RESEARCH ARTICLE OPEN ACCESS

Privacy Preserving Health Monitoring Data Using a Proxy Re-encryption

Lakshmipriya.V[1], Praveena.V(Assistant Professor)[2]
Department of Computer Science and Engineering,
SRM University, Ramapuram Campus,
Chennai-600089

----------**********----------

Abstract:

Cloud-assisted mobile health (mHealth) monitoring is a system, which applies the prevailing mobile communications and cloud computing technologies to provide feedback decision support. It has been considered as a revolutionary approach to improving the quality of healthcare service while lowering the healthcare cost. Unfortunately, it also come across a serious risk on both clients' privacy and intellectual property of monitoring service providers, which may slowdown the wide adoption of mHealth technology. The aim of the 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 involved 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, the analysis on security and performance demonstrates the effectiveness of our proposed design.

Keywords: -**Cloud computing, Data security, digital signature, encryption, Internet, Key and cloud server**

----------**********----------

1. INTRODUCTION

The Cloud Computing is the delivery of different types of services and applications from the internet. In Recent times Cloud computing has gained a lot of importance. Cloud computing has been imagined as a future possibility of next generation architecture of IT World.

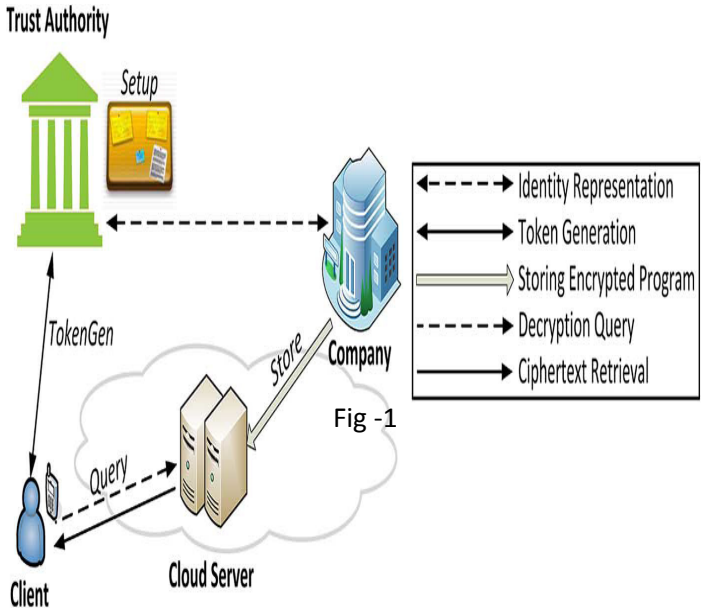

Fig -1

USER/ CLIENT

User/client gives the health data to cloud server. When the client inserts a record, it is encrypted and stored in the cloud server. Advance encryption scheme is used to encrypt the data. The cipher text is stored in the cloud server. This enhances privacy and security for the uploaded data in the third party server.

TOKEN GENERATION

To generate the private key for the attribute vector v=(v1, v2, v3 • • • , 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 skvi to the client.

QUERY

A client delivers the private key sets obtained from the TokenGen algorithm to the cloud, which runs on the AnonDecryption algorithm with the ciphertext generated within the Store algorithm. By starting from p1, the decryption result determines which ciphertext should be decrypted next. For instance, if v1 ∈ [0, t1], then the decryption result indicates the next node index L(i). After that, the cloud will use skv(L(i)) to decrypt the subsequent ciphertext CL(i). Continuing this process iteratively until it reaches a leaf node and decrypt the respective attached information.

