

SPHM Tool: A JAVA based tool for Secured Patient Healthcare Mobile Monitoring using Cloud Computing

Dr. P.RajaRajeswari¹, Sayeed Yasin², G.Jameson³

¹ (M.tech, CSE) , JNTU Kakinada, India

rajilikhitha@gmail.com

² Assoc Professor, Nimra Institute of Science and Technology

sdyasin761@gmail.com

³ Asst.Professor, Nimra Institute of Science and Technology

jameson.ganta@gmail.com

ABSTRACT

Cloud-assisted mobile health (mHealth) monitoring, which applies the prevailing mobile communications and cloud computing technologies to provide feedback decision support, 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 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 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, our security and performance analysis demonstrates the effectiveness of our proposed design.

Key Words: Mobile Health Monitoring, Security, Cloud Computing.

INTRODUCTION:

Mobile devices, like smart phones contained with least price sensors usage, 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 especially for developing countries. The Microsoft introduced project "Medi Net" 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 a 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. [6][7][8][9] This security worry will be intensifying cause of the increasing tendency on electronic health information security breaches [10,11,12,13].

II. PROBLEM STATEMENT

The problem addressed in this paper is to design a cloud assisted privacy preserving mobile health monitoring system to protect the privacy of the involved parties and their data. Moreover, the 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, our security and performance analysis demonstrates the effectiveness of our proposed design.

III. EXISTING SYSTEM

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

IV. PROPOSED SYSTEM

CAM consists of four parties: 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.

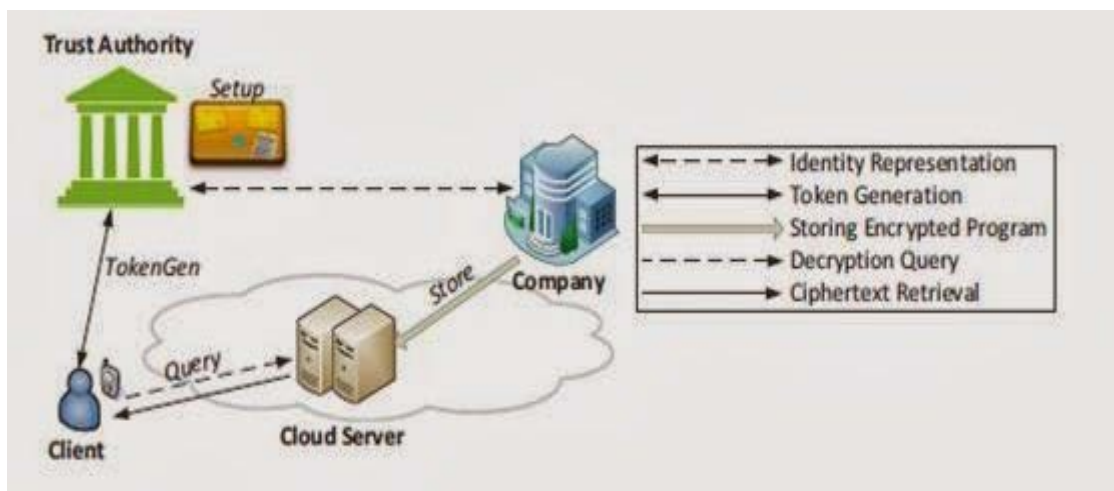


Figure 1:

V. SYSTEM DEVELOPMENT

This application has been divided in to four modules.

1) Branching Program:

This paper formally describes the branching programs, which include binary classification or decision trees as a special case. This paper only consider the binary branching program for the ease of exposition since a private query 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 v_i 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 (a_i, t_i) , where a_i is the attribute index and t_i is the threshold value with which v_{a_i} is compared at this node. The same value of a_i 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 $v_{a_i} \leq t_i$; $R(i)$ is the index of the next node if $v_{a_i} > t_i$. 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.

2) Token Generation:

To generate the private key for the attribute vector $v = (v_1, \dots, v_n)$, 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 $\text{AnonExtract}(\text{id}, \text{msk})$ on each identity $\text{id} \in S_{v_i}$ in the identity set and delivers all the respective private keys sk_{v_i} to the client.

