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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

# Providing Secure Healthcare System on Cloud

Komal Pangare*, Apoorva Kukade*, Rutuja Mane*, Prof. Madhura Sanap *

Department of Computer Engineering, Sinhgad Academy of Engineering, Pune, India *

**ABSTRACT:** Health Record of an individual personal is a vital way that can be utilized for keeping track of patient data in accurate, reliable as well as complete manner. For all intents and purposes, restorative information sharing is a basic and testing issue. Consequently in this paper, we develop a novel human services framework by using the adaptability of cloudlet. The elements of cloudlet incorporate security insurance, information sharing and interruption location. In the phase of information accumulation, we initially use Number Theory Research Unit (NTRU) technique to scramble client's body information gathered. That information will be transmitted to adjacent cloudlet in a vitality proficient form. Furthermore, we exhibit another trust model to enable clients to choose trustable accomplices who to need to share put away information in the cloudlet. The trust display additionally causes comparable patients to speak with each other about their sicknesses. Thirdly, we isolate clients' medical information and it put away in remote billow of healing facility into three sections, and give them appropriate security.

**KEYWORDS:** Privacy Protection, Data Sharing, Intrusion Detection System (IDS), Healthcare.

## I. INTRODUCTION

The medical data on the social network is beneficial to both patients and doctors, the sensitive data might be leaked or stolen, which causes privacy and security problems without efficient protection for the shared data. In Cao et al, an MRSE (multi-keyword ranked search over encrypted data in cloud computing) privacy protection system was presented, which aims to provide users with a multi-keyword method for the cloud's encrypted data [1]. Although this method can provide result ranking, in which people are interested, the amount of calculation could be cumbersome. A priority based health data aggregation (PHDA) scheme was presented to protect and aggregate different types of healthcare data in cloud assisted wireless body area network (WBANs). The article investigates security and privacy issues in mobile healthcare networks, including the privacy-protection for healthcare data aggregation, the security for data processing and misbehavior [2]. Describes a flexible security model especially for data centric applications in cloud computing based scenario to make sure data confidentiality, data integrity and fine grained access control to the application data. It gives a systematic literature review of privacy-protection in cloud-assisted health care system.

### Motivation

Here data is divided in remote cloud into different kinds and utilize encryption mechanism to protect them respectively. The IDS based on cloudlet mesh is to protect the whole healthcare system against malicious attacks.

## II. REVIEW OF LITERATURE

**A. Sajid and H. Abbas** [1]. The system is privacy-assured where cloud sees neither the original samples nor underlying data. It handles well sparse and general data, and data tampered with noise. We have proposed a privacy-aware cloud assisted healthcare monitoring system via compressive sensing. The random mapping based protection ensures no sensitive samples would leave the sensor in unprotected form. Wireless sensors are being increasingly used to monitor/collect information in healthcare medical systems. Despite the increasing popularity, how to effectively process the ever-growing healthcare data and simultaneously protect data privacy, while maintaining low overhead at sensors, remains challenging.

**R. Mitchell and I.-R. Chen** [2]. We demonstrate that our intrusion detection technique can effectively trade false positives off for a high detection probability to cope with more sophisticated and hidden attackers to support ultra safe and secure MCPS applications. For safety-critical MCPSs, being able to detect attackers while limiting the false alarm

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

probability to protect the welfare of patients is of utmost importance. We plan to analyze the overheads of our detection techniques such as the various distance-based methods in comparison with contemporary approaches. We propose and analyze a behaviour-rule specification-based technique for intrusion detection of medical devices embedded in a medical cyber physical system (MCPS) in which the patient's safety is of the utmost importance.

**Y. Shi, S. Abhilash, and K. Hwang** [3]. We have specified a sequence of authentication, authorization, and encryption protocols for securing communications among mobile devices, cloudlet servers, and distance clouds. Securing mobile cloud services is the major barrier to the integration of BTOD (bring your own devices) and BYOC (bring your own cloud) in our daily applications. We use the cloudlet mesh to perform collaborative intrusion detection among multiple cloudlets. Network attacks are a serious matter that confronts both cloud providers and massive number of mobile users who access distance clouds in our daily-life operations. We extend their work to support security functionalities in offloading the distance clouds.

**M. S. Hossain** [4]. The proposed approach uses Gaussian mixture modelling for localization and is shown to outperform other similar methods in terms of error estimation. The design and development of such systems requires access to substantial sensor and user contextual data that are stored in cyberspace. We will conduct more workload measurements to record the resource utilization of CPU, memory, storage, and network bandwidth. This enables a range of emerging applications or systems such as patient or health monitoring, which require patient locations to be tracked.

