International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 13 (2014), pp. 1329-1334

http://www. irphouse.com

Protect Integrity of Data in Cloud Assisted Privacy Preserving Mobile Health Monitoring

Shantanu Shankar Pawar[1] and R. N. Phursule[2]

[1]Student, M. E. Computer,
Jspm's Imperial College of Engineering & Research, Pune.
Pune University, Pune, Maharashtra
[2]Jspm's Imperial College of Engineering & Research, Pune.
Pune University, Pune, Maharashtra, India.
**Corresponding author*

Abstract

This cloud assisted mobile health monitoring includes mobile communication as well as cloud computing technologies to provide various services especially feedback decision support using information communication Technologies (ICT's) and mobile healthcare applications for the both parties involved in this mechanism for better security with extended privacy and data integrity by applying techniques. This system is to provide the simple user interface which can be easily understandable. It incorporated the hash based message authentication code (MAC) and MD-5 algorithm technique which can protect data integrity. This system also uses AES algorithm and outsourcing decryption technique for better privacy and security. Proposed design demonstrates mobile healthcare applications with simple user interface and protection to integrity of data in cloud-assisted privacy preserving mobile health monitoring. This system provides easeful mobile healthcare applications with good results and it is very useful to remote area peoples where hospitals not easily accessible.

Index Terms— Data Integrity, Mobile Healthcare Applications, hash based Message authentication code, MD-5, ICT's, Cloud Security, Cloud Efficiency, Trust Authority (TA).

1. Introduction

Use of low cost sensors for mobile devices improves the service provider's quality while lowering the cost. Mobile health applications are designed for remote monitoring on health status. Medinet project of Microsoft is a mobile health

application for diabetes and cardiovascular disease patients in remote areas. In Medinet project all respective details of patients could then be sent to a central server which could then run various web medical applications on these data to return timely advice to the client. Drawback includes cloud-assisted mHealth monitoring could offer a great opportunity to improve the quality of healthcare services and potentially reduce healthcare costs, there is some existing issues in reality. Without properly addressing the data management in this system, clients' privacy may be severely breached during the collection, storage, diagnosis, and Communications and computing. A recent study shows that most of peoples consider the privacy of their health information very important [1]. There is also need of data integrity in overall system which measures accuracy of data flow in system. So systems data integrity concern is at high priority which comprises also security of system. However, how to achieve this effectively without compromising data integrity, privacy and security becomes a great challenge, which should be carefully investigated [2].

2. Literature Survey

In old CAM there is need to persist accuracy in overall process of system, because in the old model, if wrong input goes to doctors then it could result in wrong prescription of suggestion from the system.

The basic CAM has the security enervation such as the identity representation set for a client's attribute vector v is known to trust authority and hence trust authority can easily infer the clients private attribute vector. Also it the client cannot protect his privacy from the cloud either because the cloud can easily find out the identity representation for the private key pk_{vi}, $i\epsilon[1, n]$ by running identity test in MDRQ. [1, 3, 4]. Modified system uses AES algorithm with hash functions which incorporate message authentication code (MAC). It also comprises the various modules which communicate with each other for better integrity and uses simple user interface.

3. System Model

System uses four modules as follows:

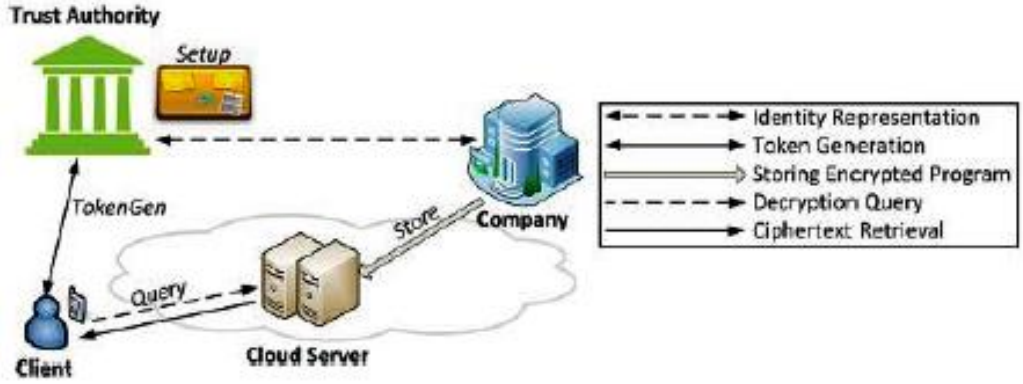

Fig. 1 System Architecture for CAM [1]

3. 1. Cloud Server

Cloud server working mechanism includes following steps: Cloud Server act as offline storage. All data are saved in encrypted format even passwords of users. Ages, gender, emails of user are not encrypted.

