Improving Robust Security for Distributing the Patient Data among Multiple Data Servers in Wireless Sensor Networks

Nikhila Reddy¹, Dr. S. Arvind², Dr. D. Baswaraj³

¹PG Student, ²,³Professor, Department of CSE, CMR Institute of Technology, Hyderabad (Telangana), India

Abstract—Recently, with the fast development and implementation of wireless medical sensors has gained increasing popularity. Monitor and record some important parameters of patients are of importance to understand the patient’s health condition. But malicious attacks happen sometimes, which can cause the patient-related information being leaked or changed. In this study, we tend to create a survey regarding some researches within the domain of privacy protection for information security and privacy problems and the privacy of the patient-related info keep within the information of the medical organization systems.

Keywords—Wireless Medical Sensor Networks (WMSNs), cryptosystem mechanism, Access Management Protocol, malicious attacks

I. INTRODUCTION

Wireless sensor Networks are widely utilized in medical fields that are observed as wireless medical sensor networks (WMSNs). The health care applications use medical sensors to sense the patient’s physiological information and transmit them wirelessly across the general public channels and store within the back-end databases. They’re thought of as promising fields where the patients will be monitored incessantly in hospitals and additionally reception. The physicians will monitor their patients remotely by accessing patients’ health information through wireless medical sensor networks. The medical researchers can use the health care application for his or her analysis purpose and perform applied mathematics analysis on patient physiological data. The patients’ information is transmitted to information server and hold on in some back-end systems. The patients’ privacy becomes vulnerable if the aid applications are deployed while not considering the safety. Therefore, a paramount necessity for aid application is security, notably within the account of patient’s privacy.

Wireless medical sensor networks once and for all are thought of as promising fields where the patients will be monitored in hospitals and additionally reception. The physicians will monitor their patients remotely by accessing patients’ health information through wireless medical sensor networks. The medical researchers can use the health care application for his or her analysis purpose and perform applied mathematics analysis on patient physiological data. The patients’ information is transmitted to information server and hold on in some back-end systems. The patients’ privacy becomes vulnerable if the aid applications are deployed while not considering the safety. Therefore, a paramount necessity for aid application is security, notably within the account of patient’s privacy.

II. SECURITY THREATS

Numerous security threats to health care applications that have an effect on patients’ information privacy are summarized as follows. Impersonation attack may be a threat to the credibility of patient’s information. During this application, a person would possibly impersonate a wireless access purpose, whereas information is being sent to an overseas location. As a result, this can cause false alerts and also the physicians may begin an emergency operation for a private who is non-existent. This will even defeat the rationale of wireless health care application. Eavesdropping may be a threat to the information privacy of patients once wrongdoer performs this kind of attack. A snoop may be equipped with intensively powerful receiving antenna and may retrieve the sensitive patient information from medical sensors and examines the patient’s health info. The listener would possibly even post the sensitive patient information on social networking sites that may be a real risk to patient privacy.

Modification may be a threat to the information integrity of patient data. The entrant will intercept the patient’s sensitive health information during transmission from the general public channels and perform some alterations on the information. This might be a threat to patients once this altered information is shipped to the doctors for watching that may lead to false readings. For instance, if a patient’s actual temperature reading is 1030 F and also the entrant alters it to some traditional temperature reading, the physician would possibly suppose that the patient’s health condition is traditional and doesn’t take any measures.

Data breach is once more a threat to the information privacy of patients. Information breach attack may be a state of affairs within which confidential patient health information has presumably been seen or utilized by a person who is unauthorized to try and do therefore. Considering an example, an information administrator who is malicious might retrieve the patient health information like his identity and residential address for his own advantage. He will claim insurance with the patient’s identity and additionally perform alternative medical frauds. Generally this kind of attack may also cause life threatening risk.
There are few additional security attacks on remote medical sensor networks like Sybil attack, grey-hole attack, denial of service attack, information spoofing etc.

