Cloud Assisted Secure Remote Health Care Services

Vikram Gokhale
VIIT, SPPU, Pune

Neha Bhansali
VIIT, SPPU, Pune

Lulua Chatriwala
VIIT, SPPU, Pune

Ipsha Chowdhury
Pawan S. Wawage
VIIT, SPPU, Pune

ABSTRACT

Health care facilities are yet to reach the most remote corners of the world. Little ignorance towards health can result in serious concerns and can also possibly cause life threatening situations.A system is proposed which can collect different parameters of an individual and upload those on a global database for the best assistance from experts from all over the globe. Cloud computing is available on various devices like PCs, Laptops, and Smartphones.To help maintain security of a database, various encryption techniques are applied. Attribute-based encryption (ABE) is a new way for public key encryption that would allow the encryption and decryption of messages based on user attributes. Given its expressiveness, attribute based encryption is currently being considered for many cloud storage and computing applications.

The aim of the system is to reduce the complexity involved in the current design and also to reduce the computation load on the client's side without compromising the privacy through trying to shift the heavy computation burden to the server instead of the client's device with limited computational power and many other constraints.

Keywords

ABE (Attribute-based encryption),ECG (Electrocardiogram), FDA (Food and drug administrator), BP (Blood Pressure).

1. INTRODUCTION

Remote health care system is development in the medical sector to increase health check in remote areas. This system measures parameters such as blood glucose level, blood pressure, ECG and stores it on the cloud. This data is accessed only by doctors and the respective patient. This paper mainly focuses on the requirements to increase the security of patients' database present in the cloud thus concentrating on users' privacy. Health care facilities are yet to reach the most remote corners of the world. Little ignorance towards health can result in serious concerns and can also possibly cause life threatening situations.

A medical device is designed to improve patient's health in diagnosis, therapy or surgery which are monitored and under strict regulations by the food and drug administration, FDA.

The categories of Mobile Medical Devices (small, hand-held) available in market are only serving the purpose of informing the patients about their Health (BP, Glucose- level, etc). Very few of these are having the feature of PC connectivity. The information about the patient's health is stored in the device memory, which is capable of holding maximum up to 50 records.

The current mobile health monitoring communication provides feedback decision support which in turn helps in enhancing the quality of healthcare services keeping the cost reasonable.

2. RELATED WORK

To name a few prevailing mobile devices such as smart phones which are equipped with low cost sensors has already enhanced the quality of healthcare services. Microsoft launched a project named "MediNet" was developed to make remote monitoring on health status of cardiovascular diseases possible in unreachable parts of the western countries[3].

In such healthcare systems, a client can deploy portable sensors in wireless body sensor networks to collect some physiological data like blood pressure, blood glucose, breathing rate, electrocardiogram etc. These physiological data can be uploaded to a central server which runs various web medical applications to return suggestions to the client in time. These web medical applications include functionalities like patter analysis, exercise, physical activity assistance, cardiac analysis systems that provide medical advice.

3. PROPOSED WORK

With rising cost of health care, aging population, technology advancement and patient's desire to stay in homes – health care is increasingly moving from medical facility into homes.

The objective is to integrate the available mobile medical devices with the feature of transmitting the patient's disease information/records directly to the concerned doctor through cloud system, who eventually will respond with the prescription to the patient. In this the patient will get benefited with the quick response based on the recorded values and doctors will get paid for their service.

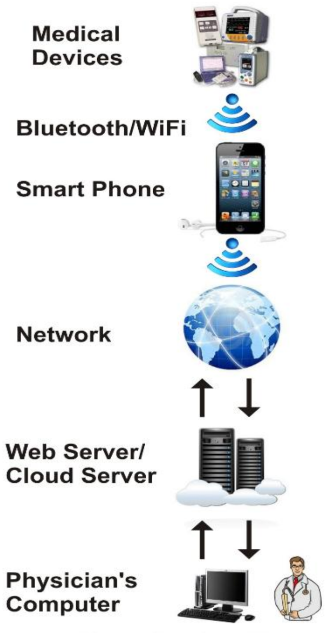

Figure 1: Overview of the proposed system

A system is proposed which can collect different parameters of an individual and upload those on a global database for the best assistance from experts from all over the globe. In such a system where the data is put on the cloud there lays a major concern about the problems in the current cloud storage and ethical security techniques. Privacy breach of the medical data of an individual should not be allowed by the system. This is where cloud security comes into picture. Cloud computing is a platform where dynamically scalable and virtualized resources are available via the internet. It has helped in re-shaping the IT industry by minimizing the budget, high availability, and easy scalability. Cloud computing is available on various devices like PCs, Laptops, and Smartphones. There are three dimensions in privacy:

1) Respondent privacy where a re-verification of the user whose database corresponds is done,

2) Owner privacy is done for the users who are only interested in the result of the queries and not in the back-end activities, and

3) User privacy helps in not revealing the queries done in the interactive databases and thus helps prevent user profiling and re-identification.

To help maintain security of a database, various encryption techniques are applied. Attribute-based encryption (ABE) is a new way for public key encryption that would allow the encryption and decryption of messages based on user attributes[13]. Given its expressiveness, attribute based encryption is currently being considered for many cloud storage and computing applications.

The aim is to design a cloud-assisted privacy preserving mobile health monitoring system which can effectively protect the client's privacy and the intellectual property of the cloud. To protect the client's privacy we will be using various encryption and decryption techniques in medical diagnostic program. The aim is to reduce the complexity involved in the current design and also to reduce the computation load on the client's side without compromising the privacy through trying to shift the heavy computation burden to the server instead of the client's device with limited computational power and many other constraints.

