

Privacy Preserving Healthcare System using secured cloud environment

Dr. M.Umashankar

Associate Professor, Department of MCA, Sona College of Technology, Salem, India.

tmus2009@gmail.com

Abstract

Wireless devices that used to measure physiological signals to help develop health management become increasingly popular in recent years. Records are conducive for follow-up health and medical care. Using different type of wireless devices and the factors of a large number of users, large number of data are lead to create a security threads and privacy problems. With the help of wireless technology and cloud computing we may solve the traditional way of problems occurred at the time of data management and data transmission in health management system. This healthcare management application to propose an integrated algorithm technique for the jointly involved parties which is included privacy and security algorithm; it can protect data integrity also. This system provides the better efficiency and it is very useful to remote areas where hospitals are not easily accessible. This research to resolve wireless sensor network security relevant issues Using several patterns can reduce database load, and users to access data efficiently; the privacy control mechanism allow users to store data securely. The results of this research exhibit that the proposed system has better secured database access and maintain privacy for all patient data than the traditional database.

Key Words : Health care management, privacy, security, cloud computing.

I. Introduction

In recent years population are increased very much and the demand for the prevention and treatment of diseases are increased, as well as increased the health awareness and health prevention has increasing attention from the people. In later days, when people got medical help, opinions and obtain treatment from medical professionals with the emerging of new modern healthcare services and technologies, healthcare service has gradually increased the concentration on prevention care and health management.

Wireless sensor signals are used for the benefits of patients in hospitals. The most important information's are stored in the database in the form of medical records; it consists of heart rate and respiratory rate. This information is collected from the different types of medical equipment and devices; these data are normally not modified. In addition, these data are private and personal information, this information is not sharable with others; it can be shared with family doctors, specialists and trusted medical personnel. These data should be protected, and the users should be permitted to set their own authorization for access. Some kind complex cases this data may be shared and used for comparison by several medical personnel they may be the different users. Here we required to maintain privacy and security for such kind of data. One of the Service of Cloud technology is Database as a Service (DaaS), it provide potential for innovative way of data storage. Although the traditional database allows users to manage, store, and retrieve data and have been successfully applied in many services, some limitations exist. Compared to traditional database services, a DaaS can support large number of users. Every day electrocardiography (ECG) and electromyography (EMG) signals accumulated in the data base the result is a huge amount of data. The characteristics of a DaaS to resolve the data storage and privacy issues of

signal storage. This research, to propose a DaaS for application on the health record data to establish data privacy protection control, it ensures users' privacy rights, signals can be stored in the cloud environment with privacy protection.

Received data is sent to the central server of the cloud that performs various applications using the automated decision support algorithms in the cloud-assisted mobile health monitoring on web which are related to medical and report the health condition of the patient along with the suggestions to the client frequently. Both malicious and non-malicious attackers have come in to this system for illegal purpose. This application has the capability to perform various processes to examine the client health. The patients concerned more about the privacy of their health information. Here the malicious attackers are more dangerous when compared to the non malicious. The inside attackers can easily hack these health care systems as they are generally a professionals. Outside attackers can be prohibited by cryptographic methods such as encryption and it is major to design preserving methods of the client's health details privacy. The cloud based health monitoring offer a quality of service and lowering of prices. While the data of the patients regarding their health is collected there may be chance for the lack of privacy during storage, communication, diagnosis and computing. The cloud server is nothing but the cloud industry which gives health monitoring and provides health care service to the individual users based on the third party. With the help of cloud computing clients can preserve the information into the cloud remotely and utilize on-demand maximum quality applications.

Major problem in addressing security and privacy in the computational work load involved in the cryptographic techniques. With the presence of cloud computing facilities

it will be wise to shift intensive competitions to cloud server from resource-constrained mobile devices. Information security is highest priority for any healthcare organization; providers must be in protecting confidential patient data. Instead, providers need to take a comprehensive approach to protecting patient information at every potential access, both inside and outside the network. Network attacks are complex with specific motives, while others are malicious. Employee threats also be considered, these threats can cause significant damage and disrupt patient care.

Challenges faced by the Healthcare organization

Security and privacy

Increase the trust of on electronic data needs to secure and protect information. Security breaches can have a negative effect on the organization's brand and credibility, usually resulting in reduced revenue.

