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 6, June 2018

Medical Data Sharing for Protection and Intrusion Avoidance in Cloudlet

Gite Snehal Sukhadeo, Patil Swati .H

Department of Computer Engineering, Jayawantrao Swant College of Engineering, Hadapsar, Pune, Maharashtra, India.

ABSTRACT: An individual's medical record is a vital form that can be used to track patient data accurately, reliably and completely. For all purposes, the exchange of repair information is a basic and test problem. Consequently, in this document, we develop a new structure for human services through the use of cloudlet adaptability. Cloudlet elements include security insurance, information exchange, and breakpoint location. In the information accumulation phase, we initially used the Numerical Theory Research Unit (NTRU) technique to encode client body information collected from a portable device. This information will be send to near cloudlets in a competent form of vitality. In addition, we show another model of trust to allow customers to choose trusted partners who want to share data stored in the cloudlet. The demonstration of trust also makes comparable patients who talk to each other about their illnesses. Third, we isolate the patient's medical information stored at a distance in three sections and provide them with adequate insurance.

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

I. INTRODUCTION

This medical information in the social network is sensitive for both patients and doctors. On data encrypted in cloud computing, a privacy protection system was presented, which main to provide users with a many keyword method for information

encrypted in the cloud [1]. Although this way can provide a result, in which people are interested, the amount of calculations can be cumbersome. A priority-based health aggregation scheme (PHDA) was presented to protect and aggregate different types of health data in the Wireless-Assisted Wireless Network (WBAN) area. The article examines security and privacy issues in mobile health care networks, including privacy protection for health data aggregation, data security and misconduct [2]. Describes a flexible security model especially for cloud-centric data-driven applications to ensure data privacy, data integrity and detailed access control to application data. Offers a systematic bibliographic review of privacy protection in the cloud-assisted healthcare system.

Motivation

We divide data in the remote cloud into different types and we use the encryption mechanism to protect, respectively. We offer cloud mesh collaboration identities to protect the entire health system from malicious attacks.

II. REVIEW OF LITERATURE

A. Sajid and H. Abbas [1]. The system is protected by privacy in which the cloud does not see neither the original samples nor the underlying date. And manipulate the noise. We have proposed a monitoring system of assisted health care in the cloud and awareness of privacy through compression sensors. The protection based on random mapping does not provide sensitive samples that leave the sensor unprotected. Wireless sensors are used to monitor / collect information in medical health systems. Despite growing popularity, the way to efficiently manage growing healthcare and protect data privacy while keeping sensor overload low remains a challenge.

