Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 5, May 2014, pg.63 – 67

RESEARCH ARTICLE

AN EFFICIENT APPROACH FOR MOBILE HEALTH MONITORING

Neena Jose[1], Jini KM[2]

[1]Department of Computer Science and Engineering
Nehru College of Engineering and Research Center, Pampady, Thrissur, Kerala, India
[2]Department of Computer Science and Engineering
Nehru College of Engineering and Research Center, Pampady, Thrissur, Kerala, India
[1] neenajose028@gmail.com; [2] jini.km@gmail.com

Abstract— Cloud-assisted privacy preserving mobile health monitoring, which applies the mobile communications and cloud computing technologies, is considered as an efficient approach for improving the value of healthcare service while lowering the healthcare cost. This method protects the privacy of the parties who are involved in this system and their data.

Keywords— Mobile health; Private proxy re-encryption; Privacy preservation

I. INTRODUCTION

Cloud computing is a concept which is used in real time communication network such as internet to explain a variety of computing idea that consist of large number of computers. This concept is used in network based services. Data is a valuable resource and are considered as assets. In this paper asset means clients information as well as information about the service provider. Privacy preservation is the protection of these assets, which is to be protected against unauthorized data disclosure, unauthorized data modification, denial of service, and lack of accountability. Usual privacy protection method is by simply removing client's personal identity information (such as names or SSN) fails to serve as an effective way for providing privacy for mobile health system due to the increasing quantity and diversity of personal identity information. It is important to note that the collected information from a mobile health monitoring system could contain client's personal physical data such as the heights, weights, and blood group, or even their fingerprints and DNA profiles. The proposed mobile health monitoring system provides a good opening for adversaries to obtain a large set of medical information, which could potentially show the way to identify an individual user.

Internet based systems are increasingly common now but an important growth area is the monitoring of health using a mobile phone. Mobile phones are now being constructed to be used with integrated health sensors to work together with external sensors for health monitoring. Sensor is an instrument that can be used to measure physical or environmental characteristics or state and can display the reading or transmit that reading for display and can be stored elsewhere. Mobile devices, such as smart phones equipped with low cost sensors can be used for health monitoring.

II. **RELATED WORKS**

Huang et al. [1] 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.

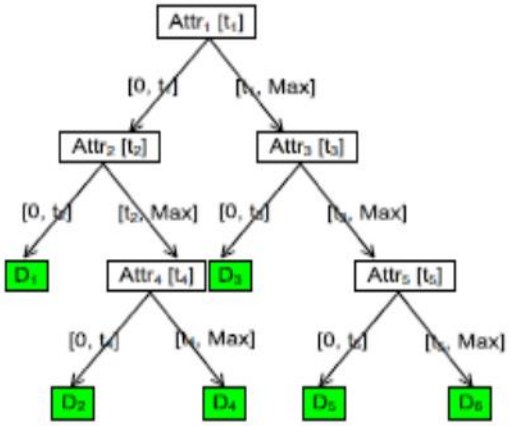

Fig 1: Branching program

P. Mohan et al. [2] "MediNet": a project launched by Microsoft which is designed to understand remote monitoring on the health status of diabetes and cardiovascular diseases in remote areas. This remote mobile health monitoring system can help the clients in such a way that they could arrange portable sensors in wireless body sensor networks. These portable sensors collect various physiological data, such as blood pressure (BP), breathing rate (BR), and Electrocardiogram (ECG) and blood glucose. There will be a central server and such physiological data could then be sent to this central server. The central server could then run various webs medical applications on these data to return appropriate advice to the client to improve their health condition. These applications may have various functionalities ranging from exercises providing various medical consultations to the client.

G. Clifford et al. [3] 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.

E. B. Fernandez et al. [4] Security in data intensive computing system means that nobody needs their data to be handled by institution or to be seen by those who could misuse it. Enterprise wants their information to be

hidden from competitors and patients do not want their medical records to be seen by unauthorized people. There are people who purposely try to misuse information either for their own gain, to make a point, or for the sake of doing damage. Some of their actions include viruses and similar attacks that damage information; some actions are to access or modify information.

