Remote Health Care Secure Services with Mobile Assistance

Vikram Gokhale, Neha Bhansali, Lulua Chatriwala, Ipsha Chowdhury
Information Technology, VIIT
vikyrocks94@gmail.com, nehabhansali82@gmail.com, lulua.rashid@gmail.com, arunchow63@gmail.com

Abstract- Remote Health Care system is a modern development in the medical field to advance the health check system in remote areas. Information technology and management systems are widely contributing to the health care sector. The proposed system will consist of a device that can measure three physiological parameters – Pulse Rate, ECG, and Blood Sugar. Once the patient has measured one of the above parameters, the readings will be transmitted to his Smartphone via Bluetooth. This system will make use of an Android application to help the patient maintain his/her records. 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.

Index Terms- ABE (Attribute-based encryption); POR (Proof of Retrievability); MHT (Merkle Hash Tree); ECG (Electrocardiogram); FDA (Food and drug administrator); BP (Blood Pressure); Secret Sharing Scheme (SSS).

1. INTRODUCTION

Remote health care system is development in the medical sector to increase health check in remote areas. The device can measure three integrated 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. 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.

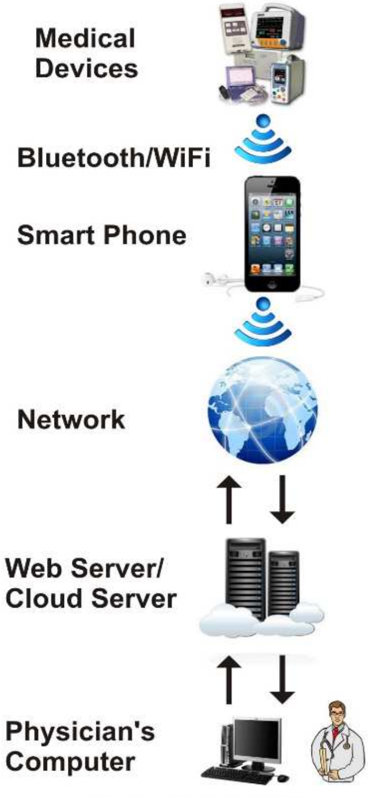

Fig. 1. Overview of the Proposed System

The workflow of the system will be as follows: the patient will capture his physiological parameters such as ECG, Blood Glucose, & Pulse Rate using the medical device. These readings will then be transferred to an Android phone via a wireless communication media like Bluetooth. These readings will be visible on an Android application, which will consist of a profile for each patient; to make the readings accessible to a doctor, the data will be stored on a Private Cloud. The data on the cloud will be made secure using a security algorithm based on ABE.

2. RELATED WORK

In India, the currently available remote health care devices are used to only calculate one physiological parameter. Our proposed system integrates three modules which can calculate three different physiological parameters – Pulse Rate, ECG, and Blood Sugar. 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.

2.1. *Homomorphic Encryption*

In Homomorphic encryption C is the cipher text, P is the plaintext. This system allows addition and multiplication operations to be performed under encryption. The client generates a key pair value for homomorphic system and sends public key along with the encrypted input to the server. For the evaluation of arithmetic circuits, server uses its homomorphic property. If the cryptosystem is only additively homomorphic, multiplication under encryption requires the help of in a single round of interaction. At the end, it sends the encrypted outcome of the computation back to who can decrypt. If security against malicious participants is required, the homomorphic encryption scheme needs the additional property of verifiability [7].

2.2. *Branching Algorithm*

In this section, we define branching programs, which include binary classification or decision trees. The algorithm basically consists of three parameters (P, L, R). Let V denote the User attributes vector (v1…vn). Let (ti, αi) denote the threshold value and index of an attribute. The first element is a set of nodes. If $i \leq l$, Pi are decision nodes. If i > l, Pi are classification nodes. Decision nodes represent internal nodes of the program while Classification or diagnosis nodes refer to the leaf nodes. For each decision node *i*, L(i) is the index of the next node if vαi ≤ ti; R(i) is the index of the next node if vαi > ti. Functions L and R are such that the resulting directed graph is acyclic. To evaluate the branching program on some attribute vector V, start at P1. If vα1 ≤ t1, set h = L(1), else h = R(1). Repeat the process recursively for Ph, and so on, until reaching one of the leaf nodes and obtaining the classification [1].

2.3. *Fine-Grained*

Fine-grained access control systems make it possible to grant different access rights to individual users and also allow flexibility in specifications to access the data.

2.4. *Secret Sharing Schemes*

In secret sharing schemes, a secret is divided into a number of parts and is given or stored at different locations with different security mechanisms. In this case, all the shareholders of the secret sharing scheme need to collaborate in order to regenerate the sensitive data. Every SSS realizes some access structure that defines the sets of parties who should be able to reconstruct the secret by using their shares.

