques to guard the patient information. During this answer, the share mind system will protect the patient information privacy as long because the variety of the compromised information servers is at the most one. If 2 of the 3 servers are compromised by the within attack, the answer becomes insecure. A. Siva Sangari and J. Martin Leo Manickam planned light weight security and authentication in wireless body space network exploitation Skipjack, a secret key coding algorithmic program that gives the secure communication between sensing element node and mobile node. Skipjack could be a block cipher that supports a 64 bit block size and an 80 bit key. Since skipjack algorithmic program uses key length of eighty bits it's subject to brute force attack. In 2013, Dan Baehr et al. used TinyECC to secure the wireless communication between sensing element nodes, during a period sensor network. TinyECC could be a public key algorithm that uses Elliptic Curve Cryptography to unravel the problems of power consumption and slow processor speeds; however it will increase the scale of the encrypted message. The code algorithmic program is very complicated and harder to implement. J. Misić and V. Misić planned a way that depends on a Central trusty Security Server (CTSS) to demonstrate that participants belong to the actual patient's cluster and to come up with the session key. CTSS makes uses of central trusty security server that ends up in central purpose of failure and it's simple for the within attacker to hack the server. The energy-efficient access management theme supported code to beat security limitations like not providing mutual authentication and is strictly exposed to Denial-of-Service attacks is mentioned. Public-key cryptography primarily based on access management theme has a lot of advantages than symmetric-key cryptography based theme due to higher scalability, low memory demand, distribution of recent nodes simply, and no key pre-distribution. The limitation is that the sensor should commune with the Key Distribution Centre (KDC) to demonstrate the user and verify the access request. First, this needs an on-line KDC each time. Any failure of the KDC can result in major problem to the network. Secondly, interacting with the KDC needs a major further overhead to the network. The most aim of this paper is to forestall the within attack by distributing the patient information securely in multiple servers and to use the Paillier cryptosystem to perform datum analysis. During this paper, an efficient answer for privacy preserving WMSNs supported a symmetric key cryptosystem is enforced by advanced encryption standard (AES) algorithm.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

III. FRAMEWORK

This paper proposes an approach that provides high finish security for the patient’s sensitive physiological information and assures most privacy for the patients. This approach deals with the protection of information by using a cryptography mechanism known as Paillier cryptosystem that includes a distinctive homomorphic property of manufacturing the total of plaintexts whereas encrypting the merchandise of cipher texts. This mechanism is an important approach during this projected system. The design of projected methodology is shown in Figure one.

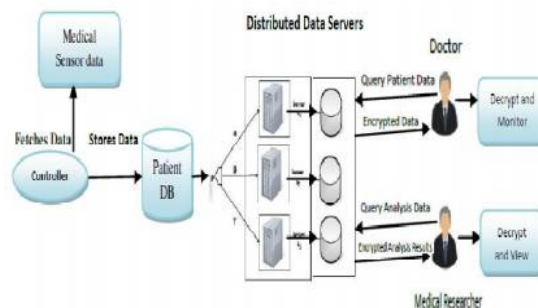


Figure 1: System design

Figure 1: System design the most focus of the projected system is securing the remote medical sensor data and acting applied math analysis on the received information. This technique makes use of 3 data servers to method the patients’ physiological information received from the bio sensors and stores the info in their various face databases for more query process. Like different tending applications, the projected system has four parts as follows. A wireless medical device network information server that stores the complete patient’s health information that’s received from the medical sensors and forwards the patient information to the patient’s information system; The information system of patients that is responsible to store the patient records and provides services for doctors or medical researchers to query the patient info system; an information access system for patients, that is used by the doctor to achieve access to the patient health records and endlessly monitor the patients remotely. An information analysis system for patients, to be employed by the medical scientist to perform applied math analysis on the patients’ information;

