Volume 4, Issue 2, February 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

RHM-Remote Health Monitoring with Dynamic Secure and Cloud Service

Karthikeyan K[1], Naveen V[2], Nikhil Vinoy[3], Nagendra Prasath S[4], Manoj Prabhu R[5]

[1]Assistant Professor, Department of Computer Science and Engineering, SNS College of Engineering, Coimbatore, Tamil Nadu, India

[2,3,4,5] UG Scholars, Department of Computer Science and Engineering, SNS College of Engineering, Coimbatore, Tamil Nadu, India

Abstract— Cloud Computing has emerged as one of the trends in the latest era of computing and storage. This raise has led the developers and programmers to include this technology in their products. Wide spread usage of mobile devices like mobile phones, tablets etc has given this growth a heavy boost. Remote mobile health monitoring has recently been distinguished as a potential, as well as a great sample of mobile health (mHealth) provisions in spite of the fact that cloud-supported mHealth monitoring could offer an incredible chance to enhance the nature of healthcare administrations and conceivably diminish healthcare costs. One of the main issues in this implementation is the privacy issues with respect to the health records and personal details. Without legitimately looking into the data management in a mHealth framework, customers' protection may be extremely intruded throughout the collection, storage, diagnosis, communications and computing. The present law keeps more tabs on assurance against unauthorized interruptions while there is little exertion on securing customers from business or companies gathering private data (like health records). In our paper we implement encryption and multi factor authentication techniques for better privacy and security using elliptic curve cryptography and MD5. Our work is found to be efficient than the homomorphic encryption and tokengen algorithm in performance and efficiency, which is a major factor regarding mobile devices. The encryption technique is resilient to DDOS attacks, MitM, spy-ware and PROBE attack.

Keywords— Cloud Computing, encryption, MD5, ECC, Threat, Privacy, mHealth.

I. INTRODUCTION

Wide spread usage of mobile devices, such as smart-phones equipped with low cost sensors, has already shown great potential in improving the quality of health-care services. Remote mobile health monitoring has already been recognized as not only a potential, but also a successful example of mobile health (mHealth) applications although cloud-assisted mHealth monitoring could offer a great opportunity to improve the quality of health-care services and potentially reduce healthcare costs. Without properly addressing the data management in an mHealth system, client's privacy may be severely breached during the collection,storage, diagnosis, communications and computing the current law is more focused on protection against adversarial intrusions while there is little effort on protecting clients from business collecting private information.Meanwhile, many companies have significant commercial interests in collecting clients' private health data and sharing them with either insurance companies, research institutions or even the government agencies.Traditional privacy protection mechanisms by simply removing clients' personal identity information (such as names or SSN) or by using anonymization technique fails to serve as an effective way in dealing with privacy of mHealth systems due to the increasing amount and diversity of personal identifiable information 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, locational, relational, computational, vocational, or reputational".Traditionally, the privacy issue is tackled with anonymization technique such as -anonymity or -diversity.However, it has been indicated that these techniques might be insufficient to prevent re-identification attack calling for more sophisticated protection mechanism instead of merely using anonymization. We believe that our proposed cryptographic based systems could serve as a viable solution to the privacy problems in mHealth systems, with Two Factor Authentication (TFA).

II. CLOUD COMPUTING

A feasible and promising approach would be to encrypt the data before outsourcing. A PHR file should only be available to the users who are given the corresponding decryption key, while remain confidential to the rest of users. Right to not only grant, but also revoke access privileges when they feel it is necessary. An alternative is to employ a central authority (CA) to do the key management on behalf of all PHR owners Cloud-computing is recognized as an alternative to traditional information technology due to its intrinsic resource-sharing and low-maintenance characteristics. In cloud computing, the cloud service providers (CSPs), such as amazon, are able to deliver various services to cloud users with the help of powerful data-centers. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures. One of the most fundamental services offered by cloud providers is data storage.Cloud computing has been envisioned as the next generation information technology (IT) architecture for enterprises, due to its long list of unprecedented advantages in

the IT history: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk. Cloud computing is transforming the very nature of how businesses use information technology.

