SJIF Impact Factor: 7.001| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)

EPRA International Journal of Research and Development (IJRD)

Volume: 5 | Issue: 12 | December 2020 - Peer Reviewed Journal

PRIVACY PROTECTION AND INTRUSION AVOIDANCE FOR CLOUDLET-BASED MEDICAL DATA SHARING

Preethi.S

Department of computer science & IT, Jain University, Bangalore, India

Article DOI: https://doi.org/10.36713/epra5789

ABSTRACT

Remote health monitoring and older health care has become a popular application with the advance of wearable medical devices. Privacy protection and intrusion avoidance for cloudlet- based medical data sharing data collected from patients through wearable devices (such as heartbeat, blood pressure, etc.) must be passed to cloud-run applications to implement various services such as expert advice, emergency assistance, etc.

The cloud storage system provides distributed clients with convenient file storage and sharing services. To solve integrity, we present identity based data outsourcing , outsourcing and original auditing concerns about outsourced documents, the program is equipped with an ideal feature that factilitates existing recommendations to protect outsourcing data.

1. INTRODUCTION

Privacy protection and intrusion avoidance the huge amount of data collected by body area network(BAN) nodes requires scalable, on-demand, powerful, and secure storage and processing infrastructure. Projects reports on Privacy protection and intrusion cloud computing plays an important role in achieving the aforementioned objects.

Project on Privacy protection and intrusion avoidance for cloudlet- based medical data sharing. The cloud computing environment connects different devices ranging from miniaturized sensor nodes to high-performance supercomputer to deliver people-centric and context-centric services to individuals and industries. The possible integration of BANs with cloud computing will introduce a viable and hybrid platform that must be able to process the enormous amount of data collected from multiple BANs

With the development of healthcare big data and wearable technology as well as cloud computing and communication technologies cloud-assisted healthcare big data computing becomes critical to meet users evergrowing demands on health consultation .The trace of the disease treatment process for the retrieval of realtime disease information .Healthcare social platform, such as Patients Like Us can obtain information from other similar patients through data sharing in terms of user's own findings. Though sharing 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 . Therefore, how to balance privacy protection with the convenience of medical data sharing becomes a challenging issue. With the advances in cloud computing, a large amount of data can be stored in various clouds including cloudlets and remote clouds facilitating data sharing and intensive computation

2. LITERATURE SURVEY

2.1"Data privacy in cloud-assisted healthcare systems: State of the art and future challenges".

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.

2.2"Behaviour rule specification-based intrusion detection for safety critical medical cyber physical systems".

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.

2.3"Cloudlet mesh for securing mobile clouds from intrusions and network attacks".

We have specified A sequence of authentication, authorization, and encryption protocols for securing communications among mobile devices, cloudlet servers, and distance clouds.

2.4 "Cloudlet-based efficient data collection in wireless body area networks".

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.

2.5 "Privacy-preserving multi-keyword ranked search over encrypted cloud data".

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.

2.6"A collaborative intrusion detection and prevention system in cloud computing".

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.

2.7 "Security models and requirements for healthcare application clouds".

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.

3. PROPOSED SYSTEM

- ✓ In this project, this paper proposes a cloudlet based human services framework. The body information gathered by wearable device is transmitted to the adjacent cloudlet. That information is additionally conveyed to the remote cloud where specialists can get for disease finding.
- ✓ In the main stage, user's vital signs gathered by wearable gadgets 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 toward 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.
- ✓ Considering the client's medical information are put away in remote cloud, we order these medical information into various types and take the relating security approach. Not with standing over three phases based information security assurance.

4. MODULES EXPLANATION

1. Patient

In this module, there are numbers of patient are there. Patient should register to the application before they do some operation into applications and register patient details are stored in patient module. After registration successful they has to login by using authorized username or email and password. After that they will do some operations like Send Appointment Request to doctor, Access Request from doctor, Receive Prescription from doctor

2. Doctor

- Doctor should Login to the application.
- Doctor can view Patient Request
- Doctor can send Request Access to Cloudlet one or two
- Doctor can view patient information's
- Doctor can update patient health records like BP,Send prescription details to patient

3. CloudLet

In this module, the Cloudlet has to login to application by using username and password. After login successful they can do some operations such as Add Doctor details, View all Doctor Information, view Patient, and view the Intruder Detection Details

4. Intruder

Intruder Login to application Intruder can view patient records and it is encrypted format Intruder can try to modify patient data means alert notification will send to patient or cloudlet

