Cloud Based Healthcare Management System using Wireless Medical Sensors

Rajashree Sonawane¹, Nikita Patil⁴, Priyanka Pujari³, Abhilasha Shahane², Sudhir Salunkhe⁵

Student¹,²,³,⁴, Assistant Professor⁵

Department of Information Technology
Rajarshi Shahu College of Engineering, Tathawade, Pune, India

Abstract:
Medical service applications unit are promising fields for remote device systems, where patients could also be checked by utilizing remote restorative device systems as Wireless Medical Sensor Networks (WMSNs). Ebb and flow WMSN welfare investigates patterns, target patients, solid correspondence, quiet state, and vitality skilled guiding, as some precedents. Because of which it is causing new advancements in human service applications whereas, not considering the security that makes persistent protection helpless. Additionally, the physiological information of a private unit is very sensitive. Hence, security could also be a foremost necessity of welfare applications, notably on account of patient’s information protection, when the patient is suffering from a very serious health issues. This venture talks about protection issues in human service applications utilizing WMSNs. Here it is very important to protect the private information of patients who are suffering from a serious health issues. This information is handled by many authorities who are responsible for maintaining, recording, organizing this patient's information where this data can be easily leaked for any intended harm. So we have an intention to protect this valuable data which keeps within assault by utilizing different knowledge servers to store a lot of information. The principle commitment of this paper is to disperse patient's knowledge safely in varied knowledge servers and enjoying out the Pillar cryptosystems to perform measurable investigation on the patient knowledge considering patient's protection.

Keywords: Wireless medical sensor network, patient data privacy, Pillar encryption, healthcare management system.

I. INTRODUCTION

A wireless sensor cloud is a cloud to monitor physical or environmental conditions such as temperature, sound, pressure, etc. In human healthcare, sensors are used to monitor the patients’ health status such as temperature level, sugar level, heart beat rate, blood pressure[4]. For instance, if the patient’s sugar level is monitored 10 times per day then the data is updated in the database which is present in the local server. Likewise, the values for blood pressure, heart beat, and temperature are also noted at regular intervals. There are many security issues such as data stealing, stealing and updating, storing the wrong values. Suppose if the intruder is trying to hack the patient details, there are many chances for the misuse of data which may lead to severe consequences. The data can also be modified by the hackers due to lack of security [6]. The treatment prescribed by the doctors can be hacked which may even lead to death of the patients. To prevent these issues, the intrusion detection system is proposed. An intrusion detection system is a system used to check the malicious activities and produces electronic reports to a management station. It consists of Pillar algorithm key cryptosystems[2]. The algorithm is used to encrypt the patient details before storing it in the database and perform decryption when needed by the physician[2]. Similar to cloud computing, healthcare cloud computing has different issues related to its security, the most important of which are: legal and policy issues, data protection, privacy protection, lack of transparency, cyber security issues, absence of security standards, and software licensing. The challenges related to cloud computing’s legal and policy issues are: liability, applicable law, compliance, copyright, data portability, and data protection. At the end, to define the relations between consumers, utilities, and third parties in the cloud, a proper policy needed in order to make sure that the cloud computing is secure. 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[2]. 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. Physiological conditions of patients are closely monitored by deploying Wireless medical device motes[5]. 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. Wireless Medical care application offers variety of challenges like, reliable transmission of information, secured knowledge[2].

II. PROBLEM DEFINITION

Development of a wireless healthcare application offers many novel challenges such as reliable data transmission, timely delivery of data, power management, node mobility support and fast event detection node computation and middleware. Further however deploying new technologies in healthcare applications without considering security often makes patient privacy unsafe.
III. LITERATURE SURVEY

1. “Sharemind: A framework for fast privacy-preserving Computations (2008).” Authors: Dan Bogdanov, Sven Laur1, and Jan Williamson

Through this paper, we present a provably secure and efficient general-purpose computation system to address this problem. Our solution for SHAREMIND is a virtual machine for privacy-preserving data processing that relies on share computing techniques. This is a standard way for securely computing functions in a multi-party computation environment. New features of our solution is in the choice of the secret sharing scheme and the design of the protocol suite. We have made many practical resolutions to make large-scale share computing feasible in practice. The protocols of SHAREMIND are information theoretically secure in the honest but curious model with three computing participants[1].

2. “SURVEY ON, ENSURING SECURITY TO THE WIRELESS MEDICAL SENSOR DATA” Authors: Kiran More, Prof. Jyoti Raghatwan.