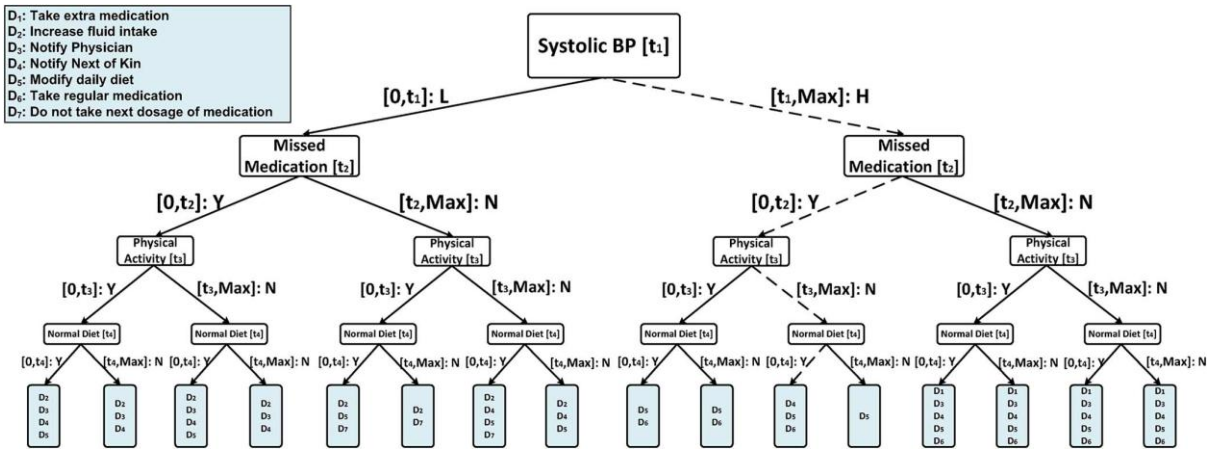

Fig. 1.Branching program in MediNet project.

While cloud computing makes these advantages more appealing than ever, it also brings new and challenging security threats toward users' outsourced data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing is actually relinquishing user's ultimate control over the fate of their data data in the cloud is being put at risk due to the following reasons. First of all, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity Second, there do exist various motivations for CSP to behave unfaithfully toward the cloud users regarding their outsourced data status. For examples, CSP might reclaim storage for monetary reasons discarding
data ,hide data loss incidents to maintain a reputation

As users no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted .Encryption does not completely solve the problem of protecting data privacy against third-party auditing but just reduces it to the complex key management domain. Unauthorized data leakage still remains possible due to the potential exposure of decryption keys Therefore, how to enable a privacy-preserving by usage of TFA.

III. REQUIREMENTS

To achieve "patient-centric" PHR sharing, a core requirement is that each patient can control who are authorized to access to her own PHR documents. Especially, user-controlled read/write access and revocation are the two core security objectives for any electronic health record system.
The security and performance requirements are:

- Data confidentiality
- On-demand revocation
- Write access control
- Scalability
- efficiency and usability

IV. EXISTING SYSTEM

SYSTEM MODEL AND CRYPTOGRAPHIC BUILDING BLOCKS

*A.Branching Program***:**

Since our mHealth monitoring program CAM builds upon branching programs, we first illustrate how a branching tree works. Clients input their related health data such as systolic blood pressure (BP), whether they missed daily medications or have 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.

A monitoring program can be modeled as a binary decision tree based on the range of the monitored measurement. We can represent measured data as an *attribute vector* and then construct the binary branching tree with the leaf nodes as the final consultation to design the medical decision support system.

Let $v = (v_1,\ldots,v_n)$ be a client's attribute vector. An attribute component is a concatenation of an attribute index and the respective attribute value. For instance, A||KW1 might correspond to "blood pressure: 130", which means that the client's blood pressure 130. Each attribute value is a C –bit integer. In this proposal, we choose C to be 32, which should

provide enough precision in most practical scenarios. A binary branching program is a triple $< \{p_1,\ldots,P_k\},L,R>$. The first element is a set of nodes in the branching tree. A nonleaf node is called a decision node while a leaf node is called 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 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 $V_a \leq t_i$;R(i) is the index of the next node if$V_{ai} > t_i$. The label nodes are attached with classification information. To evaluate the branching program on some attribute vector *v*, start from p_1 .