3) 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 p_1 , the decryption result determines which ciphertext should be decrypted next. For instance, if $v_1 \in [0, t_1]$, then the decryption result indicates the next node index $L(i)$. The cloud will then use $\text{sk}_{v(L(i))}$ to decrypt the subsequent ciphertext $CL(i)$. Continue this process iteratively until it reaches a leaf node and decrypt the respective attached information.

4) 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.

VI. SOME PRELIMINARIES AND SECURITY BUILDING BLOCKS

Branching program

In this section, we formally describe the branching programs, which include binary classification or decision trees as a special case[14,15]. We only consider the binary branching program for the ease of exposition since a private query protocol based on a general decision tree can be easily derived from our scheme. Let $v = (v_1, \dots, v_n)$

be the vector of clients' attributes. To be more specific, an attribute component v_i 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. Each attribute value is an C -bit integer. In this paper, we choose C to be 32, which

should provide enough precision in most practical scenarios. A binary branching program is a triple $\{p_1, \dots, p_k\}$, L, R . 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 (a_i, t_i) , where a_i is the attribute index and t_i is the threshold value

with which v_{a_i} is compared at this node. The same value of a_i 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 $v_{a_i} \leq t_i$; $R(i)$ is the index of the next node if $v_{a_i} > t_i$. The label nodes are attached with classification information.

To illustrate how a practical monitoring program can be transformed into a branching program, we use the monitoring program introduced in the MediNet project [16], [17]

to construct a branching program. The MediNet aims to provide automatic personalized monitoring service for patients with diabetes or cardiovascular diseases.

Clients input their related health data such as systolic blood pressure (BP), whether they missed daily medications or had an abnormal diet, and the energy consumption of physical

activity to the decision support system, which will then return a recommendation on how the clients can improve their conditions. For instance, assume a hypertension patient inputs an attribute vector consisting of the following elements "[Systolic BP: 150, Missed one medication=0 (indicating he did miss the medication), Energy Expenditure: 900 kcal, salt intake: 1000 milligrams]" and the respective threshold is " $t_1 = 130$, $t_2 = 0$, $t_3 = 700\text{kcal}$, $t_4 = 1500$ ". The health data related to the input attribute vector can be sampled either by a portable sensor or input by the client

Homomorphic encryption

Homomorphic encryption is widely used as an underlying tool for constructing secure protocols in the literature[18][19] CAM adopts a semantically secure

additively homomorphic public-key encryption technique. Intuitively, for homomorphic encryption $\text{HEnc}(\cdot)$, given two encrypted messages $\text{HEnc}(m1)$ and $\text{HEnc}(m2)$, the encryption of the addition of the two underlying messages can be computed additively as follows: $\text{HEnc}(m1+m2) = \text{HEnc}(m1) * \text{HEnc}(m2)$, where $*$ is the corresponding operation in the ciphertext space. A typical additively homomorphic encryption scheme was proposed by Paillier cryptosystem[20][21]. Homomorphic encryption enables a client to obtain the token corresponding to the input attribute vectors obliviously from TA.

Decryption outsourcing

The pairing-based IBE system [22] and its extensions such as attribute-based encryption [23][24] has a reputation of costly decryption workload due to the bilinear pairing operations in the decryption steps. Moreover, the pairing computation is considered to be especially computationally intensive for resource-constrained mobile phones. we seek decryption outsourcing to ease the computational complexity. The decryption outsourcing in ABE was first proposed by Green *et al* [25].

It enables a client to transform his secret key to the transformation key and then delegates it to an untrusted server (e.g., a cloud) to use it to transform the original ciphertext into an El Gamal encryption of the original message. The client only needs to compute simple exponentiation operations to obtain the underlying message. In CAM, we intend to apply the outsourcing decryption technique

VII. SPHM DESIGN

SPHM: A Secured patient HealthCare Mobile Monitoring using Cloud Computing. To illustrate the fundamental idea behind this design, we start with the basic scheme, and then demonstrate how improvements can be made step-by-step to meet our design goal. Some of the variables in the following illustration may have already been

defined in the previous sections. The system time is divided into multiple time periods, called *slots*, each of which can last a week or a month depending on specific application scenarios.

There is an estimated maximum number of users N requesting access to the monitoring program in any given slot.

