ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

Privacy Protection for Case Sheet Using Multiple Platform

Wabale Ashwini H[1], Thorat Nikhil V[2], Salgat Piraji R[3], Kardile Pratiksha A[4]

B.E. Students, Dept. of Computer Engineering, Jaihind College of Engineering, Pune, India

ABSTRACT: Remote case sheet systems have been broadly utilized as a part of Patient case sheet and medical applications, for example, helping facility what's more home patient observing, Medical data, Case sheets. Medical case sheet systems are more powerful stored data on distributed server. The current arrangements can secure the patient information can amid various transmission, however can't stop within assault where the persisting chairman database uncovers the delicate on different patient information. The propose of a functional way to deal with keep within assault by utilizing different information servers system to store tolerant information. The principle commitment of this paper its safely conveying the patient information in different information accessing servers and utilizing the Cluster algorithm to perform measurement to investigation on the patient information without bargaining the patients security.

KEYWORDS: Wireless medical distributed server network, Patient data privacy, Clustering algorithm.

I. INTRODUCTION

Data collection security in the Wireless medical distributed server network, each medical case sheet can securely send the patient data to the distributed database on system. Data store security in the distributed various patient database system, the patient data cannot be provided revealed even if two of three data servers are compromised by the different inside attackers. Data access security in the patient access control system, only authorized user can get access to the various patient data. The patient data cannot be disclosed to any data server during the access. Data analysis security the patient data analysis system, the authorized user can get the statistical analysis results only. The main expectations of this change are to provide better ways to exchange and share medical information and to improve the quality of services offered to the patients. In this context, medical data is supposed to be available the different online where healthcare professionals can access it at any time and from any place. Basically, it will be transmitted over Internet, dedicated Virtual Private Networks (VPN), and hospital networks.

VPN can control the medical data and patients case sheet to the server. The on-line access to medical information can have two major consequences. It can support to healthcare professional the take better decisions, it can increase to risk loss of privacy and malicious various attacks. The goal of designing and implementing the eHealth platforms is to reinforce the former to consequence and to reduce or the eliminate the second one. This paper focuses on the various strategy to widely reduce the malicious attacks' risk and to assure the privacy of various patients during the storing and exchange (sharing) of medical information by using the medical Health platform. Some clustering algorithm protocols have proved their efficiency to provide data-security for the communications over networks but they do not fully prevent attacks to no of users computers or servers. An medical e Health platform has to deal with the risks, control authentication, authorization part, and integrity. Several countries are implementing different solutions to satisfy these needs, but the evolution of the applications, methods and laws had forced on some of them to review partially or completely their approaches.

II. Need for medical data in distributed server:-

Now days much application can provide solution of patient disease and solution but not proper work able to required method. This system provides the different server such as admin, patient, doctor, nurse etc, System can provide case sheet and maintain medical data.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