If $V_{a1} \leq t_1$, set h=L (1), else h=R (1). Repeat the process recursively for p_h, and so on, until one of the leaf nodes is reached with decision information.

B.System Model for CAM:

CAM consists of four parties: the cloud server (simply the cloud), the company which provides the mHealth monitoring service (i.e., the healthcare service provider), and the individual clients (simply *clients*), and a semi-trust authority (TA), as shown in Fig. 2. The company stores its encrypted monitoring data or program (branching program) in the cloud. 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 through a mobile (or smart) phone. TA is responsible for distributing private keys to clients and collecting service fees from clients according to a certain business model such as "pay-per-use" model. TA can be considered as a collaborator or a management agent for a company (or several companies) and thus shares certain level of mutual business interest with the company. In the following, we will briefly introduce the four major steps of CAM: Setup, Store, TokenGen and Query .We only illustrate the functionality of these components here. Because the detailed input and output of those steps might vary in different schemes.

At the initial phase, TA runs the Setup phase and publishes the system parameters .mHealth monitoring program is processed as a branching program when a client wishes to query the cloud for a certain mHealth monitoring program, the i^{th} client and TA run the TokenGen algorithm.

A feasible and promising approach would be to encrypt the data before outsourcing. A PHR file should only be available to the users who are given the corresponding decryption key, while remain confidential to the rest of users. Right to not only grant, but also revoke access privileges when they feel it is necessary. An alternative is to employ a central authority (CA) to do the key management on behalf of all PHR owners Cloud-computing is recognized as an alternative to traditional information technology due to its intrinsic resource-sharing and low-maintenance characteristics. In cloud computing, the cloud service providers (CSPs), such as amazon, are able to deliver various services to cloud users with the help of powerful data-centers. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures. One of the most fundamental services offered by cloud providers is data storage.

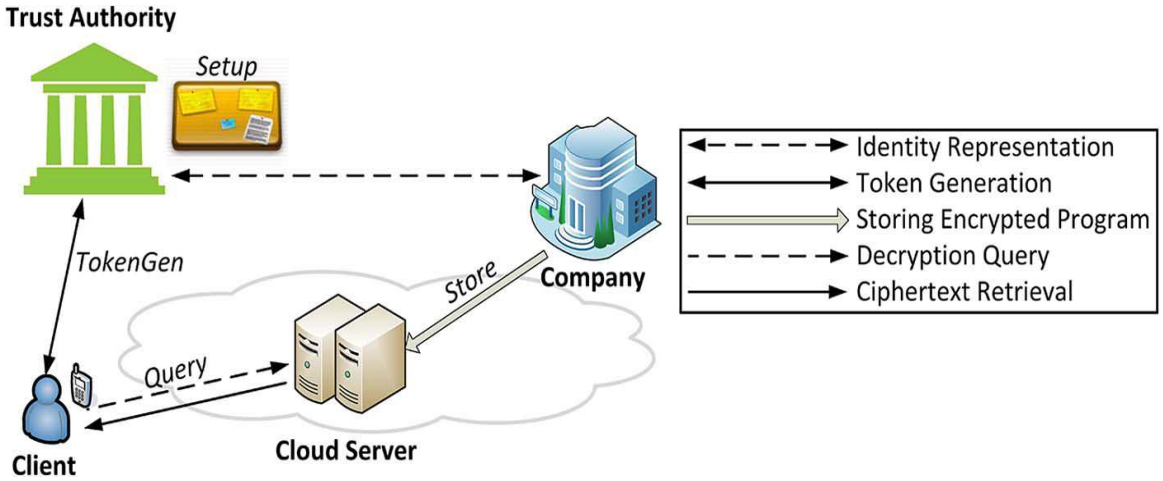

Fig. 2.System architecture for CAM.

