Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 46 (2015) 719 – 724

Procedia Computer Science

International Conference on Information and Communication Technologies (ICICT 2014)

Fine Grained Access Control and Revocation for Secure Cloud Environment - a polynomial based approach

Lija Mohan[a] and Sudheep Elayidom M.[b]

[a,b] *Department of Computer Science, Cochin University of Science & Technology, Ernakulam, Kerala, India.*

Abstract

Cloud Computing has been emerged as a prominent technology where users can upload their data and do their processing using shared resources. But there always exist a tradeoff between the performance and security of a system. The same is applicable for cloud systems also. One of the major drawback associated with Cloud computing is related to its data privacy concerns, because the service provider can access the user data on the cloud at any point of time. Hence they could accidentally or intentionally distribute, modify or even delete our information. Hence the owner should have implemented mechanisms for preventing unauthorized access to his information. This paper proposes a secure cloud environment for storing user's files which is also capable of granting fine grained access control to data. Basic cryptographic schemes along with bivariate λ-degree, symmetric polynomials are utilized for achieving this. A flexible user access revocation scheme has also been proposed.

Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies (ICICT 2014)

Keywords: ***cloud; security; polynomial; cryptography; fine grained access control***

1. Introduction

Cloud computing explores a new world of opportunities for businesses where users can upload their data and do their processing using shared resources. Improved performance, improved document format compatibility, reduced

* Corresponding author. Tel.: 09846994287
E-mail address: joinlija@gmail.com

Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies (ICICT 2014)
doi:10.1016/j.procs.2015.02.133

software costs, instant software updates, unlimited storage capacity etc are some of the advantages of cloud, but a number of security challenges need to be considered and addressed before adopting a cloud computing strategy. Cloud computing security challenges include data protection and user authentication where former deals with securing the data both at rest and in transit where as latter deals with limiting access to data and monitoring who access the data.

Encryption[10] is a solution for achieving secrecy of data. Only authorized users will possess key for decrypting data, thus making the data hidden from cloud server. But to implement fine grained access control different files should be encrypted with different keys and these keys should be distributed to users based on their access privilege. But as number of files increases, number of keys to be shared also increases and makes this system less scalable. To eliminate such difficulties we propose a polynomial based system were security of the data is implemented using encryption and fine grained access control is provided using secure λ-degree polynomials. The polynomials can be organized as a pool and files can be made associated to shares of different polynomials. Authorized users will also be provided with shares of respective polynomials, depending on their access to a file.

With respect to the points mentioned above we formulated the objective of our system as:

To design a secure cloud storage application where

- Owner can securely upload his files with minimum cryptographic operations.
- Users could be added and removed dynamically.
- Fine grained Access control of data should be provided.
- Easy Method to perform file access revocation of a user.
- Data should be hidden from cloud provider.

The remaining sections of the article is organized as : Section 2 covers Related Work, Section 3 specifies the Problem Statement, Section 4 provides a brief introduction to polynomial based Pairwise Key Sharing Approach, Section 5 illustrates the system architecture, Section 6 analyzes the security of the system and finally Section 7 concludes the article.

2. Related Work

Several types of cloud data security issues have been identified and rectified[2,3,4] with the advancement of research. Cryptographic operations[5] has got significant position in ensuring cloud data security, i.e. before uploading any data to cloud, encryption should be performed by owner and to retrieve the data at user side, decryption is done. RSA[6] algorithm can be used to implement digital signatures for cloud security. But here once the access is granted, it cannot be changed, also fine grained access control is not possible. Fine grained access control and user revocation can be provided in cloud by using one to many encryption scheme like attribute based encryption(ABE)[7]. But the method needs intensive computation and requires a lot of cryptographic operations for implementation.

Our aim is to implement a secure cloud environment where owner can upload data, by using any symmetric encryption technique and should provide fine grained access control to files without using any compute intensive operations. Here we make use of Blundo Scheme[1], a t-variate polynomial based secret sharing for providing fine grained access control and Lagrange interpolation for User Access Revocation. The method has been widely used for implementing secure key exchange in dynamic conference systems, wireless sensor networks[8] etc. Since symmetric encryption is used, only authorized users can decrypt the data, also for the cloud service provider, the data will be hidden. By creating a secure random λ-degree symmetric polynomial pool, and allocating shares of these polynomials to different users and files based on the access policy specified by owner, ensures fine grained

access control. If at later stage owner want to revoke the access of a particular user, interpolation can be applied to form a new polynomial from the remaining shares without effecting other users and files.