Quickness

Organizations want to deploy their new applications quickly to their user populations, in order to respond quickly to market events. Increasing the popularity of mobility has made the ability to have a common security approach across both Web and mobile apps to be a strong requirement.

User expediency

Doctors and nurses don't have long time to do the redundant and lengthy process; they wish to use their valuable time efficiently. This system provides easy and quick access to store the patient information.

Cost control

Because of the cost pressure health care system need an innovative idea to reduce the IT expenses. Cloud computing models and an automation of key identity-related process can help to improve the efficiencies and reduce the cost.

Integration with leading healthcare applications

Because of the organizational infrastructure the data move inside and outside the network perimeter, this scenario facing the several threads Insiders, and especially administrators, pose a significant risk due to the damage they can cause through malicious or inadvertent actions. In addition, external attacks are increasing in sophistication and frequency. With the help of an Integrated security scheme above said challenges to be removed.

Benefits of healthcare system

- Protect the integrity of your medical applications
- Secure patient records and information, claim activity, and other medical transactions to ensure high efficiency, and security
- Identify and control the employees, customers, suppliers, patients, and partners accessing your applications and system
- Reduce implementation time and cost to ensure deadlines are met and fines avoided
- Eliminate the need for investing in disparate systems from different vendors
- Secure the exchange of records and information, claim activity, and other transactions amongst healthcare providers and insurers

II. Related Works

Information security is a top priority for any organization, healthcare providers must be especially diligent in protecting confidential patient data so Network-based applications have used to transform the imaging, biomedical information, material management, patient accounting, admitting information, and online claims submissions through in wireless, wired, and mobile to the concern authority. Several research are taken up and gave different solutions.(JeongGil Ko) present some representative applications in the healthcare domain and describe the challenges they introduce to wireless sensor networks due to the required level of trustworthiness and the need to ensure the privacy and security of medical data. (Adithkiran) present a system using NFC-enabled mobile phones for facilitating the patients in a low-resource environment. Doctors can view the previous medical records by tapping the Smartphone that is enabled with a NFC reader over the NFC tag. In the same way doctors can read/write the information. (Ahmed E) introduce a framework for Healthcare Information Systems (HISs) based on big data analytics in mobile cloud computing environments.

This framework provides a high level of integration, interoperability, availability and sharing of healthcare data among healthcare providers, patients, and practitioners. Electronic Medical Records (EMRs) of patients dispersed among different Care Delivery Organizations (CDOs) are integrated and stored in the Cloud storage area; this creates an Electronic Health Records (EHRs) for each patient. Mobile Cloud allows fast Internet access and provision of EHRs from anywhere and at any time via different platforms. (Umashankar) addresses a randomized energy-conservation method that seeks to build resilient sensor networks by decreasing the number of reporting nodes increases the number of reports that need to be sent to the sink in order to get the preferred information consistency about a detected event. This is very essential for the process done with the sensors. (Ebru Celikel) introduce the design and development of a comprehensive electronic health record system (EHR) that incorporates AES encryption to assure security.(S. Kami Makki) explains Data fusion techniques reduce total network traffic in a wireless sensor network, since data fusion can integrate multiple raw data sets into one fused data set. (Hsien-Tsung) to resolve physiological signal record-relevant issues utilizing the advantages of the Database as a Service (DaaS) model. Storing a large amount of data using file patterns can reduce database load, allowing users to access data efficiently; the privacy control settings allow users to store data securely. The results of the experiment show that the proposed system has better database access performance than a traditional relational database, with a small difference in database volume, thus proving that the proposed system can improve data storage performance.

(Bhoomika.B.K) used the PIC18F46K22 microcontroller as a gateway to communicate to the various sensors such as temperature sensor and pulse oximeter

sensor. The microcontroller picks up the sensor data and sends it to the network through Wi-Fi and hence provides real time monitoring of the health care parameters for doctors. The data can be accessed anytime by the doctor. The controller is also connected with buzzer to alert the caretaker about variation in sensor output. But the major issue in remote patient monitoring system is that the data as to be securely transmitted to the destination end and provision is made to allow only authorized user to access the data.