5. SYSTEM ARCHITECTURE

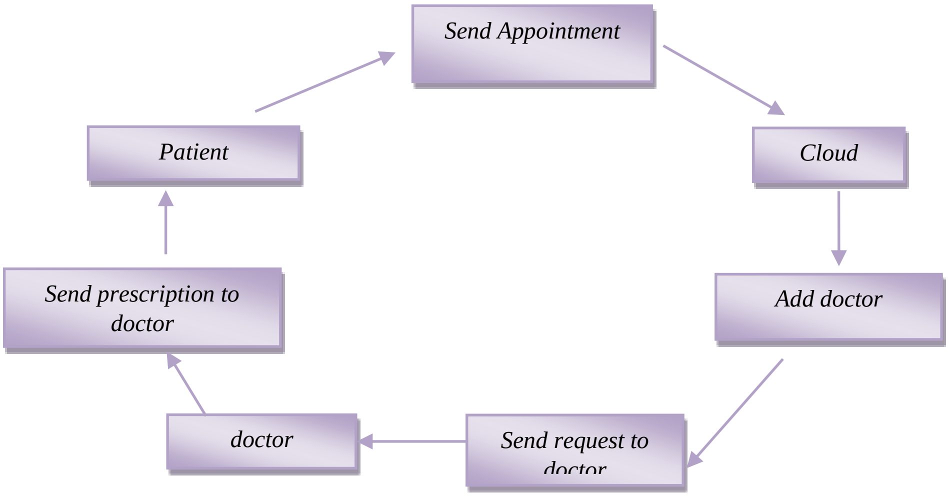
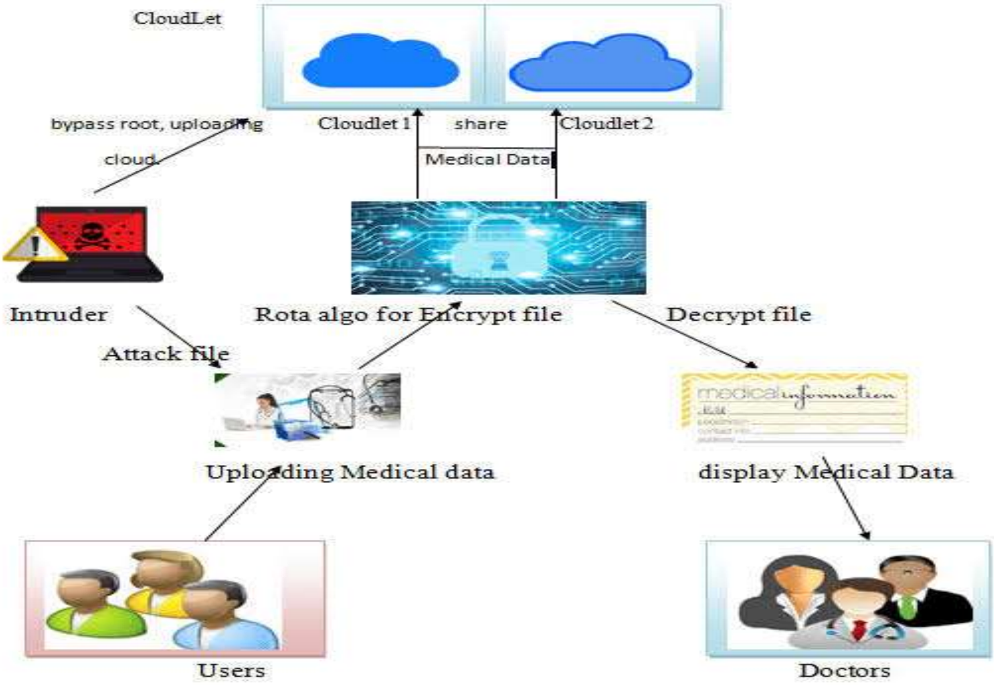


Fig.5.1 System architecture

In this figure the patient has login to application and send the appointment request to cloud owner and then cloud owner view the request of patient and choose the doctor according to patient details and doctor has to login to application and can view the patient request and send the prescription to the patient. Patient can view the prescription report and patient has to send a received message to the doctor.