At the last phase, the client delivers the token for its query to the cloud, which runs the Query phase. The cloud completes the major computationally intensive task for the client's decryption and returns the partially decrypted ciphertext to the client. The client then completes the remaining decryption task after receiving the partially decrypted ciphertext and obtains its decryption result, which corresponds to the decision from the monitoring program on the client's input.

C.Adversarial Model

We assume a neutral cloud server, which means it neither colludes with the company nor a client to attack the other. This is a reasonable model since it would be in the best business interest of the cloud for not being biased. Clients may collude with each other. We do not consider the possible side-channel attack due to the co residency on shared resources either because it could be mitigated with either system level protection or leakage resilient cryptography. Thus,

our CAM design assumes an honest but curious model, which implies all parties should follow the prescribed operations and cannot behave arbitrarily malicious. Moreover, we also target at the insider attack, which could be launched by either malicious or non malicious insiders who behave normally, but intend to discover information about the others' information. For instance, the insiders could be disgruntled employees, or the healthcare workers who have entered the healthcare business with criminal purposes. It was reported that 32% of medical data breaches in medical establishments between January 2007 and June 2009 are due to insider attacks, and the incident rate of insider attacks is rapidly increasing. The insider data breaches are also reported to cost the victimized institutions much more compared with the breaches due to outsider attacks. Furthermore, insider attacks are generally considered much harder to detect and trace since attackers are generally sophisticated professionals or even criminal rings who are adept at making victims incapable of detecting the crimes. On the other hand, while outsider attacks could be trivially prevented by directly adopting cryptographic mechanisms such as encryption, it is nontrivial to design a privacy-preserving mechanism against insider attacks because we have to balance the privacy requirements with normal operations of mHealth monitoring systems. The problem becomes especially tricky for cloud-assisted mHealth monitoring systems because we need not only to guarantee the privacy of clients' input health data, but also that of the output decision results from both cloud servers and healthcare service providers.

D.Important Cryptographic Building Blocks

To meet our design goal, we need to examine a few cryptographic techniques. Considering that querying input to a diagnostic program usually consists of a client's ID and attributes, we think the recently emerged attribute-based cryptographic techniques derived from ID-based cryptography should provide some viable solutions.

1) Bilinear Pairing

Bilinear pairing serve as the building block for the existing system Based on pairing, Boneh and Franklin proposed the first identity based encryption (IBE). A pairing is an efficiently computable, no degenerate function, e: $G \times G \rightarrow G_T$ with the bilinearity property: $e(g^r,g^s)=e(g,g)^{rs}$ for any r,sϵ Z^*_q ,the finite field modulo q, where G , and G_T are all multiplicative groups of prime order , generated by g and e(g,g) respectively. It has been demonstrated that the proposed IBE is secure under the decisional bilinear Diffie–Hellman (DBDH) assumption (which states that in the IBE setting, given (g,g^a,g^b,g^c,g,S), it is computationally difficult to decide whether $S=g^{abc}$).

*1) Homomorphic Encryption***:**

Another technique we will use for oblivious transfer protocol is homomorphic encryption, which is widely used as an underlying tool for constructing secure protocols in the literature. CAM adopts a semantically secure additively homomorphic public-key encryption technique. Intuitively, for homomorphic encryption HEnc(.), given two encrypted messages $HEnc(m_1)$ and $HEnc(m_2)$, the encryption of the addition of the two underlying messages can be computed as follows: $HEnc(m_1+m_2)= HEnc(m_1)* HEnc(m_2)$, where is the corresponding operation in the ciphertext space.

*2) Multidimensional Range Query Based on Anonymous IBE***:**

The mHealth monitoring program can be represented as a binary decision tree from the attribute vector space (Fig. 3(a)). Thus, an attribute vector can be uniquely mapped to a binary bit block with certain quantization of the measured data, leading to a binary bit represented tree (binary tree) (Fig. 3). Thus, the multidimensional range query (MDRQ) scheme can be used to design our CAM.

