A Trusted Mechanism For Providing Security Over Cloud Computing

[1]G.Vihari, [2]P.Ramaiah Chowdary, [3]Dr. S.Krishna Rao
[1,2,3]Dept. of IT, Sir C.R.R.College of Engineering, Eluru, AP, India

Abstract
The development of cloud computing is still in its initial stage, and the biggest obstacle is data security. How to guarantee the privacy of user data is a worthwhile study. This paper has proposed a secure document service mechanism based on cloud computing. Out of consideration of security, in this mechanism, the content and the format of documents were separated prior to handling and storing. In addition, documents could be accessed safely within an optimized method of authorization. This mechanism would protect documents stored in cloud environment from leakage and provide an infrastructure for establishing reliable cloud services.

Keywords
P2P, HTML, Encryption, Decryption

I. Introduction

Cloud computing is a new variation of traditional distributed computing and grid computing. The development of cloud computing is still facing enormous challenges. A major concern is about data security, that is, how to protect data from unauthorized users and leakage. In order to reduce operation costs on client end and boost the efficiency of collaboration, the cloud undertook the majority of jobs. From the view of users, losing control of the executions of jobs may increase the risk of being hacked especially when the security of entire task highly depend on the trustworthiness of the cloud. As can be seen, for both individual user and large-scale enterprises, it is an important issue to protect key data within cloud pattern. This issue, to some extent, has a great impact on the development of cloud computing. This paper has designed a secure document service mechanism for the document service based on cloud environment. We highlight that the major threats against the safety of document service and the privacy of user documents focus on two concept:

1. Documents would be intercepted and captured during transferring from client-end to the cloud and
2. Access control for documents stored in the cloud.

To guarantee the privacy of document, on the one hand, the content and the format of document were separated prior to handling and storing, because most of private information was stored in the content of documents. An optimized authorization method was proposed to assign access right for authorized users on the other hand.

II. Related Work

Cloud computing derived from traditional distributed computing where existed two main methods to satisfy the requirements of reliable data storage service. The first one heavily relied on a trusted third-party. A successful example in business is eBay [1], in which all of users' transaction information were stored at official center server. In this pattern, the most important component for data access control– authorization was deployed in the center server. The second one often used in P2P context. In decentralized P2P environment, authority did not exist and reputation based trust relation were emphasized [2-4]. The weak point of their works was that they could not give full privacy just a part of it, which determined that the above methods cannot be directly applied in cloud environment. Within another distributed pattern grid computing community, there is no consensus that how data authentication should be done within virtual organizations [5]. Thus, cloud environment needs new models to handle potential security problems. This new model should allow an information owner to protect their data while not interfering with the privacy of other information owners within the cloud [6]. From the view of client, the remote service deployed in cloud was hardly to be regarded as trustworthy in default situation. In recent studies, [7] focused on the lower layer IaaS cloud providers where securing a customers virtual machines is more manageable. Their work provided a closed box execution environment. [6] proposed Private Virtual Infrastructure that shares the responsibility of security in cloud computing between the service provider and client, reducing the risk of them both. Our aim is to provide an efficient methodology to guarantee privacy of user data in cloud computing environment.

III. Secure Document Service Mechanism

Guaranteeing full privacy of user's document was an important concept for security document service. For ideal distributed document service based on cloud computing, document handling and storing were not executed by local system in client-end but by remote cloud server that provide document service. Since the work on remote cloud server cannot be considered as trustworthy in default setting, we propose a novel mechanism to protect the privacy of user's document, which correspond with cloud computing fashion.

A. Separation of Content and Format

This paper has focused on document service in cloud and the term "data" refer to document file in general.
Document. A data stream that consist of content and format. The content of document can be browsed and handled in a specified manner that determined by its format.
For example,
<B> hello </B>
 <B> world !</B>In this fragment of an HTML file, the strings "hello" and "world !" are content which can be browsed in browser. The tags like "<***>" are format, while the couple "<B>" and "</B>" make the strings "hello" and "world !" bold and "
" gives a line break between the two words. We identify any documents with content-format combinations. For example, above HTML file can be seen as B(hello)BR()B(world!).Therefore, document handling could be seen as combination of content handling and format handling. Actually, most of private information was not stored in format but content. Making the procedure of content handling secure was essential for guaranteeing document privacy. In our design, we separated content from document and then content should be encrypted (by several sophisticated cryptographic algorithms, e.g., RSA [8], DES [9], etc.) before document being propagated and stored in remote server.