3. 2. Mobile Healthcare Service Providers

Mobile Healthcare Service Providers task includes following: Mobile Healthcare service Stores data on cloud in encrypted format. Username Password provided by mobile health service provider. Mobile healthcare service provider can view user details. They can add medical data detail such as blood pressure details with type systolic or diastolic [1, 7].

3. 3. Semi Trust Authority (STA)

Semi-trust Authority Activity includes following: STA activates user account of multiple users. STA generates token for user. STA cannot view token as it is generated & send to client. Token can be in the form of jzcv1ERHziowFuiPL8SiBg. User system gets token to retrieve query result.

3. 4. Clients

Client's activity includes following steps: Register with mobile healthcare Service provider. Client's uses various mobile healthcare applications. Semi trust authority must activate user. Clients can view their details. Clients raise queries and also view their query results using tokens. Query automatically searches semi trust authority. Example-Query is "Blood Pressure 80 missed medication".

4. C A M System Design and Architecture

The new system uses various mobile health care applications by login as a registered user, the registration facility is provided by healthcare service provider's side. After using such user's specific application he/she sends health related data to the health service provider by using semi trust authority and on cloud server information gets stored which uses our newly proposed algorithm for data integrity and for extended privacy.

4. 1. Our proposed modification to protect data integrity using AES algorithm and MD5 algorithm (hash Function)

In this project AES algorithm used with MD5 algorithm (hash function) can be used as a digital signature mechanism. Message of arbitrary length and produces as output a 128 bit "fingerprint" or "message digest" of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest. Intended where a large file must be "compressed" in a secure manner before being encrypted with a private key under a public-key cryptosystem such as PGP.

AES cipher incorporates the following:

- AddRoundKey() – round key is added to the State using XOR operation
- MixColumns() – takes all the columns of the State and mixes their data,

independently of one another, making use of arithmetic over GF(2^8)

- ShiftRows() – processes the State by cyclically shifting the last three rows of the State by different offsets
- SubBytes() – uses S-box to perform a byte-by-byte substitution of State[8, 9]

Algorithm for MD-5 Algorithm

Step 1 – append padded bits:

The message is padded so that its length is congruent to 448, modulo 512. Means extended to just 64 bits shy of being of 512 bits long. A single "1" bit is appended to the message, and then "0" bits are appended so that the length in bits equals 448 modulo 512.

Step 2 – append length:

A 64 bit representation of b is appended to the result of the previous step. The resulting message has a length that is an exact multiple of 512 bits.

Step 3 – Initialize MD Buffer

Step 3 cont.

Step 4 – Process message in 16-word blocks.

Step 4 count – Process message in 16-word blocks cont

Step 5 – output

Example

The message digest produced as output is A, B, C, D. That is, output begins with the low-order byte of A, and end with the high-order byte of D [9, 10].

