International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Survey Paper on Applying Privacy to Healthcare Data Using Cloud

Nikhita Nerkar[1], Vina M Lomte[2]

Assitant Professor, Computer Department RMDSSOE, Warje, Pune, Maharashtra, India

Abstract: ***Mobile health (mHealth) monitoring using Cloud as SAAS, which applies the common mobile communications and cloud computing technologies to provide feedback decision support, which has been considered as a revolutionary approach to improve the quality of healthcare service while lowering the healthcare cost. Well, unfortunately it also poses a serious risk on clients/ mobile users privacy and intellectual property of monitoring service providers, which could prevent the wide adoption of mHealth technology. This project is to address privacy as an important problem and design Mobile Health Monitoring with Privacy Preserving using Cloud 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: SAAS, Healthcare, Privacy, Complexity

1. Introduction

Cloud Computing is the concept which explain advancement in the technology. It is used in real time communication network such as storing bulk of data, allowing multiple users to work on the same data at a time. The data is always considered as a valuable resource. We have seen wide development of mobile devices as they are now becoming smart phones which show great potential to improve human services. Data is one of the valuable resource and is considered as attribute. To prevent this attribute means client information from being accessed by any unauthorized user or any anonymous person. The proposed mobile health monitoring system works efficiently with the privacy criteria and giving the appropriate decision to the user as a response to the query asked by the client.

The Microsoft introduced "MediNet" [1] to monitor in the status of health problems like cardiovascular and diabetes diseases in the remote countries. This concept explained us that the user can insert transportable sensors in the body. These wireless sensors gathers different physiological data like ECG,BR,BP and blood glucose and peripheral oxygen saturation .In this the sensors collect the physiological data and transfers it to the connected mobile device. This mobile device further transfers through GPRS to the web server. If the connection is found weak, the data is stored in mobile device for retransmission.

These apps may have different operations ranging from sleep pattern analyzers, physical activity assistants, exercises, to cardiac analysis systems, giving different medical consultation. Anyway ,as the rising technologies of cloud computing develop a feasible explanation can be required by including the s/w as a service model and business model pay as you go in cloud computing, which would allow small companies(healthcare service provider) to explore in this healthcare market.

2. Related Work

G. Clifford et al. [2] Wireless transmission of data's are now widely being used by each and everyone. This wireless transmission increases issues of patient privacy particularly the risk of interception of patient data during transmission. All the private data's should be protected and the definition of "private" medical data or "protected" health information varies significantly according to the situation. A few countries have no privacy standards at all, and many clinicians transmit patient data via public email accounts without encryption. At the other extreme, an ECG without any identifiers is considered "private data" in the United Kingdom. The provision of health care through using mobile health has several benefits such as lower cost of capital investment, users familiarity with devices and interfaces, natural security i.e. access requires something you know (a password) and something you have (the device), allows construction of a long term medical record, allowing detailed personalized health care, automated data upload, no need for user involvement, natural route for data feedback to the user. In health monitoring system medical information which is transmitted over the telephone or internet is considered as an example of remote home health care technology that offers promising benefits for both individual and health care system. Such applications can be particularly useful for all patients who are unable to travel or for those living in rural or under reserved urban areas.

A. Cavoukian et al. [3] Many remote home health care systems allows individuals to personalize and convert devices, with the goal of enabling greater patients freedom, reducing cost and improving the ability for patients to be able to follow the wellness and treatment plan created for them by their medical practitioners. This remote home health care systems provide long term care to patients, to keep their physical fitness, nutrition, social activity, so they may function independently in their own homes for as long as possible, can help to deal with the social and financial burden of an aging population. M. Green et al. [6] A technique which is used for encryption is the proxy re-

encryption (PRE). Proxy re-encryption permits an untrusted proxy server with a re-encryption key (rekey) rkA→B to transform a cipher text (also known as first level cipher text) encrypted for Alice (delegator) into one (second level cipher text) that could be decrypted by Bob (delegatee) without allowing the proxy to obtain any useful information on the original message. We can classify proxy re-encryption according to various properties and can be transferable or non-transferable. Unidirectionality can be defined as, the delegation from A → B does not allow passing on in the opposite direction. Key privateness means that given the rekey rkA→B, the proxy figure out no information on either the identity of the delegator or the delegatee.

