Secure Mobile Health Monitoring Using Cloud Storage

GNANAJEYARAMAN RAJARAM[1], Dr.GUNASEELAN D[2], P.K. KUMARESAN[3]

1 SBM COLLEGE OF ENGINEERING &TECHNOLOGY SBM NAGAR, THAMARAIPADI DINDIGUL Tamil Nadu INDIA2 JAZAN UNIVERSITY JAZAN Kingdom of Saudi Arabia Jizan SAUDI ARABIA3 VMKV ENGINEERING COLLEGE PERIYASEERAGAPADI SALEM Tamil Nadu INDIA

Abstract

Mobile cloud computing platforms represent a more secure way for provisioning applications and online services to users over mobile networks. Mobile cloud provisioning takes advantage of the inherent benefits of cloud computing for monitoring, security detection and malware prevention capabilities to protect its mobile users. Security and privacy preservation in is the main expectation of the cloud users in Mobile based cloud servicing. In this project, cloud based secure mobile health care model with feedback decision support is proposed. This mainly aims to improve the quality of the health care with reduced complexity and no compromise in security. This paper also mentions the difficulty imposed on client privacy and monitoring the service provider. To protect the client privacy, Boneh-Franklin Identity based encryption is proposed to reduce the decryption complexity due to the use of IBE (Identity based encryption) technique. To protect mobile Health (m-Health) service providers programs, the branching tree is expanded by random permutation and the decision thresholds used at the decision branching nodes are also randomized. It adopts the recently proposed decryption outsourcing to reduce the workload of both the company and clients by outsourcing the majority of computational task to cloud. The private proxy re-encryption technique takes care of the privacy of the clients and vulnerability of data is prevented. The main objective of the proposed architecture is preserving the privacy of the information ensuring that this information cannot be misused. In this paper we have proposed secure cloud architecture to address the user privacy problem in a cloud. By using OTP and WTP in cloud computing system, our proposed architecture achieves better goal of preserving the privacy of a user.

Keywords: cloud computing, identity based encryption, Boneh -Franklin encryption

1. Introduction

I.CLOUD COMPUTING In science, cloud computing is a synonym for distributed computing over a network and means the ability to run a program on many connected computers at the same time.The popularity of the term can be attributed to its use in marketing to sell hosted services in the sense of application service provisioning that run client server software on a remote location. Cloud Computing is the result of evolution and adoption of existing technologies and paradigms. The goal of cloud computing is to allow users to take benet from all of these technologies, without the need for deep knowledge about or expertise with each one of them. The cloud aims to cut costs, and help the users focus on their core business instead of being impeded by IT obstacles.Cloud computing is the next stage in the Internet's evolution, providing the means through which everything from computing power to computing infrastructure, applications, business processes to personal collaboration can be delivered to you as a service wherever and whenever you need. The cloud in cloud computing can be defined as the set of hardware, networks, storage, services, and interfaces that combine to deliver aspects of computing as a service. Cloud services include the delivery of software, infrastructure, and storage over the Internet (either as separate components or a complete platform) based on user demand.

2. Mobile Cloud Computing

Cloud computing and mobile are two such things. Widespread adoption of these two is changing our lives, the way we do business and most of our day-to-day chores.Research and analyst data

 ISSN 1941-2681. http://www.notoare.com/19205225

show how profoundly these technologies have created a reverberation in the technology landscape around the world. An explosion of mobile and handheld devices is also significantly contributing to world IP data traffic. To support such data demand, cloud computing seems to be the right choice because of its rapid scalability, ubiquitous network access, on-demand self-service and other features. We will find the definition of mobile cloud computing shortly. At this juncture, I would like to present some data to establish the need for cloud.Mobile Cloud Computing (MCC) is the state-of-the-art mobile distributed computing paradigm comprises three heterogeneous domains of mobile computing, cloud computing, and wireless networks aiming to enhance computational capabilities of resource-constrained mobile devices towards rich user experience. MCC provides business opportunities for mobile network operators as well as cloud providers. More comprehensively, MCC can be defined as "a rich mobile computing technology that leverages unied elastic resources of varied clouds and network technologies toward unrestricted functionality, storage, and mobility to serve a multitude of mobile devices anywhere, anytime through the channel of Ethernet or Internet regardless of heterogeneous environments and platforms based on the pay-as-you-use principle MCC realizes its vision leveraging computational augmentation approaches by which resource-constraint mobile devices can utilize computational resources of varied cloud-based resources. In MCC, there are four types of cloud-based resources, namely distant immobile clouds, proximate immobile computing entities, proximate mobile computing entities, and hybrid (combination of the other three model) Giant clouds such as Amazon EC2 are in the distant immobile groups whereas cloud let or surrogates are member of proximate immobile computing entities . Smartphones, tablets, handheld devices, and wearable computing devices are part of the third group of cloud-based resources which is proximate mobile computing entities.

3. Architechtural Model

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.

