IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage with ABE Techniques

M. H. Ranadive [1], L. K. Ahire [2]

Student, Computer Engineering, N. M. I. E. T, Talegaon-Dabhade, Pune, India [1]

Assistant Professor, Information Technology, N. M. I. E. T, Talegaon-Dabhade, Pune, India [2]

Abstract: Cloud computing is obtaining popularity because it provides various on demand services which is location independent. Cloud user can store their data on cloud server remotely. Most of them are from different trust domains. Thus cloud data security and privacy becomes critical task. Before storing the data on the cloud server, the data can be encrypted. Attribute-based encryption technique is a public key encryption which enables access control over encrypted data using different access policies and ascribed attributes. Personal health record (PHR) is an emerging health information exchange model, which is always outsourced to be stored on third party, such as cloud server. Before storing the Personal Health Information of Patients and Doctors the attribute based encryption is applied. A public auditing scheme is used which audits the tampered data on the cloud server. This scheme can totally releases the burden of PHR users about storing and maintaining their data on cloud server.

Keywords: Cloud storage, regenerating codes, public audit, privacy preserving, ABE, AES.

I. INTRODUCTION

Cloud computing is the use of computing resources such as hardware and software that are delivered as a service on the Internet. In simple terms, cloud computing is a storing and accessing data and programs over the Internet instead of computer's hard drive. Cloud storage is now gaining popularity because it offers a flexible data outsourcing service with on demand and appealing advantages such as relief of the burden for storage management, universal data access whose location is independence and avoidance of capital expenditure on hardware, software, and personal maintenances. Usually building and maintaining specialized data centers is a quite costly. So the data storage is resided with third party cloud service provider. In such situation, maintaining the privacy of user's data from unauthorized users is not an easy task. Now a day the cloud service is normally faced with a broad range of internal or external adversaries, that maliciously delete or corrupt users data but on the other hand, the cloud service providers can be act dishonestly, attempting to hide data loss and pretending that the files are still correctly stored in the cloud. A one approach is to encrypt the data before it is outsourced to the semi trusted server. To allow data owner to decide with encryption and access mechanism is the best way. Access to original data should only be given to those users having proper decryption key. Whenever the need occurs the data owner should have right to grant and revoke access privileges. One approach is used which is an attribute based encryption. Attribute based encryption is a public key encryption which enables access control over encrypted data using access policies and ascribed attributes. Personal health record (PHR) is an patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers due to the high cost of building and maintaining specialized data centers. Attribute based encryption is applied on PHR data which include doctors and patients data. Public audit ability is enabled between the two cloud storage servers to check the integrity of outsourced data.

II. LITERATURE REVIEW

Following literature is analyzed for existing methodology working and critically evaluated on some evaluation method to find shortcomings from them.

[1] "Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage" Jian Liu, Kun Huang, Hong Rong, Huimei Wang and Ming Xian proposes a public auditing scheme for the regenerating-code-based cloud storage system, where the data owners are privileged to delegate TPA for their data validity checking. To protect the original data privacy against the TPA, They randomize the coefficients in the beginning rather than applying the blind technique during the auditing process. Existing remote checking methods for regenerating-coded data only provide private auditing, requiring data owners to always stay on-line and handle auditing, as well as repairing, which is sometimes impractical. Thus a proxy is used who works in the absence of data owner for solving the regeneration problem of failed authenticators. Thus data owner has no need to always stay on-line. A couple of keys generate a novel public verifiable authenticator which protect original data privacy against the third party auditor and preserve the privacy in cloud storage.

[2] "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption"

M. Li, S. Yu, K. Ren, and W. Lou proposed a patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi trusted servers. To derive fine-grained and scalable data access control for PHRs, they influence attribute-based encryption algorithm to encrypt each patient's PHR file. They divide the users in the PHR system into different security domains that greatly reduces the key management complexity for owners as well as users. A high degree of patient's privacy is assured simultaneously by exploiting multi authority ABE. Personal health record is a patient-centric framework for health information exchange, which is always outsourced to be stored at third party cloud storage. However, there is a wide privacy concern as personal health information could be exposed to those third party cloud servers and to unauthorized parties. This scheme provides scalable and secure sharing of personal health records in cloud computing using Attribute-Based Encryption.