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 6, June 2018

R. Mitchell and I.-R. Chen [2]. We demonstrate that our intrusion detection technique can effectively exchange false positives for safe and protected MCPS applications. For critical safety MCPS, it is very important to detect the attackers by limiting the false alarm to protect the well-being of the patients. We plan to analyze the overloading of our detection techniques. We propose and analyze a rules-based technique for detecting intrusions of medical devices integrated into a cybernetic medical system (MCPS) in which patient safety is of utmost importance.
Y. Shi, S. Abhilash, and K. Hwang [3]. We have specified a sequence of authentication, authorization and encryption protocols to ensure communications between mobile devices, cloud servers and clouds away. The protection of mobile cloud services is the barrier to the integration of BTOD (bring your own devices) and BYOC (bring your own cloud) to our daily applications. We use the cloudlet to perform collaborative intrusion detection across multiple cloudlets. Cloud Networks in our daily life operations. We extend their work to support cloud security features.
M. S. Hossain [4]. Gaussian blending modelling for localization has proven to overcome other similar methods in terms of error estimation. The design and development of such systems requires access to substantial sensors and contextual user data stored in cyberspace. We will perform more workload measurements to record the use of CPU resources, memory, and storage and network bandwidth. This allows a wide range of emerging applications or systems, such as patient or health monitoring that require detection of patient positions.
M. Quwaider and Y. Jararweh [5]. For the delay of the end-to-end package by dynamically choosing the adjacent cloudlet, I know that the overall delay is reduced to a minimum. The goal was to minimize the cost of the end-to-end package by dynamically choosing data from the cloud using the cloud-based system. The performance of the proposed system has been evaluated through the extended version of the CloudSim simulator. It is scalable, on request, powerful and protects the 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 cloud. Reduce the large-scale distributed processing framework across multiple data centres with multiple clusters. The designed security framework has the ability to avoid the most common attacks, such as the MITM attack, and to delay the secure communication of GHadoop on public networks. Map Reduction activities are first planned in clusters using the Hadoop scheduling policy, and then among processing nodes that use the cluster scheduler that exists in the destination clusters.
N. Cao, C. Wang, M. Li, K. Ren, and W. Lou [7]. First of all, we offer a basic idea for classified search of multiple words in encrypted data in the cloud (MRSE). We used a methodical approach to the study of security models and security requirements for cloud applications. We discuss concepts related to EHR exchange and integration in health care and analysis. The widespread use of electronic medical records (EHR), the creation of a secure EHR exchange environment, has attracted much attention both in the health sector and in the academic community.
H. Mohamed, L. Adil, T. Saida, and M. Hicham [8]. We proposed a collaborative model of the IDS and IPS intrusion detection and prevention system, using a hybrid detection technique to address the problems of those who were attacked. Cloud computing: open source algorithm for new attack signatures. Security solutions are not yet adapted to this new concept. In fact, in that environment, the more customers and streets there are, the greater the actual intrusion. We have also incorporated the signature opening algorithm to enrich and update our database. Cloud computing has become a model for processing large volumetric data. They are able to offer a variety of fundamental aspects, such as virtualization management, error tolerance and load balancing.
R. Zhang [9]. I discovered a new EHR. We have taken a methodical approach to study security models and cloud security requirements for healthcare. We discussed important concepts in the exchange of EHR and integration in health care and analysis. The widespread use of electronic medical records (EHR), the creation of a secure EHR exchange environment has attracted many concerns both in the health sector and in the academic community.
K. Hung, Y. Zhang, and B. Tai [10]. A sleeveless blood pressure monitor was studied and tested on 30 subjects in a total of 71 studies over a five month period. The use of mobile communication is no longer limited to telephony. Wireless data and multimedia services, since 3G phones are available. The aging and global prevalence of chronic diseases has led to a great demand for home health care, in which vital signs are essential.

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 6, June 2018

III. PROPOSED SYSTEM

In this project, this document proposes a cloud-based human services framework. Body information collected from the mobile device is transmitted to the adjacent cloudlet. This information is transmitted in addition to the remote cloud. In the main phase, the vital signs of the user are collected by portable devices. At this stage, information security is the main concern. In the second phase, customer information will be transmitted in addition to the remote cloud through the cloudlets. A cloudlet is framed by a specific number of mobile phones whose properties may require, as well as some particular information. In this way, both security and information exchange are considered at this stage. Above all, we use the model of trust to evaluate the exchange of information or not. Considering that customer restoration information is stored in a remote cloud, we characterize these medicinal data in different types and adopt the related security approach. In addition to ensuring information security for more than three phases, we also consider community-oriented IDS in the light of the cloudlet. We have proposed the google map to show the record. We proposed a technique of questions and answers between the user and the doctors.