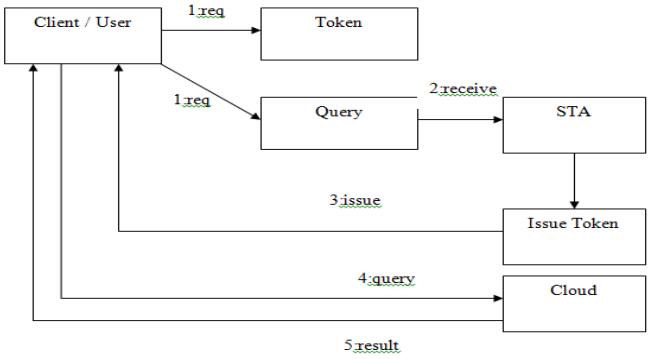

Fig -2

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 kind business model. The TA could 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 related company. However, the related company and TA could collude to obtain private health data from clientinput vectors.

SETUP

The said algorithm will be performed by TA, which publishes the system parameters for the BF-IBE scheme.

STORE

The said algorithm will be is performed by the company.

2. CLOUD COMPUTING FEATURES

The common features is to allow a Third party auditor (TPA) [11] referred as a public verifier to audit cloud data integrity without downloading the entire data from the cloud. The public verifier[11] may be a client who would like to use cloud data for the purposes such as search, computation, etc. But the

above features do not consider the efficiency of user revocation when auditing the correctness of shared data in the cloud. In the existing method ,the user is allowed to download the shared data and re-sign it during revocation. This method becomes unsuitable due to large size of data in the cloud. Many approaches allow both data owners and public verifiers to audit cloud data integrity without downloading the entire data from the cloud. To support efficient handling of multiple auditing tasks , we propose the public auditing procedure for integrity of shared data with valuable user revocation. Instead of downloading and re-signing the shared blocks by the existing user, we allow the cloud to re-sign blocks during user revocation. This is made possible by the idea of proxy re-signatures by using digital signature [1]. This system provides the facility that the data are signed out to the user who is doing modification. The data will be locked by the user which is not allowing others to update. Data modifications history which has modified date, time, user who is modified and the reason for modification are preserved .It provides the compatibility to retrieve and restore the earlier versions.

SCALABILITY

Cloud computing is scalable. Every time we require more resources we can add it to the cloud . That means Cloud computing is unlimited pool of possessions [1].

ENVIRONMENT FRIENDLY

Cloud computing makes well-organized use of hardware which helps to reduce energy cost [6].

COST EFFICIENT

Cloud computing is cost effective and efficient. User have to pay that much amount which we used for our mobile bills [4].

UP TO DATE

The software's and hardware's can be upgraded that we are using in the cloud. The provider is accountable for the overall update process of all the components [3].

IMPROVED PERFORMANCE

Every time we require some high configuration resources will be available to user on demand [1]

3. PROBLEM STATEMENT

The proposed paper is to address the identified important problem and design a cloud-assisted privacy preserving mobile health monitoring system to protect the privacy of the involved parties and their data.Without uniquely addressing the data management in mHealth system, there is a chance that, clients' privacy may be severely breached during the collection, storage, diagnosis, and communications and computing.The discussed privacy concern will be exacerbated due to the growing trend in privacy breaches on electronic health data.

4. IMPLEMENTATION

Implementation is the most crucial stage in achieving a successful system and giving the user's confidence that the new system is workable and highly effective. Through an implementation of a modified application to replace an existing one. The proposed conversation is relatively quite easily handable, provided there are no major changes in the system.

Initially as a first step the executable form of the application is to be created and loaded in the common server machine which is accessible to all the user and the server is to be connected to a network. The vital and final stage is to document the entire system which provides components and the operating procedures of the system.

BRANCHING PROGRAM

We formally describe the branching programs, which will include binary classification or decision trees as aspecial case. We need 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 the "v" be vector of clients' attributes. To be very 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 the "blood pressure: 130". For those who are having the blood pressure lower than 130 are categorized as normal, and those who are above this threshold are categorized as high blood pressure. This first element is a set of nodes in the branching tree. The node non-leaf pi is an intermediate decision node while leaf node pi is a label node. Each of the decision node is a value pair (ai, ti), where ai is the attribute index and ti is the threshold value with which vai is compared at this node. The similar value of ai may occur in the many nodes, (i.e.,) the same attribute can be evaluated more than once. For each of the decision node i, the value L(i) will be 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 the classification information. Repeat the procedure recursively for value "ph", and so on, until any one of the leaf nodes is reached withdecision information.

