Intrusion Avoidance and Privacy Protection For cloudlet based medical data sharing

[1]S.Shivani, [2]SK. Althaf Rahaman
[1]Student, [2]Assistant Professor
Science,GIS,GITAM(Deemed to be University)

Abstract - **Remote health monitoring and older health care has become a popular application with the advancement 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 (IBDO), outsourcing and original auditing concerns about outsourced documents, the program is equipped with an ideal feature that facilitates existing recommendations to protect outsourcing data. In this project we propose a cloud let based solution for providing enhanced security to patient health care data**

keywords - **cloud, cloudlet, encryption, intruders, security, wearable devices**

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 objectives.

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 supercomputers 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. Both the cloud providers and the users must take strong security measures to protect the storage infrastructure.

PURPOSE OF THE PROJECT

The current application is being designed to satisfy the day to day activities to be exhausted a typical hospital environment. Right from patient enquiry till discharge of the patient all the activities need to be automated within the online enabled application.

EXISTING SYSTEM PROBLEM

- Communication energy Causes consumption.
- Practically, medical data sharing is a critical and challenging issue
- No Trust.

PROPOSED SYSTEM

- This paper proposes a cloudlet based healthcare system. The body data collected by wearable devices are transmitted to the nearby cloudlet. Those data are further delivered to the remote cloud where doctors can access for disease diagnosis.
- According to data delivery chain, we separate the privacy protection into three stages. In the first stage, user's vital signs collected by wearable devices are delivered to a closet gateway of cloudlet. During this stage, data privacy is the main concern. In the second stage, user's data will be further delivered toward remote cloud through cloudlets.
- A cloudlet is formed by a certain number of mobile devices whose owners may require and/or share some specific data contents. Thus, both privacy protection and data sharing are considered in this stage. Evaluate trust level between users to determine sharing data or not.
- Considering the users' medical data are stored in remote cloud, we classify these medical data into different kinds and take the corresponding security policy.
- In addition to above three stages based data privacy protection, we also consider collaborative IDS based on cloudlet mesh to protect the cloud ecosystem.

NUMBER OF MODULES

- Patients
- Doctors
- Administration

ADVANTAGES OF PROPOSED SYSTEM

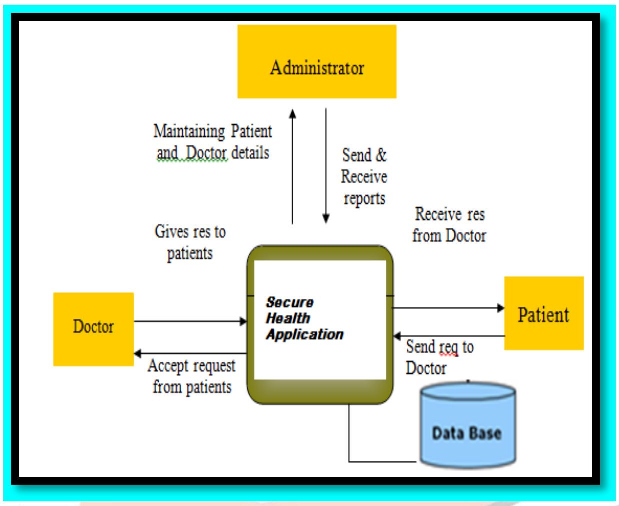
- A cloudlet based healthcare system is presented, where the privacy of users' physiological data and the efficiency of data transmissions are our main concern. We use NTRU for data protection during data transmissions to the cloudlet.
- In order to share data in the cloudlet, we use users' similarity and reputation to build up trust model. Based on the measured users' trust level, the system determines whether data sharing is performed.
- We divide data in remote cloud into different kinds and utilize encryption mechanism to protect them respectively.
- We propose collaborative IDS based on cloudlet mesh to protect the whole healthcare system against malicious attacks.

Patients

The Patients module keeps track of entire information concerning patient right from the first time he comes for diagnosis. The diagnosis results and thus the value incurred for each test are getting to be maintained Scheduling the appointments and operations are getting to be done upon synchronizing the availability of doctor also as exigency of appointment or operation.

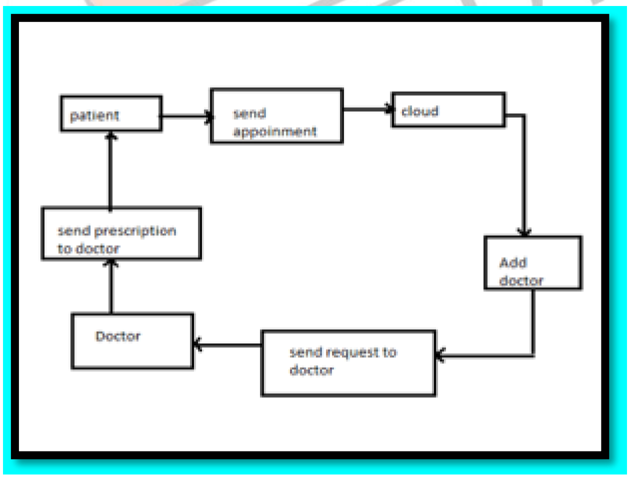
Doctors

The Doctors module keeps track of doctor's personal information and their available timings in hospital. Scheduling the appointments and operations are getting to be done upon synchronizing the availability of doctor also as exigency of appointment or operation.



Administration: The administration module will be having track of all expenses incurred during patient diagnosis. It should also maintain information related to bed occupancy in hospital. Billing is that the key activity during this module.

DATAFLOW DIAGRAM
SYSTEM ARCHITECTURE



CONCLUSION

Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing Cloud computing is the trend and emerging technology nowadays. Projects reports on Privacy Protection and Intrusion the security problem is the main problem in cloud computing. We investigated the privacy issue and shared large medical data in cloudlets and remote cloud.

Project on Privacy Protection and Intrusion We developed a system that does not allow users to transmit data to the remote cloud considering secure data collection as well as low communication costs. It allows users to transmit data to a cloudlet, however, which triggers the cloudlet data sharing problem.

REFERENCES

[1] M. Quwaider and S. Biswas, "Delay Tolerant Routing Protocol Modelling for Low Power Wearable Wireless Sensor Networks," Netw. Protoc. Algorithms, vol. 4, no. 3, pp. 15–34, 2012 .

[2] D. Chappell, "Introducing the Azure services platform," White Pap. Oct, vol. 1364, no. 11, 2008

[3] M. Quwaider, M. Taghizadeh, and S. Biswas, "Modelling on-body DTN packet routing delay in the presence of postural disconnections," EURASIP J. Wirel. Commun. Netw., vol. 2011, p. 3, 2011.

[4] T. Soyata, R. Muraleedharan, C. Funai, M. Kwon, and W. Heinzelman, "Cloud-Vision: Real-time face recognition using a mobile-cloudlet-cloud acceleration architecture," in