International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.7, pp : 834-837 1 July 2014

SPHM: A Secured Patient Healthcare Mobile Monitoring using Cloud Computing

Dr.P.RajaRajeswari[1], J.Jameson[2], V.Premalatha[2]

1- M.tech [CSE], JNTU Kakinada
rajilikhitha@gmail.com
2 -Nimra college of Engg. JNTU Kakinada

ABSTRACT :A Secured Patient Healthcare Mobile Monitoring using Cloud computing helps to keep the communication between doctor and patient confidential. It applies the prevailing mobile communications and cloud computing technologies, which is a good approach to improve the quality of healthcare service minimizing the cost. The cloud server respects the privacy of a patient and keeps it secured by protecting the medical history of the patient. This paper addresses the design of a cloud assisted privacy preserving mobile health monitoring system to protect the privacy of the involved parties and their data. The main objective of the proposed system is preserving the privacy of the information ensuring that this information cannot be misused. The patient's report will reach the doctor in encrypted format, while a master key helps to deliver the report to the doctor in decrypted format. Then the doctor's prescription will reach the patient in encrypted format by using the Outsourcing Decryption Technique while a master key helps to deliver the prescription to the patient in decrypted format. Finally, our security and performance analysis demonstrates the effectiveness of our proposed design.

Keywords: Patient Healthcare Monitoring, Decryption, Cloud Computing, mHealth.

1. INTRODUCTION

The development of cloud computing services is speeding up the rate in which the organizations outsource their computational services or sell their idle computational resources. One of the most important aspect refers to security: while some cloud computing security issues are inherited from the solutions adopted to create such services, many new security questions that are particular to these solutions also arise, including those related to how the services are organized and which kind of service/data can be placed in the cloud. Aiming to give a better understanding of this complex scenario, in this paper the main security concerns and solutions in cloud computing**[1]** are analysed.

The design problems on privacy preservation is identified and the optimum solution is provided. 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**[2],** 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**[3].**

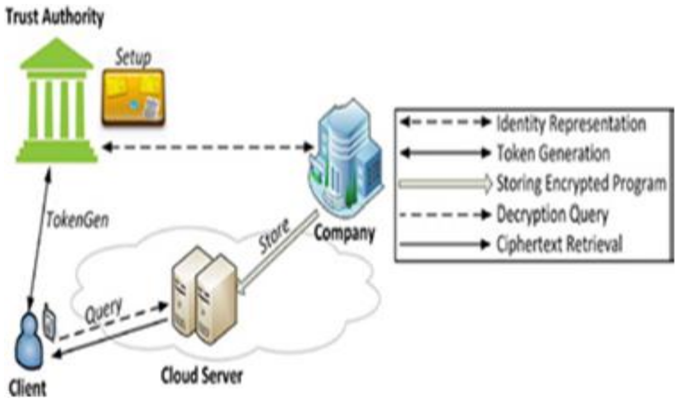
Traditionally, the privacy issue is tackled with anonymization technique such as *k*-anonymity or *l*-diversity. However, it has been indicated that these techniques might be insufficient to prevent re-identification attack **[4].** The threat of re-identification is so serious that legal communities **[5]** have already been calling for more sophisticated protection mechanism instead of merely using anonymization. We believe that our proposed cryptographic based systems could serve as a viable solution to the privacy problems in mHealth systems, and also as an alternative choice for those privacy-aware users.

As an important remark, our design here mainly focuses on insider attacks, which could be launched by either malicious or non-malicious insiders. For instance, the insiders could be disgruntled employees or healthcare workers who enter the healthcare business for criminal purpose **[6], [7].** It was reported that 32% of medical data breaches in medical establishments between January 2007 and June 2009 were due to insider attacks **[8],** and the incident rate of insider attacks is rapidly increasing **[8].**

2. EXISTING SYSTEM

Existing Cloud-assisted mobile health (mHealth) monitoring, which applies the prevailing mobile communications and cloud computing technologies to provide feedback decision support**[9],** 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 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

Figure 1: System architecture for Existing system



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 be more effective than health service provider to be online.

