ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

An Effective Mobile Online Health Monitoring System In Cloud

P. Prabha
M.Tech Student
Department of CSE,
CREC, Tirupathi, JNTU-Anathapuram, A.P, India.

R. Suresh
Associate Professor & HoD
Department of CSE,
CREC, Tirupathi, JNTU-Anathapuram, A.P, India.

ABSTRACT

Cloud-assisted mobile health (m 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 m Health 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.

Keywords— ***Mobile health (mHealth), Healthcare, Privacy, Outsourcing decryption, Key private proxy re-encryption***

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 (m Health) 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 [1]. 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. 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.

Unfortunately, although cloud-assisted m Health 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 m Health 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. It has also been reported that patients' willingness to get involved in health monitoring program could be severely lowered when people are concerned

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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 base- line 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 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.

2. EXISTING SYSTEM

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 m 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.

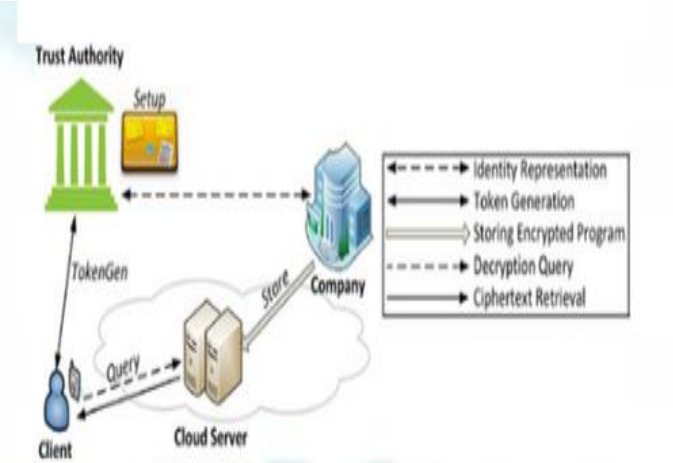

Figure 1: System architecture for Existing system

CAM 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.

3. PROPOSED SYSTEM

A secured patient healthcare monitoring in cloud infrastructure helps to keep the communication between doctor and patient confidential. 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

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

privacy of the information ensuring that this information cannot be misused. The encryption and decryption format is the soul of this project. The patient's report will reach the doctor in encrypted format, by using the Identity Based Encryption algorithm (IBE) while a master key helps to deliver the report to the doctor in decrypted format. A trusted third party, called the Private Key Generator (PKG), generates the corresponding private keys. To operate, the PKG first publishes a master public key, and retains the corresponding master private key (referred to as master key). Given the master public key, any party can compute a public key corresponding to the identity ID by combining the master public key with the identity value. To obtain a corresponding private key, the party authorized to use the identity ID contacts the PKG, which uses the master private key to generate the private key for identity ID [3].

Figure 2: System architecture for proposed system

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. While the idea of database outsourcing is becoming increasingly popular, the associated security risks still prevent many potential users from deploying it. In particular, the need to give full access to one's data to a third party, the database service provider, remains a major obstacle. A seemingly obvious solution is to encrypt the data in such a way that the service provider retains the ability to perform relational operations on the encrypted database [4].

Registration is a mandatory process to get into a hospital management system for any doctor and Patient. A doctor and Patient have to provide their personal information to the patient healthcare monitoring to create their account. Admin will assess the given detail of a user and activates their account to view the patient healthcare monitoring. After activation the user get message from admin by their mobile. An existing user can directly login to the system with their valid user name and password. Activated User can enter into patient healthcare monitoring with their valid username and password. User should have all their test reports whatever related to their disease which was advised by the doctor earlier. Cloud area serves as a storage medium where all user records are being stored. When doctor login to the patient healthcare monitoring by providing their valid user name and password, they can view the history of a patient.

When doctor wants to view the files of any patient, he will be finding all their reports in encryption format. To decrypt this test report doctor have to get the patient ID from the appropriate column. This ID, which is used as Doctor's key. This helps him to view the patient test report in decrypted format. Then doctor will decide the medicine to be prescribed, which will be entered by the doctor manually. This prescription to the user will be saved in cloud server in encrypted format. If the patient wants to view the doctor's prescription, user has to login into the patient healthcare monitoring.