A lot of work have been done to secure wireless medical sensor networks. The present solution can protect the patient data during communication, but cannot stop the inside attack wherever the administrator of the medical database reveals the sensitive patient data. Here we propose a system to prevent the inside attack by using several data servers to store patient data. Our main role is securely distributing the patient data in numerous data servers by using the Pillar and ElGamal cryptosystems to perform statistic analysis on the patient data without compromising the patient’s privacy[2].


Through this paper, we propose a lightweight and secure system for MSNs. It shows hash-chain based key updating mechanism and proxy-protected signature technique to achieve proficient secure transmission and attribute based encryption with fine-grained data access control. Furthermore, we extend the system to provide backward security and privacy preservation. Our system only requires symmetric-key encryption/decryption and hash operations and is thus suitable for the low-power sensor nodes. Also, from this paper we report the experimental results of the proposed system in a network of resource-limited motes and laptop PCs, which show its efficiency in practice[3).


We know that wireless medical sensor networks are more exposed to eavesdropping, modification, imitation and replaying attacks than the wired networks. A lot of work have been done to secure wireless medical sensor networks. Obtainable solutions can protect the patient data during communication, but cannot stop the inside attack where the administrator of the medical database reveals the sensitive patient data. Through this paper, we propose a practical approach to avoid the inside attack by using multiple data servers to store patient data. Key aspect of this is securely distributing the patient data in multiple data servers and employing the Pillar and ElGamal cryptosystems to perform statistic analysis on the patient data without compromising the patient’s privacy[4].


Deliver a healthcare monitoring system coupled with wearable sensor systems and an environmental sensor network for monitoring mature or chronic patients in their residence. This system, built in a fabric belt, containing various medical sensors that collect a suitable set of physiological healthcare indicators transmitted via low energy wireless communication to mobile devices. In this, three application scenarios are implemented using the proposed network architecture. In this group based data collection and data shows using the ad hoc mode promote outpatient healthcare services for only one medical employee assigned to a set of patients[5].


In this paper we discuss the security and privacy issues in healthcare application using WMSNs. Also, we highlight some popular healthcare projects using wireless medical sensor networks, and discuss their security. In this our aim is to discussion on these critical issues since the success of healthcare application depends directly on patient security and privacy, for ethic as well as legal reasons. Also, we discuss the issues with existing security mechanisms, and sketch out the important security requirements for such applications. In addition to the paper reviews accessible schemes that have been recently proposed to provide security solutions in wireless healthcare scenarios

IV. EXISTING SYSTEM

The security may be a dominant demand of attention applications, particularly within the case of patient privacy, if the patient has associate degree embarrassing unwellness. This project discusses the protection and privacy problems in attention application victimization WMSNs. we have a tendency to highlight some standard attention comes victimization wireless medical sensing element networks, and discuss their security the present systems solutions will merely defend the patient information throughout transmission, however cannot defend the within attack wherever the administrator of the patient information reveals the sensitive patient information[6].

Disadvantages of Existing System

1. Less secure.
2. Cannot defend within offender.
3. If any hacker get information from one dB server then whole information are going to be got to hacker.

V. HEALTHCARE MANAGEMENT SYSTEM

To prevent the patient info from the inside attacks, we tend to propose a fresh data assortment protocol, where a device splits the sensitive patient information into three components in line with a random vary generator supported hash performs and sends
them to three servers, respectively via secure channel [1]. To keep the privacy of the patient information, we tend to propose a protocol on the idea of the Pillar cryptosystem[2]. The protocol permits the user (e.g. physician) to access the patient information whereas not revealing it to any data server. To preserve the privacy of the patient data in applied mathematics analysis, we tend to propose some new privacy-preserving applied math analysis protocol on the thought of the Pillar cryptosystems [2]. These protocols allow the user (e.g., medical researcher) to perform applied math analysis on the patient data while not compromising the patient information privacy.

### Advantages of healthcare management system
1. Practical approach to prevent the inside attack by securely distributing the patient data in multiple data servers.
2. In Proposed system, Due to secured distributed database architecture we can achieve data storage & data analysis security.
3. Proposed data retrieval technique allows retrieving the data compromised server(s)

#### VI. SYSTEM ARCHITECTURE

**Figure.1. Proposed System Architecture**

**System Analysis:**
Physiological conditions of patients are closely monitored by deploying Wireless medical sensor motes[4][3]. These medical sensors are used to sense the patient’s vital body parameters and transmit the sensed data in a timely fashion to some remote location without human involvement. Using these medical sensor readings the doctor can get the details of a patient’s health status. Wireless Medical healthcare application offers a number of challenges, like, 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 at risk. To avoid the patient information from the within attacks, we have a tendency to propose a replacement information assortment protocol, wherever a device splits the sensitive patient information into 3 parts [1] according to a random number generator based on hash function and sends them to three servers, respective, via secure channels. 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[3]. 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[4].

