Privacy Preserving Cloud-assisted mobile health (mHealth) monitoring

**ABSTRACT**

Cloud-assisted mobile health (mHealth) monitoring, which applies the prevailing mobile communications and cloud computing technologies to provide feedback decision support, has been considered as a revolutionary approach to improving the quality of healthcare service while lowering the healthcare cost. Unfortunately, it also poses a serious risk on both clients’ privacy and intellectual property of monitoring service providers, which could deter the wide adoption of mHealth technology. This paper is to address this important problem and design a cloud assisted privacy preserving mobile health monitoring system to protect the privacy of the involved parties and their data. Moreover, the outsourcing decryption technique and a newly proposed key private proxy re-encryption are adapted to shift the computational complexity of the involved parties to the cloud without compromising clients’ privacy and service providers’ intellectual property. Finally, our security and performance analysis demonstrates the effectiveness of our proposed design.

**SYSTEM ANALYSIS**

**EXISTING SYSTEM:**

Traditional privacy protection mechanisms by simply removing clients’ personal identity information (such as names or SSN) or by using anonymization technique fails to serve as an effective way in dealing with privacy of mHealth systems due to the increasing amount and diversity of personal identifiable information.

Traditionally, the privacy issue is tackled with anonymization technique such as *k*-anonymity or *l*-diversity. However, it has been indicated that these techniques might be insufficient to prevent re-identification attack

**DISADVANTAGES OF EXISTING SYSTEM:**

Unfortunately, although cloud-assisted mHealth monitoring could offer a great opportunity to improve the quality of healthcare services and potentially reduce healthcare costs, there is a stumbling block in making this technology a reality. Without properly addressing the data management in an mHealth system, clients’ privacy may be severely breached during the collection, storage, diagnosis, communications and computing.

Another major problem in addressing security and privacy is the computational workload involved with the cryptographic techniques. With the presence of cloud computing facilities, it will be wise to shift intensive computations to cloud servers from resource-constrained mobile devices. However, how to achieve this effectively without compromising privacy and security become a great challenge, which should be carefully investigated.

**PROPOSED SYSTEM:**

In this paper, we design a cloud-assisted mHealth monitoring system (CAM). We first identify the design problems on privacy preservation and then provide our solutions. To ease the understanding, we start with the basic scheme so that we can identify the possible privacy breaches. We then provide an improved scheme by addressing the identified privacy problems. The resulting improved scheme allows the mHealth service provider (the company) to be offline after the setup stage and enables it to deliver its data or programs to the cloud securely.

To reduce clients’ decryption complexity, we incorporate the recently proposed outsourcing decryption technique into the underlying multi-dimensional range queries system to shift clients’ computational complexity to the cloud without revealing any information on either clients’ query input or the decrypted decision to the cloud. To relieve the computational complexity on the company’s side, which is proportional to the number of clients, we propose a further improvement, leading to our final scheme. It is based on a new variant of key private proxy re-encryption scheme, in which the company only needs to accomplish encryption once at the setup phase while shifting the rest computational tasks to the cloud without compromising privacy, further reducing the computational and communication burden on clients and the cloud

**ADVANTAGES OF PROPOSED SYSTEM:**

To protect the clients’ privacy, we apply the anonymous Boneh-Franklin identitybased encryption (IBE) in medical diagnostic branching programs.

To reduce the decryption complexity due to the use of IBE, we apply recently proposed decryption outsourcing with privacy protection to shift clients’ pairing computation to the cloud server.

To protect mHeath service providers’ programs, we expand the branching program tree by using the random permutation and randomize the decision thresholds used at the decision branching nodes.