Secure Healthcare Information Communication over Internet under patient-cloud communication model

Lovepreet Kaur¹, Manish Mahajan²
¹Research Scholar, CSE Deptt, CGC College of Engineering, Mohali
²Head of Department, CSE Deptt, CGC College of Engineering, Mohali

Abstract

The healthcare networks consist of the wireless sensors to monitor the patient's health, hence called wireless body area networks (WBANs). The healthcare networks carry the information of many patients. The information privacy becomes the primary concern for the healthcare networks. The privacy concerns raise various issues which includes the information alteration attacks leading to threat. The information alteration (like replay attack) attacks can change the healthcare emergency decisions by changing the patient information on the cloud based healthcare information model. In this paper, we have proposed a novel key exchange algorithm to enhance the level of privacy in the cloud based healthcare model. The proposed key management model is a lightweight crypto key exchange with quick response key model. The key model has been proposed to be used between the patient-cloud communications. The data privacy and confidentiality is protected by exchanging the key in the periodic fashion. The proposed model has been evaluated on the basis of various performance parameters of probability of key exposure and probability of key connectivity. The experimental results have shown the effectiveness of the proposed model.

Indexing terms/Keywords

Data Transmission time; Electrocardiogram signal; Key Management; Data privacy; Electronic Health Records

INTRODUCTION

An old age group is currently the main medicinal services concern of numerous nations on the planet. Aged patients require more healthcare facilities and efforts as they are at a stage more prone to chronic illnesses leading to greater medical costs. E-Health frameworks in view of present day data innovation are relied upon to assume a part in reducing this issue. Luckily, there have been dramatic advances in healthcare technology in terms of portability, miniaturization, speed and communication [2]. The objective of embedding medical applications to cloud computing is to reduce the restraints of traditional medical data dealing (e.g., limited physical storage, threats against security and privacy of personal data). Mobile healthcare presents mobile users the quick connectivity to medical servers for accessing resources (e.g., patient health records) simply and proficiently. Besides, m-healthcare offers hospitals and healthcare organizations a variety of on-demand services on clouds rather than owning standalone applications on local servers [3]. These little wearable devices, possessing limited energy capabilities and memory-vitality, are persistently checking key signs, for example, temperature, blood pressure, electrocardiogram signals (ECG), EEG signals, diabetic levels. However, the gathered samples of such signals can be valuable for analysing, checking, detecting, reacting, conveying to patients or doctors and other different exercises [11]. Initially, some kind of pre-handling processes like noise reduction, enhancement, data assignment, and duplicity check must be performed on the raw data collected through sensors implanted to patients. Secondly, the collected data must be categorised priority wise on the basis of vital signs from various body destinations on a patient and from numerous patients regarding their level of significance to avoid system activity clogging and to expand reliability. Thirdly, the collected vital signs are stored to cloud or central server for analysis through computation-models to get meaningful measure of patient’s health status. For example, ECG signal based on time or frequency domain analysis is a source of heart rate variability (HRV) parameter. HRV is of more prominent concern to doctors than the ECG signal as it indicates the inflated danger of cardiovascular ailments and untimely mortality as well as biological aging.

1.1. Motivation

The motivation of this effort trunks from the fact that though major work has been done to integrate the traditional healthcare services with Information and Communication Technology (ICT) infrastructures to provide e-health care service solutions yet these solutions are not much viable. There is a large scope to work on the interface of them in order to provide secure transmission of data [13]. Furthermore, ICTs infrastructures incur heavy costs installation, processing, storage, power consumption. So, cloud computing, in contrast, eliminates the need of customer to invest high on hardware computing infrastructures and provides facility of pay-per-use.
1.2 Security Issues

Security issues are of great concern when a healthcare provider shifts the medical data to Cloud-based Electronic Health Record system. The health care provider has to convince the patients about the security of their personal data by guaranteeing that the Cloud platform has the required security set up [10]. The basic building blocks of security are confidentiality, integrity and privacy; thus every secure system is built keeping in mind these basic security aspects. These basic and mandatory parts of security are important for securing data, hardware and software assets. The cloud framework proposes remarkable security challenges which should be considered in subtle elements:

Confidentiality: Confidentiality signifies that only legal parties or systems have the permission to retrieve protected data. Due to large number of people accessing cloud services and applications, the threat of data breach rises in the cloud. Various issues like multi-tenancy, application privacy and security, data remanence etc. covers the concept of confidentiality [9]. Multi-tenancy points towards the resource sharing pool of cloud computing such as memory, applications, networks and information. Cloud computing provides the facility that multiple users use the same resource at the system level, software level, and application level. In spite of the fact that clients are confined at a virtual level, equipment is not isolated. In a multitenant framework, a product application is intended to practically segment its information and setup so that every customer association meets expectations with a modified virtual application occasion. Multi-tenancy is compared to multitasking in operating systems. Multitasking, in cloud computing, refers to multiple tasks, such as processes being executed while sharing common processing resources such as a memory, CPU cycles. Multi-tenancy leads to a number of privacy and confidentiality threats. Cloud infrastructures are based on principle of object reusability, but reusable objects are very sophisticated to handle. Information privacy could be ruptured inadvertently, because of information remanence. Information remanence is the remaining representation of information that have been somehow ostensibly deleted or evacuated. Because of virtual detachment of legitimate drives and absence of equipment partition between numerous clients on a solitary framework, information remanence may prompt the unwilling exposure of private information. User authentication is required for protecting a user’s account against theft similarly data confidentiality is required for monitoring access to objects in cloud infrastructure such as memory, devices, software, network etc. Electronic authentication is a means of authenticating the user identity electronically to an information system. There is strong need of authentication because unauthorized access can lead to privacy breach into users account on a cloud. Software confidentiality is a major counterpart of data confidentiality for the security practice. In a cloud environment the client has to trust the security applications provided by the cloud owning organisation. Software applications dealing with user’s personal data must be certified. Also, the cloud supplier is in charge of giving secure cloud patterns, which ought to guarantee clients protection.

Privacy: Privacy is required to control the revelation of individual data. Associations managing individual information are obliged to obey to a nation's legitimate structure that guarantees suitable security and privacy insurance. The cloud exhibits various lawful difficulties towards security issues included in information put away in numerous areas in the cloud, also expanding the danger of confidentiality and privacy breach. Rather than its information being put away on the organization’s servers, information is stored on the cloud provider’s servers, which may be in Finland, China, or anywhere in the world. This fundamental of distributed computing clashes with different lawful necessities, for example, the Asian laws states the right of an association to know the location of individual information collected by them is lying at all times.

Integrity: Another important aspect of Data Security is integrity. Integrity implies that assets (data, hardware, software) can be modified, updated or deleted only by authorized users. Data Integrity means to protect the deletion, fabrication or modification of data from unauthorized parties. Setting proper access permissions (read, write) for entity’s admittance are
valuable against misappropriated or stolen data and services. Furthermore, such procedures also offer the discemibility of regulating who, when or what have altered data or system. Authorization is the mechanism set by the system administrative for controlling what level of access should be allocated to a particular authenticated user in order to secure resources. Because of large number of users and access points in a cloud environment, authorization is pivotal in guaranteeing that just approved elements can communicate with information. A distributed computing supplier is trusted to keep up information honesty and precision. The cloud model introduces various dangers including modern insider attacks on these information qualities. Software Integrity means protecting any unauthorized deletion, modification, or fabrication of any program in software. Deletion, modification or fabrication can be deliberate or accidental. For example a disappointed representative may deliberately change a program to come up short when certain conditions are met or when a certain time limit is crossed in order to take revenge of disgruntled. Cloud computing provides a software interface or Application Interface for customers to interact with cloud facilities. The security of application interface is also of major concern in security of cloud services because an unauthorized user can gain control over interface and alter or fabricate the incoming/outgoing data to cloud. Again the responsibility of software’s integrity lies with cloud owner or administrator. Similarly the issue of hardware and network integrity needs to be addressed by the cloud provider, as he has the control over underlying hardware and network channels.

**Figure 2: Basic security mechanisms for security of data in cloud healthcare environment**

1.4 Paper organization

The rest of the paper is structured as follows: Section 2 outlines the related work. An architectural outline of our proposed Healthcare Information Privacy and Integrity Protection Algorithm (HIPIPA) is described in Section 3 followed by implementation and performance aspects in Section 4; Section 5 concludes the paper.