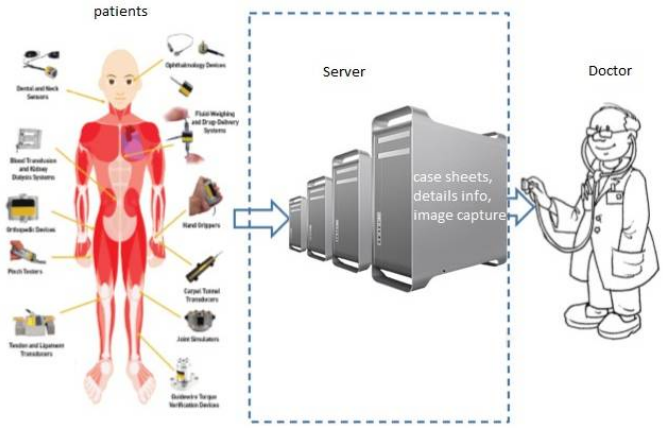


Fig 1. Block Diagram on distributed server

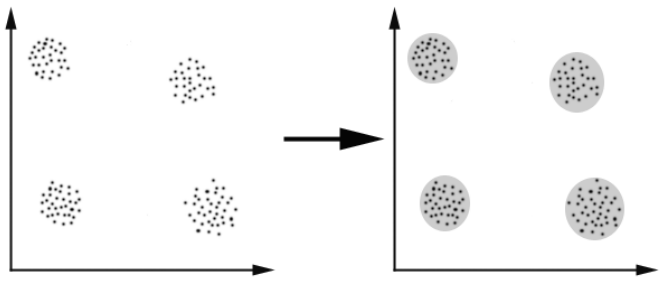
II. RELATED WORK

In this Project, we are using three data server to store patient data. Patient data is distributed in multiple data servers. doctor provide online case sheet to patient so that he can give treatment to the patient. we are providing security using Cluster algorithm cryptosystems without compromising the patients privacy.

III. SECURITY ALGORITHM

Clustering algorithm used to provide security to server management in distributed. Clustering can be considered the most important *unsupervised learning* problem; so, as every other problem of this kind, it deals with finding a *structure* in a collection of unable data. A loose definition of clustering could be “the process of organizing objects into groups whose members are similar in some way”. A *cluster* is therefore a collection of objects which are “similar” between them and are “dissimilar” to the objects belonging to other clusters.

Matrix Multiplication:-



k-means is one of the simplest unsupervised learning algorithms that solve the well known clustering problem. The procedure follows a simple and easy way to classify a given data set through a certain number of clusters (assume k clusters) fixed apriori. The main idea is to define k centers, one for each cluster.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

Steps:

Let $X = \{x_1,x_2,x_3,\ldots\ldots,x_n\}$ be the set of data points and $V = \{v_1,v_2,\ldots\ldots,v_c\}$ be the set of centers.

1) Randomly select the '*c*' cluster centers.

2) Calculate the distance between each data point and cluster different centers.

3) Assign the data point to the cluster center provide whose distance from the cluster center is minimum of all the cluster centers..

4) Recalculate the new cluster center using no of:

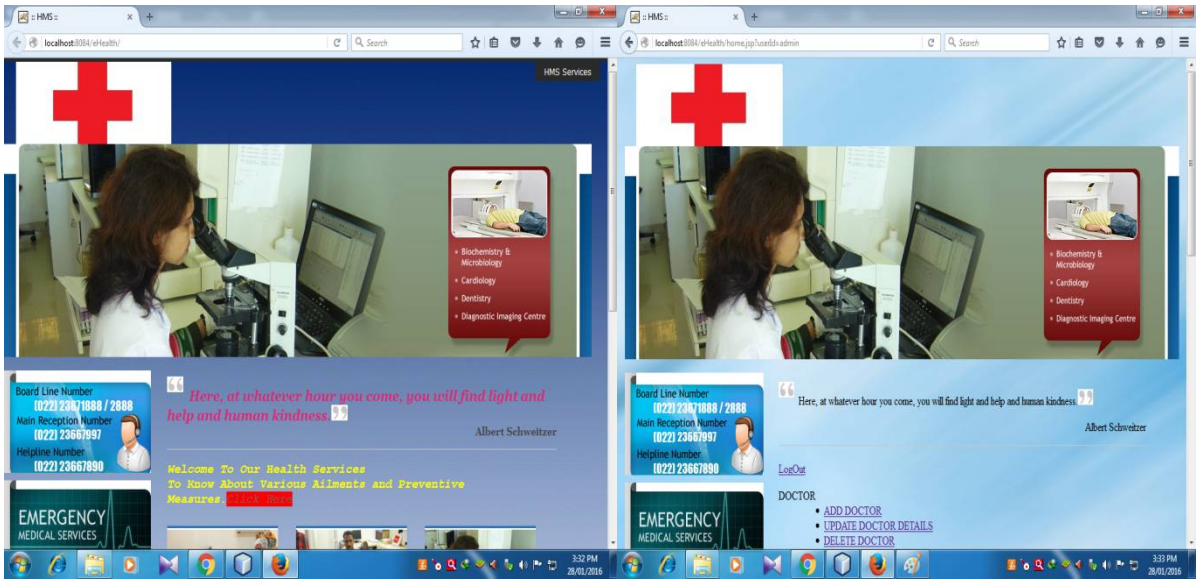
$$v_i = (1/c_i) \sum_{j=1}^{c_i} x_i$$

where, 'c_i' represents the number of data points in i^{th} cluster.

