An Enhancement of Privacy and Efficiency of health care monitoring in Cloud Infra Structure

[1]Mr. NARAHARI NARASIMHAIAH,
Research scholar, Bharathiar University, Tamilnadu, India
narasimhaiah.narahari@gmail.com

[2]Dr. R. PRAVEEN SAM,
Professor Head, Dept. of C.Sc.,
Andhra Pradesh, India, praveen_sam75@yahoo.com

Abstract- Cloud-assisted mobile health 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 technology. The cloud server respects the privacy of a patient and keeps it secured by protecting the medical history of the patient. The main objective of the proposed system is preserving the privacy of the information ensuring that this information cannot be misused. The patient's report will reach the doctor in encrypted format, by using the Identity Based Encryption (IBE) while a master key helps to deliver the report to the doctor in decrypted format. Then the doctor's prescription will reach the patient in encrypted format by using the Outsourcing Decryption Technique while a master key helps to deliver the prescription to the patient in decrypted
format.

I.Introduction

Wide deployment of mobile devices, such as smart phones equipped with low cost sensors, has already shown great potential in improving the quality of healthcare services. Remote mobile health monitoring has already been recognized as not only a potential, but also a successful example of mobile health (mHealth) applications especially for developing countries. The development of cloud computing services is speeding up the rate in which the organizations outsource their computational services or sell their idle computational resources. Even though migrating to the cloud remains a tempting trend from a financial perspective, there are several other aspects that must be taken into account by companies before they decide to do so. One of the most important aspect refers to security: while some cloud computing security
issues are inherited from the solutions adopted to create such services, many new security questions that are particular to these solutions also arise, including those related to how the services are organized and which kind of service/data can be placed in the cloud. Aiming to give a better understanding of this complex scenario, in this article we identify and classify the main security concerns and solutions in cloud computing, and propose taxonomy of security in cloud computing, giving an overview of the current status of security in this emerging technology [1]. Cloud-assisted mobile health (Health) 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 Health technology. This 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.

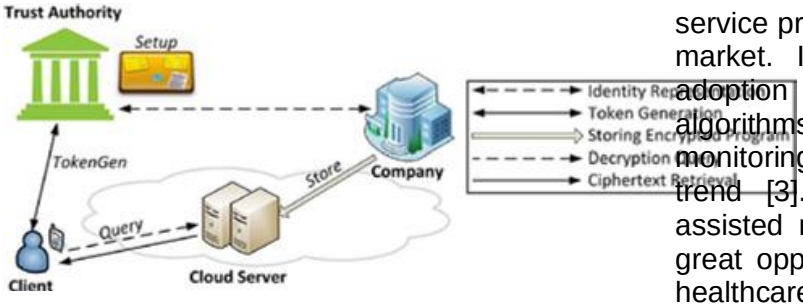

Fig1.System Architecture

consists of four parties: the cloud server (simply the cloud), the company who provides the mHealth monitoring service (i.e. the healthcare service provider), and the individual clients (simply clients), and a semi-trusted authority (TA). The company stores its encrypted monitoring data or program in the cloud server. Individual clients collect their medical data and store them in their mobile devices, which then transform the data into attribute vectors. The attribute vectors are delivered as inputs to the monitoring program in the cloud server through a mobile (or smart) device. A semi-trusted authority is responsible for distributing private keys to the individual clients and collecting the service fee from the clients according to a certain business model such as pay-as-you-go business model. The TA can be considered as a collaborator or a management agent for a company (or several companies) and thus shares certain level of mutual interest with the company. However, the company and TA could collude to obtain private health data from client input vectors. which could then run various web medical applications on these data to return timely advice to the client. These applications may have various functionalities ranging from sleep pattern analyzers, exercises, physical activity assistants, to cardiac analysis systems, providing various medical consultation [2]. Moreover, as the emerging cloud computing technologies evolve, a viable solution can be sought by incorporating the software as a service (SaaS) model and pay-as-you-go business model in cloud computing, which would allow small companies (healthcare service providers) to excel in this healthcare market. It has been observed that the adoption of automated decision support algorithms in the cloud-assisted mHealth monitoring has been considered as a future trend [3]. Unfortunately, although cloud-assisted mHealth monitoring could offer a great opportunity to improve the quality of healthcare services and potentially reduces 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. A recent study shows that 75% Americans consider the privacy of their health information important or very important [4]. It has also been reported [5] that patients' willingness to get involved in health monitoring program could be severely lowered when people are concerned with the privacy breach in their voluntarily submitted health data. This privacy concern will be exacerbated due to the growing trend in privacy breaches on electronic health data. Although the existing privacy laws such as HIPAA (Health Insurance Portability and Accountability Act) provide baseline protection for personal health record, they are generally considered not applicable or transferable to cloud computing environments [6]. Besides, the