Here a basic introduction about branching algorithm for Blood pressure (BP) is given. Branching algorithm is a binary decision tree. All the non-leaf nodes are the decision nodes whereas all the leaf nodes are the label nodes which are used for final consultation. Each decision node is a pair of attribute and its threshold value. Suppose the blood pressure count of an individual is 150, his daily medication is regular and normal diet is not followed, whatever consultation has to be given will be branched to the leaf node. All the data regarding consultation present in the leaf node will then be encrypted by suitable encryption techniques. We will use various encryption techniques which will ensure the privacy of client as well as of service provider [2].

4. HOW TO ENSURE PRIVACY?

It has been found that cloud computing is a new paradigm for database management systems. . In such a system where the data is put on the cloud there lays a major concern about the problems in the current cloud storage and ethical security techniques. Privacy breach of the medical data of an individual should not be allowed by the system. This is where cloud security comes into picture. Cloud computing is a platform where dynamically scalable and virtualized resources are available via the internet.

The present bucket-based data authentication methods are used but they face few problems that the original spatial data distribution may be exposed because of the poor data grouping strategy [17]. The overhead of data transmission authentication is extremely high. The proposal of privacy-aware query authentication which guarantees data confidentiality and query result integrity for users is being planned.

Timely function based data grouping technique is developed to privately partition a spatial database into small groups generating the signature of each group. The correctness and completeness of outsourced data while answering a range of queries to users is checked through this signature.

5. CONCLUSION

In this paper, we design a cloud-assisted secure privacy preserving health monitoring system, which will protect the privacy of clients along with the intellectual property ofmobile Health service providers.Also continue to develop a comprehensive healthcare information processing platform, integrating the technologies of wearable sensing, database, information sharingsecurity and privacy terms.To maintain the privacy of mobile health service providers, we propose to use branching algorithm which includes random permutation and decision thresholds.This will indeed help the people in the remote parts of the world to get expose to health care services.

6. REFERENCES

[1] Fei Chen, Liu, A.X,"Privacy and integrity preserving multi-dimensional range queries for cloud computing", in IEEE Networking conference, 2014.

[2] M. Jang, Min Yoon, and Jae-Woo Chang, "A Privacy-aware Query Authentication Index for Database Outsourcing", in IEEE transaction on BigComp.,Pages 72-76, 2014.

[3] Huang Lin, Jun Shao, Chi Zhang, and Yuguang Fang, Fellow, IEEE, "CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 6, JUNE 2013

[4] Peng Wei Wang,Zhi Jun Ding, Chang Jun Jiang, and Meng Chu Zhou, Fellow, IEEE, "Design and Implementation of a Web-Service-Base Public-Oriented Personalised Health Care Platform", IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS, VOL. 43, NO. 4, JULY 2013

[5] G. Wang, Q. Liu, J. Wu, and M. Guo, Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers", in ACM conference on Computer and communications security, 2011.

[6] R. A. Popa, C. M. S. Redfield, N. Zeldovich, and H. Balakrishnan, "CryptDB: Protecting confidentiality with encrypted query processing", in Proc. 23rd ACM Symp. Operating Systems Principles, pp. 85100, Oct.2011.

[7] M. Barni, P. Failla, R. Lazzeretti, A.Sadeghi, and T. Schneider, "Privacy preserving ECG classification with branching programs and neural networks", IEEE Transactions on Information Forensics Security, 2011.

[8] Shyamal Patel, Bor-rong Chen, Thomas Buckley, Ramona Rednic, Doug McClure, Daniel Tarsy, Ludy Shih, Jennifer Dy, Matt Welsh, Paolo Bonato, "Home

Monitoring of Patients with Parkinson’s Disease via Wearable Technology and a Web-based Application”, 32nd Annual International Conference of the IEEE EMBS Buenos Aires, Argentina, August 31 - September 4, 2010

[9] C. Gentry, ”Fully homomorphic encryption using ideal lattices”, in Proc. 41st ACM Symposium on Theory of Compututation, pp. 169178, 2009.

[10] C. Gentry, ”Fully homomorphic encryption using ideal lattices”, in Proc. 41st ACM Symposium on Theory of Compututation, pp. 169178, 2009.

[11] 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 Engineering in Medicine and Biology Society, 2008.

[12] J. Bethencourt, A. Sahai, and B. Waters, ”Cipher text-policy attribute based encryption”, in Proceedings of IEEE Symposium on Security and Privacy, 2007.

[13] J. Brickell, D. Porter, V. Shmatikov, and E. Witchel, ”Privacy preserving remote diagnostics”, in Proc. 14th ACM Conf. Computer and Communications Security, 2007.

[14] V. Goyal, O. Pandey, A. Sahai, and B. Waters,” Attribute-based encryption for fine grained access control of encrypted data”, in ACM conference on Computer and communications security , 2006.

[15] H. Hacigumus, B. Iyer, C. Li, and S. Mehrotra, ”Executing SQL over encrypted data in the database-service-provider model”, in Proc. ACM SIGMOD Intl Conf. Manage. Data, pp. 216227, 2002.

[16] D. Boneh and M. Franklin, ”Identity based Encryption from the weil pairings”, in Proceeding CRYPTO ’01 Proceedings of the 21st Annual InternationalCryptology Conference on Advances in Cryptology, 2001.

[17] Stuart Haber, William G. Horne, Tomas Sander, and Danfeng Yao, ”Privacy-Aware Verification of Aggregate Queries on Outsourced Databases with Applications to Historic Data Integrity”

[18] Qian Wang1, Cong Wang1, Jin Li1, Kui Ren1, and Wenjing Lou2, “Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing”

[19] Ichiro YAMADA and Guillaume LOPEZ, ”Wearable Sensing Systems for Healthcare Monitoring”.