6. DATA FLOW DIAGRAM



6.1Data Flow Diagram Dataflow Diagram

It is a defined as a graphical representation of how the data flow through a data system and also models its process aspects. The DFD represents what type of data is given to system in form of out and what kind of output will be received from the output

7. RELATED WORK

Our work is closely related to cloud-based privacy preserving and cloudlet mesh based collaborative IDS. We will give a brief review of the works in these aspects. Cloud-based Privacy Preservation Despite the development of the cloud technology and emergence of more and more cloud data sharing platforms, the clouds have not been widely utilized for healthcare data sharing due to privacy concerns . There exist various works on conventional privacy protection of healthecare data .

In Lu et al. a system called SPOC, which stands for the secure and privacy-preserving opportunistic computing framework, was proposed to treat the storage problem of healthcare data in a cloud environment and addressed the problem of security and privacy protection under such an environment.

The article proposed a compound resolution which applies multiple combined technologies for the privacy protection of healthcare data sharing in the cloud environment. In Cao et al. an MRSE (multikeyword 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. Although this method can provide result ranking, in which people are interested, the amount of calculation could be cumbersome. In Zhang et al. a priority based health data aggregation (PHDA) scheme was presented to protect and aggregate different types of healthcare date in cloud assisted wireless boby 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. 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. give a systematic literature review of privacyprotection in cloud-assisted healthcare system.

Collaborative IDS based on cloudlet mesh A number of prior works have studied different intrusion detection systems with quite some advances. For example, proposed a behavior-rule specification-based technique for intrusion detection. The main contribution is the performance outperforms other methods of anomaly-based techniques.

Proposed a collaborative model for the cloud environment based on distributed IDS and IPS (intrusion prevention system). This model makes use of a hybrid detection technique to detect and take corresponding measures for any types of intrusion which harm the system, especially distributed intrusion. However, collaborative IDS based on the cloudlet mesh structure is a new kind of intrusion detection technique, which was first proposed in Shi et al.

8. ADVANTAGES AND DISADVANTAGES

8.1 ADVANTAGES

- A cloudlet based healthcare system is presented, where the privacy of users' physiological data and the efficiencyof data transmissions are our main concern. We use NTRU for data protection during data transmissions to thecloudlet.
- So as to share information in the cloudlet, we utilize client comparability and notoriety to develop confide in show.
- We isolate information in remote cloud into various types and use encryption system to ensure them individually.

8.2 DISADVANTAGES

- Sources communication energy feeding.
- Virtually, medical records sharing is a dangerous and stimulating issues
- Causes communication energy consumption. Practically, medical data sharing is a critical and challenging issue No Trust.

9. CONCLUSIONS

In this paper, we investigated the problem of privacy protection and sharing large medical data in cloudlets and the remote cloud. We 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 transmit data to a cloudlet, which triggers the data sharing problem in the cloudlet. Firstly, we can utilize wearable devices to collect users' data, and in order to protect users privacy Cost and detection rate of the entire IDS system. The optimal configuration is shown to use 4 IDS's with a 75% detection rate under a minimum system cost of 0.02. Only relative costs are shown here. make sure the transmission of users' data to cloudlet in security. Secondly, for the purpose of sharing data in the cloudlet, we use trust model to measure users' trust level to judge whether to share data or not. Thirdly, for privacy-preserving of remote cloud data, we partition the data stored in the remote cloud and encrypt the data in different ways, so as to not just ensure data protection but also accelerate the efficacy of transmission. Finally, we propose collaborative IDS based on cloudlet mesh to protect the whole system. The proposed schemes are validated with simulations and experiments.

10. REFERENCES

1. *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.*
2. *K. He, J. Chen, R. Du, Q. Wu, G. Xue, and X. Zhang, "Deypos: Deduplicatable dynamic proof of storage for multi-user environments," 2016.*
3. *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.*
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. *K. Dongre, R. S. Thakur, A. Abraham et al., "Secure cloud storage of data," in Computer Communication and Informatics (ICCCI), 2014 International Conference on. IEEE, 2014, pp. 1–5.*
6. *M. S. Hossain, G. Muhammad, M. F. Alhamid, B. Song, and K. AlMutib, "Audiovisual emotion recognition using big data towards 5g," Mobile Networks and Applications, pp. 1–11, 2016.*
7. *J.-J. Yang, J.-Q. Li, and Y. Niu, "A hybrid solution for privacy preserving medical data sharing in the cloud environment," Future Generation Computer Systems, vol. 43, pp. 74–86, 2015.*
8. *W. Xiang, G. Wang, M. Pickering, and Y. Zhang, "Big video data for light-fieldbased 3d telemedicine," IEEE Network, vol. 30, no. 3, pp. 30– 38, 2016.*