B. Document Partition

Usually, document handling often did not cover the whole content and format but a part of them. It is not necessary to re-store the whole document, but just its partition that were handled. It is believed that partitioning the document prior to handling and only updating the modified partition could reduce the overhead of document service and the possibility of the whole document being damaged and hacked. If the size of document partition were rather large, the possibility of this partition being updating were somewhat high than of a smaller partition. Because

Because it was more possible that handling happened in a larger partition. Unfortunately, if the handling that only changed punctuation or a letter happened

in a very large partition, the efficiency of transferring and storing document would be affected.

C. Document Authorization

Data authorization can be implemented by public-key cryptography in traditional network environment. Correspondingly, cloud computing environment was lacking in nature pre-trusted party that was responsible for authentication and authorization.

General Authorization Method (Method 1). In general practice, the document owner had charge of authorizing other users for accessing documents. We denoted the public and private key of OwnerI as BI , PI and the public and private key of UserJ as BJ , PJ , respectively. BI (c) depicted that content c was encrypted with OwnerI 's public key and the procedure of decryption could be written as PI (BI (c)). If OwnerI wanted to authorize UserJ for accessing document, OwnerI required encrypt the content by UserJ 's public key, namely BJ (PI (c)). This method could be implemented relatively easily. Document owners overhead of encrypting content, however, would be in conformity with the number of users who were authorized.

D. Optimized Authorization Method (Method 2)

(a) Construct two encryption functions f(x), g(x), both of them have the following properties:

i. It is hard to find inverse functions for both functions.

ii. For any M, when f(M) = N, there must be g(N) = M. Also, for

any M, when g(M) = N, there must be f(N) = M. As summarize, g(f(M)) = f(g(M)) = M.

iii. It is hard to find inverse function for f(g(x)) and to decompose f(g(x)) as the combination of f(x) and g(x). Denote f(g(x)) as H(x).

iv. It is hard to find inverse function for f(g(g(x))) and to decompose f(g(g(x))) as the combination of f(x) and g(x). Denote f(g(g(x))) as I(x).

v. For any M, when f(M) = N, there is H(N) = f(M).

vi. For any M, when f(M) = N, there is I(N) = f(g(M)).

(b) Suppose H(x) existed and encrypted document BI (c) stored in cloud server, when OwnerI authorized UserJ for access to BI (c), H(x) would be submitted to cloud server. Cloud server would then automatically compute H(BI (c)) and send it to UserJ . H(BI (c)) could be generated as BJ (c) by UserJ . It is easy for UserJ to decrypted BJ (c) by using PJ .

(c) Suppose I(x) existed,when UserJ obtained encrypted contentBJ (PI (c)),

content c could be generated by computing BI (PJ ((BJ (PI (c))))).

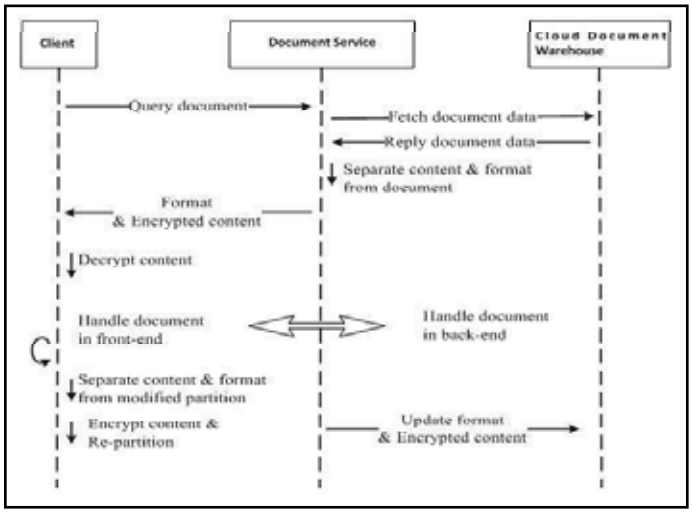

Fig. 1: Separation of Content and Format

IV. Secure Document Service Arche Type

We provided the model of our mechanism, as follows: As fig. 1 depicted, Documents were stored in"Cloud Document Warehouse". The handling involved document format was completely done by"Document Service", while owner in client-end was responsible for encryption and decryption of document content. To save document, client must re-encrypt partitioned content and then send it to "Document Service". There were two kinds of authorization procedures (Fig. 2). For Method 1, by decryption, client can get the access to documents from"Document Service". There was a pre-requirement, for Method 2, of the existence of H(x) and I(x). Using Method 2 can significantly reduce the overhead of authorization of Client H and the complexity of procedure of sharing documents among clients.