current law is more focused on protection against adversarial intrusions while there is little effort on protecting clients from business collecting private information. Meanwhile, many companies have significant commercial interests in collecting clients' private health data [7] and sharing them with either insurance companies, research institutions or even the government agencies. It has also been indicated [8] that privacy law could not really exert any real protection on clients' data privacy unless there is an effective mechanism to enforce restrictions on the activities of healthcare service providers. 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. Authors in [1], designed a cloud-assisted Health monitoring system (CAM). To reduce clients' decryption complexity, they incorporated the recently proposed outsourcing decryption technique [25] 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.

II. Related Work

the high privacy of the health care services. The privacy of health care services very difficult in the remote processing. Its avoided by we using the cloud based technologies provide the privacy on the health care data's. Here we using the cloud assisted privacy preserving mobile health Monitoring system to provide privacy. Under this system we using the re-encryption scheme to reduce the complexity of the encryption. The CAM have three kinds of design for processing. The final design only using the re encryption scheme. Here we using the four parties for remote processing such as cloud server, individual clients, semi trust authority, mHealth monitoring system. The existing system is follows the HIPAA (Health Insurance Portability and Accountability Act). the current law is more focused on protection against adversarial intrusions while there is little effort on protecting clients from business collecting private information. Meanwhile, many companies have significant commercial interests in collecting clients' private health data and sharing them with either insurance companies, research institutions or even the government agencies. Its provide the protection of the personal records. It encrypt the user data's. its takes more time for the information retrieval. 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 [9]. It is worth noting that the collected information from an mHealth monitoring system could contain clients' personal physical data such as their heights, weights, and blood types, or even their ultimate personal identifiable information such as their fingerprints and DNA profiles [10]. According to [11], personal identifiable information (PII) is—any information, recorded or otherwise, relating to an identifiable individual. Almost

any information, if linked to an identifiable individual, can become personal in nature, be it biographical, biological, genealogical, historical transactional, locational, relational, computational, vocational, or reputational‖ In other words, the scope of PII might not necessarily be restricted to SSN, name and address, which are generally considered as PII in the traditional sense. Indeed, the state of the art re-identification techniques [12], [13] have shown that any attribute could become personal identifiable information in practice [9]. Moreover, it is also noted that although some attribute may be uniquely identifying on its own, ―any attribute can be identifying in combination with others, while no single element is a (quasi)-identifier, any sufficiently large subset uniquely identifies the individual‖ [12]. The proposed mobile health monitoring scenario provides a good opportunity for adversaries to obtain a large set of medical information, which could potentially lead to identifying an individual user. Indeed, several recent works [14]–[16] have already shown that even seemingly benign medical information such as blood pressure can be used to identify individual users. Furthermore, it is also observed that future mobile health monitoring and decision support systems might have to deal with other much more privacy-sensitive features such as DNA profiles, from which an adversary may be able to re-identify an individual user. Traditionally, the privacy issue is tackled with anonymization technique such as anonymity or diversity. However, it has been indicated that these techniques might be insufficient to prevent re-identification attack[9]. The threat of re-identification is so serious that legal communities have already been calling for more sophisticated protection instead of merely using anonymization. We believe that our proposed cryptographic based systems could serve as a viable solution to the privacy problems in mHealth systems, and also as an alternative choice for those privacy-aware users.

