IJDCST @Feb-March Issue- V-2, I-3, SW-10
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Emerging Data Sharing Services in Cloud Computing Using Attribute Based Encryption

[1]SK.Gopala Krishna , [2]D.T.R.Subba Reddy
Dept. Computer Science & Engineering, Guntur Engineering College,Guntur, India.
Head of the Department of CSE, Guntur Engineering College, Guntur,India

ABSTRACT: Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. To keep sensitive user data confidential against un-trusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. These solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine grained data access control is desired. Open issue by defining and enforcing access policies based on data attributes and allowing the data owner to delegate most of the computation tasks involved in fine grained data access control to un-trusted cloud servers without disclosing the underlying data contents. Several schemes employing attribute-based encryption (ABE) have been proposed for access control of outsourced data in cloud computing. It is implemented using cipher text policy by encrypting and decrypting the data in the cloud so that the cloud system becomes more scalable and flexible by enforcing data owners to share their data with data consumers controlled by the domain authority.

KEY WORDS: Attribute-based Encryption, key distribution, cloud computing.

I. INTRODUCTION

Cloud computing is computing that includes a large number of computers associated through a communication network such as the Internet, similar to utility computing [4]. In science, cloud computing is a synonym for distributed computing over a network, and means the ability to run a program or application on many connected computers at the same time. Network-based services, which appear to be delivered by real server hardware and are in fact served up by virtual hardware simulated by software running on one or more real machines, is often called cloud computing. Such simulated servers do not physically exist and can therefore be relocated around and scaled up or down on the fly without disturbing the end user, somewhat like a cloud becoming larger or smaller without being a physical object [3].

In common usage, the term "the cloud" is fundamentally a metaphor for the Internet [5]. Marketers have further made popular the phrase "in the cloud" to refer to software, platforms and infrastructure that are sold "as a service", i.e. remotely through the Internet. Typically, the seller has actual energy-consuming servers which host products and services from a remote location, so end-users don't have to; they can simply log on to the network without installing anything. The major models of cloud computing service are known as software as a service, platform as a service, and infrastructure as a service [3].

Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid)

over a network[6]. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services. The cloud also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. This can work for allocating resources to users.

Security in cloud computing:

As cloud computing is achieving increased popularity, concerns are being voiced about the security issues introduced through adoption of this new model.[4][7] The effectiveness and efficiency of traditional protection mechanisms are being reconsidered as the characteristics of this innovative deployment model can differ widely from those of traditional architectures.[8] An alternative perspective on the topic of cloud security is that this is but another, although quite broad, case of "applied security" and that similar security principles that apply in shared multi-user mainframe security models apply with cloud security[9].

Cloud computing offers many benefits, but is vulnerable to threats. As cloud computing uses increase, it is likely that more criminals find new ways to exploit system vulnerabilities. Many underlying challenges and risks in cloud computing increase the threat of data compromise. To mitigate the threat, cloud computing stakeholders should invest heavily in risk assessment to ensure that the system encrypts to protect data, establishes trusted foundation to secure the platform and infrastructure, and builds higher assurance into auditing to strengthen compliance. Security concerns must be addressed to maintain trust in cloud computing technology.

II. RELATED WORK

Hans Löhr stated that we point out several shortcomings of current e-health solutions and standards, particularly they do not address the client platform security, which is a crucial aspect for the overall security of e-health systems. To fill this gap, we present a security architecture for establishing privacy domains in e-health infrastructures. Our solution provides client platform security and appropriately combines this with network security concepts. Moreover, we discuss further open problems and research challenges on security, privacy and usability of e-health cloud systems.