In order to safeguard the patient’s remote medical sensor information against totally different attacks, the prevailing solutions are providing encryption primarily based approaches for information transmission. They embrace public key cryptography or secret key cryptography. In secret key primarily based mechanisms, it’s assumed that the parallel keys area unit pre-deployed in servers and sensors earlier. In this style of resolution, AES cryptosystem is employed for cryptography and Message authentication code for authentication. In public key primarily based mechanisms, RSA or Diffie-Hellman key exchange protocol is employed for generating secret keys and for cryptography.

The Paillier cryptosystem is employed for providing assured security for patient information throughout transmission. This cryptosystem has a new profit in its homomorphic properties wherever by providing only a group of plaintexts and also the public key parameters, the merchandise of the plaintexts is achieved. On the decrypting facet, the user will rewrite the received information and obtain the total of the plaintexts. Paillier cryptosystem will be helpful for those applications which require high of the road security and summation of the set of plaintexts. The existing solutions will give privacy to the patients’ information by making certain protection against outside attacks however fails to provide protection against the within attacks. A number of the prevailing solutions don’t give security in any respect and a few solutions do give security for the information transmitted over channels. The prevailing resolution deals with security of patient data by victimization 3 servers to store patient info. They split the received information from sensors into 3 elements and sends to a few servers employing a secure channel wherever the key keys area unit pre-deployed in sensors and servers. This solution will give protection to the sensitive patient information as long as only 1 information server is compromised. If the attacker is productive in compromising 2 of the 3 information servers then the prevailing resolution may be a failure.

The projected system provides a sensible approach to overcome this issue and additionally provides protection against within attacks. In the proposed system, although the attacker is productive in compromising 2 of the 3 information servers, the solution remains secure.

II. RELATED WORK

A survey on secure health care observation victimization wireless sensor networks was done by Kumar and Lee wherever they create use of sure server protocol for key management. Sure server primarily based scheme provide stronger security, however in real time setting, it might become one purpose for the complete network failure. Sure server isn't suited to essential applications as a result of there could occur issues like providing less space for storing, poor measurability, 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 leveling and helps in avoiding bottleneck issues.

D. Bogdanov, S. Laur, J. Williamson projected 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 data. During this resolution, the share mind system will defend the patient knowledge privacy as long because the range of the compromised knowledge 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 projected light-weight weight security and authentication in wireless body space network victimization Skipjack, a secret key encoding formula that gives the secure communication between sensor node and mobile node. Skipjack could be a block cipher that supports a 64 bit block size and a eighty bit key. Since skipjack formula 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, in an exceedingly time period sensing element network. TinyECC could be a public key formula that uses Elliptic Curve Cryptography to unravel the problems of power consumption and slow processor speeds; however it will increase the dimensions of the encrypted message. The computer code formula is extremely advanced and tougher to implement.

J. Misic and V. Misi projected a way that depends on a Central sure Security Server (CTSS) to demonstrate that participants belong to the actual patient’s cluster and to get the session key. CTSS makes uses of central sure security server that results in central purpose of failure and it's straightforward for the inside attacker to hack the server.
The energy-efficient access management scheme supported ECC to overcome security limitations like not providing mutual authentication and is strictly exposed to Denial-of-Service attacks is mentioned in Public-key cryptography primarily based access management scheme has a lot of edges than symmetric-key cryptography based theme due to higher measurability, low memory demand, distribution of recent nodes simply, and no key pre-distribution. The limitation is that the sensing element should communicate with the Key Distribution Centre (KDC) to demonstrate the user and verify the access request. First, this needs an on-line KDC anytime. Any failure of the KDC can result in major problem to the network. Secondly, interacting with the KDC needs a significant additional overhead to the network. The main aim of this paper is to stop the within attack by distributing the patient knowledge firmly in multiple servers and to use the Paillier cryptosystem to perform data point analysis. During this paper, an efficient resolution for privacy conserving WMSNs supported a cruciate key cryptosystem is enforced by advanced encryption standard (AES) formula.

III. FRAME WORK

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 employing a cryptography mechanism known as Paillier cryptosystem that incorporates a unique homomorphic property of manufacturing they add of plaintexts whereas encrypting the product of cipher texts. This mechanism is a necessary approach during this projected system. The design of projected methodology is shown in Figure 1.