**M. Quwaider and Y. Jararweh** [5]. The proposed work also attempts to minimize the end-to-end packet delay by choosing dynamically a neighbour cloudlet, so that the overall delay is minimized. The goal was objective to minimize end-to-end packet cost by dynamically choosing data collection to the cloud using cloudlet based system. Performance of the proposed system was evaluated via extended version of CloudSim simulator. The huge amount of data collected by BAN nodes demands scalable, on-demand, powerful, and secures storage and processing infrastructure.

**J. Zhao, L. Wang, J. Tao, J. Chen, W. Sun, R. Ranjan, J. Kołodziej, A. Streit, and D. Georgakopoulos** [6]. We describe an EHR security reference model for managing security issues in healthcare clouds, which highlights three important core components in securing an EHR cloud. The goal of this research is to advance the Map Reduce framework for large-scale distributed computing across multiple data centres with multiple clusters. The designed security framework has the ability to prevent the most common attacks, such as MITM attack, replay attack, and delay attack, and ensures a secure communication of GHadoop over public networks. The Map Reduce tasks are firstly scheduled among the clusters using Hadoop's data-aware scheduling policy and then among compute nodes use the existing cluster scheduler on the target clusters.

**N. Cao, C. Wang, M. Li, K. Ren, and W. Lou** [7]. We first offer a basic idea for the multi keyword ranked search over encrypted cloud data (MRSE) based on effective comparison measure of coordinate matching. We have taken a methodical approach to investigating security models and security requirements for healthcare application clouds. We have discussed important concepts related to EHR sharing and integration in healthcare clouds and analyzed the arising security and privacy issues in access and management of EHRs. The widespread use of electronic health record (EHR), building a secure EHR sharing environment has attracted a lot of attention in both healthcare industry and academic community.

**H. Mohamed, L. Adil, T. Saida, and M. Hicham** [8]. We propose a collaborative model consists of the Intrusion Detection and Prevention System functions based distributed IDS and IPS, with the use of a hybrid detection technique for addressing the problems of attacks encountered, specifically distributed attacks such as port scanning attacks and distributed internally established within a Cloud Computing environment by users entitled to access, including the integration of the Signature Apriori Algorithm for generating new attack signatures whose objective is to develop the functioning of our security system to be able to detect and block various types of attacks and intrusions. Security solutions are not yet adapted to this new concept. Indeed, in such an environment, the more customers and paths, the greater the intrusion is effective. We also incorporate the signature apriori algorithm to enrich and update our database

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

signature to analyze and compare information received. Cloud Computing has emerged as a model to process large volumetric data. They add that Cloud Computing deals with different fundamentals like virtualization management, fault tolerance and load balancing.

**R. Zhang** [9]. We describe an EHR security reference model for managing security issues in healthcare clouds, which highlights three important core components in securing an EHR cloud. We have taken a methodical approach to investigating security models and security requirements for healthcare application clouds. We have discussed important concepts related to EHR sharing and integration in healthcare clouds and analyzed the arising security and privacy issues in access and management of EHRs. The widespread use of electronic health record (EHR), building a secure EHR sharing environment has attracted a lot of attention in both healthcare industry and academic community.

**K. Hung, Y. Zhang, and B. Tai** [10]. As an important part of this system, a cuff less BP meter has been developed and tested on 30 subjects in a total of 71 trials over a period of five months. Use of mobile communication is no longer limited to telephony. New interests and demands are wireless data and multimedia services, as 3G phones are available. The world's ageing population and prevalence of chronic diseases have lead to high demand for tele-home healthcare, in which vital-signs monitoring is essential.

## III. PROPOSED SYSTEM

In this project, the paper proposes a cloudlet based human services framework. The body information is gathered & transmitted to the adjacent cloudlet. That information is additionally conveyed to the remote cloud where specialists can get to for disease finding. In the main stage, user's vital signs are gathered by the system and are conveyed to gateway of cloudlet. In this stage, information security is the primary concern. In the second stage, client's information will be additionally conveyed towards remote cloud through cloudlets. A cloudlet is framed by a specific number of cell phones whose proprietors may require as well as offer some particular information substance. In this manner, both security assurance and information sharing are considered in this stage. Especially, we utilize trust model to assure trust level between users to decide sharing information or not. Considering the clients' restorative information is put away in remote cloud, it characterize these medical data into various types and takes the relative security approach. In addition to over three phases based information it gives security assurance. Additionally consider community oriented IDS in light of cloudlet work to ensure the cloud eco framework. We propose the google map for displaying register hospital on map with route. We propose some question and answer technique between user and doctors.