E. Shaw et al. [4] Case studies and survey research indicate that there is a division of information technology specialist who is particularly vulnerable to emotional pain, disappointment, dissatisfaction and consequent failures of judgment which can lead to an increased risk of damaging acts or vulnerability. This report is not an attempt to transmit doubts on an entire professional category whose role in the modern computer based economy has become so crucial. However, it's better to understand the motivations, psychological form and threat signals associated with those insiders who do pose a threat to the information systems.

There can be insider attacks and outsider attacks. The insider attacks could be started by either malicious or non malicious insiders. The insiders could be irritated employees or health care workers who enter the health care business for criminal purpose. The insider attacks have cost the ill-treated institutions much more than what outsider attacks have caused. Furthermore, insider attackers are usually much harder to deal with because they are generally sophisticated professionals or even criminal charms who are expert at escaping intrusion detection. On the other hand, while outsider attacks could be slightly prevented by directly accepting cryptographic methods such as encryption, it is significant to design a privacy preserving method against the insider attacks because it is crucial to balance the privacy restrictions and maintenance of normal operations of mobile health.

3. MHM System

3.1 Problem Statement:

This system will address the important problem of data security and design a cloud-assisted privacy preserving mobile health monitoring system to protect the privacy of the involved parties and their data. The intended system will consist of implementation in a mobile based environment. Integration of cloud server and users' device to provide efficient storage and accessibility. Providing complete security of user data in accompany with mobile environment.

3.2 Existing System

In Existing System CAM model is present as a web based project. A website that allows user login, Trusted Authority login and the company i. e. service provider. Our aim is to provide the service in an easier and in a mobile way. Users will have this service as an mobile app so the convenience or the usage is increased. Existing system misses the mobile part which our system will be implementing.

3.3 Proposed System

The proposed models will be a User module, a Trusted Authority module and a Service Provider module. User module consists of an android app which will allow users to use the application in mobile environment. It will present before the user a login and through which access to app showing their requests, also user will be able to query the app for their schedule of medication.

Trusted Authority module will act as an interface between user and service provider. It will hold the information provided by the users and provide the users with keys. The information is held by the trusted authority is in encrypted format so no way of information leak.

The System 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.

This system consists of 4 main parties:
1. The Client (mobile user)
2. Semi trusted Third Party
3. Service Provider (Company)
4. The Cloud

The company i.e. service provider stores it encrypted monitoring information (branching program) in the server cloud .The individual stores its personal Identification Information (PII) on the mobile device in form of attribute vectors. These attributes are further stored into the cloud under the persons information when he registers at a certain time.The branching done at the company level is the concept where node by node encryption is done and when query is fired node by node decryption is done and final results are matched at the end of the tree.

The cloud-assisted mobile monitoring program builds on branching program where the branching program is a triple. It can be represented as < {t1,…..,tk},L, R>. Here the first element is the set of nodes in the branching tree. Second element is the non leaf node in the branching tree also called decision node and the third element is the leaf node in the branching tree also called label node. Each decision node otherwise called non leaf node is a pair where the first element is the attribute index and the second element is the threshold value. The same attribute index value may occur in many nodes which mean that the same attribute may be evaluated more than once. Clients input their health data such as blood pressure, sugar level, whether they missed any daily medications or have an irregular diet, and the energy consumption of physical activity to the system service

provider. On receiving this information the service provider will return an advice to the client on how the clients can improve their health condition. Branching program is used in cloud-assisted mobile health monitoring and an example of branching program is shown below.