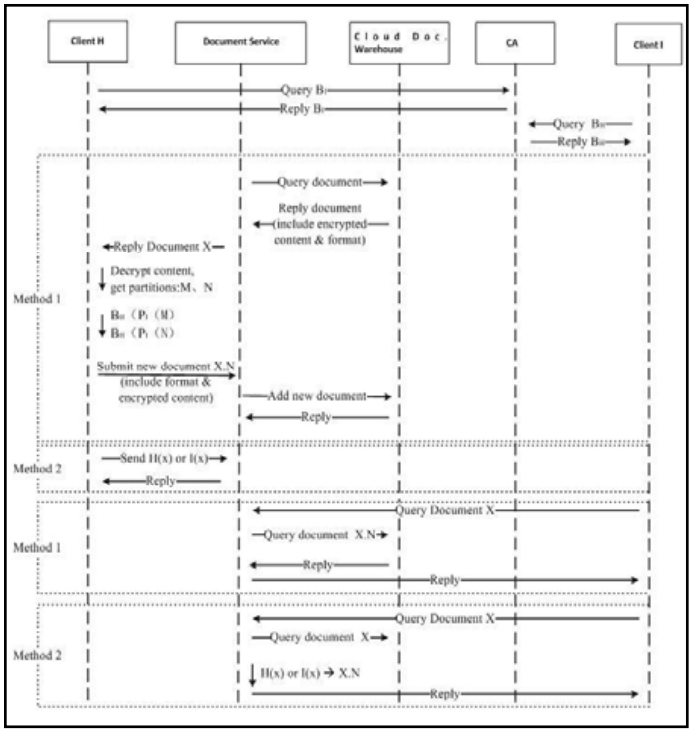

Fig. 2: Procedure of Authorization

V. Conclusion and Future Work

The mechanism of security document service for cloud computing environment has been proposed and an archetype has been given. In this mechanism, content and format were fig. 1. Separation of Content and Format separated from document to keep their

privacy. Also, an optimized authorization method has been proposed for assigning access right of document to authorized users. In the near future, we will highlight several fields where new approaches for implementing secure document service are required, particularly in constructing appropriate functions of H(x) and I(x) for authorization. In this direction, the most significant result would be a novel file format that can perfectly keep privacy of content.

References

[1] Resnick, P., Zeckhauser, R.,"Trust among strangers in Internet transactions: Empirical analysis of eBay's reputation system", Advances in Applied Microeconomics: A Research Annual 11, pp. 127–157 (2002)

[2] Kamvar, S., Schlosser, M., Garcia-Molina, H.,"The eigentrust algorithm for reputation management in P2P networks", In: Proceedings of the 12th international conference on World Wide Web, pp. 640–651. ACM, New York (2003)

[3] Xiong, L., Liu, L.,"Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities", IEEE transactions on Knowledge and Data Engineering 16(7), pp. 843–857, 2004.

[4] Rahbar, A., Yang, O.,"Powertrust: A robust and scalable reputation system for trusted peer-to-peer computing", IEEE Transactions on Parallel and Distributed Systems 18(4), pp. 460–473, 2007.

[5] Antonioletti, M., Atkinson, M., Baxter, R., Borley, A., Hong, N., Collins, B., Hardman, N., Hume, A., Knox, A., Jackson, M., et al.,"The design and implementation of Grid database services in OGSA-DAI", Concurrency and Computation: Practice & Experience 17(2), pp. 357–376 (2005)

[6] Krautheim, F.J.,"Private virtual infrastructure for cloud computing", In: HotCloud, USNIX (2009)

[7] Nuno Santos, K.P.G., Rodrigues, R.,"Towards trusted cloud computing", In: Hot- Cloud, USNIX (2009)

[8] Rivest, R., Shamir, A., Adleman, L.,"A method for obtaining digital signatures and public-key cryptosystems 1978.

[9] Biham, E., Shamir, A.,"Differential cryptanalysis of DES-like cryptosystems", Journal of Cryptology 4(1), 3–72 (1991)

Mr. G.Vihari is working as an Asst. Professor, in I.T Department, Sir C. R. Reddy College of Engg, Eluru, A.P., India. He has received his B.Tech (CSE) from Al-Ameer College of Engineering, Visakhapatnam and M.Tech (I.T) from Gitam Institute of Technology, GITAM University Visakhapatnam A.P., INDIA .His research interests include, Cloud Computing, Networks security, Web security, Software Engineering and Computer Networks

Mr. P.Ramaiah Chowdary is working as an Asst.Professor, in Department of I.T , Sir C. R. Reddy College of Engg, Eluru, A.P.,India. He has received his B.Tech(I.T) from SSIET, Nuzvid, A.P and M.Tech(S.E.) from Gitam Institute of Technology,GITAMUniversity,VisakhapatnamA.P., INDIA His research interests include Cloud Computing ,Software Engineering, Neural Networks, Fuzzy logic, and Computer Networks.