Ming Li, Shucheng Yuy, Ning Ca and Wenjing Lou stated that personal health record (PHR) has emerged as a patient-centric model of health information exchange, which features storing PHRs electronically in one centralized place,such as a third-party cloud service provider. Although thisgreatly facilitates the management and sharing of patients' personal health information (PHI), there have been serious privacy concerns about whether these service providers canbe fully trusted in handling patients' sensitive PHI. To ensure patients' control over their own privacy, data encryption has been proposed as a promising solution. However, key functionalitiesof a PHR service such as keyword searches by multiple users become especially challenging with PHRs stored in encrypted form. Basically, users' queries should be performed in a privacypreserving way that hides both the keywords in the queries and documents. More importantly, in order to prevent unnecessary exposure of patients'

PHI from unlimited query capabilities, eachuser's query capability should be authorized and controlled in a fine-grained manner, which shall be achieved with a high level of system scalability. Existing works in searchable encryption are unable to meet the above requirements simultaneously.

C. Cachin in his paper stated that there is a problem of efficient distributed storage of information in a message-passing environment where both less than one third of the servers, So to overcome these problem author introduced first implementation of non-skipping timestamps which provides optimal resilience and withstands Byzantine clients; it is based on threshold cryptography.

Kui Ren Stated in his paper cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. So to overcome the drawbacks author used a flexible distributed storage integrity auditing mechanism, utilizing the homomorphic token and distributed erasure-coded data.

III. EXISTING SYSTEM

In Existing system a PHR system model, there are multiple owners who may encrypt according to their own ways, possibly using different sets of cryptographic keys. Letting each user obtain keys from every owner who's PHR she wants to read would limit the accessibility since patients are not always online. An alternative is to employ a central authority (CA) to do the key management on behalf of all PHR owners, but this requires too much trust on a single authority (i.e., cause the key escrow problem).

We consider a PHR system where there are multiple PHR owners and PHR users. The owners refer to patients who have full control over their own PHR data, i.e., they can create, manage, and delete it. There is a central server belonging to the PHR service provider that stores all the owners' PHRs. The users may come from various aspects; for example, a friend, a caregiver or a researcher. Users access the PHR documents through the server in order to read or write to someone's PHR, and a user can simultaneously have access to multiple owners' data.

A typical PHR system uses standard data formats. For example, continuity-of-care (CCR) (based on XML data structure), which is widely used in representative PHR systems including Indivo [27], an open-source PHR system adopted by Boston Children's Hospital. Due to the nature of XML, thePHRfiles are logically organized by their categories in a hierarchical way.

IV. PROPOSED SYSTEM

Attribute-Based Encryption (ABE):

Using ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of users.

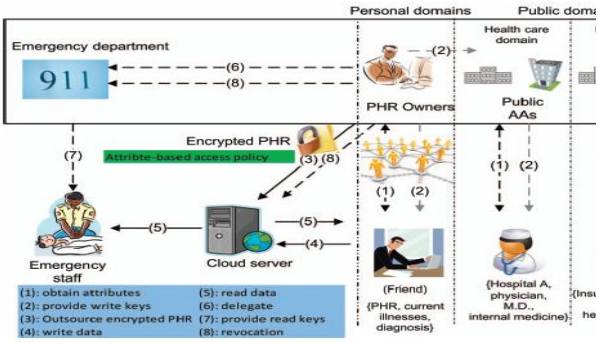


Fig. 1. The proposed framework for patient-cent cure and scalable PHR sharing on semi-trusted under multi-owner settings.

We examine existing access control schemes based on ABE. Several efforts followed in the literature to try to solve the expressibility problem. Ciphertexts are not encrypted to one particular user as in traditional public key cryptography. A user is able to decrypt a ciphertext only if there is a match between his decryption key and the ciphertext. ABE schemes are classified into key-policy attribute-based encryption (KP-ABE) and cipher text-policy attribute-based encryption (CP-ABE).

KP-ABE, the authority determines what combinations of attributes must be present in order for this user to decrypt and gives the user the corresponding private key.

CP-ABE in that it allows complex rules specifying which private keys can decrypt which cipher texts. The private keys are associated with sets of attributes or labels and we encrypt to an access policy which specifies which keys will be able to decrypt.

Cipher-Text Policy:The trusted authority calls the algorithm to create system public parameters and master key. The public parameters will be made public to other parties and Master Key will be kept secret. Attributes asso- ciated with the ciphertext satisfy the tree access structure, can the user decrypt the ciphertext.