VIII. EXPERIMENTAL RESULTS

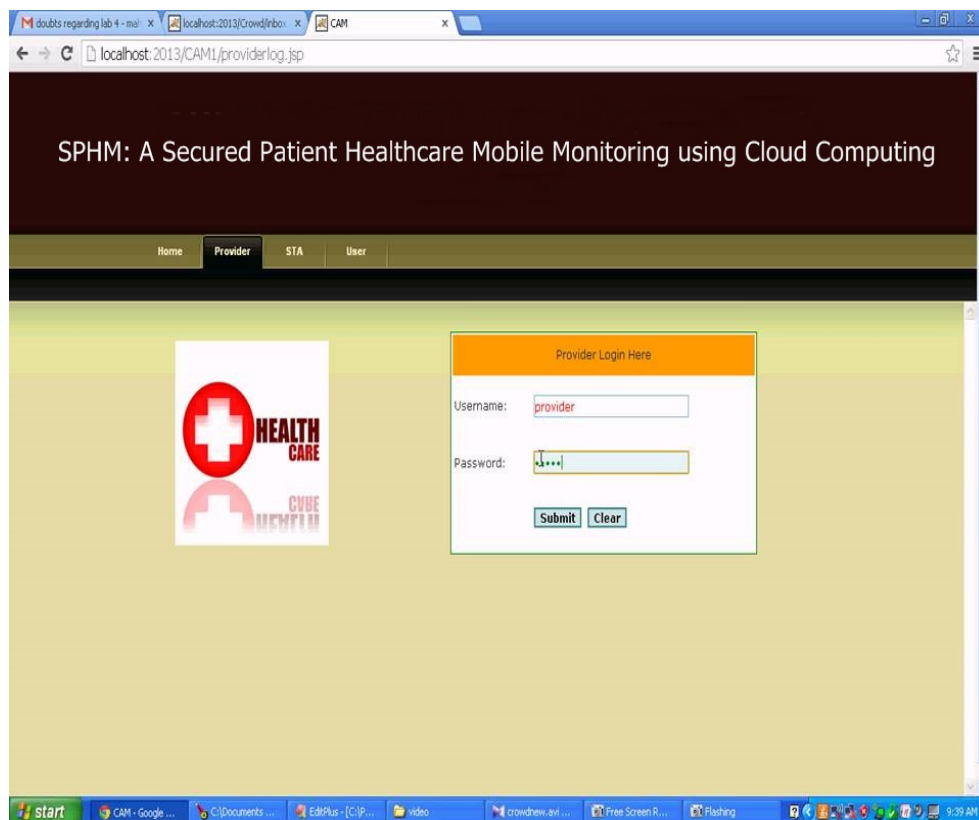


Figure 2:

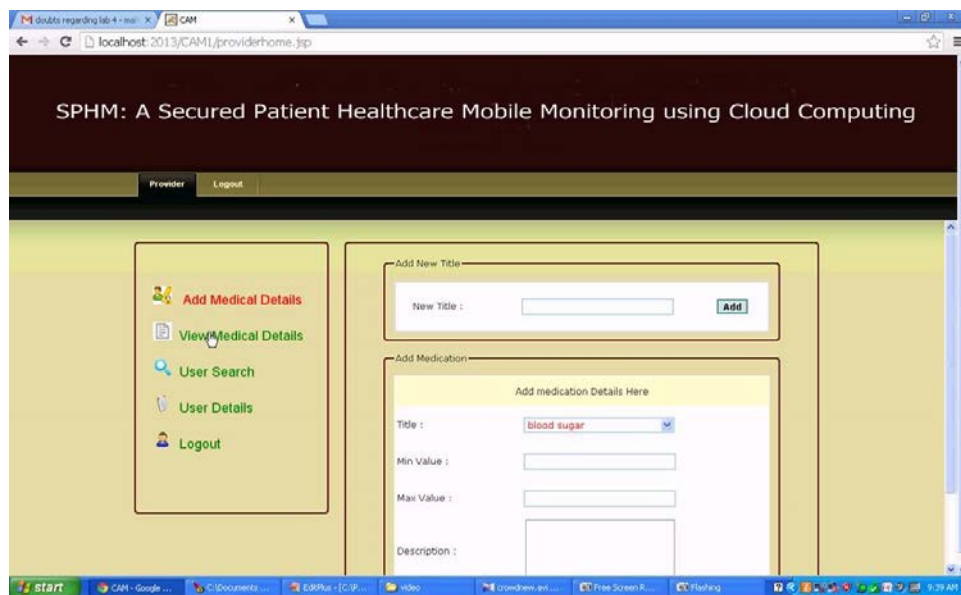


Figure 3:

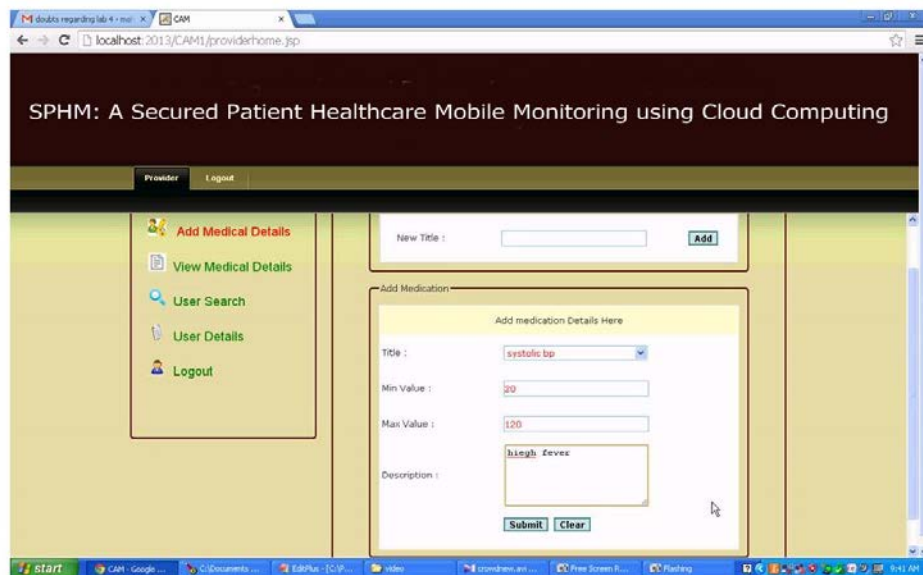


Figure 4:



Figure 5:

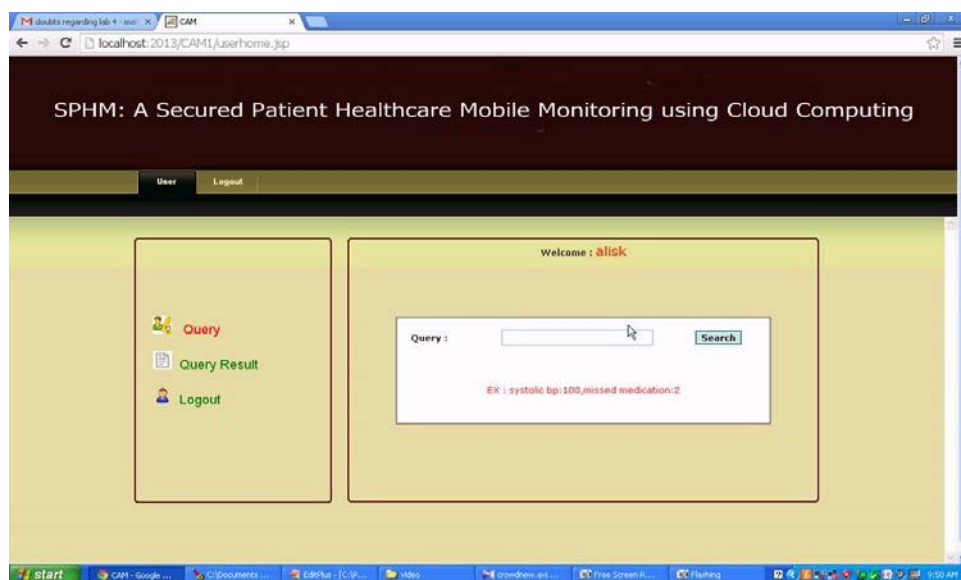


Figure 6:



Figure 7:

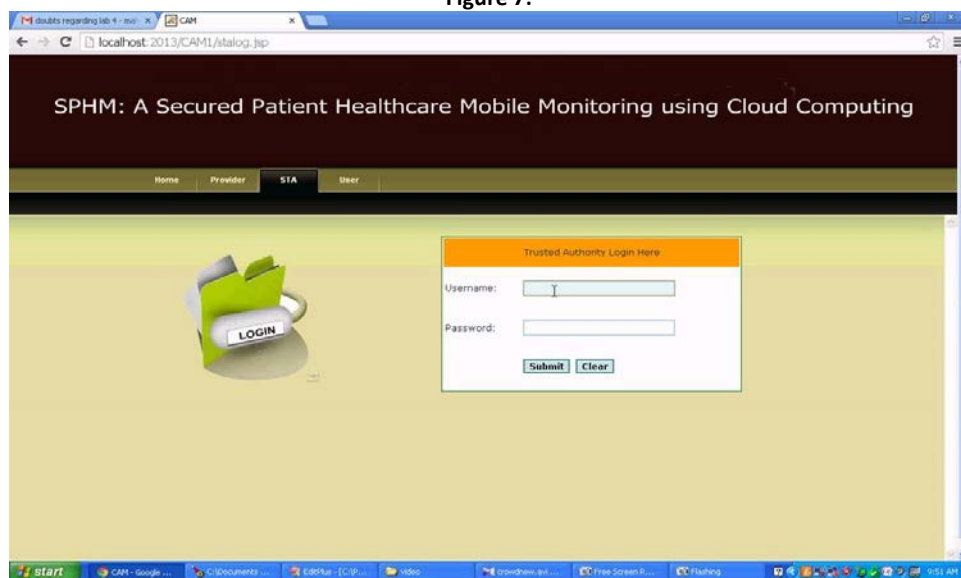


Figure 8:

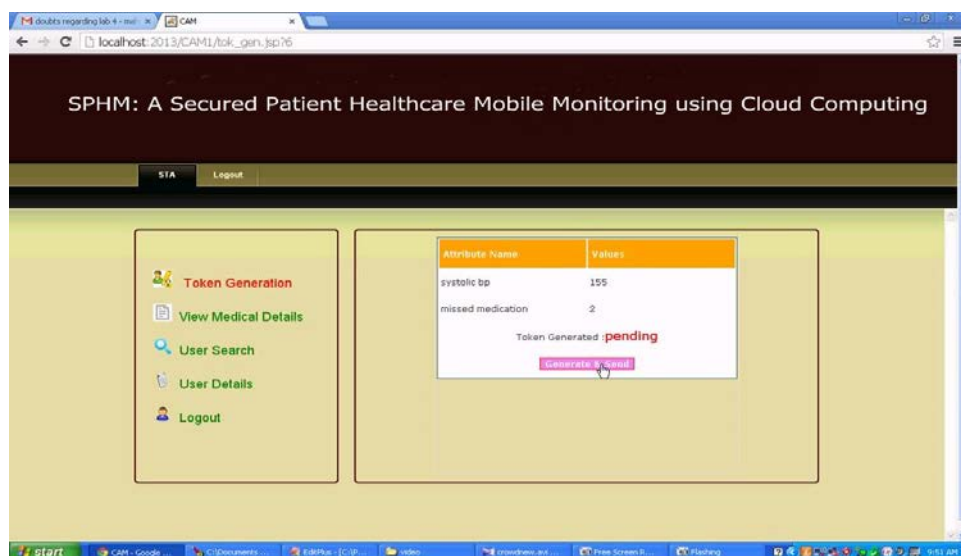


Figure 9:



Figure 10:



Figure 11:



VII. CONCLUSION

In this Paper, I have designed a cloud-assisted privacy preserving mobile health monitoring system, called SPHM, which an effectively protect the privacy of clients and the intellectual proerty of mHealth service providers. To protect the clients' privacy, I have applied the anonymous Boneh-Franklin identity based encryption (IBE) in medical diagnostic branching programs. To reduce the decryption complexity due to the use of IBE, I have applied recently proposed decryption outsourcing with privacy protection to shift clients' pairing computation to the cloud server. To protect mHeath service providers' programs, I have expanded the branching program tree by using the random permutation and randomize the decision thresholds used at the decision branching nodes. Finally, to enable resource constrained small companies to participate in mHealth business, my SPHM design helps them to shift the computational burden to the cloud by applying newly developed key private proxy re-encryption technique. My SPHM has been shown to achieve the design 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.: <http://www.ncbi.nlm.nih.gov/pubmed/19162765>.
2. Tsanas, M. Little, P. McSharry, and L. Ramig, "Accurate tele monitoring of parkinson's disease progression by noninvasive speech tests," Biomedical 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. V. Dhukaram, C. Baber, L. Elloumi, B.J. van Beijnum, and P. D.Stefanis, "End-user perception towards pervasive cardiac health care services: Benefits, acceptance, adoption, risks, security, privacy and trust," in Pervasive Health, 2011, pp. 478–484.
6. CISCO, "Cisco Visual Networking Index : Global Mobile Data Traffic Forecast Update , 2011-2016," Tech. Rep., 2012.
7. Y. Li, Y. Zhang, and R. Yuan, "Measurement and Analysis of a Large Scale Commercial Mobile Internet TV System," in ACM IMC, pp. 209–224, 2011.
8. T. Taleb and K. Hashimoto, "MS2: A Novel Multi-Source Mobile-Streaming Architecture," in IEEE Transaction on Broadcasting,
9. X. Wang, S. Kim, T. Kwon, H. Kim, Y. Choi, "Unveiling the BitTorrent Performance in Mobile WiMAX Networks," in Passive andActive Measurement Conference, 2011.
10. A. Nafaa, T. Taleb, and L. Murphy, "Forward Error Correction Adaptation Strategies for Media Streaming over Wireless Networks," in IEEE Communications Magazine, vol. 46, no. 1, pp. 72–79, 2008.
11. J. Fernandez, T. Taleb, M. Guizani, and N. Kato, "Bandwidth Aggregation-aware Dynamic QoS

- Negotiation for Real-Time Video Applications in Next-Generation Wireless Networks,” in IEEE Transaction on Multimedia, vol. 11, no. 6, pp. 1082–1093, 2009.
12. T. Taleb, K. Kashibuchi, A. Leonardi, S. Palazzo, K. Hashimoto, N. Kato, and Y. Nemoto, “A Cross-layer Approach for An Efficient Delivery of TCP/RTP-based Multimedia Applications in Heterogeneous Wireless Networks,” in IEEE Transaction on Vehicular Technology, vol. 57, no. 6, pp. 3801–3814, 2008.
 13. K. Zhang, J. Kong, M. Qiu, and G.L Song, “Multimedia Layout Adaptation Through Grammatical Specifications,” in ACM/Springer Multimedia Systems, vol. 10, no. 3, pp.245–260, 2005.
 14. M. Wien, R. Cazoulat, A. Graffunder, A. Hutter, and P. Amon, “Real-Time System for Adaptive Video Streaming Based on SVC,” in IEEE Transactions on Circuits and Systems for Video Technology, vol. 17, no. 9, pp. 1227–1237, Sep. 2007.
 15. H. Schwarz, D. Marpe, and T. Wiegand, “Overview of the Scalable Video Coding Extension of the H.264/AVC Standard,” in IEEE Transactions on Circuits and Systems for Video Technology, vol. 17, no. 9, pp. 1103–1120, Sep. 2007.
 16. 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,” in Engineering in Medicine and Biology Society, 2008. EMBS 2008. 30th Annual International Conference of the IEEE. IEEE, 2008, pp. 755–758.
 17. Farmer, O. Gibson, P. Hayton, K. Bryden, C. Dudley, A. Neil, and L. Tarassenko, “A real-time, mobile phone-based telemedicine system to support young adults with type 1 diabetes,” Informatics in primary care, vol. 13, no. 3, pp. 171–178, 2005.
 18. 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.
 19. A. C.-C. Yao, “How to generate and exchange secrets (extended abstract),”in FOCS. IEEE, 1986, pp. 162–167.
 20. P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in EUROCRYPT, 1999, pp. 223–238.
 21. I. Damgård and M. Jurik, “A generalisation, a simplification and some applications of paillier’s probabilistic public-key system,” in Public Key Cryptography, ser. Lecture Notes in Computer Science, K. Kim, Ed.,vol. 1992. Springer, 2001, pp. 119–136.
 22. D. Boneh and M. K. Franklin, “Identity-based encryption from the weil pairing,” in CRYPTO, 2001, pp. 213–229.
 23. A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in EUROCRYPT, 2005, pp. 457–473.
 24. V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in ACM Conference on Computer and Communications Security, 2006, pp. 89–98.
 25. M. Green, S. Hohenberger, and B. Waters, “Outsourcing the decryption of abe ciphertexts,” in Usenix Security, 2011.