A. Cavoukian et al. [5] 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) $rk_{A \rightarrow B}$ 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 $A \rightarrow B$ does not allow passing on in the opposite direction. Key privateness means that given the rekey $rk_{A \rightarrow B}$, the proxy figure out no information on either the identity of the delegator or the delegatee.

S. Al-Fedaghi et al. [7] defines Personal Identifiable Information (PII). According to him PII is the information recorded or otherwise, connecting to an identifiable individual. If any information is connected to an identifiable individual, it can become personal in nature. Recently, a number of current works have already shown that even blood pressure can be used to identify individual users. It is also observed that future mobile health monitoring and decision support systems might have to deal with other much more privacy-sensitive features such as DNA profiles. Another major issue in addressing security and privacy is the computational workload involved with the cryptographic techniques. With the current cloud computing facilities, it will be intelligent to transfer intensive computations to cloud servers from resource controlled mobile devices.

P. Dixon et al. [8] various companies have significant profitable interests in collecting client's private health data and sharing this information with the insurance companies, or research institutions or even the government agencies. It has also been indicated that privacy law could not really apply any real protection on client's data privacy unless there is an effective mechanism to implement boundaries on the activities of healthcare service providers.

L. Ponemon Institute et al. [9] According to the study more than 73% of respondents do not trust the central government, including departments such as the US department of health and human service, to protect the privacy of their health records. In contrast, 71% of respondents do trust health care providers such as hospital such as hospitals, clinics and physicians to protect the privacy of their health report. Significantly smaller number of respondents believes it is very important to have stricter rules to prevent private companies from having access to health records without the respondent's permission.

E. Shaw et al. [10] 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.

III. **CLOUD ASSISTED PRIVACY PRESERVING MOBILE HEALTH MONITORING**

In the basic cloud assisted mobile health monitoring, the monitoring program delivered by the company is encrypted using multi dimensional range query scheme and the cipher text is stored in the untrusted cloud. In multi dimensional range query system, a sender encrypts a message under a range [r1, r2], and a receiver with the privacy key corresponding to the range [r1, r2] can decrypt the original message. The company then sends some re-encryption keys to the cloud. The key private property can promise that no valuable information about the original identities, related to the thresholds of the intermediate nodes, is leaked to the cloud. By adjusting proxy re-encryption, it's easy to reduce the encryption workload for the company.

Even though proxy re-encryption has been recognized as a significant tool for access control on the cloud, property re-key generation efficiency should be added to the proxy re-encryption plan in order to make it as a more efficient means for outsourcing encryption to the cloud. Rekey generation efficiency essentially means that the calculation of the re-key generation should be much less than that of the first level encryption in proxy re-encryption, which is really useful when the proxy re-encryption scheme give outs to outsource immense public key encryption operations. In the latest cloud assisted privacy preserving mobile health monitoring system, a new identity-based key private proxy re-encryption scheme is used with lower cost of re-key generation comparing with the original encryption algorithm. Multi dimensional range queries play a very important role in cloud assisted mobile health monitoring design because all the comparisons between the clients input vector and the respective thresholds at intermediate decision nodes are implemented using multi dimensional range queries. At each decision node, the respective threshold is represented as two minimum root sets: [0, ti] and (ti, Max] where ti is the threshold value.

Cloud-assisted privacy preserving mobile health monitoring consists of four segments. They are the cloud server, the company who provides the mobile health monitoring service (the healthcare service provider), and the individual clients, and a semi-trusted authority (TA). The company stores its encrypted monitoring information or program in the cloud server. Individual clients gather their medical data and store them in their mobile devices, which then convert this medical data into attribute vectors. The attribute vectors are sent as inputs to the monitoring program in the cloud server through a mobile 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 coworker 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 join together to obtain private health data from client input vectors.