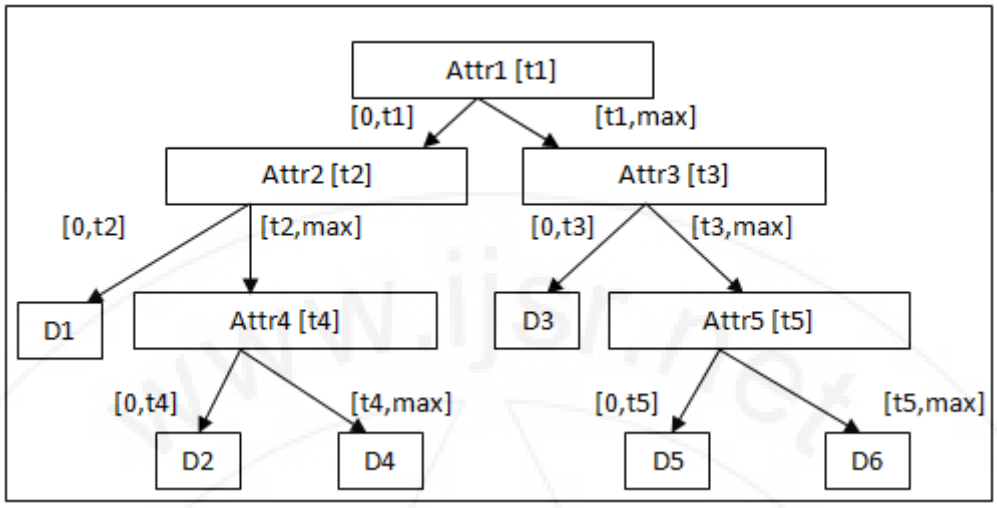

Figure 1: Branching Program at the company level

3.4 Semi Trusted Authority

TA works as an intermediate between the cloud server and the client. This protects client from getting access directly of the server cloud. It protects the cloud from direct storage or retrieval of the client's data. It allows the user to communicate or generate a query only if the user is authorised user with a token. As soon as the client becomes the authorised user it gets the token which is used for further communication.

3.5 The Client

Client is the user or we can say a user application which will allow the user to raise the query and get the decisions depending upon the raised query. This application saves the token given to it by TA at the time of registration. Once token given to the user is never the same for the different user.

Our proposed system accepts the newly outsourcing of decryption to significantly decrease the work pressure of both the client as well as the company outsourcing the bulk of the computational operations to the cloud while maintaining the company offline after the initialization phase.

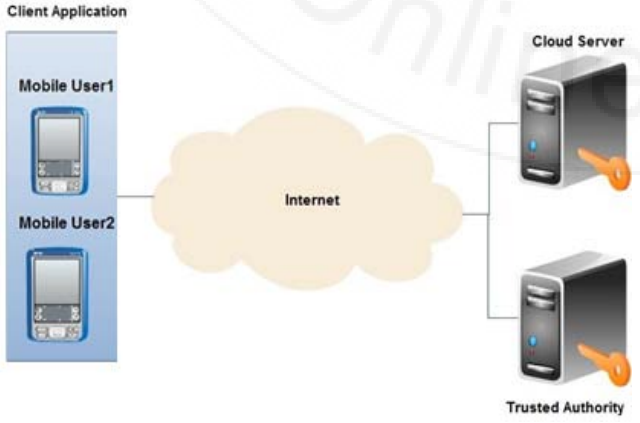

Figure 2: System Architecture

4. Conclusion

This new mobile health monitoring system ensures more security and efficiency which means that the cloud obtains no information on either the individual client query. The cloud obtains no useful information on the company's branching program due to the semantic security of the proxy re-encryption. The key privacy can promise that the cloud obtains no useful information on the branching program while completing all the computationally serious encryption operation for the company. On the other hand, the trusted authority and the company have the motivation to plan to obtain information on the client query. However, this attack cannot succeed because trusted authority obtains no information during the private key generation method. But here the problem is when two clients inputs the same medical data they may get the same recommendation without referring the previous health record.

5. Acknowledgment

I take this opportunity to express my profound gratitude and deep regards to my guide Prof. Vina Lomte, Asst. Professor, RMDSSOE for her exemplary guidance, monitoring and constant encouragement throughout the course of this thesis. The blessing, help and guidance given by her time to time shall carry me a long way in the journey of life on which I am about to embark.

I also take this opportunity to express a deep sense of gratitude to Prof. D. N Rewadkar, Associate Professor [Head of Department],RMDSSOE and Prof. Trupti Gedam, Asst. Professor, RMDSSOE, for her cordial support, valuable information and guidance, which helped me in completing this task through various stages. I am obliged to staff members of RMDSSOE, for the valuable information provided by them in their respective elds. I am grateful for their cooperation during the period of my assignment.

Lastly, I thank almighty, my parents, brother, sisters and

friends for their constant encouragement without which this assignment would not be possible.

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

[3] 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.

[4] E. Shaw, K. Ruby, and J. Post, "The insider threat to information systems: The psychology of the dangerous insider," Security Awareness Bulletin , vol. 2, no. 98, pp. 1 – 10, 1998.

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

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

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