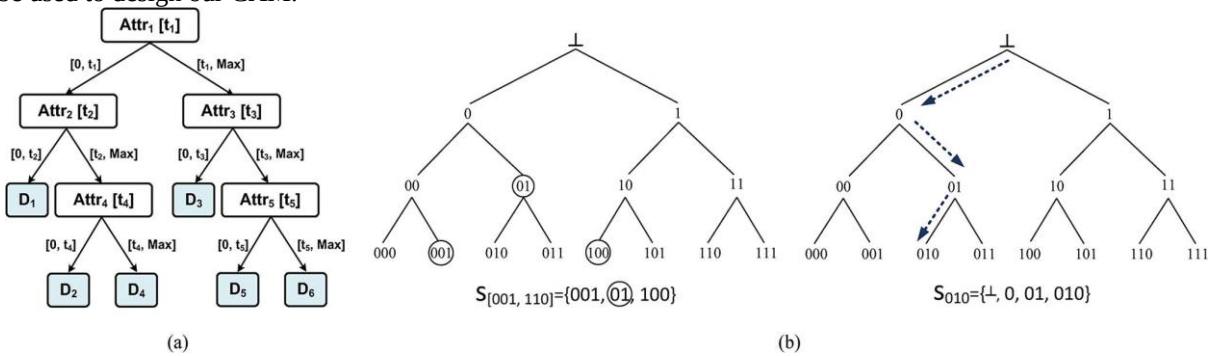

Fig. 3.Branching Program (a)Generic Branching Program (b)basic idea of MDRQ

In MDRQ, a sender encrypts a message under a range $[r_1, r2]$ (or a range of C-bit block v), and a receiver with private keys falling into this range$[r_1,r_2]$ (or a range of -bit block) can decrypt the underlying message.The basic idea of MDRQ is as follows: a C-level binary-tree is employed to represent the C-bit data (or the range). The root of this binary tree is labeled as . The left child node of a non leaf node p is labeled as p0 and the right. The child node is labeled as p1. As a result, all the leaves from left to right will be labeled with a binary string from 0…, 0 to1…, 1,which correspond to all the possible C-bit data. To represent arrange $[r_1, r_2][0,2^c-1]$, a minimum set of roots of sub trees covering all the leaf nodes in this range is used. Apparently, the minimum root representation set is unique for a specific range and contains only at most 2C-1 elements. To represent a –bit data, we first find the respective leaf node, then use the collection of all nodes on the path from the root to this leaf node.

MDRQ can be constructed from an anonymous identity-based encryption (A-IBE) scheme. Compared with the traditional IBE scheme where a Ciphertext can only preserve the privacy of an underlying message; the anonymous IBE scheme can preserve the privacy of both the receiver identity and the underlying message.To encrypt a message *m* under a range $[r_1,r_2]$ (or a vector),a sender treats each element in $S_{[r1,r2]}$ (or S_v) as an identity in the identity space in the A-IBE scheme and encrypt s*m* under all those identities one by one. Thus, only when a receiver's (the attribute value) falls into this range can he decrypt the message since this is the only case when there is an intersection identity between $S_{[r1,r2]}$ and S_v.

MDRQ plays a vital role in our CAM design because all the comparisons between a client's attribute vector and the respective thresholds at decision nodes are implemented using MDRQ. To be more specific for MDRQ in our CAM design, we adapt the Boneh–Franklin IBE (BF-IBE) scheme [31] as the underlying anonymous IBE scheme since it is one of the most efficient existing anonymous IBE schemes.

In CAM, we intend to apply the outsourcing decryption technique to MDRQ based on the BFIBE scheme. The BF-IBE based outsourcing decryption is shown below.

AnonSetup(): This algorithm is exactly the same as the original BF-IBE.
AnonMaskExtract(id,mask): This algorithm is performed by TA and a client.
AnonEnc(id,PP,tk_{id}*,m)* : This algorithm is exactly the same as the original BF-IBE and output $C_{id}=(c_1,c_2,c_3)$.
Transform(C_{id}*,*tk_{id}*)*: This algorithm is performed by the cloud.
AnonMaskDecryption (C'_{id}*, z)*: This algorithm is performed by the client.

3) Key Private Proxy Reencryption (PRE):

Another technique we will use is the proxy re-encryption (PRE) Proxy re-encryption allows an un-trusted proxy server with a re-encryption key (rekey) $rk_{A\rightarrow B}$ to transform a ciphertext (also known as first level ciphertext) encrypted for (delegator) into one (second level ciphertext) that could be decrypted by (delegate) without leaking any useful information on the underlying message.