## IV. SYSTEM ARCHITECTURE

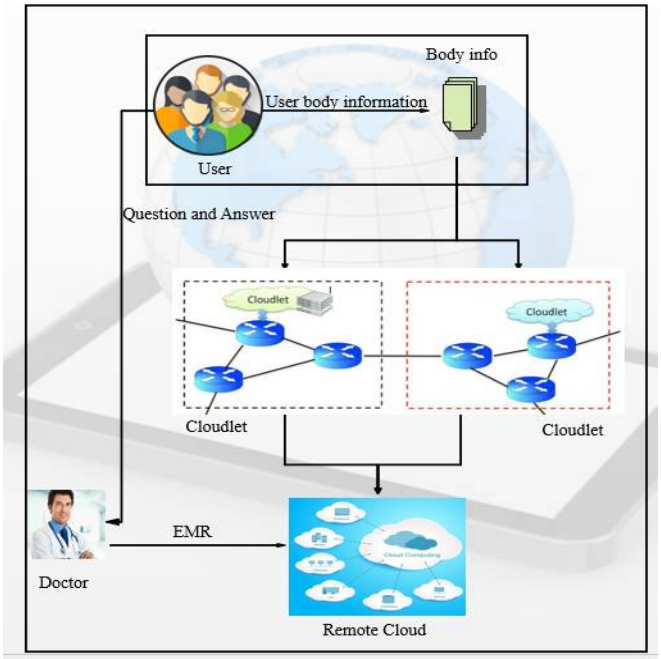



Fig 1. Architecture Diagram

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

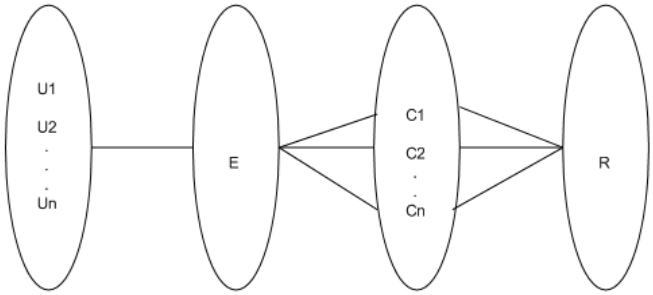
Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

User enters the body information and we provide the privacy of user information and transmit it to cloudlet. Using cloudlet it transfer this information to remote cloud. User share their information based on cloudlet. User request for sharing information to other user and then trusted authority checks both users body information similarity. After that user share their information. User asks question to doctor and doctor provide the answer.

## VI. MATHEMATICAL MODEL

**Mapping Diagram:**




Where,
$U_1$, $U_2$… $U_n$ =Users
E=Encrypted User Body Information
C1, C2=Cloudlet
$C_1$, $C_2$… $C_n$ = Cloudlet information

**Set Theory:**
S={s, e, I, O, ø}
Where,
s = Start of the program.
1. Log in with webpage.
2. Load medical data on cloudlet.
e = End of the program.
Retrieve the user EMR report from remote cloud.
I= {U, Nc}
I = Input of the program.
U = User's body info/symptoms.
Nc = Select number of User for sending request.
O = Output of the program.
Giving a medical report.
I, O ϵ U
Let U be the Set of System.
U= {User, E}
Where User, E are the elements of the set.
User=Cloudlet
E=Encryption

**Space Complexity:**
The space complexity depends on Presentation and visualization of discovered patterns. More the storage of data more is the space complexity.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

**Time Complexity:**
Check No. of patterns available in the datasets= n

If (n>1) then retrieving of information can be time consuming. So the time complexity of this algorithm is $O^{(n^n)}$.
ø= Failures and Success conditions.

**Failures:**
1. Huge database can lead to more time consumption to get the information.
2. Hardware failure.
3. Software failure.

**Success:**
1. Search the required information from available in database.
2. User gets result very fast according to their needs.

## VII. ALGORITHM

**Number Theory Research Unit (NTRU):-**
**Input: -** F, G, Message.
**Output: -** encrypt and decrypt message.
Step 1: Two small polynomial f and g.
Step 2: The large modulo p and modulo q.
Step 3: The inverse of f modulo q and the inverse of f modulo p.
Step 4: f * fq = 1 (mod q) and f * fp = 1 (mod p)
Step 5: Generating fp = f-1 (mod p) and fq = f-1 (mod q).
Step 6: The private key pair and the public key h is calculated using p, fq and g.
Step 7: public key is h = pfq * g (mod q).

Step 8: Encryption uses m, r and the public key h to generate e, the encrypted message that is as follows:
e = r * h + m (mod q).

Step 9: First uses the private key f to calculate:
a = f * e (mod q).

Step 10: c = fp * b (mod p)

If decryption is successfully completed, then the polynomial c will be equal to the original message.