A. Data Collection Protocol

This is the primary readying innovate the projected system that is between the medical device information server and therefore the 3 knowledge servers that is handled by the controller. Here the 3 completely different secret keys are hardcoded into the 3 servers and within the controller system to transmit information securely. The controller splits the patient information (e.g., temperature reading) into 3 random elements exploitation the Split data rule and sends to a few information servers by encrypting with secret key based mostly AES rule. the initial worth of patient information ρ is split into 3 elements as, $\rho = \alpha + \beta + \gamma$ it shows that the initial worth is split into 3 elements α, β, γ specified their total equals the initial worth. This split part are 1st decrypted and keep by 3 information servers in their various databases. Here, SHA-3 hashing technique is employed to ascertain the authentication of the user.

B. Access control Protocol

This section is an initialization part before the doctors may gain access to the patient’s physiological information. during this section, 1st the general public and secret keys are generated for Paillier cryptosystem mechanism and Digital Signature rule is employed for making digital signatures to verify whether or not the doctor has the authority to achieve access to the patient information. Once the doctor queries the patient information, he has got to 1st submit his digital signature to the 3 data servers. The servers can verify the signatures and checks for the access management policies of the doctor. If he’s authorized then server SR1 picks a random worth r_1 happiness to the set of integers and encrypts the split worth α using Paillier encryption and sends C_1 to information server SR2. The data server SR2 picks a random worth r_2 belonging to the set of integers and encrypts the split worth β Paillier encryption and sends the product of C_1C_2 to the information server SR3. The data server SR3 picks a random value r_3 belonging to the set of integers and encrypts the split value γ using Paillier encryption and sends the product of $C_1C_2C_3$ to the doctor. The

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

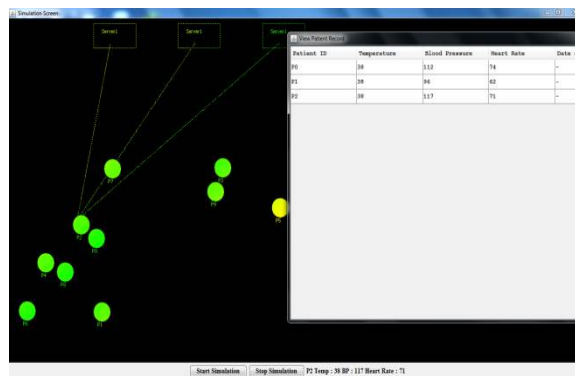
doctor will decrypt the information and acquire the worth $\rho = \alpha + \beta + \gamma$ wherever ρ is that the original patient health attribute value.

C. statistical Analysis Protocol

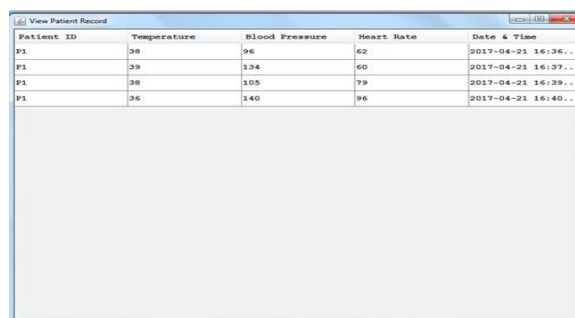
This section is used by the medical researchers who need to get the analysis results only. Varied analyses are performed like average analysis, variance analysis, correlation analysis and regression analysis. The medical researcher should 1st generate a digital signature and submit a question on that analysis he desires the servers to perform. When the 3 information servers receive the request, they 1st check for the authentication of the medical scientist and his access management policies. If the researcher is allowed, the 3 servers join forces to perform computations on the patient information and code the info exploitation Paillier secret writing theme as shown before and forward them to the researchers. When receiving the statistical analysis results, the scientist decrypts the information and views the analysis results.