3. Proposed system

A secured patient healthcare monitoring in cloud infrastructure helps to keep the communication between doctor and patient confidential. The encryption and decryption format is the soul of this project. The patient's report will reach the doctor in encrypted format, a master key helps to deliver the report to the doctor in decrypted format.

Our Proposed system consists of four components: 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. 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.

4. SYSTEM ARCHITECTURE

Architecture Flow:

3-Tier Architecture:

The three-tier software architecture (a three layer architecture) emerged in the 1990s to overcome the limitations of the two-tier architecture. The third tier (middle tier server) is between the user interface (client) and the data management (server) components. This middle tier provides process management where business logic and rules are executed and can accommodate hundreds of users (as compared to only 100 users with the two tier architecture) by providing functions such as queuing, application execution, and database staging.

The three tier architecture is used when an effective distributed client/server design is needed that provides (when compared to the two tier) increased performance, flexibility, maintainability, reusability, and scalability, while hiding the complexity of distributed processing from the user. These characteristics have made three layer architectures a popular choice for Internet applications and net-centric information systems

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.

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.

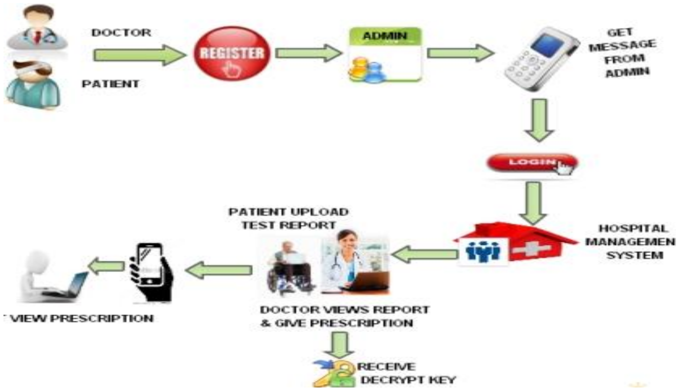
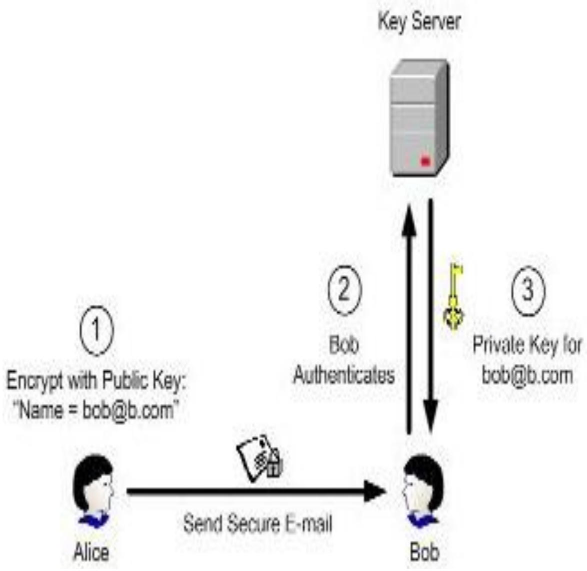

DOCTOR
PATIENT
REGISTER
ADMIN
GET MESSAGE FROM ADMIN
LOGIN
HOSPITAL MANAGEMEN SYSTEM
PATIENT UPLOAD TEST REPORT
DOCTOR VIEWS REPORT & GIVE PRESCRIPTION
VIEW PRESCRIPTION
RECEIVE DECRYPT KEY

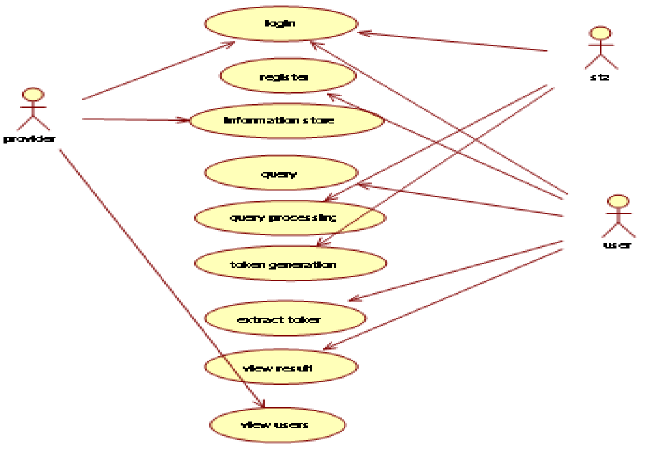
Fig: SYSTEM ARCHITECTURE FOR PROPOSED SYSTEM

