OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

Secure Multi-Owner Group Signature Based Secure M-Health Records in Cloud

B. Anitha[1], V. Udhaya Kumar[2]

[1]M.Tech Student Department of Computer Science and Engineering PRIST University Pondicherry, India
[2]Assistant professor Department of Computer Science and Engineering PRIST University Pondicherry, India

ABSTRACT: *Cloud-assisted mobile health 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. 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.*

Keywords: *MHealth, monitoring, decryption*

I. Introduction

We design a cloud-assisted mobile health monitoring system (CAM). We first identify the design problems on privacy preservation and then provide our solutions. To ease the understanding, we start with the basic scheme so that we can identify the possible privacy breaches. We then provide an improved scheme by addressing the identified privacy problems. The resulting improved scheme allows the mobile health service provider (the company) to be offline after the setup stage and enables it to deliver its data or programs to the cloud securely. To reduce clients' decryption complexity, we incorporate the recently proposed outsourcing decryption technique into the underlying multi-dimensional range queries system to shift clients' computational complexity to the cloud without revealing any information on either clients' query input or the decrypted decision to the cloud. To relieve the computational complexity on the company's side, which is proportional to the number of clients, we propose a further improvement, leading to our final scheme. It is based on a new variant of key private proxy re-encryption scheme, in which the company only needs to accomplish encryption once at the setup phase while shifting the rest computational tasks to the cloud without compromising privacy, further reducing the computational and communication burden on clients and the cloud**.**

II. Problem Definition

Major problem in addressing security and privacy is the computational workload involved with the cryptographic techniques. With the presence of cloud computing facilities, it will be wise to shift intensive computations to cloud servers from resource-constrained mobile devices. However, how to achieve this effectively without compromising privacy and security becomes a great challenge, which should be carefully investigated.

The problem becomes especially trickier for cloud assisted mobile health systems because we need not only to guarantee the privacy of clients' input health data, but also that of the output decision results from both cloud servers and healthcare service providers (which will be referred to as the company in the subsequent development).

III. Problem Description

We first identify the design problems on privacy preservation and then provide our solutions. To ease the understanding, we start with the basic scheme so that we can identify the possible privacy breaches. We then provide an improved scheme by addressing the identified privacy problems. The resulting improved scheme allows the mobile health service provider (the company) to be offline after the setup stage and enables it to deliver its data or programs to the cloud securely. To reduce clients' decryption complexity, we incorporate the recently proposed outsourcing decryption technique into the underlying multi-dimensional range queries system to shift clients' computational complexity to the cloud without revealing any information on either clients' query input or the decrypted decision to the cloud.

IV. Feasibility Study

Feasibility analysis tells how the present system is compatible with the resource present with developing team. The objective is to determine quickly at the minimum expense how to solve a problem. The following feasibility studies are conducted to the feasibility of proposed system.

The feasibility study is term in three ways as followed:

- Technical feasibility
- Behavioral feasibility
- Economical feasibility

A. Technical Feasibility

Technical feasibility center on the computer system (hardware, software etc.) and to what extend it can support the proposed system. This system uses ASP.NET with c# as front end and SQL as back end. Since the system needs much user interface, the design and implementation can be done.

B. Behavioral Feasibility

The annotation overhead is very small. So that the performance of the fully automatic static verification is acceptable, and that the performance overhead of the runtime checking is limit. So this system is operationally feasible**.**

C. Economic Feasibility

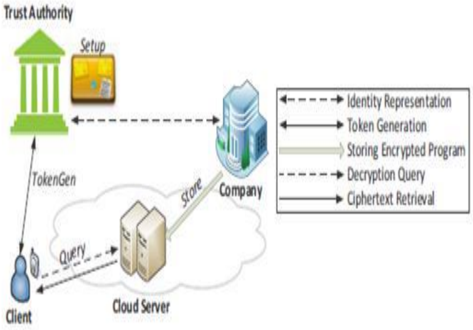
The current project is economically feasible because the project duration is 6 months and the man power is one. All the necessary hardware and software are provided in the organization.
The basic COCOMO estimation:
A development project is sized at 3.7 KLOC.
The basic COCOMO equation for effort (E) in staff-months(SM) is:
Effort(SM) = 2.4(KLOC) 1.05 = 2.4(3.7)1.05 = 2.4(3.885) = 9.324 staff-months.
Development time (TDEV): TDEV = 2.5(SM) 0.38 = 2.5(9.324)0.38 = 2.5(3.54312) = 6 months.
The average number of staff members(S):
Staff = Effort / TDEV = 10 staff-months / 6 months = 1. 5 staff members on average.
The productivity rate (P):
Productivity = Size / Effort = 3700 LOC / 9.324 staff-months = 396 LOC/staff-months
So the implementation of the project is no so costlier and the system is economically feasible.

