Privacy Protection and Intrusion Avoidance forCloudlet-based Medical Data Sharing

ABSTRACT:

With the popularity of wearable devices, along with the development of clouds and cloudlet technology, there has beenincreasing need to provide better medical care. The processing chain of medical data mainly includes data collection, data storage anddata sharing, etc. Traditional healthcare system often requires the delivery of medical data to the cloud, which involves users' sensitiveinformation and causes communication energy consumption. Practically, medical data sharing is a critical and challenging issue. Thusin this paper, we build up a novel healthcare system by utilizing the flexibility of cloudlet. The functions of cloudlet include privacyprotection, data sharing and intrusion detection. In the stage of data collection, we first utilize Number Theory Research Unit (NTRU)method to encrypt user's body data collected by wearable devices. Those data will be transmitted to nearby cloudlet in an energyefficient fashion. Secondly, we present a new trust model to help users to select trustable partners who want to share stored data in thecloudlet. The trust model also helps similar patients to communicate with each other about their diseases. Thirdly, we divide users'medical data stored in remote cloud of hospital into three parts, and give them proper protection. Finally, in order to protect thehealthcare system from malicious attacks, we develop a novel collaborative intrusion detection system (IDS) method based on cloudletmesh, which can effectively prevent the remote healthcare big data cloud from attacks. Our experiments demonstrate the effectivenessof the proposed scheme.

EXISTING SYSTEM:

- Lu etal. proposed a system called SPOC, which stands for the secureand privacy-preserving opportunistic computing framework, waspropposed to treat the storage problem of healthcare data in acloud environment and addressed the problem of security andprivacy protection under such an environment.
- 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).

DISADVANTAGES OF EXISTING SYSTEM:

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

PROPOSED SYSTEM:

- This paper proposes a cloudletbased healthcare system. The body data collected by wearabledevices are transmitted to the nearby cloudlet. Those data arefurther delivered to the remote cloud where doctors can access fordisease diagnosis.
- According to data delivery chain, we separatethe privacy protection into three stages. In the first stage, user'svital signs collected by wearable devices are delivered to acloset gateway of cloudlet. During this stage, data privacy is themain concern. In the second stage, user's data will be furtherdelivered toward remote cloud through cloudlets.
- A cloudlet isformed by a certain number of mobile devices whose ownersmay require and/or share some specific data contents. Thus, bothprivacy protection and data sharing are considered in this stage.Especially, we use trust model to evaluate trust level between usersto determine sharing data or not.
- Considering the users' medicaldata are stored in remote cloud, we classify these medical datainto different kinds and take the corresponding security policy.
- Inaddition to above three stages based data privacy protection, wealso consider collaborative IDS based on cloudlet mesh to protectthe cloud ecosystem.

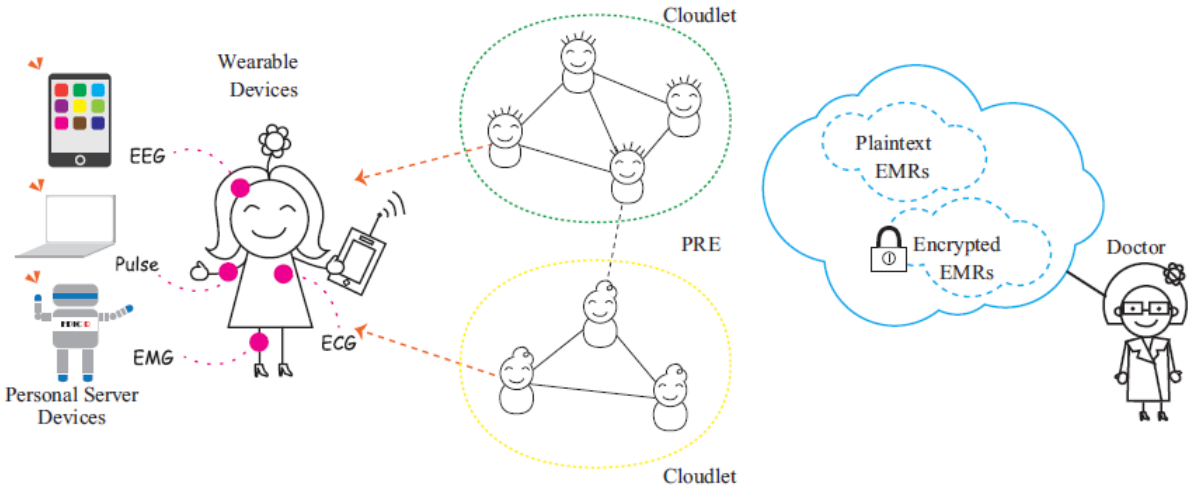
ADVANTAGES OF PROPOSED SYSTEM:

- A cloudlet based healthcare system is presented, wherethe privacy of users' physiological data and the efficiencyof data transmissions are our main

concern. We useNTRU for data protection during data transmissions to thecloudlet.

- ❖ In order to share data in the cloudlet, we use users'similarity and reputation to build up trust model. Basedon the measured users' trust level, the system determineswhether data sharing is performed.
- ❖ We divide data in remote cloud into different kinds andutilize encryption mechanism to protect them respectively.
- ❖ We propose collaborative IDS based on cloudlet meshto protect the whole healthcare system against maliciousattacks.

SYSTEM ARCHITECTURE:



SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

- ➢ System : Pentium Dual Core.

- Hard Disk : 120 GB.
- Monitor : 15'' LED
- Input Devices : Keyboard, Mouse
- Ram : 1 GB

SOFTWARE REQUIREMENTS:

- Operating system : Windows 7.
- Coding Language : JAVA/J2EE
- Tool : Netbeans 7.2.1
- Database : MYSQL

REFERENCE:

Min Chen, *Senior Member*, *IEEE*, Yongfeng Qian, Jing Chen,Kai Hwang, *Fellow*, *IEEE*, Shiwen Mao, *Senior Member*, Long Hu, "Privacy Protection and Intrusion Avoidance forCloudlet-based Medical Data Sharing", **IEEE Transactions on Cloud Computing, 2017.**