A λ -degree symmetric polynomial secret sharing scheme is proved to be λ –secure[1], i.e. only if 'λ' users are compromised, the attacker can gain access to a file.

3. Problem Statement

Bob need to upload some confidential information like his Health Record, Conference Schedule, Company Data, Research work etc. to Cloud.

The requirements are:

i. Only authorized users can view Bob's documents.

ii. From among the authorized users, different users are given different access permissions. For e.g. His Professors can only see his research work, Company employees can only see the company data etc.

iii. In case any dispute arises with a user, Bob should be able to revoke that user's access to the respective files without affecting other peoples.

iv. Cloud Storage Provider should not be able to view the contents of any of Bob's files.

4. Polynomial Based Pairwise Key Sharing Approach

To pre-distribute the pair wise keys, generate a bivariate t-degree polynomial $f(x, y) = \sum_{i,j=0}^{t} a_{ij} x^i y^j$ over a finite field F_q, (here q is a large prime), such that the polynomial possess the property of $f(x, y) = f(y, x)$. (i.e. the polynomial should be symmetric). It is assumed that each entity (file and user) has a unique ID. For each entity i, the application computes a polynomial share of f(x, y), that is, f(i, y). This polynomial share is distributed to entity i. Thus, for a user u1 to access file f1, then u1 can compute key f(u1,f1) by evaluating f(u1,y) at point f1 and application computes encryption key of file f1 for user u1, f(f1,u1) by evaluating f(f1,y) at point u1. Due to symmetric property of polynomial, f(u1,f1) = f(f1,u1) . Thus the entities u1 and f1 establish a pair wise common key.

5. System Architecture

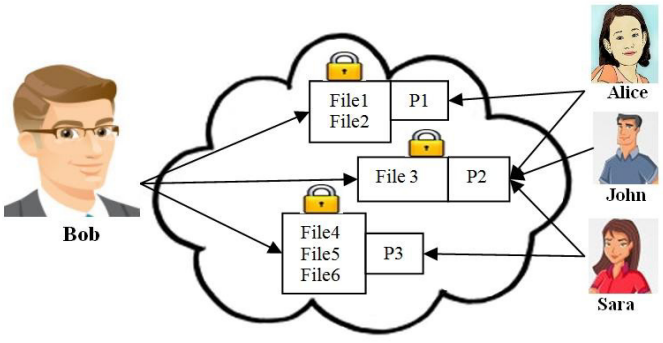

Fig. 1. Architecture for Storing Files in Cloud Server. Each file is associated with a Polynomial, P

Figure 1 gives an overview of the architecture followed for implementing secure file storage in cloud. Here Bob uploads different files encrypted with his secret key to the cloud. Since the file is encrypted, cloud server does not have visibility to the content of files. For each file Bob should associate a λ-degree random polynomial. If different files have same access policy, then they can share the same polynomial. For e.g. in figure File1 and File2 are having same access policy; hence they share the same polynomial P1. Each file will be assigned with a share of its associated polynomial. For e.g. in figure, Share of P1 will be assigned to File1 and File2. In addition to this, each authenticated user will be rewarded with a share of the Polynomial depending on his/her accessibility to the file. In figure, Sara possess shares of Polynomials, P1 and P2, therefore she can access files File3, File4, File5 and File6, where as John can access only File3 because has got only share of P2.

5.1 Granting Access to a File:

If an authenticated user request for a file, the cloud server will provide the file, encrypted with the key obtained by substituting the unique id of user in that file's share of polynomial. To decrypt it, user should generate the key by substituting file's identity in his own share of polynomial. According to Blundo scheme[1], if the λ-degree polynomial associated with the file is symmetric, then the encryption key obtained by substituting user's id in the File's share will be same as decryption key obtained by substituting File's identity in user's share. Thus only users having share of the polynomial will be able to decrypt the file.

5.2 User Revocation:

If some conflict occurs with any of the existing user's then Bob can revoke their access to corresponding files without affecting other users. In the figure, suppose Bob need to revoke the access of SARA then he assigns a new polynomial for File3 by using shares of File3, John and Alice, also compute new Polynomial to File4, File5 and File6 by combining each of these file's share and John's share. Therefore with the existing shares Sara could not access the files again.