III. Privacy Architecture for Biomedical Cloud Computing

In this work we presented two-tier architecture for security and privacy in biomedical clouds. We combined the power of decentralized management and access control, provided by cryptographic credentials, with the ability to perform privacy-preserving set operations on data. The first part of our architecture enables biomedical data owners to easily hand out access to physicians, researchers, etc. They in turn, may delegate further access to their collaborators. Of course, even though such an approach provided great flexibility in terms of sharing information, it is insufficient on its own when we would like to avoid revealing information unnecessarily. Secrecy Outage Capacity of Fading Channels This paper considers point to point secure communication over flat fading channels under an outage constraint. More specifically, we extend the definition of outage capacity to account for the secrecy constraint and obtain sharp characterizations of the corresponding fundamental limits under two different assumptions on the transmitter channel state information (CSI).First, we find the outage secrecy capacity assuming that the transmitter has perfect knowledge of the legitimate and eavesdropper channel gains. Towards Ensuring Client-Side Computational Integrity (A position paper) This paper proposes a practical strategy that maybe used to achieve both confidentiality and integrity on the client, for many important classes of computation. We point out problems with the fully homomorphism encryption approach and over a more immediate solution that in our experience meshes well with real-world scenarios, such as the two case studies we

present. GenoDroid: Are Privacy Preserving Genomic Tests Ready for Prime Time? This paper explored the viability and practicality of privacy-agile computational genomic tests in the portable and pervasive setting of modern smart phones. We combined domain knowledge in biology, genomics, ubiquitous computing, and applied cryptography, to design and build a personal genomic toolkit, called GenoDroid. We implemented it on the Android platform, assessed its conducted pilot usability study that produced some encouraging results. We certainly plan to incorporate support for additional genetic tests in GenoDroid, Encrypted Signal Processing for Privacy Protection We introduce the fusion of signal processing and cryptography as an emerging paradigm to protect the privacy of users. While service providers cannot access directly the content of the encrypted signals, the data can still be processed in encrypted form to perform the required signal processing task. The solutions for processing encrypted data are designed using cryptographic primitives like homomorphic cryptosystems and secure multiparty computation (MPC).

1. Health data collection
2. AES implementation
3. Token generation
4. Cipher text retrieval

Health data collection: The company stores its encrypted monitoring data or program in the cloud. Individual clients collect their medical data and store them in their mobile devices, which then transform the data into attribute vectors. The attribute vectors are delivered as inputs to the monitoring program in the cloud through a mobile (or smart) phone. TA is responsible for distributing private keys to clients and collecting service fees from clients according to a certain business model such as “pay-per-use” model.

AES implementation To protect the client’s privacy, we apply the anonymous AES in medical diagnostic branching programs. To reduce the decryption complexity due to the use of AES, we apply recently proposed decryption outsourcing with privacy protection to shift client’s pairing computation to the cloud server.

Token generation To generate the private key for the attribute vector, a client first computes the identity representation set of each element in and delivers all the identity representation sets to TA. Then TA runs the on each identity in the identity set and delivers all the respective private keys to the client.

Cipher text retrieval: The cloud is required to generate the cipher texts for clients by running the Re Encryption algorithm. Each run of Re Encryption algorithm costs the cloud exactly two pairing computations. For each client, the cloud needs to perform those Computations. The resulting public key cipher texts along with the original symmetric key cipher texts constitute the Cipher text sets for the client.