Kp-Abe Policy: We utilize KP-ABE to escort data encryption keys of data Files. These construction helps us to immediately enjoy fine-grandness of access control. CP-ABE scheme decryption keys only support user attributes that are organized logically as a single unit. Users can only use all possible combinations of attributes in a single set issued in their keys to satisfy policies as shown in the fig.2.

$a \equiv g^k \pmod p$; gcd(k,p-1) = 1; else a=1?
Message *M* (digraph, triblock graphs)
Public Key $(g, p, y \equiv g^k \pmod p)$
$M \equiv (xa + xb) \bmod (p-1)$

Where *k= Random secret value*
x= Private Key

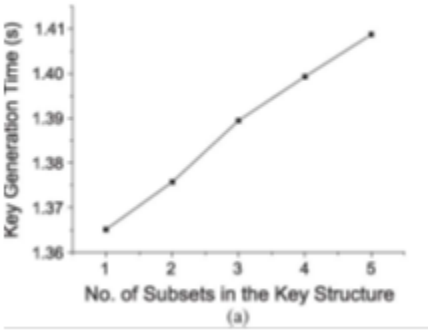
Digital Signature (a,b) sent with M
$Y^a a^b \equiv g^M \pmod p$
The Math:
$g^M = g^{(xa + xb)} \bmod p$
$(g^x)^a (g^k)^b = y^a a^b \pmod p$
If *M* is modified, congruence would be violated

Fig.2: Kp-Abe Policy

V. EXPERIMENTAL RESULTS

Our experimental results shows that, theproposed system attribute based encryption(ABE) is addressing the addresses the unique challenges brought by multiple PHR owners and users, in that we greatly reduce the complexity of key management while enhance the privacy guarantees compared with

previous works. It is implemented using cipher text policy by encrypting and decrypting the data in the cloud so that the cloud system becomes more scalable and flexible by enforcing data owners to share their data with data consumers controlled by the domain authority.



Figure(3).New user/domain authority grant

The above graph represents the key generation in proposed system for providing more security in sharing personal health records in cloud computing.

VI. CONCLUSION

In this paper, we have proposed a novel framework of secure sharing of personal health records in cloud computing. Considering partially trustworthy cloud servers, we argue that to fully realize the patient-centric concept, patients shall have complete control of their own privacy through encrypting their PHR files to allow fine-grained access. The framework addresses the unique challenges brought by multiple PHR owners and users, in that we greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works. We utilize ABE to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications, and affiliations. Furthermore, we enhance an existing MA-ABE scheme to handle efficient and on-demand user revocation, and prove its security. Through implementation and simulation, we show that our solution is both scalable and efficient.

VII. REFERENCES

[1]. Attribute-Based Encryption for Access Control of Outsourced Data in Cloud Computing using Hasbe.

[2]. Cloud Computing Security: From Single to Multi-Clouds by Mohammed A. AlZain #, Eric Pardede #, Ben Soh #, James A. Thom.

[3]. Cloud computing from wimkipedia.

[4]. Securing Virtual and Cloud Environments". In I. Ivanov et al. Cloud Computing and Services Science, Service Science: by Mariana Carroll, Paula Kotzé, Alta van der Merwe.

[5]. Cloud Computing entry". By NetLingo.

[6]. The NIST Definition of Cloud Computing". National Institute of Standards and Technology. Retrieved 24 July 2011.

[7]. Secure virtualization: benefits, risks and constraints, 1st International Conference on Cloud Computing and Services Science by M Carroll, P Kotzé, Alta van der Merwe (2011).

[8] "Addressing cloud computing security issues". Future Generation Computer Systems by Zissis, Dimitrios; Lekkas (2010).

[9]. Securing the Cloud: Cloud Computer Security Techniques and Tactics by Waltham.

[10]. Securing the E-Health Cloud by Hans Löhr.

[11]. Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing by Ming Li, Shucheng Yuy, Ning Ca and Wenjing Lou.

[12]. "Google, Microsoft Say Hipaa Stimulus Rule Doesn't Apply to Them,"