

Mobile Health Monitoring Technique using Cloud Computing

Ashwini Jadhav, V. Bhiksham, P. Vishwapathi

Abstract: Mobile health monitoring it is new technology in mobile health using different type's sensor. Using sensor measure different values and those values compared to threshold value until single value not reached. That single value is last value, as per last value doctor are suggest how to control your heath. This technique is one of mobile application which helps to generate token for user and give report or result on mobile.

Index Terms: Token, Trusted Authority, client, Server, Company, Branching, decryption query.

I. INTRODUCTION

CAM is Cloud Assisted Mobile Health Monitoring System. This system consists of following four parties:

- 1) *Cloud server:* simply called as server
- 2) *Company:* the company provides mobile health monitoring service also called as the healthcare service provider
- 3) *Individual Clients:* simply called as clients.
- 4) *Trusted Authority:* This is semi-trusted authority

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. Consider a neutral cloud server, which means it neither colludes with the company nor a client to attack the other side. Company is the service provider which gives service related to health monitoring system.

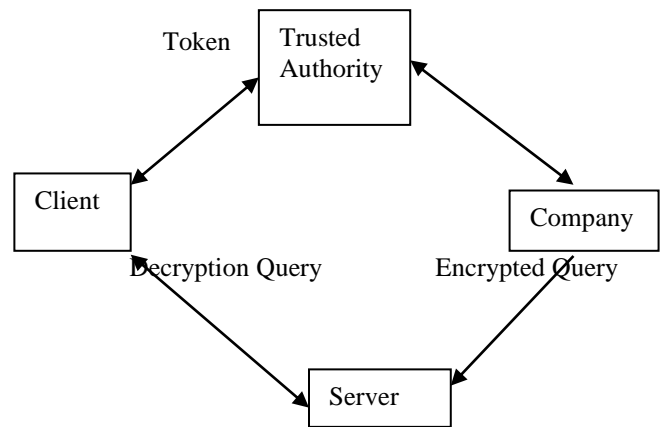


Fig. 1 Architecture

II. EXISTING SYSTEM

Existing Cloud-assisted mobile health (mHealth) monitoring the more powerful mobile communications and cloud computing technologies and in that new innovation in healthcare service in lower cost. And more security provides to client and company to protect private information from others .The existing system not portable to cloud computing environment. The system helps to improve the quality of healthcare service by reducing the cost of healthcare. But this system is risky for both clients' privacy and for monitoring service provider.

III. PROPOSED SYSTEM

The new technique consists of following four parties:

- Cloud Server
- Company
- Trusted Party
- Clients

The cloud server act as server which store complete information on internet. The cloud server also referred as cloud. The company act as a service provider .This provides service related with mobile health monitoring. Company stores its encrypted monitoring information about client in the server. Clients medical information and store them in their mobile, and then transfer the information into input. The input send to cloud server as inputs through a mobile. A trusted party is responsible for generate private key or token and distribute the every clients and collecting fees from the clients as business rule.

Revised Manuscript Received on 30 September 2014.

* Correspondence Author

Ms. Ashwini Jadhav*, Department of Computer Science and Engineering, JNTU, CMR Engineering College, Hyderabad, India.

Prof. V. Bhiksham, Department of Computer Science & Engineering, JNTU, CMR Engineering College, Hyderabad, India.

Prof. P. Vishwapathi, Department of Computer Science and Engineering, JNTU, CMR Engineering College, Hyderabad, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an [open access](http://creativecommons.org/licenses/by-nc-nd/4.0/) article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

A. Advantages

- Reducing the communication burden on clients and the server.
- The server cannot know anything about the user's search privacy, access privacy

IV. IMPLEMENTATION

Implementation is the stage of the theoretical design to working system. The implementation stage involves careful planning, designing, testing and investigation of the existing system and it's constraints on implementation designing of methods to achieve changeover methods. In implementation various modules are designed as follows:

- Branching Program
- Token Generation
- Query
- Semi Trusted Authority

ProblemStatement

Traditional privacy protection mechanisms by simply removing clients personal identification information identifiable. It is important noting that the collected information from an mHealth system could contain clients' 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, location, relational, computational, vocational, or reputational

