

Cam: Cloud-Assisted Privacy Preserving Mobile Health Monitoring

Gandeti Saikalyan , Sri.S.K.Alisha, Sri.V.Bhaskara Murthy
Mca Student, Senior Assistant Professor, Associate Professor
Dept Of Mca
B.V.Raju College, Bhimavaram

ABSTRACT

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 mHealth 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.

I.INTRODUCTION

To facilitate our discussion, we first elaborate our cloudassisted mHealth monitoring system (CAM). 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), 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. We assume a neutral cloud server, which means it neither colludes with the company nor a client to attack the other side.

II.EXISTING SYSTEM

Existing 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 mHealth technology.

Disadvantages:

1. Existing privacy laws such as HIPAA (Health Insurance Portability and Accountability Act) provide baseline protection for personal health record, they are generally considered not applicable or transferable to cloud computing environments.

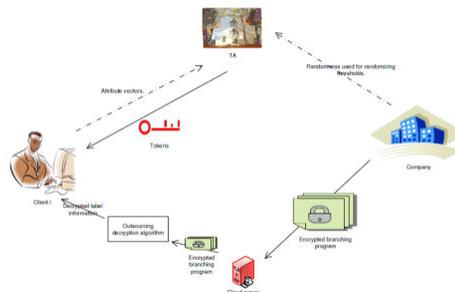
III.PROPOSED SYSTEM

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), 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.

ADVANTAGES:

1. Reducing the computational and communication burden on clients and the cloud.
2. The cloud cannot know anything about the user's search privacy, access privacy.

IV.SYSTEM ARCHITECTURE



V.IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and its constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Problem Statement:

Traditional privacy protection mechanisms by simply removing clients' personal identity information (such as names or SSN) or by using anonymization technique fails to serve as an effective way in dealing with privacy of mHealth systems due to the increasing amount and diversity of personal identifiable information [9]. It is worth noting that the collected information from an mHealth monitoring system could contain clients' personal physical data such as their heights, weights, and blood types, or even their ultimate personal identifiable information such as their fingerprints and DNA profiles. According to, personal identifiable information (PII) is "any information, recorded or otherwise, relating to an identifiable individual. Almost any

information, if linked to an identifiable individual, can become personal in nature, be it biographical, biological, genealogical, historical, transactional, locational, relational, computational, vocational, or reputational”.

Scope:

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), 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.

MODULE DESCRIPTION:

Branching Program:

we formally describe the branching programs, which include binary classification or decision trees as a special case. We only consider the binary branching program for the ease of exposition since a private query protocol based on a general decision tree can be easily derived from our scheme. Let v be the vector of clients' attributes. To be more specific, an attribute component v_i is a concatenation of an attribute index and the respective attribute value. For instance, $A||KW1$ might correspond to “blood pressure: 130”. Those with a blood pressure lower than 130 are considered as normal, and those above this threshold are considered as high blood pressure. The first element is a set of nodes in the branching tree. The non-leaf node

p_i is an intermediate decision node while leaf node p_i is a label node. Each decision node is a pair (a_i, t_i) , where a_i is the attribute index and t_i is the threshold value with which v_{a_i} is compared at this node. The same value of a_i may occur in many nodes, i.e., the same attribute may be evaluated more than once. For each decision node i , $L(i)$ is the index of the next node if $v_{a_i} \leq t_i$; $R(i)$ is the index of the next node if $v_{a_i} > t_i$. The label nodes are attached with classification information. Repeat the process recursively for p_h , and so on, until one of the leaf nodes is reached with decision information.

Token Generation:

To generate the private key for the attribute vector $v=(v_1, \dots, v_n)$, a client first computes the identity representation set of each element in v and delivers all the n identity representation sets to TA. Then TA runs the $AnonExtract(id, msk)$ on each identity $id \in S_{v_i}$ in the identity set and delivers all the respective private keys sk_{v_i} to the client.

Query:

A client delivers the private key sets obtained from the TokenGen algorithm to the cloud, which runs the AnonDecryption algorithm on the ciphertext generated in the Store algorithm. Starting from p_1 , the decryption result determines which ciphertext should be decrypted next. For instance, if $v_1 \in [0, t_1]$, then the decryption result indicates the next node index $L(i)$. The cloud will then use $sk_{v(L(i))}$ to decrypt the subsequent ciphertext $CL(i)$. Continue this process iteratively until it reaches a leaf node and decrypt the respective attached information.

Semi Trusted Authority

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.

VI.CONCLUSION

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 identitybased encryption (IBE) in medical diagnostic branching programs. To reduce the decryption complexity due to the use of IBE, we apply recently proposed decryption outsourcing with privacy protection to shift clients' pairing computation to the cloud server. To protect mHealth 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 resourceconstrained 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 telemonitoring 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.