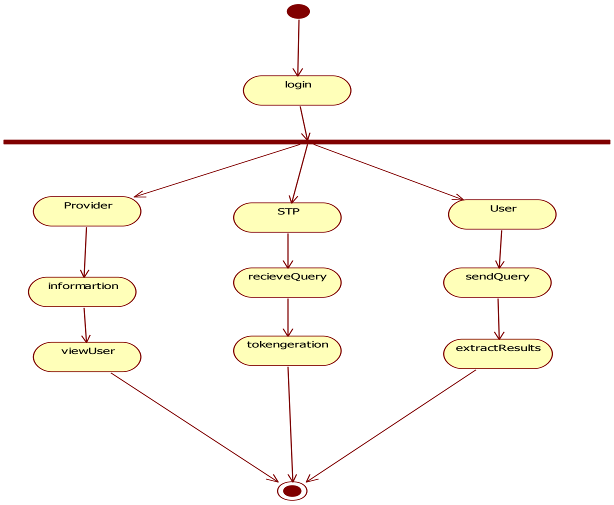
At the last phase, the client delivers the token for its query to the cloud, which runs the Query phase. The cloud completes the major computationally intensive task for the client's decryption and returns the partially decrypted cipher text to the client. The client then completes the remaining decryption 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.

EXAMPLE OF IBE

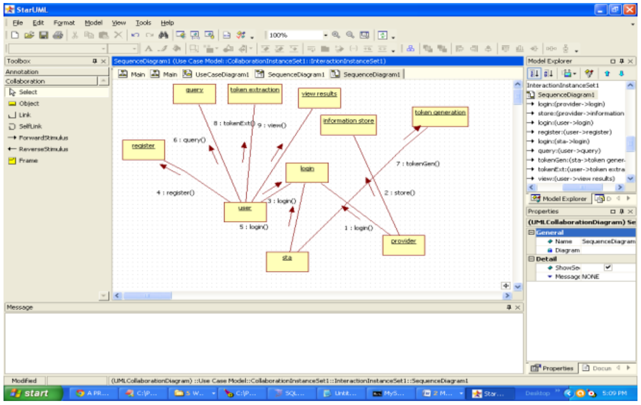

Key Server
1
Encrypt with Public Key: "Name = bob@b.com"
2
Bob Authenticates
3
Private Key for bob@b.com
Send Secure E-mail
Alice
Bob

ACTIVITY DIAGRAM OF OUR PROPOSED SYSTEM





Collaboration Diagram



SequenceDiagram1 (Use Case Model::CollaborationInstanceSet1::InteractionInstanceSet1)

InteractionInstanceSet1
SequenceDiagram1
login:(provider->login)
store:(provider->information
login:(user->login)
register:(user->register)
login:(sta->login)
query:(user->query)
tokenGen:(sta->token gener-
tokenExt:(user->token extra
view:(user->view results)

(UMLCollaborationDiagram) ::Use Case Model::CollaborationInstanceSet1::InteractionInstanceSet1::SequenceDiagram1

5. Experimental Result

Registration is a mandatory process to get into a hospital management system for any doctor and Patient.

The following modules are created for effective generation of the proposed system output

Branching Program:

we formally describe the branching programs, which include binary classification or decision trees as aspecial case.