## VIII. EXPERIMENTAL SET UP

Let us consider the table 1 for the trust level.

| Reputation is bad | Similarity is Low | Reputation is Average | Similarity is high |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 0.05 | 0.08 | 0.2 | 0.3 |
| 0.08 | 0.1 | 0.23 | 0.35 |
| 0.1 | 0.13 | 0.3 | 0.4 |
| 0.12 | 0.2 | 0.4 | 0.5 |
| | | | |

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

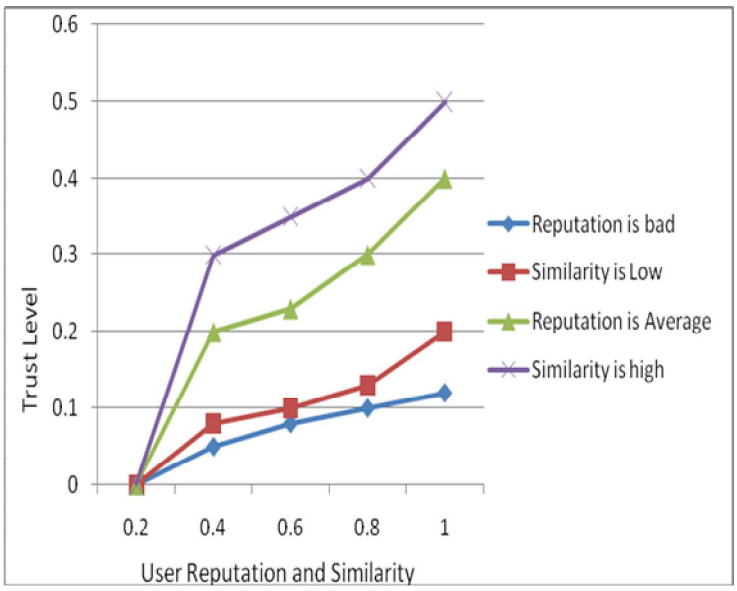
International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

Graph




Explanation:
Given graph show the user reputation and similarity of users. This provides user information to share the information or not.

## IX. CONCLUSION

In this project, the investigation is done of the problem related to privacy protection and sharing large medical data in cloudlets and the remote cloud. Developed a system which does not allow users to transmit data to the remote cloud in consideration of secure collection of data, as well as low communication cost. However, it does allow users to send data to a cloudlet, which triggers the data sharing problem in the cloudlet. Firstly, we can utilize body info module to collect users' data, and in order to protect user's privacy, NTRU mechanism is used to make sure the transmission of users' data to cloudlet is secure. Secondly, for the purpose of sharing data in the cloudlet, the trust model is used to measure users' trust level to judge whether to share data or not. Thirdly, for privacy-preserving of remote cloud data, the data is partitioned on remote cloud and it encrypts the data in different ways, so as to not just ensure data protection but also accelerate the efficiency of transmission. Finally, IDS based on cloudlet mesh to protect the whole system is used. User can asks the question to the doctor online and doctor gives the answer to user.

## REFERENCES

[1] A. Sajid and H. Abbas, "Data privacy in cloud-assisted healthcare systems: State of the art and future challenges," Journal of Medical Systems, vol. 40, no. 6, pp. 1–16, 2016.
[2] R. Mitchell and I.-R. Chen, "Behaviour rule specification-based intrusion detection for safety critical medical cyber physical systems," Dependable and Secure Computing, IEEE Transactions on, vol. 12, no. 1, pp. 16–30, 2015.
[3] Y. Shi, S. Abhilash, and K. Hwang, "Cloudlet mesh for securing mobile clouds from intrusions and network attacks," in The Third IEEE International Conference on Mobile Cloud Computing, Services, and Engineering,(Mobile Cloud 2015). IEEE, 2015.
[4] M. Quwaider and Y. Jararweh," Cloudlet-based efficient data collection in wireless body area networks," Simulation Modelling Practice and Theory, vol. 50, pp. 57–71, 2015.
[5] M. S. Hossain, "Cloud-supported cyber–physical localization framework for patients monitoring," 2015.
[6] J. Zhao, L. Wang, J. Tao, J. Chen, W. Sun, R. Ranjan, J. Kołodziej, A. Streit, and D. Georgakopoulos, "A security framework in g-hadoop for big data computing across distributed cloud data centres," Journal of Computer and System Sciences, vol. 80, no. 5, pp. 994–1007, 2014.
[7] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 1, pp. 222–233, 2014.

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

International Journal of Innovative Research in Computer and Communication Engineering

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Website: www.ijircce.com*

**Vol. 6, Issue 5, May 2018**

[8] H. Mohamed, L. Adil, T. Saida, and M. Hicham, "A collaborative intrusion detection and prevention system in cloud computing," in AFRICON, 2013. IEEE, 2013, pp. 1–5.
[9]R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," in Cloud Computing (CLOUD), 2010 IEEE 3rdInternational Conference on. IEEE, 2010, pp. 268–275.
[10] K. Hung, Y. Zhang, and B. Tai, "Wearable medical devices for telehome healthcare," in Engineering in Medicine and Biology Society, 2004. IEMBS' 04.26th Annual International Conference of the IEEE, vol. 2. IEEE, 2004, pp. 5384–5387.