5. KEY-PRIVATE PROXY RE-ENCRYPTION

The model Proxy re-encryption (PRE) allows a proxy to convert a ciphertext encrypted under one keyinto an encryption of the same message under another key. The important idea is to place as little trustand provide as little information to the proxy as necessary to allow it to perform its translations.

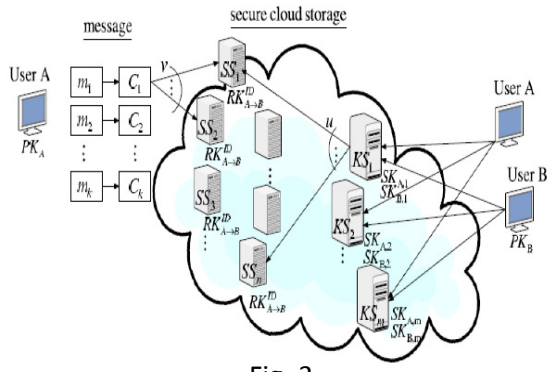

Fig -3

At the very least, the proxy should not be able to learn the keys of the participants or thecontent of the messages it re-encrypts. Even though, in all the prior proxy re-encryption schemes, it is easy for the proxy to evaluate between which participants a re-encryption key can transform ciphertexts.

This could be a problem in practice. For example, in a secure distributed system, contentowners may propose to use the proxy to help re-encrypt sensitive information without revealing tothe proxy and identity of the recipients.

In this work, we propose key-private (or anonymous) re-encryption keys as an additionaluseful property of PRE schemes. We identify and formulate a definition of what it means for a PRE schemeto be secure and key-private. Surprisingly, it shows that this property is not captured byprior definitions or achieved by prior schemes, including even the most secure obfuscation of PRE byHohenberger et al. (TCC 2007). Finally, we propose the rst key-private PRE construction andprove its CPA-security under a simple extension of Decisional Bilinear Die Hellman assumptionand its key-privacy under the Decision Linear assumption in the standard model.

6. DATA PROVIDER

The user will enter their credentials such as username and password and the DB serverwill check the username and password whether it is valid or not. Suppose if the user enters wrong username and

password the server will not allow the user to access the resources. If the username and password is valid means the user will be granted to access the resources. After Successful login the data provider will going to preserve the data using geometric perturbation and going to send that data to the service provider.

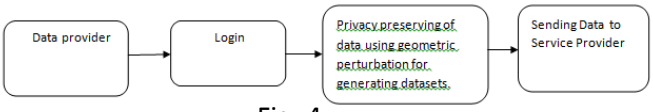

Fig -4

7. SERVICE PROVIDER

The user will enter their credentials such as username and password and the DB server will check the username and password whether it is valid or not. Suppose if the user enters wrong username and password the server will not allow the user to access the resources. If the username and password is valid means the user will be granted to access the resources. The data received from the data provider will be decrypted by the service provider and the service provider will generate models for that particular data received from the data provider.

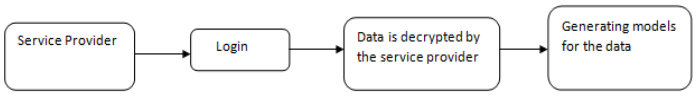

Fig -5

8. COMPARING WHICH MODEL IS BEST

In this module, we going to identify the models which are generated by the service provider and going to choose which model is best by data mining algorithm.