[3] "Enabling data integrity protection in regenerating coding based cloud storage: Theory and implementation"

H. Chen and P. Lee design and implement a practical data integrity protection scheme for a specific regenerating code, while preserving its fundamental properties of fault tolerance and repair-traffic saving. DIP scheme is designed under a mobile Byzantine adversarial framework, and enables a client to verify the integrity of random subsets of outsourced data against malicious corruptions. It works under the simple assumption of thin-cloud storage and allows different parameters to be fine-tuned for a performance security trade-off. This implements and evaluates the overhead of DIP scheme in a real cloud storage test bed under multiple parameter choices. This further analyzes the security strengths of DIP scheme via mathematical models. It demonstrates that remote integrity checking can be feasibly integrated into regenerating codes in practical deployment. This evaluate the running times of different basic operations such as Upload, Check, Download, and Repair, for different parameter choices.

[4] "Towards secure and dependable storage services in cloud computing"

C. Wang, Q. Wang, K. Ren, and W. Lou proposes an effective and flexible distributed storage verification techniques with explicit dynamic data support to ensure the availability of users data in the cloud. It depends on erasure correcting code in the file distribution preparation model to supply redundancies and assurance about the data dependability against Byzantine servers, where a storage server can be fail in random ways. This construction highly minimizes the communication as well as storage overhead as compared to the old replication-based file distribution model. By using homomorphic token with distributed verification of erasure-coded data, this achieves the correctness of storage insurance as well as data error localization, when the data corruption has been detected during the verification of storage correctness. This scheme can give the guarantee of simultaneous localization of data errors and the identification of the misbehaving servers.

[5] "Distributed data possession checking for securing multiple replicas in geographically dispersed clouds"

J. He, Y. Zhang, G. Huang, Y. Shi, and J. Cao provides theories for resolving the Finding an Optimal Spanning Tree in a Complete Bidirectional Directed Graph (FOSTCBDG) problem through counting all the available paths that viruses attack in clouds network environment. Also, This help the cloud users to achieve efficient multiple replicas data possession checking by an approximate algorithm for tackling the FOSTCBDG problem, and the effectiveness is demonstrated by an experimental study. This paper, provide a novel efficient Distributed Multiple Replicas Data Possession Checking (DMRDPC) scheme to overcome the two disadvantages of centre-oriented checking. The DMRDPC scheme first finds an optimal spanning tree to define the partial order of scheduling multiple replicas data possession checking. This is a very complex task, since bandwidths have geographical diversity on different links of different replicas and the bandwidths between two replicas are asymmetric, and thus it is necessary to find an optimal spanning tree with the verifier as the root in a Complete Bidirectional Directed Graph (CBDG), which connects the verifier and all the replicas. Then, according to the scheduling partial order, the data possession checking from the verifier, who checks all of its children, is started. Those replicas that have passed the verification can go on checking the data possession of their children. If some replicas fail in the checking, they can obtain one copy from its parent before they continue checking the data possession of their own children.

[6] "Above the clouds: A Berkeley view of cloud computing"

The goal of Fox, R. Grifth, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica to explain various terms, gives simple formulas to quantify relationship between of cloud and conventional Computing, and identify the top technical and non-technical obstacles as well as opportunities of Cloud Computing. IT organizations have expresses the concerns of major critical issues such as security that exist with the widespread implementation of cloud computing. These types of concern come from the fact that data is stored remotely from the customer's location; it can be stored at any location. Security is most argued-about issues in the cloud computing field; many enterprises look at cloud computing warily due to projected security risks.