IV. EXPERIMENTAL RESULTS

The planned technique is predicted to secure the patient physiological information throughout transmission and this solution is secure although 2 of the 3 information servers are compromised by the individual. That is, as long collectively of the 3 servers isn't compromised, the projected system assures high end security to the patients. In any of the server application, define access to login as admin and then create the users. The communications between the medical sensors and the three servers; the communications between the user (e.g., physicians or medical professional) and three servers; the communications among the three servers;



Add the users of access type either patient information retrieval or average analysis protocol. PIR will retrieve the specified patient information as shown below.



Patient ID	Temperature	Blood Pressure	Heart Rate	Date & Time
P1	38	96	62	2017-04-21 16:36...
P1	39	124	60	2017-04-21 16:37...
P1	38	105	79	2017-04-21 16:39...
P1	36	140	96	2017-04-21 16:40...

Average analysis protocol will average all the values for the patients as shown below.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Patient ID	Temperature	Blood Pressure	Heart Rate	Date & Time
P0	98	112	74	2017-04-01 16:30:00.0
P1	98	94	67	2017-04-01 16:30:04.0
P2	98	117	71	2017-04-01 16:30:08.0
P3	97	94	73	2017-04-01 16:30:09.0
P4	81	80	80	2017-04-01 16:37:03.0
P5	97	139	77	2017-04-01 16:37:18.0
P6	94	147	60	2017-04-01 16:37:17.0
P7	97	119	84	2017-04-01 16:37:24.0
P8	98	100	63	2017-04-01 16:37:31.0
P9	98	143	61	2017-04-01 16:37:38.0
P0	80	131	76	2017-04-01 16:37:45.0
P1	98	124	60	2017-04-01 16:37:52.0
P2	97	81	81	2017-04-01 16:38:00.0
P3	97	86	63	2017-04-01 16:38:07.0
P4	98	159	80	2017-04-01 16:38:14.0
P5	98	90	97	2017-04-01 16:38:21.0
P6	98	129	87	2017-04-01 16:38:28.0
P7	94	121	79	2017-04-01 16:38:35.0
P8	98	119	80	2017-04-01 16:38:42.0
P9	98	150	80	2017-04-01 16:38:49.0
P0	96	94	89	2017-04-01 16:38:56.0
P1	98	103	79	2017-04-01 16:39:03.0
P2	81	137	71	2017-04-01 16:39:10.0
P3	81	139	79	2017-04-01 16:39:17.0

V. CONCLUSION

We have surveyed differing kinds of security technique to secure the wireless medical sensor information. Here, we additionally planned the Paillier cryptosystem and ElGamal cryptosystem to encoding and coding of information. Planned resolution will preserve the patient information privacy as long together of 3 data server isn't compromised. Additionally needs that the amount of the compromised information servers is at the most one.

REFERENCES

- [1] 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, "A k-anonymity privacy-preserving approach in wireless medical monitoring environments," J. Personal Ubiquitous Comput., vol. 18, no. 1, pp. 61–74, 2014.
- [3] D. Bogdanov, S. Laur, and J. Willemsen, "Sharemind: A framework for fast privacy-preserving computations," in Proc. 13th Eur. Symp. Res. Comput. Security, 2008, pp. 192–206.
- [4] R. Chakravorty, "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.
- [6] J. Daemen, G. Bertoni, M. Peeters, and G. V. Assche. (2012, Jul. 6). Permutation-based encryption, authentication and authenticated encryption. Proc. Directions Authenticated Ciphers, Stockholm, Sweden [Online]. Available: <http://www.hyperelliptic.org/DIAC/slides/PermutationDIAC2012.pdf>
- [7] S. Dagtas, G. Pekhteryev, Z. Sahinoglu, H. Cam, and N. Challa, "Real-Time and secure wireless health monitoring," Int. J. Telemed. Appl., pp. 1–10, Jan. 2008.
- [8] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theory, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.
- [9] (2013, Jul.). Digital signature standard (DSS). FIPS PUB 186-4 [Online]. Available: <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>
- [10] 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.