SECURED HEALTH MONITORING SYSTEM IN MOBILE CLOUD COMPUTING

J. Mamatha[1], A.Ramachandra Reddy[2]
[1]*M.Tech, CSE Dept, MLRIT, Hyderabad*
[2]*M.Tech, Asst. Professor, MLRIT, Hyderabad*

Abstract— **With the help of cloud computing, customers can preserve their information into the cloud remotely and utilize on-demand max-quality apps. With the help of a shared pool of calculating resources configurable. Information outsourcing: customers are relieved from the crisis of information preserve and managing. When clients keep their information (bulk size) on the cloud, the integrity of data protection is challenging task. Public audit enabling for cloud data preserving safety is must need. Client can rise query about an external audit party to verify the integrity of their transferred information. Mobile health (mHealth) monitoring in cloud, which imposes the cloud computing technologies and prevailing mobile communications to give feedback decision support, has been taken as a radical approach to increasing the quality of medical service while decreasing the medical price. Regrettably, it also contains a critical risk on both users' privacy and cerebral property of checking service providers, which could block the huge mHealth technology adoption. This thesis is to notice this main crisis and design a cloud supported secured storage mobile monitoring system of health to store the security of the involved people and their information. Moreover, the outsourcing decryption technique and a freshly proposed key secure proxy re-encryption are inherited to transfer the complexity computational of the undertaken parties to the cloud without compromising users' service and security providers' intellectual property. At last, our privacy and operation analysis indicates the efficiency of our proposed design.**

I. INTRODUCTION

Huge usage of mobile devices, like smart phones contained with least price sensors, has already explored outstanding potential in increasing the healthcare services quality. Health monitoring remote mobile has already been came into light as not only a potential, but also succeeded mobile health (mHealth) applications example specially for developing countries. The Microsoft introduced project "MediNet" is developed to know remote monitoring on the status of health problems like cardiovascular and diabetes diseases in remote countries like Caribbean [1]. In those a remote mHealth monitoring system, a user could insert transportable sensors in body sensor networks which are wireless to gather different physiological, like Electrocardiogram (ECG/EKG), breathing rate (BR), blood pressure (BP), and blood glucose and peripheral oxygen saturation (SpO2). That physiological information could then be forwarded to a central server, which could then perform different web medical apps on this information to return appropriate advice to the user. These apps may have different operations ranging from sleep pattern analyzers, physical activity assistants, exercises, to cardiac analysis systems, giving different medical consultation [2]. Anyway, as the rising technologies of cloud computing develop a feasible explanation can be required by including the s/w as a service (SaaS) model and business model pay-as-you-go in cloud computing, which would allow small companies (healthcare service providers) to explore in this healthcare market. It has been noticed that the inheritance of automated decision defend mHealth monitoring algorithms which is cloud-assisted has been taken as a future [3].

Although cloud-assisted mHealth monitoring can provide way to increase the healthcare services potentially and quality decreases healthcare expenditure, there is a block which is stumbling in developing this technology a practical word. Without accurate finding the information management in an mHealth system, users' privacy may be critically breached while gathering, communications, diagnosis, preserving and computing. A new research indicates that seventy five percent USA people believe the security of their health records and data are essential or very essential [4]. And also it has been statement [5] that patients' eagerness to get concerned in health monitoring agenda could be strictly lowered when clients are worried with the security breach in their willingly presented health information. This security worry will be intensifying cause of the increasing tendency on electronic health information security breaches.

II. PROBLEM STATEMENT

A privacy protection mechanisms which are traditionally using works by throwing out users' private identity data like

SSN or by utilizing anonymization technique wont succeeded to work as an efficient way in handling with security of mHealth systems cause of the growing amount and diversity of private couple of identifiable information. It costs nothing that the gathered data from a mHealth monitoring system could maintain users' private physical information like as weights, blood types, and heights or even their very private identifiable data like as their DNA and fingerprints profiles. As per PII (private identifiable information) is "any data, saved or otherwise, matching to an identifiable individual. Almost any data, if match to an identifiable individual, can become private in characteristics, be it relational, biographical, locational, biological, historical, genealogical transactional, computational, reputational or vocational.

Existing system:

Existing mHealth monitoring system in the cloud, which operates the prevailing cloud computing technologies and mobile communications to give feedback decision support, has been undertaken as a ultimate approach to increase the healthcare service quality while decreasing the healthcare price. Desperately, it also contains a serious crisis on both users' intellectual and security property of monitoring service providers, which could they determine the huge adoption of mHealth technology.

Cons of existing system: The existing system privacy rules like as Health Insurance Portability and Accountability Act (HIPAA) gives a baseline for health record which is private one, they are normally under taken not transferable or operatable to cloud computing environments.