3. METHODOLOGY

As more and more people are getting connected to the internet every day, the data traffic has increased exponentially, resulting in the huge increase in the transfer of sensitive data to third-party sites and server. This leads to more and more vulnerability as the data can be easily misused. Also, since third-party service providers are utilized for the purpose of storing the data on the Cloud, there is a possibility that this data may be hampered by the service provider – intentionally or unintentionally. A new system is being developed for this problem. It is called Key-Policy Attribute Based Encryption (KP-ABE). In this, cipher text is labeled with a set of attributes and the private keys are associated with access structures that control which cipher text a user is able to decrypt. Traditionally the sensitive data is stored on the third-party servers such as email, etc. However, this puts a bottleneck on the system. If the server was to be hacked, a large amount of information is lost. One method of avoiding such problems is to store data in encrypted form. So if the server was compromised, the amount of data lost will be limited. If the data is stored in encrypted form, then it becomes difficult to share the data with other parties as the owner will have to share sensitive private keys with the parties giving them all data or decryption will be an issue as the amount of data may be huge and not all is intended for a particular third-party. This is where ABE i.e. Attribute Based Encryption comes to help. In ABE, user's key and cipher text are labeled with sets of descriptive attributes and a particular key can decrypt a cipher text only if the attributes of cipher text and the user's key match. The current cryptosystem allows for decryption when at least a certain number of attributes overlap between a cipher text and a private key. Another method to solve this problem is to make use of a Third Party Auditor who is appointed by the client to check the integrity of his data on the Cloud [18].

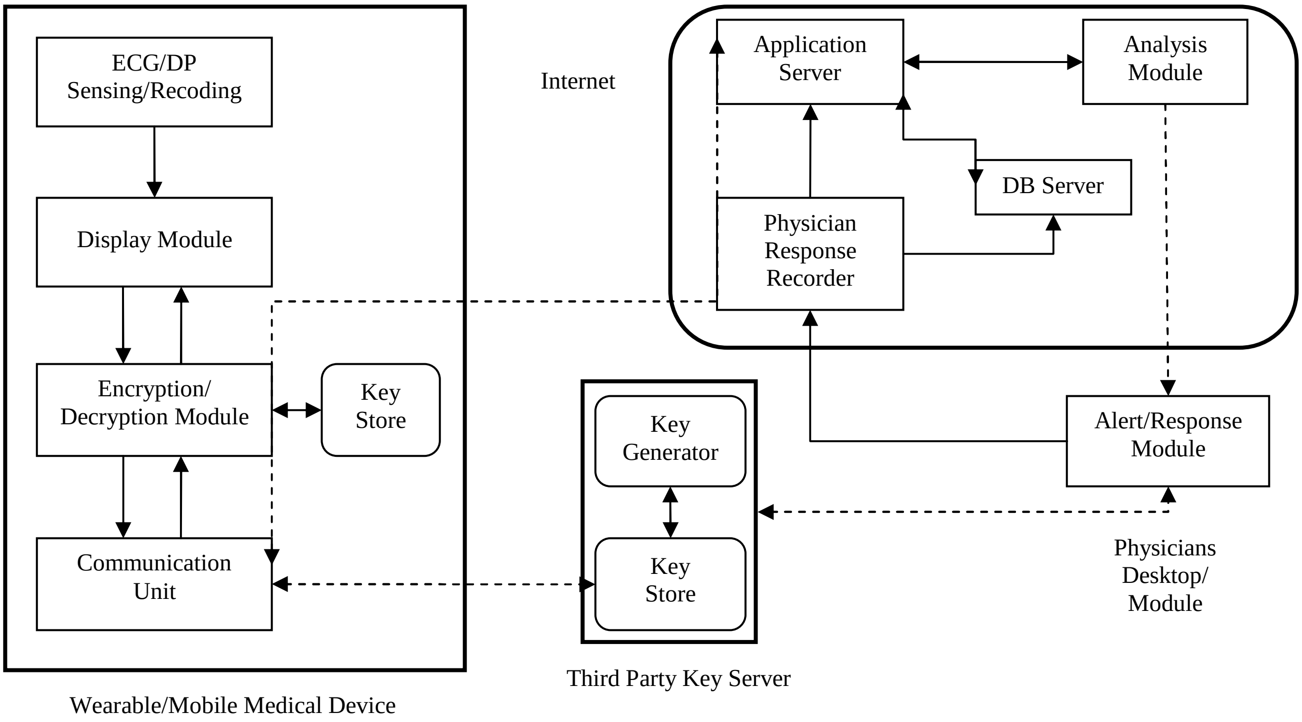

Fig. 2. Methodology

3.1. *Hill Cipher Encryption*

Hill cipher is a polygraphic substitution cipher based on linear algebra. In hill cipher encryption each character is represented by modulo. The key is used to encrypt the plaintext. The encryption procedure includes the multiplication of the key and the plaintext matrices. The result is the cipher text matrix. In decryption, in order to retrieve the original plaintext, the cipher text matrix is multiplied with the inverse of the key.

The limitations of hill cipher encryption include that not every key generated will have an inverse, and the determinant of the key may have common factors with the modular base.

Acknowledgments

We take this opportunity to thank our project guide Prof. P.S. Wawage and Prof. L.A. Kamble for their valuable guidance and for providing all the necessary facilities, which were indispensable in the completion of this paper. We would also like to thank Savitribai Phule Pune University for providing financial aid to our project.

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] "Ciphertext policy Attribute based Encryption with anonymous access policy" A.Balu1, K.Kuppusamy2 Research Associate, 2 Associate Professor Department of Computer Science & Engg.,Alagappa University, Karaikudi, Tamil Nadu, India. by A Balu - 2010

[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 International Cryptology 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".