**Privacy Protection and Intrusion Avoidance for Cloudlet-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.

**Index Terms**—privacy protection, data sharing, collaborative intrusion detection system (IDS), healthcare.

**EXISTING SYSTEM:**

* Previous work suggested the combination of socialnetworks and healthcare service to facilitate the trace of thedisease treatment process for the retrieval of realtime diseaseinformation.
* There exist various works on conventionalprivacy protection of healthecaredata . In Lu etal., a system called SPOC, which stands for the secureand privacy-preserving opportunistic computing framework, wasproposed to treat the storage problem of healthcare data in acloud environment and addressed the problem of security andprivacy protection under such an environment.
* In Cao et al. [11], an MRSE (multikeywordranked search over encrypted data in cloud computing)privacy protection system was presented, which aims to provideusers with a multi-keyword method for the cloud’s encrypted data.

**DISADVANTAGES OF EXISTING SYSTEM:**

* Although this method can provide result ranking, in which peopleare interested, the amount of calculation could be cumbersome.
* How to make sure the data sharing in cloudlet will notcause privacy problem?
* How to effectively protect the whole system from maliciousattacks?

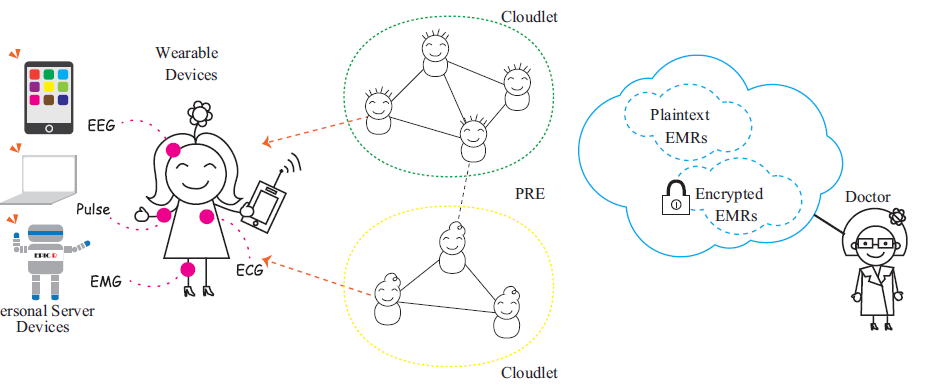
**PROPOSED SYSTEM:**

* 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.

**ADVANTAGES OF PROPOSED SYSTEM:**

* We use mechanism tomake sure the transmission of users’ data to cloudlet in secure.
* We usetrust model to measure users’ trust level to judge whether to sharedata or not.
* For privacy-preserving of remote cloud data,we partition the data stored in the remote cloud and encrypt thedata in different ways, so as to not just ensure data protection butalso accelerate the efficacy of transmission.

**SYSTEM ARCHITECTURE:**



**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium Dual Core.
* Hard Disk : 120 GB.
* Monitor : 15’’ LED
* Input Devices : Keyboard, Mouse
* Ram : 1GB.

**SOFTWARE REQUIREMENTS:**

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

**REFERENCES**

* 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] M. S. Hossain, “Cloud-supported cyber–physical localization framework for patients monitoring,” 2015.
* [3] 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.
* [4] M. S. Hossain and G. Muhammad, “Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring,” *Computer Networks*, vol. 101, pp. 192–202, 2016.
* [5] R. Zhang and L. Liu, “Security models and requirements for healthcare application clouds,” in *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*. IEEE, 2010, pp. 268–275.