RELATED WORK

The swift load move to the clouds has put major concern issues towards the success of communication and information security. From a security point of view, large number of challenges has been encountered regarding the privacy of data, security of servers, confidentiality, integrity etc. There is a need of pre-distribution key mechanism. Vishwanathan et al. [11] presented an innovative platform for organizing and harnessing the computing capabilities (power, CPU utilization, bandwidth, memory) of ubiquitous devices such as laptops, desktops, tablets, PDAs, DVRs, medical terminals etc. in home and hospital settings. The author discussed various optimized communication solutions as well as algorithms required for the transmission of vital signs. The proposed framework deals with vital sign monitoring using controlled sensors, the monitoring of data is real-time processing to obtain meaningful physiological parameters such as pulse rate, diabetic level etc. Burns et al. [1] introduced “Sensing Health with Intelligence, Modularity, Mobility and Experimental Reusability” (SHIMMER)—an open source, expandable, patient monitoring and diagnostic sensing platform equipped with power management hardware, supports a library of applications. The subsequent SHIMMER wireless platform leads many other medical research platforms and is used widely in almost 30 countries comprising prominent universities and research and development organizations. Chan et al. [2] discussed the drawbacks occurring in e-Health monitoring systems because it is constrained with patients in smart rooms fitted with monitoring devices. Such monitoring is not well-worth in view of the flexibility and mobility issues regarding patients. The authors proposed a multi-agent framework for ECG and weight monitoring supporting mobility of patients, including a group of intelligent agents that collects and organizes the patient data and recommend actions to patients and medical staff. The e-Health sensors communicate using Bluetooth technology with GSM mobile phones. The software was developed over Symbian operating
Zhang et al. [12] discussed the major security requirements, models, and access management for EHR in healthcare application clouds and presented an EHR security reference model for securing an EHR cloud. Finally, the authors demonstrated the effectiveness of EHR security reference model via a use-case scenario and described the other security countermeasures and future scope of security techniques. Zissis et al. [14] firstly evaluated the main cloud security requirements and then tried to present a practical solution to eliminate these potential threats. The authors introduced a Trusted Third Party concept, guaranteeing particular security attributes inside of a cloud situation, built upon cryptography, Public Key, Hash functions to guarantee an authentic, integrity and confidential data and communication. The arrangement exhibits a flat level of administration, accessible to every authentic entity. Fatemi et al. [4], [7] proposed an encryption based security model for cloud server and client based sensors for growing the reliability of cloud computing. In this model, the key generation is done through cloud application and public and private keys are stored in cloud servers. Besides, the encryption and decryption is performed in client window. For choosing the best fit encryption algorithm among various encryption algorithms, a comparative study was concluded by analyse the strength and weakness of well-liked asymmetric key encryption algorithms (RSA, MD5) on the basis of time, key size, rounds and overall performances. Kaur et al. [6] proposed a “Cloud based Intelligent Health Care Service” (CBIHCS) for performing real-time monitoring of diabetic patients, data collected through wireless sensor equipment’s. Principal Component Analysis algorithm was applied for attribute selection. K-NN, having high success rate for identifying diseases in real-life scenario, is used along Naive Bayes for user health status grouping as diabetic and Non-diabetic. Experimental results of application performance are demonstrated over Amazon EC2. An economical, handy health care solution thus becomes accessible through CBIHCS.

PROPOSED SCHEME

The intended scheme is especially proposed for cloud-based healthcare sensor networks. The heart rate is computed on the Holter device and forwarded to the cloud healthcare record management server. The data communication between Holter and cloud healthcare records management server must be secured to protect the privacy of the user data for any data forgery attacks. Such data forgery attacks can be intimated for information falsification or fabrication, which can affect the health service decision in the critical condition. If the hacker will update and forward the data as normal heart rate using the replay attack with information fabrication, when the original patient information is showing the critical level heartbeat, the cloud-based healthcare record management service will not raise alarm for patient’s critical situation. So, there is a strong need to authenticate the sensors who update the patient data to cloud server. The following mechanism has been proposed for the purpose of secure information exchange using the combination of key exchange and information encryption methods.

Algorithm 1: Healthcare Information Privacy and Integrity Protection Algorithm (HIPIPA)

1. Collect the ECG signal using Holter from the Patient’s body
2. Compute the heart beat rate using the built-in ECG evaluation module
   a. Input ECG signal
   b. Neutralize the signal noise from the ECG signal
   c. Remove the baseline drift from the ECG signal
   d. Input the data record interval \( t \) to track (standard between 0.4s to 1.2s with step size of 0.02) [For Physionet Datasets]
   e. Input the sampling frequency \( f_s \)
   f. Prepare the signal index by calculating the interval over frequency
   g. Find the autocorrelation on the signal using the formula below:

   \[
   r_k^n = \frac{\sum_{t=k+1}^{n} (y_t - \bar{y})(y_{t-k} - \bar{y})}{\sum_{t=1}^{n} (y_t - \bar{y})^2} \quad (1)
   \]
   h. Sum of the detected peaks with adjusted according to the interval continuity gives the heart beat rate.
3. Encrypt the data using the data encryption module on Holter using the 128-bit block with 128-bit key under 9-round encryption.
4. The Holter sends the data send request to the cloud server during the initial phase of the communication.
5. The cloud healthcare management service (CHMN) approves the clients after verifying their legitimacy. The connection request is denied if the client is not found legitimate. The cloud approves the legitimate users with the approval accepted acknowledgement (APACA).

6. If holter receives the APACA, it selectively forward the heartbeat rate pre-calculated and encrypted over the given network.