IV. SYSTEM ARCHITECTURE

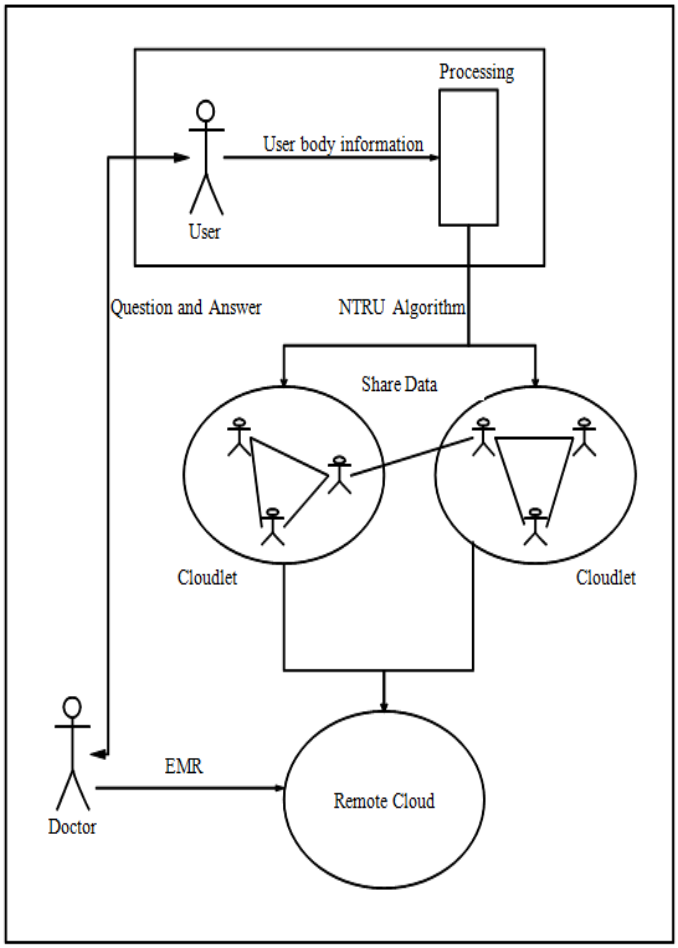


Fig 1. Architecture Diagram

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 6, June 2018

User body information and provides the privacy for user information and transmits to cloudlet. But we provide the privacy of user information. Using cloudlet we transfer this information to remote cloud. User share their information based on cloudlet. User request for sharing information to other user and then trust authority check the both user body information similarity. After that user share their information. User asks question to doctor and doctor provide the answer.

V. MATHEMATICAL MODEL

Mathematical Function and Notation used in the Algorithms:
The key generation scheme is used to generate the private and public key pair. The process begins by choosing two small polynomials f and g, where small is defined as having coefficients much smaller than the large modulo p and modulo q.

The user must compute the inverse of f modulo q and the inverse of f modulo p such that f * fq = 1 (mod q) and f * fp = 1 (mod p). The inverse of f is calculated both modulo p and modulo q, generating fp = f-1 (mod p) and fq = f-1 (mod q). The values of f and fp are retained as the private key pair and the public key h is calculated using p, fq and g [8]. The public key is as follows:
h = pfq * g (mod q) (1)

NTRU encryption
The encryption process starts by generating a polynomial message m whose coefficients lie in an interval of length q, which is normally cantered around zero. A small random blinding polynomial, r, is then generated and used to obscure the message [8]. The final 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) (2)

NTRU decryption
The decryption process first uses the private key f to calculate:
a = f * e (mod q) (3)
The coefficients of a must be chosen in the proper interval of length q to ensure the highest probability that the decryption process will be successful. Once the coefficients of a are chosen on the proper interval, a is reduced modulo p and the second private key is used to compute:
b = a (mod p) (4)
c = fp * b (mod p) (5)
If decryption has successfully completed, then the polynomial c will be equal to the original message

VI. 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).

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 6, June 2018

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)

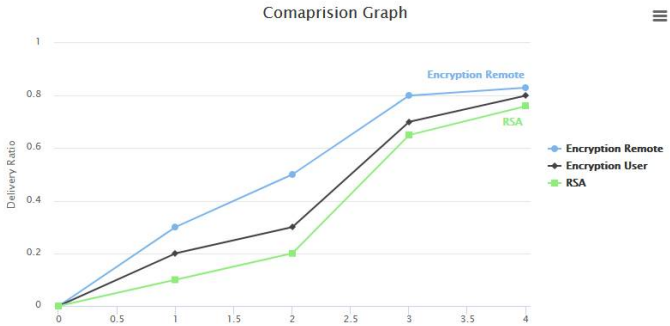
If decryption has successfully completed, then the polynomial c will be equal to the original message.

VII. EXPERIMENTAL SET UP

Let us consider the table 1 for the trust level.

Trust Level	Similarity
0	0.2
0.53	0.4
0.3	0.6
0.8	0.8

Graph



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

VIII. CONCLUSION

In this project, we analyze the problem of privacy protection and share large medical data in Cloudlet and in the remote cloud. We are a system that does not allow users to transmit data to the remote cloud in view of a secure data collection, as well as low communication costs. However, it allows users to send data to a cloudlet, which triggers the problem of data sharing in the cloudlet. First of all, we can use portable devices to collect user data and to protect users' privacy, we use the NTRU mechanism to ensure the transmission of user data to the cloud in security. Trust the cloudlet, we use trust to measure users Third, to preserve the privacy of remote data in the cloud, we divide data stored in the remote cloud and encrypt data in different ways Finally, we proposed cloud-based IDS collaboration to protect the whole system. Response to the user.

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 6, June 2018

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.
[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.