Proposed system:

CAM maintains of 4 parties: the cloud server nothing but the cloud, the industry who gives the mHealth monitoring service nothing but providers of healthcare service, the individual users and third party or a semi-trusted authority (TA). The industry preserves its encrypted monitoring information or program in the server of cloud. Individual users gather their medical information and preserve them in their cell phones, which then manipulate information into attribute vectors. The attribute vectors are given to the monitoring program as inputs in the cloud server via a smart phone or a mobile device. A semi-trusted authority or third party is responsible for sharing private keys to the individual users and gathering the service fee from the users as per that a certain business model like as pay-as-you-go. The TA or third party can be under taken as a management agent or a collaborator for a company or lots of companies and thus distributes certain level of mutual interest with the industry.

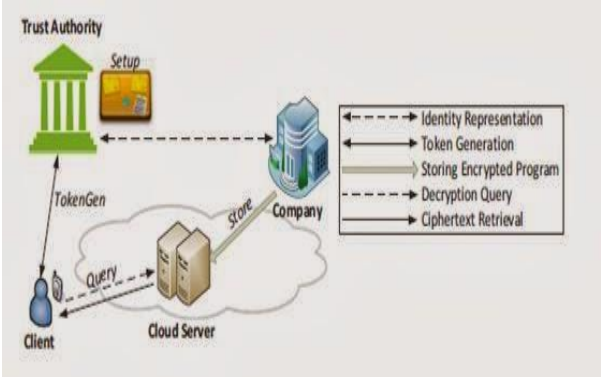


Figure: Proposed CAM model which includes cloud server, clients and semi trusted party.

Any have, the company and TA could collude to take the information of private health information from user input vectors. Pro's of proposed system: Reducing the communication and calculation load on cloud and the clients. The cloud cannot know anything about the user's search privacy, access privacy.

III. SYSTEM DEVELOPMENT

Branch structure of tree Program:

Normally the branching programs described as, which contains classification of binary or decision trees as a different case. We only undertake the branching program of binary for the flexibility of exposition since a private query protocol based on a normal decision tree can be normally explained from our scheme. Vector of clients' will be the V be the attributes. To be clearly, Vi is an attribute component is a concatenation of an attribute value and the respective attribute index. For instance, A||KW1 might correspond to "BP: 130". Those with a BP lower than 130 are taken as normal, and which are above this threshold are undertaken as high BP. The initial element is a collection of nodes in the branching tree. The node with non-leaf pi is an intermediate decision node where pi the leaf node is a label node. Every decision node forms a pair (Ti ,Ai), where Ti is the threshold value and Ai is the attribute index with which Vai is measure up to at this node. The similar value of ai may appear in nodes lot, i.e., the similar attribute may be examined more than once. L(i) is the index for every decision node i of the upcoming node if Vai $\leq$Ti; the next node index is R(i) if Vai > ti. The label nodes are combined with classification data. Repeat the process for ph recursively, and so on, til one node of the leaf nodes is out with decision information.

Generation of a Token:

To create attribute private key for the vector V=(V1, · · · , Vn), initially user calculates each element of the identity representation set in V and gives to TA all the n identity representation sets. Then TA operates the A non Extract (id, msk) on each and every id identity. In the identity set Svi and gives all the private keys Skvi to the user respectively.

Query:

A user gives the private key sets gained from the algorithm of Token Gen to the cloud, which operates the A non Decryption algorithm on the cipher text developed in the Store algorithm. Initiating from p1, the decryption output explains which cipher text have to be decrypted further. For example, if v1 < [t1, 0], then the output of decryption indicates the next node L(i) index. The cloud will then utilizes Skv (L(i)) to subsequent cipher text CL(i) decryption. We have to proceed this process recursively until it gets a leaf node and decrypt the combined data respectively.

Semi Trusted or third party Authority:

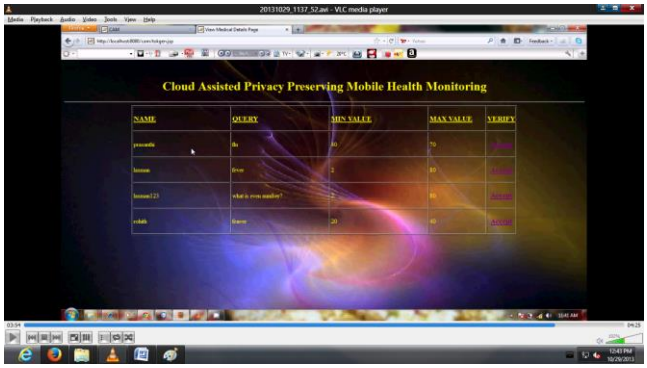
This authority takes distributing private keys responsibility to the individual users and gathering the service expenditure from the users based upon a business model like pay-as-you-go model. The TA can be under taken as a management agent or a collaborator for a company (or many companies) and thus gives certain mutual interest level with the company. Any have, the TA and company could collude to gain private health data from user input vectors.