V. Proposed System

In this paper, we design a cloud-assisted mobile health monitoring system (CAM). We first identify the design problems on privacy preservation and then provide our solutions. We then provide an improved scheme by addressing the identified privacy problems. The resulting improved scheme allows the mobile health service provider (the company) to be offline after the setup stage and enables it to deliver its data or programs to the cloud securely. To reduce clients' decryption complexity, we incorporate the recently proposed outsourcing decryption technique into the underlying multi-dimensional range queries system to shift clients' computational complexity to the cloud without revealing any information on either clients' query input or the decrypted decision to the cloud. It is based on a new variant of key private proxy re-encryption scheme, in which the company only needs to accomplish encryption once at the setup phase while shifting the rest computational tasks to the cloud without compromising privacy**.**

VI. System Architecture

The company stores its encrypted monitoring data or program (branching program) in the cloud. 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 through a mobile (or smart) phone. TA is responsible for distributing private keys to clients and collecting service fees from clients according to a certain business model such as "pay-peruse" model. TA can be considered as a collaborator or a management agent for a company (or several companies) and thus shares certain level of mutual business interest with the company.

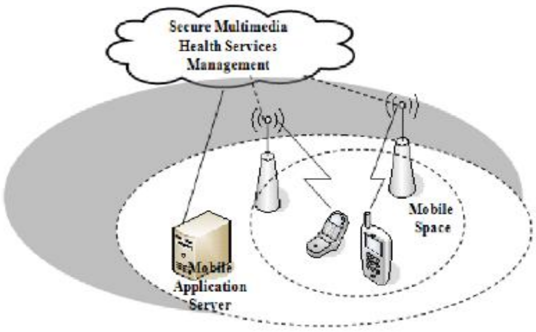


At the initial phase, TA runs the Setup phase and publishes the system parameters. Then, the company first characterizes the flow chart of an mobile health monitoring program as a branching program which is encrypted under the respective directed branching tree. Then the company will deliver the resulting cipher text and its company index to the cloud, which corresponds to the Store algorithm in the context. When a client wishes to query the cloud for a certain mobile health monitoring program, the i-th client and TA run the Token Gen algorithm. The client sends the company index to TA, and then inputs its private query (which is the attribute vector representing the collected health data) and TA inputs the master secret to the algorithm. The client obtains the token corresponding to its query input while TA gets no useful information on the individual query.

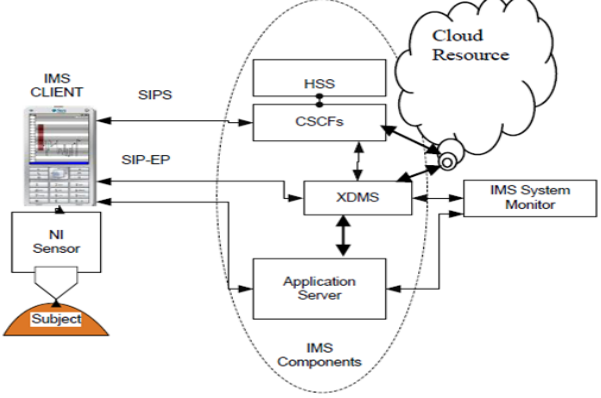
At the last phase, the client delivers the token for its query to the cloud, which runs the Query phase. The cloud completes the major computationally intensive task for the client's decryption and returns the partially decrypted cipher text to the client. The client then completes the remaining decryption task after receiving the partially decrypted cipher text and obtains its decryption result, which corresponds to the decision from the monitoring program on the client's input. The cloud obtains no useful information on either the client's private query input or decryption result after running the Query phase.

VII. Data Flow Diagram

A data flow diagram is graphical tool used to describe and analyze movement of data through a system.