5) Recalculate the distance between each data point and new obtained cluster centers.

6) If no data point was reassigned then stop, otherwise repeat from step 3.

IV. RESULT



Module 1: Login and home page

Login window can provide authority user and home

Module 2(a): Doctor add, update, delete**.**

This module use adds, update, Delete Doctor

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

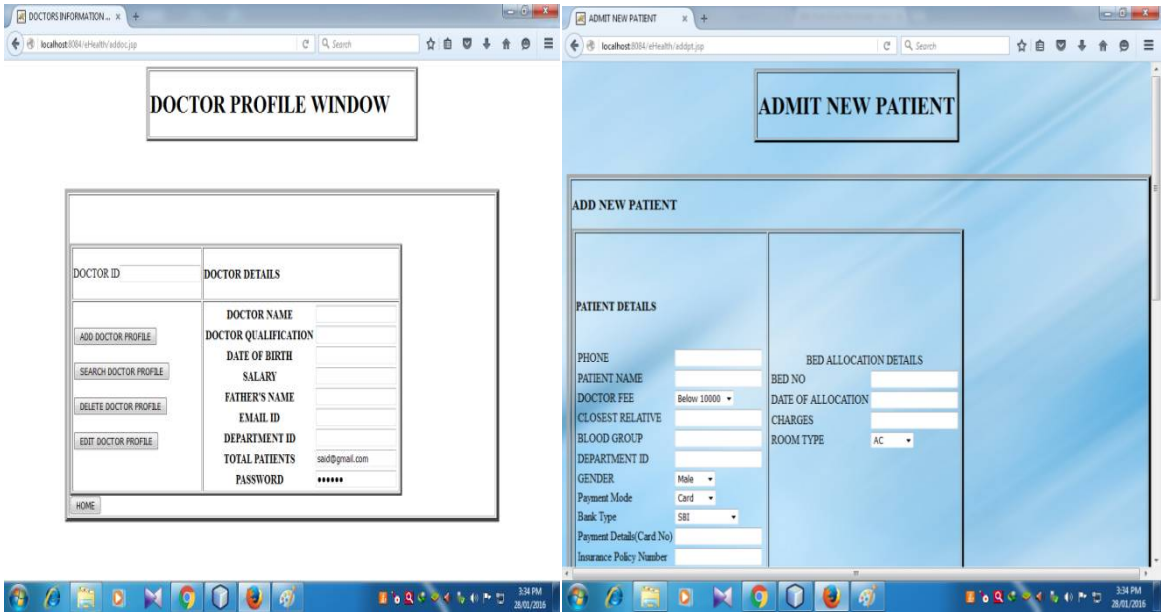
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

Page linking to doctor, patients, case sheets.

Registration window.



Module 2(b): Doctor add, update, delete**.**
This module use add , update, Delete patients window.

Module 4: Case Sheet**.**
This module use add , update, Delete Case sheets record.