IV. RELATED WORK

CAM contains of 4 parties: the cloud server nothing but the cloud, the healthcare service provider (i.e. the mHealth monitoring service provider company) the clients and finally TA (a semi-trusted authority). The company preserves its encrypted monitoring program or data in the server of cloud. Clients assemble their health information and preserve them in their cell phones, which then convert the information into attribute vectors. These are carried as inputs (i.e attribute vectors) to the cloud server monitoring program via a mobile (or tablet) device. A TA is in charge for private keys distribution to the individual users and gathering the service charge from the users according to a convinced business model like business model pay-as-you-go.

Most of current private tele monitoring schemes [51] is based on anonymization, which are ineffective as we alluded earlier. Some part of work concentrates on diagnostic programs confidentiality preserving. At the end of protocol function, a user gains nothing from diagnostic program but the result of diagnostic while the company obtains no information on the client's private data. All the existing solutions require the client run oblivious transfer protocol several instances of with the corporation after setup stage, which indicates the corporation has to be in online continuously. All the current solutions are based on confused circuits, which involves a user must download the complete circuit to his/her device and finish the decryption by his/her own. Besides, the private processing or computation of medical data has also fascinated concentration over the cloud from both the security community and signal processing society.. These mechanisms can be separated into couple of categories: offering a explanation for a specific situation like genomic test which is private or private classification of users' electrocardiogram (ECG) information, or offering a general framework for personal processing of monitored data or electronic health records. Even if these methods are cloud computing based, they do not highlight on to workload transferring way of the occupied parties without breaching the security of the involved parties in the cloud. Since our application scenario assumes the users clutch moderately resource-restricted smart phones in a cloud supported environment, it would be useful if a user could change the computational workload to the cloud. However, there appears none minor approach to garbled circuit decryption outsourcing currently. Our proposed system accepts the newly proposed outsourcing of decryption to significantly decrease the work pressure of both the clients and company by outsourcing the bulk of the computational operations to the cloud while maintaining the company offline after the initialization phase.

V. RESULTS



VI. CONCLUSION

In this research, we developed a cloud-assisted privacy storing mobile health monitoring system, known as CAM, which can perfectly helps the security of users and the mHealth service providers intellectual proerty. To secure the users' privacy, we use the anonymous based upon encryption (IBE) of Boneh-Franklin identity in medical diagnostic branching programs. To decrease the decryption difficulty due to the usage of IBE, recently we used proposed decryption outsourcing with privacy preserving to shift clients' combining calculation to the cloud server. To secure providers' mHeath service programs, we extended the splitting theme tree nothing but branching with the help of various permutation and variant the decision thresholds utilized at the branching nodes which was decided. At last, to enable resource restricted small industries to involve in mHealth circle; our CAM structure helps them to transfer the calculation complexity to the cloud by using newly invented key private proxy re-encryption technique. Our CAM has been explored to get the structure objective.

REFERENCES

[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." Conference Proceedings of the International Conference of IEEE Engineering in Medicine and Biology Society, vol. 2008, no. 3, pp. 755–758. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/19162765

[2] A. Tsanas, M. Little, P. McSharry, and L. Ramig, "Accurate telemonitoring of parkinson's disease progression by noninvasive speech tests," iomedical Engineering, IEEE Transactions on, vol. 57, no. 4, pp. 884– 893, 2010.

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

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

[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 PervasiveHealth, 2011, pp. 478–484.

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

[8] E. B. Fernandez, "Security in data intensive computing systems," in Handbook of Data Intensive Computing, 2011, pp. 447–466.

[9] A. Narayanan and V. Shmatikov, "Myths and fallacies of personally identifiable information," Communications of the ACM, vol. 53, no. 6, pp. 24–26, 2010.

[10] P. Baldi, R. Baronio, E. D. Cristofaro, P. Gasti, and G. Tsudik, "Countering gattaca: efficient and secure testing of fully-sequenced human genomes," in ACM Conference on Computer and Communications Security, 2011, pp. 691–702.

[11] 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.

[12] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," in Security and Privacy, 2008. SP 2008. IEEE Symposium on. IEEE, 2008, pp. 111–125.

[13] ——, "De-anonymizing social networks," in IEEE Symposium on Security and Privacy. IEEE Computer Society, 2009, pp. 173–187.

[14] 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.

[15] S. Al-Fedaghi and A. Al-Azmi, "Experimentation with personal identifiable information," Intelligent Information Management, vol. 4, no. 4, pp. 123–133, 2012.

AUTHOR DETAILS:

First Author: ***J. Mamatha*** received B.Tech Degree in Information Technology from KITS Engineering College for Women's in the year 2012. She is currently M.Tech student in Computer Science and Engineering from Marri Laxman Reddy Institute of Technology. And her research interested areas in the field of Cloud Computing, Mobile Computing and Data Mining.

Second Author: ***A. Ramachandra Reddy*** working as an Asst. Professor in Marri Laxman Reddy Institute of Technology. He has completed his M.Tech CSE and he has 7 years of teaching experience. His research interested areas are Data Mining, Network Security and Cloud Computing.