III.SYSTEM ARCHITECTURE

In Cloud Computing most of the cloud users and cloud service providers are from different trust domains. It turns out that on one side sensitive data should be encrypted before uploading to the cloud servers; on the other side, a secure data access control mechanism should be provided before cloud users have the liberty to outsource sensitive data to the cloud storage. Similar to any un trusted storage case, generated issue's can be resolved by using a cryptographic-based data access control mechanism. Under the multi-owner settings, a novel ABE-based model

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

for patient-centric secure sharing of PHRs is presented in cloud computing environments. To address the key management challenges, it conceptually divides the users in the system into different types of domains, i.e. public and personal domains (PSDs). In Cloud Computing, Cloud users could access the system via various low-end devices such as mobile phones, which do not have much computation power. Therefore, the proposed access control mechanism should be efficient enough in the sense that the computation load addressed on both the PHR Admin and PHR Users should be affordable to these low-end devices. Keeping these challenges in mind, a cryptographic based data access control mechanism for Cloud Computing with ABE is proposed.

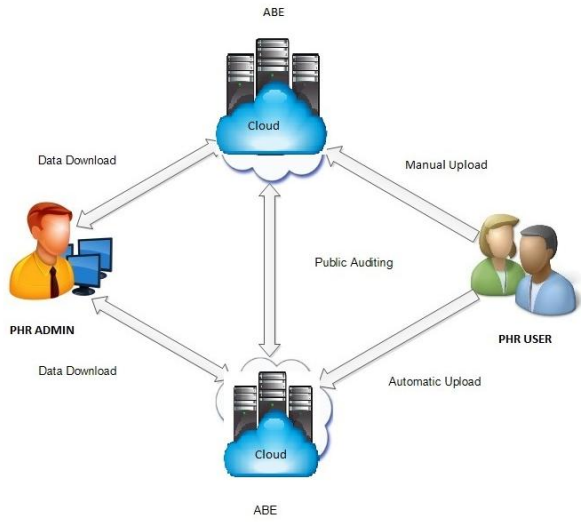

Fig 1: System Architecture

Fig 1 shows the system architecture. This architecture has four necessitates parties in a network:

1) The PHR USER
The PHR USER can manually upload the data on the cloud server.
2) The cloud server (CS)
Uploaded data is encrypted by using ABE. Cloud Server will store the encrypted data. Cloud Server provides high-quality services utilizing a number of servers with considerable storage space and computation power.
3) The PHR ADMIN
PHR ADMIN can download the data on the cloud. Before the download, data is decrypted by using ABE. PHR ADMIN can store the downloaded data on another one cloud server.
4) The Cloud Server (CS)
PHR ADMIN has the only access of this cloud server. PHR ADMIN can upload and download the data from this cloud server. Thus the PHR USER data automatically uploaded on the second cloud.

Public Auditing is done by the PHR ADMIN. To preserve the data integrity, PHR ADMIN will compare the data with second cloud server. Thus PHR USER has no need to stay on-line continuously.

A. Algorithm
I) ABE:
An attribute based encryption scheme consists of four fundamental algorithms: Setup, Key Generation, Encryption and Decryption.

1) Setup
The setup algorithm takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK.

2) Key Generation (MK, S)
The key generation algorithm takes as input the master key MK and a set of attributes S that describe the key. It outputs a private key SK.

3) Encryption (PK, A, M)
The encryption algorithm takes as input the public parameters PK, a message M, and an access structure A over the universe of attributes. The algorithm will encrypt M and produce a ciphertext CT such that only a user that possesses a set of attributes that satisfies the access structure will be able to decrypt the message. Assumption is that the ciphertext implicitly contains A.

4) Decryption (PK, CT, SK)
The decryption algorithm takes as input the public parameters PK, a ciphertext CT, which contains an access policy A, and a private key SK, which is a private key for a set S of attributes. If the set S of attributes satisfies the access structure A then the algorithm will decrypt the ciphertext and return a message M.

IV. EXPERIMENTAL RESULTS

The system is built using C# .Net to evaluate the efficiency and effectiveness. The experiments performed on P IV processor, 512MB RAM under Windows 7. The system requires Internet Modem as specific hardware to run; any standard machine is capable of running the application.
For experiments, Google spreadsheets and sales force spreadsheets is used as a dataset to store the data on the cloud storage server. Users can upload spreadsheets directly from their computers. Table 1 gives comparison of Computation values for number of records of Doctor, Patient and Staff.
Fig 2 shows the public auditing result for the number of records of doctor, patients and staff. The values taken for the graph are randomly selected values.