V. MODULE DESCRIPTION

Branching

The branching is a decision trees. We only the binary branch information for the easy to taking general decision about information about client, Let I_i be the input of clients'. An input I_i is a concatenation of an input index and the respective input value. For Example: Blood pressure lower than 100 are considered as normal, and those above 100 are considered as more Blood pressure. The first element is a node in the decision tree. Each decision node is a pair (I_i, t_i) , where I_i is the Input and t_i is the threshold value with which N_{ai} is compared at this root node. The same value of I_i may occur in many nodes. For each decision node i , $L(i)$ is the next node if $N_{ai} \leq t_i$; $R(i)$ is the index of the next node if $N_{ai} > t_i$. Repeat the process recursively, until one of the leaf nodes is reached decision information. It can be represented as $\{t_1, \dots, t_k\}, L, R$. Here the first element is the set of nodes. Second element is the non leaf node and the third element is the leaf node. Each decision node otherwise called non leaf node is a pair where the first element is the attribute index and the second element is the threshold value. Clients input their health data such as blood pressure, temperature whether they missed any daily medications, then service provider on receiving this information and the service provider suggestion to clients.

Token Generation

This module helps to generate token using input vector $I = (i_1, i_2, \dots, i_n)$, first identify the entire input element and then after deliver to trusted party. Trusted party extract element using extract algorithm and generate token.

Query

A client transfer the set of private keys generated from the Token generation algorithm to the cloud server, the cloud

server runs the decryption algorithm on the cipher text generated in the Store algorithm.

Trusted party (TP)

A trusted party is providing private key every client and collecting fees from client according to rules of business.

VI. PROCESS DIAGRAM

Provider

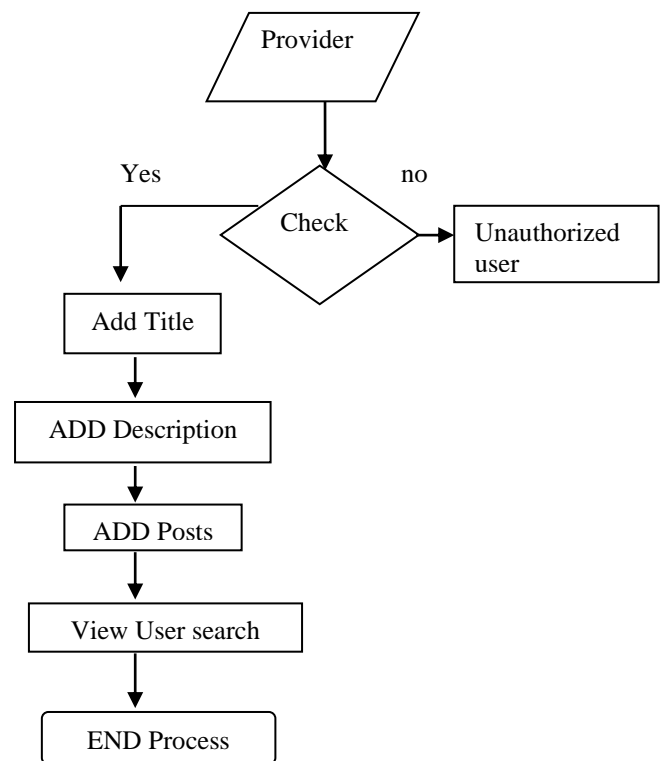


Fig. 2 Provider Process Diagram

This provider module helps to add title with his details like description, posts and view user search. First it will check whether entered user is authorized or not. If entered user is authorized, system allows adding title, adding description and posts. Finally gives view records according to user search.