Setup ():This algorithm is performed by TA.
Ext (id,mask):This algorithm is performed by TA and a client.
Rekey (id_1*,*id_2*,msk)*:This algorithm is performed by TA.
Enc(id,m): : This algorithm is performed by the company.
ReEnc(C_{id}*,*rk_{id}*,*id_z*)*: This algorithm is performed by the proxy.
Dec(sk_{id}*,* C'_{id}*)*: This algorithm is performed by a client.

Theorem: Under the decisional bilinear Diffie–Hellman (DBDH) assumption and random oracle, neither the original nor re-encrypted ciphertext reveals any useful information on the message under chosen ciphertext attack, nor both the original ciphertext and the rekey preserve identity anonymity under chosen ciphertext attack.

The equation of an elliptic curve is given as,

$$y^2 = x^3 + ax + b$$

Few terms that will be used,
E -> Elliptic Curve
P -> Point on the curve
n -> Maximum limit (This should be a prime number **)**

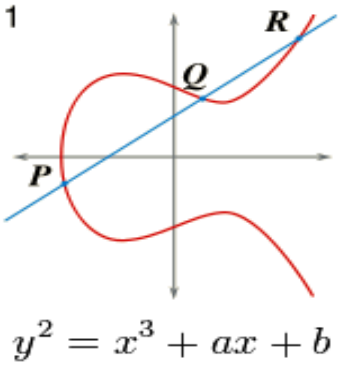

Fig. 4.. Simple Elliptic Curve

Key Generation*:*

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.

Now, we have to select a number **'d'** within the range of **'n'**.

Using the following equation we can generate the public key

Q = d * P

d = The random number that we have selected within the range of (**1 to n-1**). **P**is the point on the curve.
'Q' is the public key and 'd' is the private key.

Encryption:

Let 'm' be the message that we are sending. We have to represent this message on the curve. This have in-depth implementation details. All the advance research on ECC is done by a company called certicom.
Conside *'m'* has the point *'M'* on the curve *'E'.* Randomly select 'k' from [1 - (n-1)].
Two cipher texts will be generated let it be **C1** and **C2**.

$$C1 = k*P$$
$$C2 = M + k*Q$$

C1 and C2 will be send.

Decryption:

We have to get back the message 'm' that was send to us,

$$M = C2 – d * C1$$

M is the original message that we have send.

Proof:

M = C2 – d * C1
'M' can be represented as 'C2 – d * C1′
C2 – d * C1 = (M + k * Q) – d * (k * P) (C2 = M + k * Q and C1 = k * P)
= M + k * d * P – d * k *P (canceling out k * d * P)
= M (Original Message)

V. PERFORMANCE EVALUATION

A.Security:

The cloud obtains no information on either the individual query vector or the company diagnostic branching program as in our first improvement. The cloud obtains no information on the company's branching program due to the semantic security of the proxy re-encryption and symmetric key encryption scheme .A client can only gain information on his decision result and certain side information on the relevant nodes leading to his decision result.

B.Efficiency:

A few experiments was held. We used a laptop with a 2.4 GHz processor with a 4 GB of RAM to simulate the cloud server and the company, and 1 GHz AMR-based iPhone with 512 MB RAM to simulate a client. 100 randomized runs a maximum of k=1000 nodes in the branching program.
The communications between the company and TA is low since the company only needs to deliver the description of a pseudo random function and permutation function, and $N*k$ randomized thresholds to TA.

VI. FURTHER WORK

Another line of work focuses on privacy preserving diagnostic program. At the end of the protocol, a client obtains nothing on the diagnostic program but the diagnostic result while the program owner, i.e., the company obtains no information on the individual private data. All the existing solutions require a client to run multiple instances of oblivious transfer protocol with the company after setup phase, which means the company has to stay online constantly. All the current solutions are based on garbled circuits, which implies a client must download the whole circuit to his device and complete the decryption. Besides, the private computation or processing of medical information over cloud has also attracted attention from both the security community and signal processing community.