The security issue is been addressed by transmitting the data through the password protected Wi-Fi module ESP8266 which will be encrypted by standard AES128 and the users/doctor can access the data by logging to the html webpage. At the time of extremity situation alert message is sent to the doctor through GSM module connected to the controller. Hence quick provisional medication can be easily done by this system. This system is efficient with low power consumption capability, easy setup, high performance and time to time response (K.Sravani), to provide feedback decision support that has been an essential approach to improve the excellence and to reduce the cost of healthcare services provided. The system creates a serious risk on both user's privacy and intellectual property of monitoring by the service providers. It also discourages the broad acceptance of portable Health services. The portable healthcare application for the mutually involved parties in this mechanism is for the better security with extended privacy and data integrity by applying techniques. This portable health care maintenance system is to propose simple user interface which is easily understood even by the illiterates and the payment is done online. It integrated hash function algorithm technique and privacy aware security algorithm which can protect data integrity.

III. Problem Definition

In the Health care system addressed the major problem is security and privacy using traditional way of security techniques. The above said problems to be solved with the use of cloud computing facilities, it might be changed the demanding computations to cloud server computation. Solutions that allow access to electronic medical records (EMRs), medical management systems, imaging, biomedical information, material management, patient accounting, admitting information, and online claims submissions are becoming commonplace in wireless, wired, and mobile scenarios. Now a day's the health care system can need to merge the above tools into one infrastructure and communicate and collaborate more effectively, it leads to reduce errors and improve the efficiency in patient care with lower cost. This cloud assisted health systems not only to guarantee the privacy of client's health related data and also guarantee the output data from cloud server and health care services.

IV. Proposed System

The main idea of the designed system is used to monitoring of the patients, updates their medical records immediately and stores this information in cloud storage at the same time it provides the security and privacy of the patient's record. The Proposed System uses microcontroller, temperature

sensor pulse dosimeter sensor, GSM MODEM. The Microcontroller collects the data from the sensors and sends the data through Wi-Fi Protocol. The Secured data sent can be accessed anytime by the authorized person by using the corresponding IP address in any one of the Internet Browser at the user device. Hence continuous monitoring of patient data is achieved. We use the XML format to record large amounts of streaming data, such as ECG data. There is no need to modify or delete data, and no need to perform complex SQL commands. Observations data are also sent through the same way to the storage. The Proposed System has the five trusted authorities such as client, data storage, server, company and token generator. The token generator is responsible for generation of token and to get information from the cloud. Based on the user request the tokens are generated and encrypted and it is sent to the cloud server. Cloud authorizes to send a unique key to the users for their respected request. Company gives sensor data to the client server. Server get it and processed with token which is generated by the token generator after that the data to be stored in the data storage. Activate a Web server for patient mode in keeping the server safe from hackers requires explicit attention. Every Web server's should be configured to the security parameters. This security software offers timely protection for Web and other application servers. It can protect the entire network against the hackers and other unauthorized users. With the help of constantly collected information on the various system resources, the system audit trails to determine if any security breach has taken place. Support of self-contained agents it can be sending alert message to the user of the specific asset being protected, this protection system monitor's activity on a specific network segment and analyzes network traffic and a management system that alerts security personnel of potential events. Proposed system consists of a sensor and a dedicated platform an access router it can provide strong, coordinated protection to both network segments and individual resources. Providers should take a systematic, approach to plan and deploy a well secure network infrastructure. As the risks and security concerns for healthcare networks grow various aspects to be considered and evaluated this approach should include a careful evaluation of each area of the network, identification of potential threats, development of a practice security policy, and implementation of network security technologies. Any critical conditions may happen immediately an alert message to be sent to the doctor's cell phone through GSM modem, at the same time the buzzer alert sent to the caretaker. The doctors can view the sent data by logging to the html webpage using unique IP and page refreshing option is given so continuously data reception achieved. In the designed system would be connected more sensors to internet which measures various health parameters and would be beneficial for patient monitoring. Wi-Fi mesh type network to increase in the communication range. In this paper treats the security is one of the most important in cloud computing , here data vendor stores their data to remote servers and clients also access required data from remote cloud servers which is not restricted and managed by data vendors.

