PRIVACY PRESERVING OF HEALTH MONITORING SERVICES IN CLOUD

Mrs. Ramya.R [1], Mrs. Shruthi.G [2]

[1]M. Tech. Student, [2]Assistant Professor, Department of CSE,
Don Bosco Institute of Technology, Bangalore, (India)

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. Authors in existing system, proposed a new variant of proxy re-encryption scheme, in which health care companies only needs to accomplish encryption once at the setup phase while shifting the rest computational tasks to the cloud without compromising privacy. The work in existing system[1] , however does not consider how charging must be implemented in this system, health care companies survive only on the charging the user for accessing the service. Health care companies want to charge differentially for the different services and also reconciliation reports must be generated, so user cannot deny claim if they have used the service. We extend the paper for differential charging of services and reconciliation of payments.

*Keywords**: Healthcare, Privacy, Cost Analysis (Charging), Service Execution, Outsourcing decryption***

1 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 Microsoft launched project "MediNet" is designed to realize remote monitoring on the health status of diabetes and cardiovascular diseases in remote areas in Caribbean countries [2].

In such a remote mHealth monitoring system, a client could deploy portable sensors in wireless body sensor networks to collect various physiological data, such as blood pressure (BP), breathing rate (BR), Electrocardiogram (ECG/EKG), peripheral oxygen saturation (SpO2) and blood glucose. Such physiological data could then be sent to

a central server, 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.

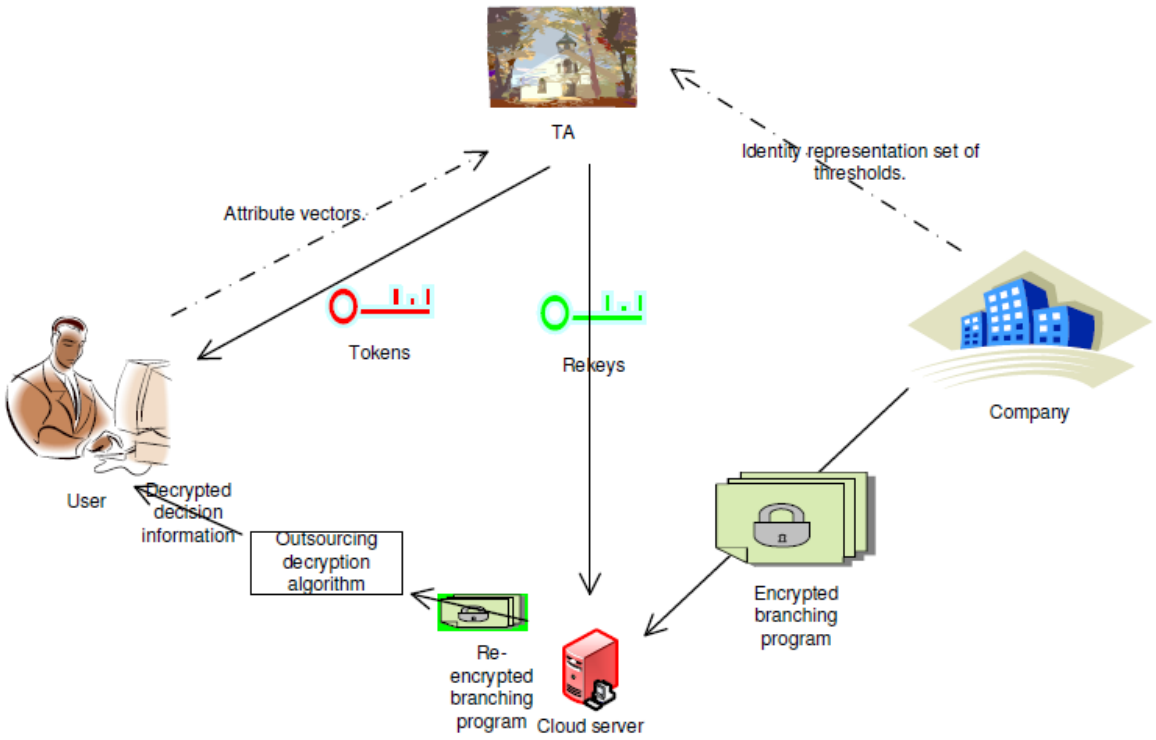

Fig 1: CAM with Full Privacy and High Efficiency

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 mHealth 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.

Charging is important source of income for the health care providers. But providing privacy for users and health care providers. In this paper, we propose a solution for differential charging of services without compromising the privacy.

II THE PROBLEM STATEMENT

Cloud-assisted mobile health (mHealth) monitoring[1] 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. Without properly addressing the data management in an mobile Health system, clients' privacy may be severely breached during the collection, storage, diagnosis, communications and computing.

Health care providers want to charge their services differentially. The user privacy must not be scarified in any case and cloud must mediate the payments between the user and the health care provider. The mediation system must be fair and must be able to detect cheating behavior of health care provider claiming more money or user denying the usage of service.

III THE PROPOSED SYSTEM

Service provider provides the services in the encrypted form to the service Execution engine in the cloud. In addition for different service flow, differential charges will be specified by the service provider is given to the service execution engine in the cloud. User provides the services request to the cloud, the service request of user is executed in the service execution engine as in the [1]. When user access the service a transaction token is generated and a mapping from transaction id to the user pseudonym is generated and stored in a secure storage in cloud. The service cost for the accessing the service is got from the service execution engine and transaction id vs. service cost is generated and saved in a secure storage in cloud. Also transaction id is encrypted with the master key of the cloud and the encrypted id and the total service cost is sent to the service provider. Service provider can claim the service cost at any point of time.