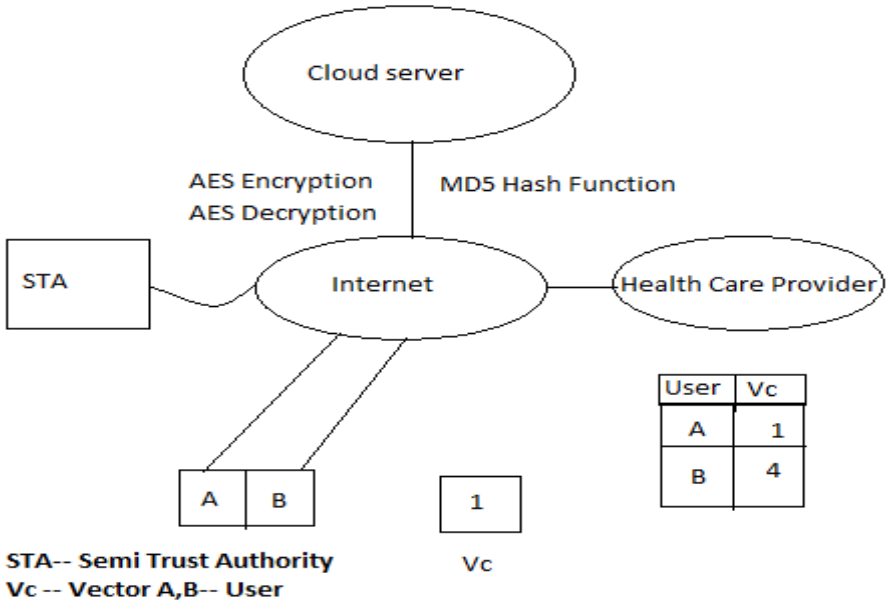

Fig. 2 Our Modification to Protect Integrity

5. Results

5. 1. Data Integrity

Data integrity deals with maintaining and assuring the accuracy and consistency of data over all phases of Information Lifecycle Management. Data Integrity for CAM cloud assisted privacy preserving mobile monitoring system is extension to the basic CAM cloud assisted model and it can be done by applying modification to the existing system and applying algorithm based on the data integration extension to the CAM cloud assisted model of system.

5. 2 Simple User Interface

As our system uses information communication technology (ICT) such as smart phones with android system it provides simple graphical user interface which is easy to understand and easy to use. This mobile health applications are developed in such a way that it provides simple interface which is easy to learn for the peoples who lives in rural area/remote area. As simple interface as well as simple method to use provides less training required for uneducated peoples which lives in rural area/remote area.

5. 3. Security

The cloud obtains no information on either the individual query vector or the company diagnostic branching program as in our first improvement. A client can only gain information on his decision result and certain side information on the relevant nodes leading to his decision result as in the first improvement, which we consider to be reasonable since we commonly know that a doctor usually tells his patients their information in reality [9].

6. Conclusions and Future Scope

Use of Integrity is a vital aspect in health-care systems. This system provides data integrity by applying new modification to existing system for better accuracy measured in all phases of system. We use simple graphical user interface for health related applications which is easily learnable for rural area peoples, who are uneducated. This system is very useful in rural/remote areas where hospitals and health related facility is available far away from their home. This newer system also provides SMS alert for the users. We apply recently proposed decryption outsourcing with privacy protection to shift clients' pairing computation to the cloud server. To protect mHeath 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.

This system has future scope on client's privacy protection using outsourcing decryption technique. In this system security can be obtained by using proposed new branching program which replaces existing drawback of system. There is further scope in improvement over bilinear pairing, homomorphic encryption, multidimentional range query based on anonymous IBE, decryption outsourcing, private re-encryption for CAM cloud assisted mobile health monitoring system.

7. References

[1] CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring Huang Lin, Jun Shao, Chi Zhang, and Yuguang Fang, *Fellow, IEEE* IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 6, JUNE 2013

[2] M. Barni, P. Failla, V. Kolesnikov, R. Lazzeretti, A. Sadeghi, and T. Schneider, "Secure evaluation of private linear branching programs with medical applications, " *Computer Security-ESORICS 2009*, pp. 424–439, 2009.

[4] S. Dziembowski and K. Pietrzak, "Leakage-resilient cryptography, " in *Proc. IEEE 49th Ann. IEEE Symp. Foundations of Computer Science, 2008 (FOCS'08)*, 2008, pp.

[5] A. Tsanas, M. Little, P. McSharry, and L. Ramig, "Accurate telemonitoring of parkinson's disease progression by noninvasive speech tests, " *IEEE Trans. Biomed. Eng.*, vol. 57, no. 4, pp. 884–893, Apr. 2010.

[6] 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 *Proc. Pervasive Health*, 2011, pp. 478–484.

[7] E. De Cristofaro, S. Faber, P. Gasti, and G. Tsudik, "Genodroid: Are privacy-preserving genomic tests ready for prime time?" in *Proc. 2012.*

[8] Bruce schneier"*Applied Cryptography*" 2nd Edition published by John Wiley&SonsInc.

[9] William stallings "*Cryptography and Network Security*" 3rd Edition published by Pearson Education Inc and Dorling Kindersley Publishing Inc.

[10] National Institute of Standards and Technology, *The Keyed-Hash Message Authentication Code (HMAC)*, Federal Information Processing Standards Publication # HMAC, 2001.