### VII. ALGORITHMS

A) Paillier Public-Key Cryptosystem:
This is composed of key generation, encryption and decryption algorithms as follows.
1) Key generation
Select two large prime numbers $p$ and $q$ randomly and independently of each other such that: $\text{gcd}(pq,(p - 1)(q - 1)) = 1$
Compute: \( N = pq, \lambda = \text{lcm}(p-1, q-1) \)
Where \( \text{lcm} \) stands for the least common multiple.
Select random integer \( g \) where \( g \in \mathbb{Z}_N^* \) and ensure \( N \) divides the order of \( g \) by checking the existence of the following modular multiplicative inverse:

\[
\mu = \left( L \left( g^\lambda \pmod{N^2} \right) \right)^{-1} \pmod{N}
\]
where function \( L \) is defined as: \( L(u) = \frac{u-1}{N} \)
The public (encryption) key \( \text{pk} \) is \((N,g)\).
The private (decryption) key \( \text{sk} \) is \((\lambda,\mu)\).
If using \( p,q \) of equal length, one can simply choose
\[
g = N + 1, \lambda = \varphi(N)^{-1} \pmod{N}
\]
where \( N = pq \) and \( \varphi(N) = (p-1)(q-1) \)

2) Encryption:
Let \( m \) be a message to encrypt, where \( m \in \mathbb{Z}_N^* \)
Select random \( r \) where \( r \in \mathbb{Z}_N^* \)
Compute ciphertext as:
\[
C = g^m \cdot r^\lambda \pmod{N^2}
\]

3) Decryption:
Let \( c \) be the ciphertext to decrypt, where the ciphertext:
\( c \in \mathbb{Z}_N^* \).
Compute the plaintext message as:
\[
m = \left( c^\lambda \pmod{N^2} \right) \cdot \mu \pmod{N}
\]

VIII. KEY CHALLENGES
Some of the threats that are harmful to the wireless medical sensors networks are:
Modification of data – Here the attacker can change or remove part of the information that is obtained. The changed data is then sent back to the receiver. Changing in the health data may lead to serious problems.
Data Breach – Threat to the patient’s data privacy where an unauthorized user gets access to the data is called as data breach.
Eavesdropping – Eavesdropping is where, the attacker uses powerful receiver antennas and obtains the sensitive information from the channel and can misuse it. Also, a risk to the data privacy.
Replaying – After the eavesdropping, the information that is obtained is sent back to the sender stating for a different purpose by the attacker.

IX. MOTIVATION
In a wireless medical sensor cloud, 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 cloud. Some work has been done to secure the wireless medical sensor cloud using efficient symmetric key cryptosystems. Any type of efforts can protect the patient data during transmission, but cannot stop the inside attack where the administrator of the medical database reveals the sensitive patient data[3]. To avoid the inside attack, more advanced cryptographic techniques, such as attribute based encryption. Though, an unauthorized person may use the patient data (such as, patient identity) for their personal benefit, such as for fraudulent insurance claims, medical fraud, and sometimes this may even pose life-threatening risks[6]. This motivate us to provide security to Patient Medical data when data is share on distributed system.

X. CONCLUSION
We have investigated the safety and privacy problems inside the medical detector data assortment storage and queries. Based upon which we have given a complete resolution for privacy-preserving medical detector network through the ad-hoc network. To retain the privacy of the patient data, we tend to project a current data assortment protocol that splits the patient data into three numbers and stores them in three data servers, serially. As long as joined data server is not compromised, the privacy of the patient data are preserved. For the legitimate user e.g. doctor to access the patient data, we tend to projected associate access management protocol, where three data servers work to produce the patient data. Simply just in case any two of three server’s square measure compromised the protected system provides a proxy based totally data retrieval system.

XI. REFERENCES
[2]. “A survey on provide security to wireless medical sensor data” Authors: Kiran More, Prof. Jyoti Raghavtwan. e-ISSN: 2395 -0056.
[4]. “Privacy Protection for Wireless Medical Sensor Data” Authors: Xun Yi, Athman Bouguettaya, Dimitrios Georgakopoulos, Andy Song and Jan Willemsen. 1545-5971 (c) 2015 IEEE.