Secure Multimedia Health Services Management
Mobile Space
Mobile Application Server

VIII. Ims-Based Mobile Health Monitoring With Cloud Support



A. Outsourcing Decryption

The basic CAM has the following security weaknesses .First, the identity representation set for a client’s attribute vector v is known to TA, and hence TA can easily infer the client’s private attribute vector. Second, the client cannot protect his privacy from the cloud either because the cloud can easily find out the identity representation for the private key skvi, i ∈ [1, n] by running identity test in MDRQ. The cloud can simply encrypt a random message under any attribute value v′ until it can use sky to successfully decrypt the cipher text, which means there is a match between v′ = vi and hence it successfully finds out vi. Third, neither can the data privacy of the company be guaranteed since the identity representation of the respective range is revealed to the cloud whenever the decryption is successful due to the match revealing property (see Sec. II-D3) of MDRQ. The cloud can finally find out the company’s branching program since it has the private keys of all the system users.

To rectify these weaknesses in the basic CAM, we provide the following improvement in this module. The high level idea is as follows: in order to avoid leaking the attribute vector to TA, the client obliviously submits his attribute vectors to TA so that he can obtain the respective private keys without letting TA get any useful information on his private vector. The client runs the outsourcing decryption of MDRQ to ensure the cloud completes the major workload while obtaining no useful information on his private keys. On the other hand, the company will permute and randomize its data using homomorphism encryption2 and MDRQ so that neither the cloud nor a client can get any useful information on its private information on branching program after a single query. Meanwhile, the company is also required to include the randomness in the randomization step in the encryption sent to TA to ensure that TA can successfully generate tokens for clients.

B. Healthcare

Feature of Mobile Health All the major health failure problem classification to this page.

a. Login

i. Login the all authorized administrator user to login and give diagnosis the patient.

ii. Registration

iii. User Directory

iv. User Treatment Commands

v. User Profile

b. Privacy Block

In this Module, security tools and offers the necessary modifications to meet our design needs.

c. Bilinear Pairing:

Bilinear pairing is crucial to our design, which would further serve as the building block of the proposed CAM.

d. Homomorphic Encryption:

Another technique we will use for oblivious transfer protocol is homomorphic encryption, which is widely used as an underlying tool for constructing secure protocols. CAM adopts a semantically secure additively homomorphic public-key encryption technique.

C. Mobile Health Information

The proposed re-encryption scheme incorporates the outsourcing decryption so that the other security and efficiency characteristics in the final CAM should be inherited here. By using our newly-proposed key private proxy re-encryption, we are design our highly efficient CAM with full Privacy in this module**.**

D. Cloud user

We create a local Cloud and provide priced abundant storage services. The users can upload their data in the cloud. We develop this module, where the cloud storage can be made secure. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users’ trusted domain. Similar to we assume that the cloud server is honest but curious. That is, the cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes, but will try to learn the content of the stored data and the identities of cloud users**.**

E. Group Manager

Group manager takes charge of followings,

1. System parameters generation,
2. User registration,
3. User revocation, and
4. Revealing the real identity of a dispute data owner.

Therefore, we assume that the group manager is fully trusted by the other parties. The Group manager is the admin. The group manager has the logs of each and every process in the cloud. The group manager is responsible for user registration and also user revocation too.

F. Group Member

Group members are a set of registered users that will

1. Store their private data into the cloud server and
2. Share them with others in the group.

Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company. The group member has the ownership of changing the files in the group. Whoever in the group can view the files which are uploaded in their group and also modify it. The group meme

G. File Security

- Encrypting the data file.
- File stored in the cloud can be deleted by either the group manager or the data owner. (i.e., the member who uploaded the file into the server).

H. Group Signature

A group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers. Besides, the designated group manager can reveal the identity of the signature's originator when a dispute occurs, which is denoted as traceability.

I. User Revocation

User revocation is performed by the group manager via a public available revocation list (RL), based on which group members can encrypt their data files and ensure the confidentiality against the revoked users.

XI. CONCLUSION

In this paper, 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 mobile health service providers. To protect the clients' privacy, we apply the anonymous Boneh-Franklin identity based 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 m Heath 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 resource constrained small companies to participate in mobile health business.

REFERENCES

[1]. [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," in Engineering in Medicine and Biology Society, 2008. EMBS 2008. 30th Annual International Conference of the IEEE. IEEE, 2008, pp. 755–758.

[2]. [2] A. Tanas, 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]. [3] G. Clifford and D. Clifton, "Wireless technology in disease management and medicine," Annual Review of Medicine, vol. 63, pp. 479–492, 2012.

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

[5]. [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 Pervasive Health, 2011, pp. 478–484.

[6]. [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]. [7] N. Singer, "When 2+ 2 equals a privacy question," New York Times, 2009.