IV. Conclusion

In this paper Cloud Computing technology provides human advantages such as economical cost reduction and effective resource management. However, if security accidents occur, economic damages are inevitable. Our paper proposed “A secured patient healthcare monitoring in cloud infrastructure” for effective resource. 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. Finally, to enable resource-constrained small companies to participate in mHealth business, our CAM design helps them to shift the computational burden to the cloud by applying newly developed key private proxy re encryption technique.

References

[1] P. Mohan, D. Marin, S. Sultan, and A. Deen, —Medinet: Personalizing the self-care process for patients with diabetes and cardiovascular disease
using mobile telephony,‖ in Proc. 30th Ann. Int. Conf. IEEE Engineeringin Medicine and Biology Society, 2008 (EMBS 2008), 2008,pp. 755–758.

[2] A. Tsanas, M. Little, P. McSharry, and L.Ramig, —Accurate telemonitoringof parkinson's disease progression by noninvasive speech tests,‖IEEE
Trans. Biomed. Eng., vol. 57, no. 4, pp. 884–893, Apr. 2010.

[3] G. Clifford and D. Clifton, —Wireless technology in disease managementand medicine,‖ Ann. Rev. Medicine, vol. 63, pp. 479–492, 2012.

[4] L. Ponemon Institute, Americans' Opinions on Healthcare Privacy,2010 [Online]. Available: http://tinyurl.com/4atsdlj

[5] A. V. Dhukaram, C. Baber, L. Elloumi, B.-J.vanBeijnum, and P. D.Stefanis, —End-user perception towards pervasive cardiac healthcareservices:
Benefits, acceptance, adoption, risks, security, privacy andtrust,‖ in Proc. Pervasive Health, 2011, pp. 478–484.

[6] M. Delgado, —The evolution of health care it: Are current U.S. privacypolicies ready for the clouds?,‖ in Proc. SERVICES, 2011, pp. 371–378.

[7] N. Singer, —When 2 2 equals a privacy question,‖ New
York Times, Oct. 18, 2009 [Online]. Available:http://www.nytimes.com/2009/10/18/business/18stream.html

[8] E. B. Fernandez, —Security in data intensive computing systems,‖inHandbook of Data Intensive Computing
NewYork,NY,USA:Springer, 2011, pp. 447–466.

[9] A. Narayanan and V. Shmatikov, —Myths and fallacies of personally identifiable information,‖ Commun.ACM, vol. 53, no. 6, pp. 24–26, 2010.

[10] P. Baldi, R. Baronio, E. D.Cristofaro, P. Gasti, and G.Tsudik, —Countering gattaca: Efficient and secure testing of fully-sequenced human
genomes,‖ in Proc. ACM Conf. Computer and Communications Security, 2011, pp. 691–702.

[11] A. Cavoukian, A. Fisher, S. Killen, and D. Hoffman, —Remote home health care technologies:Howto ensure privacy? Build it in: Privacy by
design,‖ Identity in the Information Society, vol. 3, no. 2, pp. 363–378,2010.

[12] A. Narayanan and V. Shmatikov, —Robust de anonymization of large sparse datasets,‖ in Proc. IEEE Symp. Security and Privacy, 2008
(SP2008), 2008, pp. 111–125.

[13] A. Narayanan and V. Shmatikov, —De-anonymizing social networks,‖in Proc. IEEE Computer Society, IEEE Symp. Security and Privacy,2009,
pp. 173–187.

[14] I. Neamatullah,M. Douglass, L. Lehman, A. Reisner,M. Villarroel,W. Long, P. Szolovits, G. Moody, R. Mark, and G. Clifford, —Automated deidentification
of free-text medical records,‖ BMC Med. Inform. DecisionMaking, vol. 8, no. 1, p. 32, 2008.

[15] S. Al-Fedaghi and A. Al-Azmi, —Experimentation with personal identifiable information,‖ IntelligentInf.Manage.,vol. 4, no. 4, pp. 123–
133,2012.
pp. 193–202, 2007.