This paper proposed a new algorithm for cloud background which includes the different security schemes to achieve the privacy. The proposed algorithm is highly efficient, Secure and Privacy aware for cloud environment. The cloud is a very essential component for the facilitating

electronic health record sharing. To improve the current environment the data to be accessed from anywhere anytime in addition it preserves the privacy of health data. It allows the authentic users to retrieve the data easily from the database using flexible patterns. From the cloud storage this process to retrieve the data quickly with the help of parallel computational queries. The main aim of this research is to continuous monitoring of the patients over internet, here the registration is the primary process which is used for authentication, and the register user can send and retrieve the information. In our proposed method to be balanced the load and increase the performance and also balance the storage space and processor load by using different cloud servers.

V. Conclusion

This research address a cloud assisted monitoring health care system with privacy preserving the sensitive data. The Cloud technology and security process are used to provide an advantages to increase the efficiency and accuracy with the privacy. This approach includes a vigilant evaluation of the network, and identified the potential threats, increase of a practice security guidelines, and implementation of network security technologies. Proposed method to resolve wireless sensor network security relevant issues Using several patterns can reduce database load, and users to access data efficiently; the privacy control mechanism allow users to store data securely. The Future work of the project is very essential in order to make the design system more advanced. In the designed system the enhancement would be connecting more sensors to internet which measures various other health parameters and would be beneficial for patient monitoring i.e. connecting all the objects to internet for quick and easy access.

REFERENCES

- [1] Adithkiran Bandarkavte, Jagadeesh Sai. D, “NFC Based Secure HealthCare Monitoring System” , International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 4, April 2016
- [2] Ahmed E. Youssef, “A FRAMEWORK FOR SECURE HEALTHCARE SYSTEMS BASED ON BIG DATA ANALYTICS IN MOBILE CLOUD COMPUTING ENVIRONMENTS”, International Journal of Ambient Systems and Applications (IJASA) Vol.2, No.2, June 2014 .
- [3] JeongGil Ko, Chenyang Lu, Mani B. Srivastava, John A. Stankovic, Fellow IEEE, Andreas Terzis, and Matt Welsh , “Wireless Sensor Networks for Healthcare “,Proceedings of the IEEE , Vol. 98, 0018-9219/\$26.00 _2010 IEEE No. 11, November 2010
- [4] Jin Wang, Hassan Abid, Sungyoung Lee, Lei Shu, Feng Xia, “A Secured Health Care Application Architecture for Cyber-Physical Systems”,
- [5] K.Sravani#1, B.Bindusha Reddy#2, R.R.V.N.V.Kumari#3, G.Vijay Kumar*, “A Portable and Secure Healthcare Maintenance System”, International

Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 2079-2083

- [6] Bhoomika.B.K , Dr. K N Muralidhara , “Secured Smart Healthcare Monitoring System Based on Iot “, International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 3 Issue: 7
- [7] Hsien-Tsung Chang^{1,2*}, Tsai-Huei Lin, “A Database as a Service for the Healthcare System to Store Physiological Signal Data”, PLOS ONE | DOI:10.1371/journal.pone.0168935 December 29, 2016
- [8] Ebru Celikel Cankaya¹ Than Kywe², “A Secure Healthcare System: From Design to Implementation” ,ScienceDirect Procedia Computer Science 62 (2015) 203 – 212
- [9] RANDOLPH C. BARROWS, JR., MD, PAUL D. CLAYTON, PHD, “ Privacy, Confidentiality: and Electronic Medical Records , Journal of the American Medical Informatics Association Volume 3 Number 2 Mar / Apr 1996.
- [10] Umashankar M ., “ Power Efficient Data Fusion Assurance Mechanism for Wireless Sensor Networking”, International Journal of Advanced Research in Computer Science, Volume 5, No. 5, May-June 2014
- [11] J.Benaloh, M.Chase, E.Horvitz and K.lauter,”Patient control encryption: ensuring privacy on electronic medical records”, in ccws 09, 2009, pp, 103-114.
- [12] Mrs. Ramya.R, Mrs.Shruthi.G, Privacy Preserving Of Health Monitoring Services In Cloud, International Journal of Advance Research In Science And Engineering IJARSE, Vol. No.3, Issue No.6, June 2014.