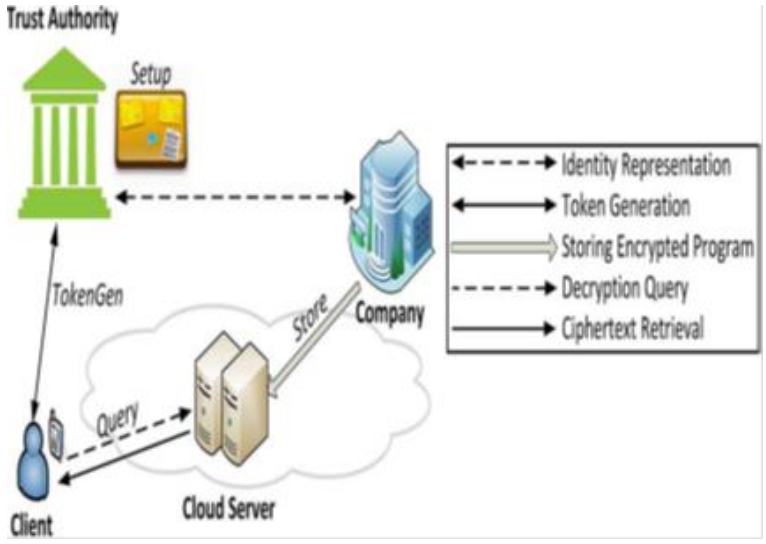

Fig 2: System Architecture

The four major steps of cloud assisted privacy preserving mobile health monitoring systems are Setup, Store, TokenGen and Query. At the system initialization, trusted authority runs the Setup phase and publishes the system parameters. Then the companies will states the flow chart of the mobile health monitoring program as a branching program, which is encrypted under the respective directed branching tree. Then the company will

send the resulting cipher text and the company index to the cloud, which match to the Store algorithm in the framework.

When a client wants to query the cloud for a certain mobile health monitoring program, the client and trusted authority runs the token generation algorithm. The client sends the company index to trusted authority, and then inputs its private query (which is the attribute vector representing the collected health data) and trusted authority put in the master secret to the algorithm. The client gets the token corresponding to its query input while trusted authority gets no useful information on the individual query. During the last phase, the client delivers the token for its query to the cloud, which corresponds to the Query phase.

The cloud completes the major computationally serious job for the client's decryption and returns the partially decrypted cipher text to the client. The client then performs the remaining decryption job after receiving the partially decrypted cipher text and gets its decryption result. The cloud obtains no valuable information on either the client's private query input or decryption end result after running the Query phase. Cloud-assisted privacy preserving mobile health monitoring can stop the cloud from deducing useful information from the client's query input or output related to the received information from the client.

In cloud assisted privacy preserving mobile health monitoring, the system time is break up into multiple time periods, called slots. Each slot can last a week or a month depending on particular applications. There is a predictable maximum number of user's requesting contact to the monitoring program in any given slot. In cloud assisted privacy preserving all the costly operations the company needs to carry out is the calculation of the cipher texts delivered to the cloud and then it could stay offline until the end of a slot. All the company then performs the first level encryption in the proxy re-encryption.

IV. CONCLUSION

The new cloud assisted privacy preserving 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.

REFERENCES

[1] Huang Lin, Jun Shaoy, Chi Zhangz, and Yuguang Fang, Fellow, IEEE *Tranasctions on image processing* vol:8 no:6 year 2013*, "*CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring".

[2] 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.

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

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

[5] 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.

[6] M. Green and G. Ateniese, "Identity-based proxy re-encryption," in ACNS, ser. Lecture Notes in Computer Science, J. Katz and M.Yung, Eds., vol. 4521. Springer, 2007, pp. 288–306.

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

[8] P. Dixon, "Medical identity theft: The information crime that can kill you," in *The World Privacy Forum*, 2006.

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

[10] 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.