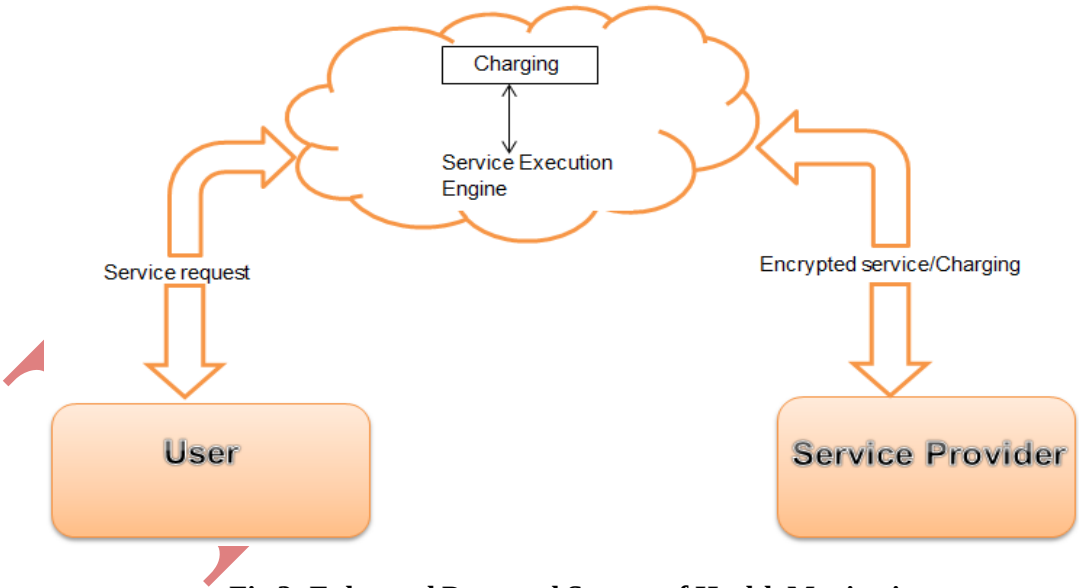

Fig 3: Enhanced Proposed System of Health Monitoring

At that time, the cloud charging system will calculate the total service cost summing up all transactions cost and verify the validity of service provider's claim. If the claim is valid the amount in paid to service provider by claiming the amount from the service users by referring to the transaction information. In case the validity of service providers claim is false, the charging system will request for the encrypted transaction id.

Once the service provider provides the encrypted transaction id, it will validate the transaction and generate reconciliation report for the service provider. Cloud generates a bill for the user whenever he accesses the service. The bill consists of encrypted transaction id and service cost. The payment is automatically subtracted from the users cloud account. Whenever user claims not accessing the service the transaction id and the time of access is given to the user to counter his claim.

IV CONCLUSION AND FUTURE WORK

4.1 Conclusion

In this paper, we have proposed a charging framework to the privacy preserving cloud based health care service solution proposed in [1], which can effectively protect the privacy of clients and the intellectual property of health service providers. Our proposed solution is safe against cheating attacks from both the users and the service providers. Finally, to enable resource constrained small companies to participate in health business.

4.2 Future Work

Our future work will be on migrating the charging solution to a Trusted third party (TTP) to secure against cheating clouds or attacks on the cloud service providers.

REFERENCES

[1] Huang Lin , Jun Shao "CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring" IEEE 2013.

[2] H. L¨ohr, A.-R. Sadeghi, and M. Winandy, "Securing the e-health cloud," in Proceedings of the 1st ACM International Health Informatics Symposium, ser. IHI '10, 2010, pp. 220–229.

[3] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted personal health records in cloud computing," in ICDCS '11, Jun. 2011.

[4] "The health insurance portability and accountability act." [Online]. Available: http://www.cms.hhs.gov/HIPAAGenInfo/01 Overview.asp

[5] "Google, microsoft say hipaa stimulus http://www.ihealthbeat.org/Articles/2009/4/8/.

[6] "At risk of exposure – in the push for electronic medical records, concern is growing about how well privacy can be safeguarded," 2006. [Online].

[8] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in CCSW '09, 2009, pp. 103–114.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in IEEE INFOCOM'10, 2010.

[10] C. Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," in Journal of Computer Security, 2010.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in CCS '06, 2006, pp. 89–98.

[12] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," IEEEWireless Communications Magazine, Feb. 2010.

[13] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in ACM CCS, ser. CCS '08, 2008, pp. 417–426.

[14] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes," 2009.

[15] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ASIACCS'10, 2010. [30] S. Kurosawa, H. Nakayama, N. Kato, and A. Jamalipour,

[16] S. Narayan, M. Gagn´e, and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure," ser. CCSW '10, 2010, pp. 47–52.

[17] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Patient self-controllable access policy on phi in ehealthcare systems," in AHIC 2010, 2010.

[18] L. Ibraimi, M. Asim, and M. Petkovic, "Secure management of personal health records by applying attribute-based encryption," Technical Report, University of Twente, 2009.

[19] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in IEEE S& P '07, 2007, pp. 321–334.

[20] J. A. Akinyele, C. U. Lehmann, M. D. Green, M. W. Pagano, Z. N. J. Peterson, and A. D. Rubin, "Self-protecting electronic medical records using attribute-based encryption,"

[21] M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in CCS '09, 2009, pp. 121–130.

[22] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Ciphertext policy attribute based encryption with efficient revocation," Technical Report, University of Waterloo, 2010.

[23] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 99, no. PrePrints, 2010.

[24] S. Jahid, P. Mittal, and N. Borisov, "Easier: Encryption-based access control in social networks with efficient revocation," in ASIACCS, Hong Kong, March 2011.

[25] S. Ruj, A. Nayak, and I. Stojmenovic, "Dacc: Distributed access control in clouds," in 10th IEEE TrustCom, 2011.