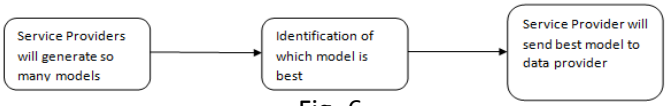

Fig -6

9. MODELS RECEIVED BY DATA PROVIDER

In this module, the data provider will receive the best model which is generated by the service provider.

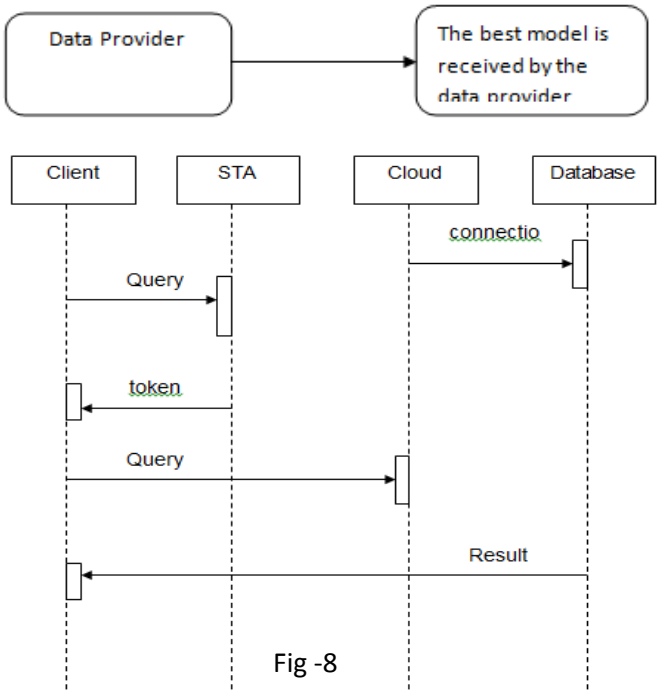

Fig -8

10. CONCLUSION AND FUTURE DIRECTIONS

CONCLUSION

In this project, we design a cloud-assisted privacy preserving mobile health monitoring system environment, called CAM, which can effectively protect the privacy of clients and the intellectual property of mHealth service providers. To protect mHeath service providers' programs, we have expanded the branching program tree by using the randompermutation and randomize the decision thresholds used at the decision branching nodes.So, finallyto enable resource-constrained small companies to participate in mHealth business, our CAM design helps them to move away the computational burden to the cloud by applying newly developed key private proxy re-encryption technique.Our proposed CAM has been shown to achieve the design objective.

Fig -7

FUTURE ENHANCEMENT:

As the emerging cloud computing technologies evolve, a most viable solution can be sought by incorporating the software as a service model and business model in cloud computing, which would allow small companies (healthcare service providers) to excel in this healthcare market. It has been observed and understandsthat the adoption of automated decision support algorithms in the cloud-assisted mHealth monitoring has been considered as a future trend

11. REFERENCES:

[1] 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 Med. Inform. Decision Making*, vol. 8, no. 1, p. 32, 2008.

[2] S. Al-Fedaghi and A. Al-Azmi, "Experimentation with personal identifiable information," *Intelligent Inf.Manage.*, vol. 4, no. 4, pp. 123–133,2012.

[3] J. Domingo-Ferrer, "A three-dimensional conceptual framework for database privacy," *Secure Data Manage.*, pp. 193–202, 2007.

[4] T. Lim, *Nanosensors: Theory and Applications in Industry, Healthcare,and Defense*. Boca Raton, FL, USA: CRC Press, 2011.

[5] X. Zhou, B. Peng, Y. Li, Y. Chen, H. Tang, and X. Wang,"To release or not to release: Evaluating information leaks in aggregate human-genome data," *Computer Security-ESORICS 2011*,pp. 607–627, 2011.

[6] R. Wang, Y. Li, X. Wang, H. Tang, and X. Zhou, "Learning your identity and disease from research papers: Information leaks in genome wide association study," in *Proc. 16th ACM Conf. Computer and Communications Security*, 2009, pp. 534–544, ACM.