3.1 Branching Program

It describes the branching programs, which include binary classification or decision trees as a special case.Let v be the vector of clients attributes. To be more specific, an attribute component vi 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 pi is an intermediate decision node while leaf node pi is a label node. Each decision node is a pair (ai, ti), where ai is the attribute index and ti is the threshold value with which vai is compared at this node. The same value of ai 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 vai ti; R(i) is the index of the next node if vai ¿ ti. The label nodes are attached with classification information. Repeat the process recursively for ph, and so on, until one of the leaf nodes is reached with decision information. However, the company and TA could collude to obtain private health data from client input vectors

3.2 B.Token Generation:

To generate the private key for the attribute vector v=(v1, , vn), 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 AnonExtract(id, msk) on each identity id Svi in the identity set and delivers all the respective private keys skvi to the client.

3.3 C.Query

A client delivers the private key sets obtained from the TokenGen algorithm to the cloud, which runs the Anon Decryption algorithm on the ciphertext generated in the Store algorithm. Starting from p1, the decryption result determines

which ciphertext should be decrypted next. For instance, if v1 [0, t1], then the decryption result indicates the next node index L(i). The cloud will then use skv(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.

3.4 D. 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.

Fig. 1: Topography of cloud management system

4. Design Methodology

A. Identity-Based Encryption (IBE) Identity-Based Encryption (IBE) takes a breakthrough approach to the problem of encryption key management. IBE can use any arbitrary string as a public key, enabling data to be protected without the need for certificates. Protection is provided by a key server that controls the dynamic generation of private decryption keys that correspond to public identities and the key servers base root key material. By separating authentication and authorization from private key generation through the key server, permissions to generate keys can be controlled dynamically on a granular policy driven basis, facilitating granular control over access to information in real time. The IBE algorithm consists of four operations: 1. Setup, which initializes a key server 2. Encrypt, which encrypts a message for a given user 3. Key Generation, which generates a private key for a given user 4. De-crypt, which given a private key, de-crypts a message

4.1 B.Anonymous Decryption

An anonymous decryption system, the management of which is facilitated and initialization of which is readily and reliably carried out. A shuffling management center transmits a security parameter and common public information generated on the basis of the security parameter to decryption shuffle centers.The decryption shuffle centers generate public keys and decryption keys and returns the public keys to the shuffling management center. Conclusion and future work Data privacy is one of the biggest challenges in Cloud Computing. By the introduction of the OTP/ WTP password protection schemes, the privacy of the user will now be assured to a great extent. The OTP provides a user new password each time and WTP provides the task for a frequent user to use OTP so he/she would opt for WTP.In future, this proposed model could be used to get the secure cloud computing environment which would be a great enhancement in the privacy preservation.

References

[1] Y. Lin and I Chlamtac,, *"Wireless and Mobile Network Architecture"*, , Vol. , No. , pp.1537. , .

[2] F. Koushanfar, M. Potkonjak, V. Prabhu, J. Rabaey,, *"Processors for Mobile Applications"*, , Vol. , No. , pp.603, , September 2000. .

[3] A. Agarwal, D. Gupta, , *"Security Requirements Elicitation Using View Points for Online System"*, , Vol. , No. , pp.1238-1243,, July 2008..

[4] B. Chun, P. Maniatis,, *"Augmented Smartphone Applications Through Clone Cloud Execution"*, , Vol. , No. , , May 2009 .

[5] , *"Generic Authentication Architecture (GAA). Generic Bootstrapping Architecture (GBA)"*, , Vol. , No. 3GPP TS 33.220;, , December 2006..

[6] K. Yang, S. Ou., , *"On Effective Offloading Services for Resource-Constrained Mobile Devices Running Heavier Mobile Internet Applications. I,"*, , Vol. , No. , pp.53 63, January 2008. .

[7] S. Beji, N. E. Kadhi,, *"An Overview of Mobile Applications Architecture and the Associated Technologies,"*, , Vol. , No. , pp. 77 83, , July 2008. .

[8] F. Mekuria,, *"Issues in Mobile Broadband Networks &Services."*, , Vol. , No. , , 10-12, Dec. 2008,.

[9] Armbrust et.al.,, *"Above the clouds: A Berkeley View of cloud compuring."*, , Vol. , No. , , February 10, 2009. .

[10] K. Rikitaki,et.al, *"Ubiquitous Health Monitoring System,"*, , Vol. , No. , , Jan.2009. .

[11] , *"The open IMS core project:"*, , Vol. , No. , , .

[12] S.Loreto, et.al., *"IMS service development API and Test-bed"*, , Vol. , No. , . Pp. 26-31. , April 2010.

[13] M. Weitzel, et. Al,, *"A web 2.0 model for patient centered health informatics applications."*, , Vol. , No. , , July 2010. .

[14] M.T. Nkosi, F. Mekuria,, *"Mobile Government for Improved Service Delivery.,"*, , Vol. , No. , , 19-21 May, 2010,.