7. Server decrypts the patient information on arrival and updates its appropriate record.

8. After the authorized session time expires, the CHRMS sends the question key to the holter.

9. Holter replies with appropriate answer key

10. CHRMS verifies the key and re-authorize the communication if key matches successfully and terminate otherwise.

**PERFORMANCE ANALYSIS**

Various secure and reliable key agreement schemes for healthcare sensor network authentication such as q-composite scheme, E–G scheme, Liu's and Zhou’s schemes, has been projected, centred around symmetric polynomials [5]. The proposed model is based upon the strong and flexible cryptographic key management scheme for healthcare networks.

![Figure 3: Calculation of Key connectivity at deployment](image)

The proposed model is improvising the fast key exchange scheme with the higher order of security levels for the protection of the data confidentiality and privacy. The alteration attacks must be protected in order to secure the patient information. The alteration or replay attacks can be used to influence the healthcare organization decision for the specific patients, which can badly affect the person’s health. The performance of the proposed model for the level of security has been evaluated using the parameters of key connectivity at deployment and the probability of key exposure of the keys being exchanged between the two ends.

The key connectivity is the performance metric which signifies the probability of the connection generation using the given key model. The probability key connectivity indicates the level of connectivity and connection down time due to key connectivity. The proposed model has been evaluated with the highest level of the probability of key connectivity using the proposed key management model. The results has been obtained in the form of key connectivity probability signifies the maximum success rate and probability of connectivity using the proposed model. The probability of key connectivity has been recorded at 1 for all of the data or key transactions. The key failure is the major concern behind the dis-connectivity caused by key management models. The proposed model keeps the highest efficiency in the case of the key connectivity.

The proposed model has been also evaluated on the basis of probability of key exposure. The probability of key exposure signifies the probability of the keys being exposed to the hackers during the communications. The key exposure may cause the long-term information leakage affect to the patient specific healthcare communications. The key exposure probability must be at the lower levels in order to ensure the privacy and confidentiality of the patient data being propagation on the channel secured using the probability of the key exposure.
The resilience in mobile adversaries towards gamma and beta

The proposed model key exposure probability of falling down with the number of keys exchanged is rising. The less is the number of keys, the higher is the probability of the key exposure. The proposed model is using the cryptographic key exchange between the Holter and cloud healthcare system. The initial probability of the key exposure during the first key exchange is at 0.48, which is coming down with the rising number of keys being exchanged. The decreasing probability of key exposure is indicating the effectiveness of the proposed key exchange model.

The data updation time table has been built on the basis of response time taken by server to update the records. The total elapsed time contains the time taken for key generation, key transfer, update query and response reply with answer key from the server side. The sixteen update intervals have been recorded in the following table, in which latency, due to online cloud service, is also covered.

**Table I. The data update time calculated during each interval**

<table>
<thead>
<tr>
<th>Update Interval</th>
<th>Elapsed Time taken on each update interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>7.09</td>
</tr>
<tr>
<td>2</td>
<td>3.31</td>
</tr>
<tr>
<td>3</td>
<td>3.55</td>
</tr>
<tr>
<td>4</td>
<td>3.22</td>
</tr>
<tr>
<td>5</td>
<td>3.19</td>
</tr>
<tr>
<td>6</td>
<td>3.22</td>
</tr>
<tr>
<td>7</td>
<td>3.20</td>
</tr>
<tr>
<td>8</td>
<td>3.29</td>
</tr>
<tr>
<td>9</td>
<td>3.39</td>
</tr>
<tr>
<td>10</td>
<td>3.21</td>
</tr>
<tr>
<td>11</td>
<td>3.02</td>
</tr>
<tr>
<td>12</td>
<td>3.25</td>
</tr>
<tr>
<td>13</td>
<td>2.93</td>
</tr>
<tr>
<td>14</td>
<td>2.94</td>
</tr>
<tr>
<td>15</td>
<td>2.91</td>
</tr>
<tr>
<td>16</td>
<td>2.90</td>
</tr>
</tbody>
</table>
CONCLUSION

The proposed model is based upon the cloud healthcare system security. The proposed model has suggested the use of cryptographic key exchange model with the data encryption for the security of the cloud healthcare record management service. The proposed key exchange model uses the Advance Encryption Standard (AES) and RSA encryption algorithms for the purpose of key cryptography. The proposed model has proved its effectiveness on the basis of the parameters of probability of key connectivity and key exposure. The probability of key connectivity is indicating the highest possible connectivity level enabled by the proposed model. The probability of key exposure is the parameter indicating the possibility of the key being exposed to the hacking attempts. The key probability comes down with higher number of sensor and keys being transmitted across the given network. In the future, the proposed model can be enhanced using the quick AES or RSA algorithm, which may lower the response time between the holter device and the cloud record management system. The quick and stronger encryption algorithm is always the key behind the performance enhancement of the proposed model.

REFERENCES