USER

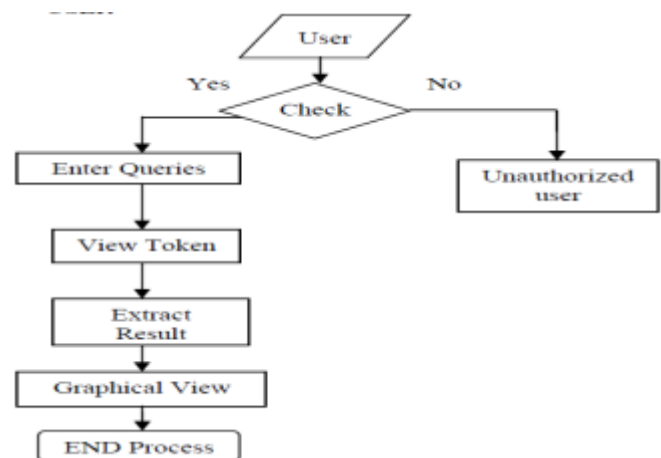
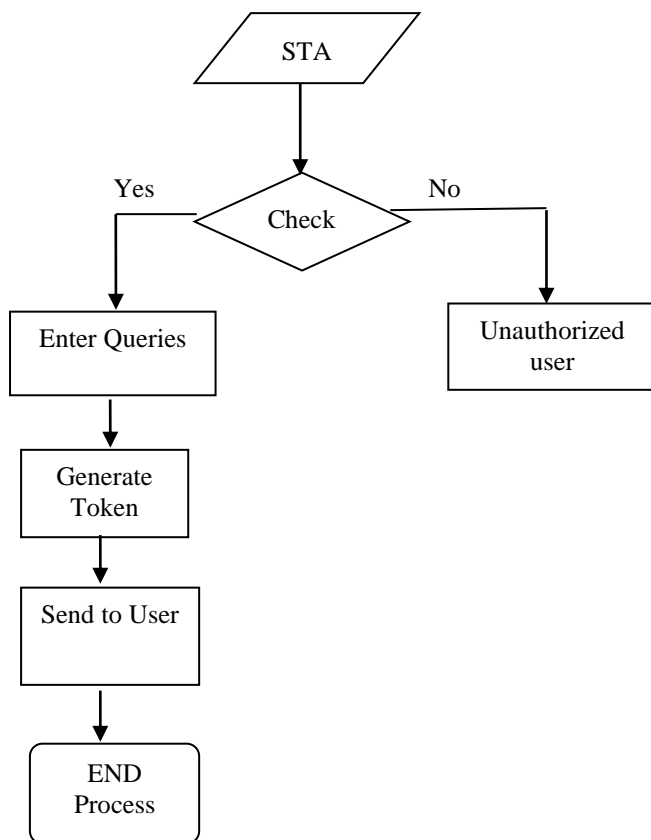


Fig. 3 User Process Diagram



Initially system checks whether entered user is authorized or not. If user is correct then this allows user to enter queries after this step token is generated. Finally we can extract the result and graphical view

STA



STA Helps to Send Result or Token to the User

VII. CONCLUSION

The mhealth monitoring system provides more security using cryptography technology. The key privacy is use branching program while completing the entire operation end. On the other hand, the trusted authority have encouraged to plan to obtain information on the client query. However, this attack cannot succeed because trusted authority provides private key using cryptography.

REFERENCES

1. Huang Lin, Jun Shaoy, Chi Zhangz, and Yuguang Fang, Fellow, IEEE Transactions on image processing vol:8 no:6 year 2013, "CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring".
2. 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.
3. G. Clifford and D. Clifton, "Wireless technology in disease management and medicine," Annual Review of Medicine, vol. 63, pp. 479–492, 2012.
4. A. Cavoukian, A. Fisher, S. Killen, and D. Hoffman, "Remote home health care technologies: how to ensure privacy? build it in: Privacy by design," Identity in the Information Society, vol. 3, no. 2, pp. 363–378, 2010.
5. M. Green and G. Ateniese, "Identity-based proxy re-encryption," in ACNS, ser. Lecture Notes in Computer Science, J. Katz and M. Yung, Eds., vol. 4521. Springer, 2007, pp. 288–306.

6. S. Al-Fedaghi and A. Al-Azmi, "Experimentation with personal identifiable information," Intelligent Information Management, vol. 4, no. 4, pp. 123–133, 2012.
7. P. Dixon, "Medical identity theft: The information crime that can kill you," in The World Privacy Forum, 2006.
8. L. Ponemon Institute, "Americans' opinions on healthcare privacy, available: <http://tinyurl.com/4atsdlj>," 2010.
9. E. Shaw, K. Ruby, and J. Post, "The insider threat to information systems: The psychology of the dangerous insider," Security Awareness Bulletin, vol. 2, no. 98, pp. 1–10, 1998.

AUTHOR PROFILE



Ms. Ashiwini Jadhav, M Tech (CSE) perusing from CMR Engineering College, Hydrabad, India. Total teaching experience 2 yrs (SBNM, Ploytechnic College)



Prof. V. Bhiksham, working as Assoc. Prof. at CMR Engineering college, currently he is pursuing Ph.D. from JNTU Hyderabad and done M.Tech(SE) from JNTU, Hyderabad. He is having total 10 years of teaching and 1 year of industry experience and had published 4 papers in National and 2 papers in International journals. His areas of interest are Computer Networks, Software Engineering and Information Security.

Prof. P. Vishvapathi, had done M.Tech in Central University, Hyderabad and presently pursuing Ph.D. from JNTU Hyderabad. He has rich experience of 22 years, 6 years in industry worked in USA, 16 years of Teaching Experience. The department is guided by a team of 2 Professors, 4 Associate Professors and 9 Asst. Professors. The department is also equipped with excellent infrastructure and latest equipment to explore technological advancements in the relevant fields.