![Figure 1: System Architecture](image)

The main focus of the projected system is securing the remote medical sensor information and acting applied mathematics analysis on the received information. This method makes use of 3 information servers to method the patients’ physiological information received from the bio sensors and stores the information in their various rear databases for more question process. Like other healthcare applications, the projected system has four elements as follows.

- A wireless medical sensor network information server that stores the whole patient’s health information that’s received from the medical sensors and forwards the patient information to the patient’s info system.
- The Info system of patients that is accountable to store the patient records and provides services for doctors or medical researchers to question the patient info system.
- An information access system for patients that is employed by the doctor to realize access to the patient health records and endlessly monitor the patients remotely.
- An information analysis system for patients, to be utilized by the medical research worker to perform applied mathematics analysis on the patients’ information.

A. Information Assortment Protocol

This is the primary preparation innovate the projected system that is between the medical sensor information server and therefore the 3 data servers that is handled by the controller. Here the 3 totally different secret keys square measure hardcoded into the 3 servers and within the controller system to transmit information firmly. The controller splits the patient knowledge (e.g., vital sign reading) into 3 random components exploitation the Split Information algorithmic rule and sends to a few information servers by encrypting with secret key based mostly AES algorithmic rule. The initial worth of patient information ρ is split into 3 components as,

$$\rho = \alpha + \beta + \gamma \quad \ldots \ldots \quad (1)$$

Equation (1) shows that the initial worth is split into 3 components α, β, γ such they add equals the initial worth. This split half are initial decrypted and hold on by 3 information servers in their various databases. Here, SHA-3 hashing technique is employed to envision the authentication of the user.
B. Access Management Protocol

This phase is an initialization section before the doctors might gain access to the patient’s physiological knowledge. In this phase, initial the general public and secret keys are generated for Paillier cryptosystem mechanism and Digital Signature algorithm is employed for making digital signatures to verify whether or not the doctor has the authority to realize access to the patient information. Once the doctor queries the patient information, he has got to initial submit his digital signature to the 3 information servers.

The servers can verify the signatures and checks for the access management policies of the doctor. If he is authorized then server SR1 picks a random value r1 happiness to the set of integers and encrypts the split worth α using Paillier secret writing and sends C1 to knowledge server SR2. The information server SR2 picks a random worth r2 happiness to the set of integers and encrypts the split worth β Paillier secret writing and sends the merchandise of C1C2 to the information server SR3.

The data server SR3 picks a random worth r3 happiness to the set of integers and encrypts the split worth ϒ victimization Paillier encryption and sends the merchandise of C1C2C3 to the doctor. The doctor will decode the information and procure the worth \( \rho = \alpha + \beta + \Upsilon \) wherever \( \rho \) is that the original patient health attribute worth.

C. Applied Mathematics Analysis Protocol

This section is employed by the medical researchers WHO need to get the analysis results only. Numerous analyses are performed like average analysis, variance analysis, correlation analysis and multivariate analysis. The medical researcher ought to initial generate a digital signature and submit a question on that analysis he needs the servers to perform. When the 3 information servers receive the request, they initial check for the authentication of the medical researcher and his access management policies. If the research worker is allowed, the 3 servers work to perform computations on the patient information and inscribe the information victimization Paillier secret writing theme as shown before and forward them to the researchers. When receiving the statistical analysis results, the research worker 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. This answer is successful in providing protection against outside attacks and additionally within attacks wherever the malicious administrator of the information of patients might capture the patient health information and perform medical frauds for his personal benefits. Therefore the planned system accomplished to produce patient privacy victimization the Paillier cryptosystem mechanism.

V. Conclusion

Providing security and privacy of Medical information is achieved by keeping the patient information in 3 Servers wherever sensitive information are keep in encrypted format and it's shared with approved users only. Secure the communication between medical sensors and information servers, we used the light-weight encoding scheme and mac generation scheme supported SHA-3 proposed.

Acknowledgement

We thanks to all concerned authors, research scholars referred in this paper for accessing useful information.

REFERENCES


