Semi-Trusted Authentication for Health Data in Cloud

Rajeswari.M[1], Anjelin Lilly Jasmine.P[2], V.Komaladevi[3], K.Monika[4]

[1]Assistant professor, [2,3,4] Students, Department of Information Technology.

[1,2,3,4] Velammal Institute of Technology, Anna University. Chennai - 601 204

ABSTRACT:-

Cloud-assisted health monitoring, which applies the widespread mobile communications and cloud computing technologies to provide feedback decision support, has been considered as a activist 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 discourage the wide adoption of Health technology.

This project is to address this important problem and design a cloud-assisted privacy preserving 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. Proving secure and performance analysis demonstrates the effectiveness in cloud environment.

Keywords:

Healthcare, Privacy, Decryption, Proxy Re-encryption, Complexity, Service Providers, Security, Performance.

I. INTRODUCTION

FAST access to health data enables better healthcare service provisioning, improves quality of life, and helps saving life by assisting timely treatment in medical emergencies. Anywhere-anytime-accessible electronic healthcare systems play a vital role in our daily life. Services supported by mobile devices, such as home care and remote monitoring, en-able patients to retain their living style and cause minimal interruption to their daily activities. In addition, it significantly reduces the hospital occupancy, allowing patients with higher need of in-hospital treatment to be admitted.

While these e-healthcare systems are increasingly popular, a large amount of personal data for medical purpose are involved, and people start to realize that they would completely lose control over their personal information once it enters the cyberspace. According to the government website, around 8 million patients' health information was leaked in the past two years. There are good reasons for keeping medical data private and limiting the access. An employer may decide not to hire someone with certain diseases. An insurance company may refuse to provide life insurance knowing the disease history of a patient. Despite the paramount importance, privacy issues are not addressed adequately at the technical level and efforts to keep health data secure have often fallen short. This is because protecting privacy in the cyberspace is significantly more challenging. Thus, there is an urgent need for the development of viable protocols, architectures, and systems assuring privacy and security to safeguard sensitive and personal digital information. Outsourcing data storage and computational tasks becomes a popular trend as we enter the cloud computing era.

We design a cloud-assisted Health monitoriTng system (CAM).We first identify the design problems on privacy preservation and then provide our solutions. To ease the understanding, we start with the basic scheme so that we can identify the possible privacy breaches. We then provide an

improved scheme by addressing the identified privacy problems. The resulting improved scheme allows the Health service provider (the company) to be offline after the setup stage and enables it to deliver its data or programs to the cloud securely. To reduce clients' decryption complexity, we incorporate the recently proposed outsourcing decryption technique into the underlying multidimensional range queries system to shift clients' computational complexity to the cloud without revealing any information on either clients' query input or the decrypted decision to the cloud. To relieve the computational complexity on the company's side, which is proportional to the number of clients, we propose a further improvement, leading to our final scheme. It is based on a new variant of key private proxy re-encryption scheme, in which the company only needs to accomplish encryption once at the setup phase while shifting the rest computational tasks to the cloud without compromising privacy, further reducing the computational and communication burden on clients and the cloud.

II. LITERATURE SURVEY

[1] This paper defines Cloud computing and provides the architecture for creating Clouds with market-oriented resource allocation by leveraging technologies such as Virtual Machines (VMs) and also provides insights on market-based resource management strategies that encompass both customer-driven service management and computational risk management to sustain Service Level Agreement (SLA)-oriented resource allocation.

[2] The key used to protect disk files is typically kept in RAM, so a locked laptop can be unlocked by cooling it, interrupting the power, rebooting with a new operating system kernel, and reading out the key. This emphasizes once more the need for engineers who build security applications to take a holistic view of the world.

[3] This paper proposed to develop a new cryptosystem for fine-grained sharing of encrypted data called Key-Policy Attribute-Based Encryption (KP-ABE) and supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).

[4] This paper present ciphertext-policy attribute-based encryption, using encrypted data can be kept confidential even if the storage server is untrusted; attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt.

[5] This paper describes an innovative technical solution in the area of secure messaging that exploits Identifier-based Encryption (IBE) technology. It illustrates the advantages against a similar approach based on traditional cryptography and PKI.

[6] A Proof-of-concept prototype implementation of RDM2000 to demonstrate the feasibility of the proposed framework and provide secure protocols for managing delegations.