We only consider the binary branching program for the ease of exposition since a privatequery 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 *vi* 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 (*ai*, *ti*), where *ai* is the attribute index and *ti* is the threshold value with which *vai* is compared at this node. The same value of *ai* 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 *vai* ≤ *ti*; *R*(*i*) is the index of the next node if *vai* > *ti*. 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:

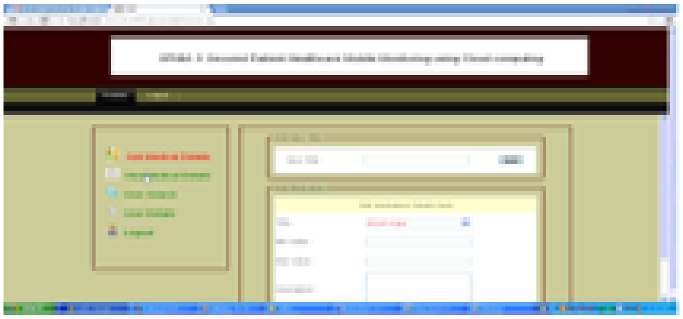
To generate the private key for the attribute vector v=(*v*1, · · · , *vn*), a client first computes the identity representation set of each element in v and delivers all the *n* identity representation sets to TA. Then TA runs the AnonExtract(id, msk) on each identity id ∈ *Svi* in the identity set and delivers all the respective private keys sk*vi* 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 p1, the decryption result determines which ciphertext should be decrypted next. For instance, if *v*1 ∈ [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.



6. Advantages

The identity-based encryption scheme is that if there are only a finite number of users, after all users have been issued with keys the third party's secret can be destroyed. The authenticity of the public keys is guaranteed implicitly as long as the transport of the private keys to the corresponding user is kept secure (Authenticity, Integrity, Confidentiality). When the receiver contacts the PKG to retrieve the private key for this public key, the PKG can evaluate the identifier and decline the extraction if the expiration date has passed. Generally, embedding data in the ID corresponds to opening an additional channel between sender and PKG with authenticity guaranteed through the dependency of the private key on the identifier Paper

7. Conclusion

This paper addresses a cloud-assisted privacy preserving mobile health monitoring system, called CAM, which effectively protect the privacy of clients and the intellectual property of mHealth service providers. Cloud Computing technology provides human advantages such as economical cost reduction and effective resource management. However, if security accidents occur, economic damages are inevitable. Our paper proposed "A secured patient healthcare monitoring in cloud infrastructure" for effective resource consists of Identity Based Encryption (IBE) in which a master key helps to deliver the report and Outsourcing Decryption Technique in which a master key helps to viewing the prescription.

REFERENCES:

i. *Nelson Gonzalez, Charles Miers, Fernando Red´ıgolo, Marcos Simpl´ıcio, Tereza Carvalho, Mats Naslund and Makan Pourzandi "A quantitative analysis of current security concerns and solutions for cloud computing" Gonzalez et al. Journal of Cloud Computing: Advances, Systems and Applications 2012,1:1*

ii. *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.*

iii. *M. Delgado, "The evolution of health care it: Are current U.S. privacy policies ready for the clouds?" in SERVICES, 2011, pp. 371–378.*

iv. *Dr. Sandeep Sharma & Navdeep Kaur Khiva," Secure Cloud Architecture for Preserving Privacy in Cloud Computing using OTP/WTP", Global Journal of Computer Science and Technology Cloud and Distributed. Volume 13 Issue 3 Version 1.0 Year 2013.*

v. *P. Ohm, "Broken promises of privacy: Responding to the surprising failure of anonymization," UCLA Law Review, vol. 57, p. 1701, 2010.*

vi. *P. Institute, "Data loss risks during downsizing," 2009.*

vii. *P. Dixon, "Medical identity theft: The information crime that can kill you," in The World Privacy Forum, 2006, pp. 13–22.*

viii. *K. E. Emam and M. King, "The data breach analyzer," 2009,[Available at: http://www.ehealthinformation.ca/dataloss].*

ix. *I. Neamatullah, M. Douglass, L. Lehman, A. Reisner, M. Villarroel, W. Long, P. Szolovits, G. Moody, R. Mark, and G. Clifford, "Automated de-identification of free-text medical records," BMC medical informatics and decision making, vol. 8, no. 1, p. 32, 2008.*