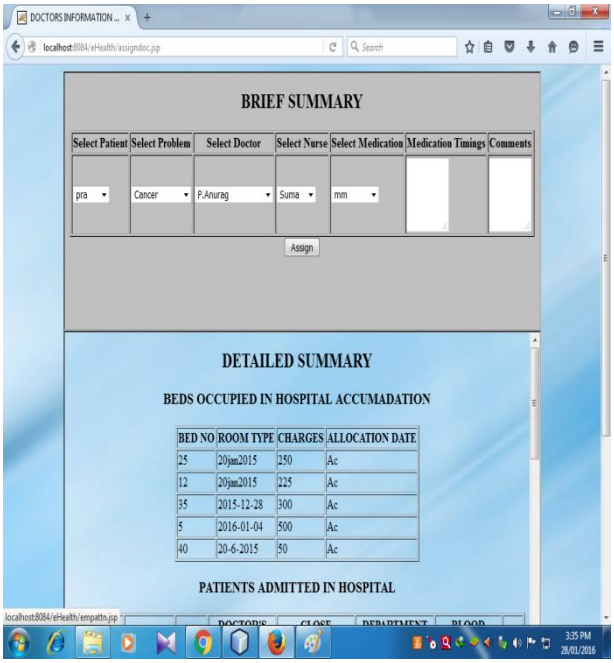


Fig .Result Screen

- This module use adds, update, Delete patient's window. This module use add, update, Delete Case sheets record.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

V. CONCLUSION

In this paper, we have investigated the security and privacy issues in the medical distributed data collection, storage and queries and presented a complete solution for privacy-preserving medical distributed network. To secure the communication between the medical various and data servers, we used the lightweight encryption scheme and MAC generation scheme based on Cluster algorithm proposed in. To keep the privacy of the various patient data, we proposed a new data collection protocol which splits the various patient data into three numbers stores them in three data servers, respectively. As long as one data server is not be compromised, the privacy of the patient data can be to preserved different user. For the legitimate user (e.g., physician) to access the patient information, we proposed an access control protocol, three data servers cooperate the provide the user with the patient data. For the legitimate various user (e.g., medical researcher) to perform statistical analysis on the patient data, we proposed some new various protocols for average, correlation, variance and regression analysis, where the three data servers the cooperate to process the patient data without disclosing on to the patient privacy and then provide the various user with the statistical analysis results

REFERENCES

[1] Advanced Encryption Standard (AES). FIPS PUB 197,November26,2001.http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
[2] F. Hu, M. Jiang, M. Wagner, D. C. Dong. Privacy-Preserving Telecommunication cardiology Sensor Networks: Toward a Low-Cost Portable Wireless Hardware/Software Co-design. IEEE Trans. Inform. Tech. Biomed, 11: 619-627, 2007.
[3] Y. M. Huang, M. Y. Hsieh, H. C. Hung and J. H. Park. Pervasive, Secure Access to a Hierarchical Sensor Based on Healthcare Monitoring system Architecture in Wireless Heterogeneous Networks. IEEE J. Select. Areas Common. 27: 400-411, 2009
[4] J. H. Lim, Y. Chen, R. Musaloiu-E., A. Terries and G. M. Masson.MEDiSN: Medical Emergency Detection in Sensor to Networks. ACM Trans. Embed. Compute. Syst. 10: 1-29, 2010.
[5] P. Kumar, Y. D. Lee and H. J. Lee. Secure Health Monitoring Using Medical Wireless Sensor various Networks. In Proc. 6th International Conference on Networked Computing and Advanced Information Management, pages 491-494, Seoul, Korea, 16-18 August 2010
[6] P. Kumar and H. J. Lee. Security Issues in Healthcare Applications Using Wireless Medical Sensor various Networks: A Survey. Sensors 12: 55-91, 2012.
[7] X. H. Le, M. Khalid, R. Shankar, S. Lee. An Efficient Mutual Authentication Access Control Scheme for Wireless Sensor Network in Healthcare. J. Networks 27: 355-364, 2011.
[8] H. J. Lee and K. Chen. A New Stream Cipher text for Ubiquitous Application. In Proc. ICCIT'07, South Korea, 2007.

BIOGRAPHY

Wabale Ashwini, Thorat Nikhil, Salgat Piraji, and Kardile prtiksha are BE Students in the Computer Engineering Department, Jaihind College of Engineering (Pune), Savitribai Phule,Pune.