VII. CONCLUSION

*The System and Threat Model***:**

The cloud user, who has large amount of data files to be stored in the cloud; the cloud server, which is managed by the cloud service provider to provide data storage service and has significant storage space and computation resources.Users rely on the CS for cloud data storage and maintenance. They may also dynamically interact with the CS to access and update their stored data for various application purposes.

1) *Storage correctness***:** to ensure that there exists no cheating cloud server.
2) *Privacy preserving:* to ensure that users' data content from the information collected.
3) *Minimum computation overhead***:**The user initializes the public and secret parameters of the system by sending an SMS to cloud server.

In cloud computing, outsourced data might not only be accessed but also updated frequently by users for various application purposes. Portions of the work presented in this paper have previously appeared as an extended abstract. We have revised the paper a lot and improved many technical details as compared.

REFERENCES

[1] Mohan P, D. Marin, S. Sultan, and A. Deen, "*Medinet: Personalizing the self-care process for patients with diabetes and cardiovascular disease using mobile telephony,*" in Proc. 30th Ann. Int. Conf. IEEE Engineering in Medicine and Biology Society, 2008 (EMBS 2008), 2008,pp. 755–758.

[2] Danezis G and B. Livshits, "*Towards ensuring client-side computational integrity*," in Proc. 3rd ACM Workshop on Cloud Computing Security Workshop, 2011, pp. 125–130.
[3] Huang Lin, Jun Shao, Chi Zhang, and Yuguang Fang, "*CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring*" in IEEE Transactions on Information Forensics and Security, VOL. 8, NO. 6, JUNE 2013, pp.985-- 997.
[4] Cavoukian A, 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] Cong Wang, Sherman S M Chow, Kui Ren, Wenjing Lou, "*Privacy-Preserving Public Auditing for Secure Cloud Storage*" in IEEE Transactions on Computers, Vol.62, No. 2, February 2013, pp 362-- 375.
[6] Cloud Security Alliance, "*Top Threats to Cloud Computing*", http://www.cloudsecurityalliance.org, 2010.
[7] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, "*Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud*" in IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 6, June 2013, pp 1182 --1191.
[8] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou, "*Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption*", IEEE Transactions on Parallel and Distributed System, Vol. 24, NO. 1, January 2013, pp 131 -- 143.
[9] Dong C, G. Russello, and N. Dulay, "*Shared and Searchable Encrypted Data for Untrusted Servers*," J. Computer Security, vol. 19, pp. 367-397, 2010.
[10] Zheng Y, "*Privacy-Preserving Personal Health Record System Using Attribute-Based Encryption*," master's thesis, Worcester Polytechnic Inst., 2011.
[11] Jiadi Yu, Peng Lu, Yanmin Zhu, Guangtao Xue, Minglu Li, "*Toward Secure Multikeyword Top-k Retrieval over Encrypted Cloud Data*" in IEEE Transactions on Dependable and Secure Computing, Vol. 10, No. 4, July/August,2013, pp 239 --250.
[12] Amazon.com, "*Amazon Elastic Compute Cloud*", http://aws.amazon.com/ec2/ ,2009

AUTHOR'S PROFILE

Prof.K.Karthikeyan is an Assistant Professor in the Department of Computer Science and Engineering at SNS College of Engineering, Coimbatore. His areas of specializations are software Engineering, Soft Computing and Data Mining applications.

Naveen is pursuing his bachelor's degree in Computer Science and Engineering at SNS college of Engineering, affiliated to Anna University, India. His area of interest lies in Cloud computing and Networking.

Nikhil Vinoy is pursuing his bachelor's degree in Computer Science and Engineering at SNS college of Engineering, affiliated to Anna University, India. His area of interest lies in Cloud Computing.His research area is on Networking.

Nagendra Prasath is pursuing his bachelor's degree in Computer Science and Engineering at SNS college of Engineering, affiliated to Anna University, India. His area of interest lies in Cloud computing.

Manoj Prabhu is pursuing his bachelor's degree in Computer Science and Engineering at SNS college of Engineering, affiliated to Anna University, India. His area of interest lies in Network Security.