[7] This paper proposes a fully functional identity-based encryption scheme (IBE). The scheme has chosen cipher text security in the random oracle model assuming a variant of the computational Diffie Hellman problem.

[8] This paper introduces a systematic approach to specify delegation and revocation policies using a set of rules.

III. SYSTEM ARCHITECTURE

The system architecture is shown in Fig 1.
CAM consists of four parties:

1. The cloud server (simply the *cloud*)
2. The company which provides the health monitoring service (i.e., the healthcare service provider)
3. The individual clients (simply *clients*)
4. A semi trust authority (TA).

IV. SYSTEM DESCRIPTION

The design of the proposed Cloud-Assisted Health Monitoring system (CAM) is highlighted below:

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, QUERY.

i) At the initial phase, TA runs the phase and publishes the system parameters. Then, the company first characterizes the flow chart of a Health monitoring program as a branching program which is encrypted under the respective directed branching tree. Then the company will deliver the resulting ciphertext and its company index to the cloud, which corresponds to the algorithm in the context.

ii) When a client wishes to query the cloud for a certain Health monitoring program, the -th client and TArun the algorithm. The client sends the company index to TA, and then inputs its private query (which is the attribute vector representing the collected health data) and TA inputs the master secret to the algorithm.

iii) The client obtains the token corresponding to its query input while TA gets no useful information on the individual query.

iv) At the last phase, the client delivers the token for its query to the cloud, which runs the 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. The cloud obtains no useful information on either the client's private query input or decryption result after running the phase. Here, we distinguish the query input privacy breach in terms of what can be inferred from the computational or communication information. CAM can prevent the cloud from deducing useful information on a client's query input or output corresponding to the received information from the client.

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 Health monitoring systems. The problem becomes especially tricky for cloud-assisted Health 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.

V. IMPLEMENTATION

The proposed solution is implemented in Java using Net Beans. The client first register and after get activated by the TA can able to login to the cloud. Then the client raises the query and once the TA generated token for the request client can view the results for his/her query. Fig1 shows the user requesting the query. Fig2 shows the client viewing the results for the query. Fig3 and Fig4 shows the adding of medical data and to add comments.

FIG 1:

FIG 2:

FIG 3:

FIG 4:

VI. CONCLUSION AND FUTURE WORK

In this paper, we design a cloud-assisted privacy preserving health monitoring system, called CAM, which can effectively protect the privacy of clients and the intellectual property of Health service providers. To protect the clients' privacy, we apply the anonymous Boneh–Franklin identity-based encryption (IBE) in medical diagnostic branching programs. To reduce the decryption complexity due to the use of IBE, we apply recently proposed decryption outsourcing with privacy protection to shift clients' pairing computation to the cloud server.

As future work, we plan to devise mechanisms that can detect whether users' health data have been illegally distributed, and identify possible source(s) of leakage (i.e., the authorized party that did it).

REFERENCES

[1] R. Buyya, C. ShinYeo, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Gen. Computer Sys., vol. 25, issue 6, June 2009, pp. 599-616.

[2] A.Ross , "Technical Perspective A Chilly Sense of Security," CACM, vol. 52, issue. 5, May 2009, pp. 90-90.

[3] Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 89-98.

[4] Bethencourt, J. Carnegie Mellon Univ., Pittsburgh, PA Sahai, A. and Waters, B, "Ciphertext-Policy Attribute-Based Encryption," in Proc. IEEE May 2007, pp. 321-334.

[5] M. C. Mont, P. Bramhall, and K. Harrison, "A flexible role-based secure messaging service: Exploiting IBE technology for privacy in health care," presented at the 14th Int. Workshop Database Expert Syst. Appl., Prague, Czech Republic, 2003.

[6] L. Zhang, G. J. Ahn, and B. T. Chu, "A rule-based framework for rolebased delegation and revocation," ACM Trans. Inf. Syst. Security, vol. 6,no. 3, pp. 404-441, 2003.

[7] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing. Extended abstract in CRYPTO 2001," siam j. Comput., vol. 32, no. 3, pp. 586-615, 2003.

[8] L.Zhang, G. J. Ahn, and B. T. Chy, "A role-based delegation framework for healthcare information systems," in 7th ACM Symp. Access Control Models Technology, Monterey, CA, USA, 2002, pp.125-134.