Table 1
Computation values on varying on no of users

Doctor	Patient	Staff
10	20	100
20	30	3
4	100	70
6	4	200
100	8	40

DOI 10.17148/IJARCCE.2016.5698

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

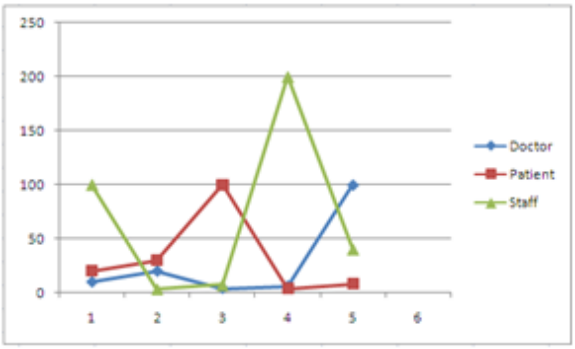

Fig 2: Auditing result on number of users

V. CONCLUSION

Cloud Computing is a field of plenty of challenges and of paramount importance, is still in its infancy now, and many research problems are yet to be determined. System uses encryption or decryption keys of user's data and remotely stores on the server. Every storage server has an encrypted file system that encrypts the client's data and stores that data on cloud server. The system guarantees that the client's data is stored only on trusted storage servers and it cannot be accessed by intruders. Administrator can perform auditing tasks. Resulted encryption method is secure and easy to use.

ACKNOWLEDGMENT

We would like to extend sincere gratitude towards our guide Prof**. L.K. Ahire** (PG Coordinator), Prof. **S. B. Ingle**, HOD (Comp dept., NMIET, Talegaon) who have been there for constant guidance and provided support to achieve success in our endeavor.

REFERENCES

[1] Jian Liu, Kun Huang, Hong Rong, Huimei Wang, and Ming Xian. "Privacy-preserving public auditing for regenerating-code-based cloud storage". 2013.

[2] 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", Parallel and Distributed Systems, IEEE Transactions on, 24(1):131,143, 2013.

[3] Armando Fox, R. Grifth, Anthony Joseph, Randy Katz, Andrew Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, and Ion Stoica. "Above the clouds: A Berkeley view of cloud computing," Dept. Elect. Eng. Comput. Sci., Univ. California, Berkeley, CA, USA, Tech. Rep. UCB/EECS-2009-28, 2009.

[4] Henry CH Chen and Patrick PC Lee. "Enabling data integrity protection in regenerating- coding-based cloud storage: Theory and implementation", Parallel and Distributed Systems, IEEE Transactions on, 25(2):407- 416, 2014.

[5] Giuseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring, Lea Kissner, Zachary Peterson, and Dawn Song, "Provable data possession at untrusted stores", In Proceedings of the 14th ACM conference on Computer and communications security, pages 598-609. Acm, 2007.

[6] [6] Shafi Goldwasser, Silvio Micali, and Ronald L Rivest, "A digital signature scheme secure against adaptive chosen-message attacks", SIAM Journal on Computing, 17(2):281-308, 1988.

[7] Jing He, Yanchun Zhang, Guangyan Huang, Yong Shi, and Jie Cao,"Distributed data possession checking for securing multiple replicas in geographically-dispersed clouds", Journal of Computer and System Sciences, 78(5):1345-1358, 2012.

[8] Hovav Shacham and Brent Waters, "Compact proofs of retrievability", In Advances in Cryptology-ASIACRYPT 2008, pages 90-107. Springer, 2008.

[9] Cong Wang, Qian Wang, Kui Ren, Ning Cao, and Wenjing Lou. "Toward secure and dependable storage services in cloud computing". Services Computing, IEEE Transactions on, 5(2):220-232, 2012.

[10] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-replica provable data possession," in Proc. 28th Int. Conf. Distrib. Comput. Syst. (ICDCS), Jun. 2008, pp. 411–420.