5 CONCLUSIONS

In this paper, we design a cloud-assisted privacy preserving mobile health monitoring system, called CAM, which can effectively protect the privacy of clients and the intellectual property of mHealth service providers. To protect the clients' privacy, we apply the anonymous Boneh-Franklin identity- based encryption (IBE) in medical diagnostic branching programs. To reduce the decryption complexity due to the use of IBE,

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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. Our CAM has been shown to achieve the design objective.

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." Conference Proceedings of the International Conference of IEEE Engineering in Medicine and Biology Society , vol. 2008, no. 3, pp. 755–758.[Online]. Available:http://www.ncbi.nlm.nih.gov/pubmed/19162765

[2] A. Tsanas, M. Little, P. McSharry, and L. Ramig, "Accurate tele monitoring of parkinson's disease progression by noninvasive speech tests," Biomedical Engineering, IEEE Transactions on , vol. 57, no. 4, pp. 884–893, 2010.

[3] G. Clifford and D. Clifton, "Wireless technology in disease management and medicine," Annual Review of Medicine, vol. 63, pp. 479–492, 2012.

[4] L. Ponemon Institute, "Americans' opinions on healthcare privacy, available: http://tinyurl.com/4atsdlj," 2010.

[5] A. V. Dhukaram, C. Baber, L. Elloumi, B.-J. van Beijnum, and P. D. Stefanis, "End-user perception towards pervasive cardiac healthcare services: Benefits, acceptance, adoption, risks, security, privacy and trust," in PervasiveHealth , 2011, pp. 478–484.

[6] M. Delgado, "The evolution of health care it: Are current u.s. privacy policies ready for the clouds?" in SERVICES, 2011, pp. 371–378.

[7] N. Singer, "When 2+ 2 equals a privacy question," New York Times, 2009.

[8]E. B. Fernandez, "Security in data intensive computing systems," in Handbook of Data Intensive Computing , 2011, pp. 447–466.

[9] A. Narayanan and V. Shmatikov, "Myths and fallacies of personally identifiable information," Communications of the 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 ACM Conference on Computer and Communications Security , 2011, pp. 691–702.

[11] A. Cavoukian, A. Fisher, S. Killen, and D. Hoffman, "Remote home health care technologies: how to 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 Security and Privacy, 2008. SP 2008. IEEE Symposium on . IEEE, 2008, pp. 111–125.

[13] "De-anonymizing social networks," in IEEE Symposium on Security and Privacy . IEEE Computer Society, 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 de-identification of free-text medical records," BMC medical informatics and decision making , vol. 8, no. 1, p. 32, 2008.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[15] S. Al-Fedaghi and A. Al-Azmi, "Experimentation with personal identifiable information," Intelligent Information Management, vol. 4, no. 4,pp. 123–133, 2012.

[16] J. Domingo-Ferrer, "A three-dimensional conceptual framework fordatabase privacy," Secure Data Management
, pp. 193–202, 2007.

[17] T. Lim, Nanosensors: Theory and Applications in Industry, Healthcare, and Defense . CRC Press, 2011.

[18] X. Zhou, B. Peng, Y. Li, Y. Chen, H. Tang, and X. Wang, "To release or not to release: evaluating information leaks in aggregate human-genome data," Computer Security–ESORICS 2011 , pp. 607–627, 2011.

[19] R. Wang, Y. Li, X. Wang, H. Tang, and X. Zhou, "Learning your identity and disease from research papers: information leaks in genome wide association study," in Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009, pp. 534–544.

[20] P. Ohm, "Broken promises of privacy: Responding to the surprising failure of anonymization," UCLA Law Review , vol. 57, p. 1701, 2010.

[21] P. Institute, "Data loss risks during downsizing," 2009.

[22] P. Dixon, "Medical identity theft: The information crime that can kill you," in The World Privacy Forum, 2006, pp. 13–22.

[23] K. E. Emam and M. King, "The data breach analyzer," 2009, [Available at: http://www.ehealthinformation.ca/dataloss].

Author Details

P. Prabha, M.Tech Student Branch (CSE) Department of CSE , CREC, Tirupathi, JNTU-Anathapuram, A.P, India. Email id:prabharoyal17@gmail.com., Her current interests include Computer Networks and Data Mining.