For creating a new polynomial from existing shares, Bob can use Lagrange Interpolation. While interpolating, to obtain a polynomial of degree t, there should be t+1 shares. This idea can be used in our approach to generate a new polynomial from existing shares. i.e.

i) If number of shares (excluding share of user whose access is to be withdrawn) < t+1 :
   Interpolate the shares to generate a new polynomial.
ii) Else if number of shares (excluding share of user whose access is to be withdrawn) >= t+1 :
   Divide the shares into groups such that each group contains less than t-1 shares. Interpolate each of these groups to obtain a new polynomial. Associate the polynomials with corresponding files.

As a result of user revocation, one file may get associated to more than one polynomial and hence acquire more than one share. In that case to generate the correct encryption key for a user, the application should know the polynomial to which user is associated. To discover a common polynomial, initially when the user request for a file access he should add two more fields: MSG and $E_{PWK}(MSG)$; i.e. a "message" (generated randomly) and that "message" encrypted with the pairwise key. On receiving these data, the cloud application can verify which of the polynomial's share is being used for generating the key 'K' by substituting the user's id in all polynomial shares associated with the file and verifying whether $E_k(MSG)=E_{PWK}(MSG)$.

6. Security Analysis

This section analyzes the performance of our system with respect to 2 aspects:

i. *The security of our system*
ii. *Accurate Symmetric Polynomial Derivation by Lagrange Interpolation*

Let n be a positive integer, $Z_n = \{0,1,2\ldots, n-1\}$ and $S_n = \{1, 2,\ldots, n\}$; p is a prime number, $F_p = Z_p = \{0, 1,\ldots,p-1\}$ is a prime finite field with p elements, and F_P^* is the multiplicative group of F_p; $Z^s{}_r = \{x_0, x_1,\ldots, x_{s-1}) | \text{ xi } \varepsilon\ Z_r\}$, when r = p is a prime, Z_m^p is an m-dimensional linear space defined over F_p; $F_p[x]$ represnts the set consisting of all polynomials with coefficients in F_p; and let $P\{A = t\}$ represents the probability of an event that a discrete random variable A takes some random value 't' in a sample space.

6.1 Definition of Symmetric Polynomials:

A symmetric m-variate[9] polynomial of degree k containing 'm' variables is defined as

$$F(x_1,\ldots, x_m) = \sum_{(j1,\ldots,jm)\ \varepsilon\ Zmk+1} a_{j1\ldots jm}\, x_1^{j1}\ldots x_m^{jm},\ a_{j1}..a_{jm}\ \varepsilon\ F_p \tag{1}$$

where $F(x_1, \ldots, x_m) = F(x_{\sigma(1)}, \ldots, x_{\sigma(m)})$ for any permutation $\sigma(x)$ of $S_m = \{1,2, \ldots, m\}$.

Here equation (1) can be rewritten as :

$$\boldsymbol{F}(x_1, x_2, \ldots, x_m) = \sum_{j\varepsilon S} a_j \sigma \tag{2}$$

here $j = (j_1,j_2, ..., j_m)$ with $0 \le j_1 \le j_2 \le \ldots \le j_m$, $j_i\ \varepsilon\ Z_{k+1}$,
perm(j) denotes the set consisting of all permutations on j,

$$S = \{j= (j_1,j_2, \ldots, j_m)\} \mid \ 0 \le j_1 \le j_2 \le \ldots \le j_m \le k\ \},\ aj = a_{j1}, \ldots, a_{jm} \text{ and } \sigma_j = \sum_{(j1', \ldots, jm')\ \varepsilon\ perm(j)} x_1^{j1'}, \ldots, x_m^{jm'} \tag{3}$$

T(t, m) denotes the cardinality of set S. Here T(t,m) equals the distinct m objects chosen from set with t+1 elements. Hence :

$$T(t, m) = |S| = \binom{m+t}{t}$$

This is equal to the number of coefficients of a symmetric polynomial in m variables with degree k. Thus any T(t, m) random values from F_p determines a symmetric *m*-variate polynomial of degree t.

6.2 T-secure system

A t-degree bivariate polynomial is always (t + 1)-secure, because the adversaries must compromise atleast (t + 1) nodes holding valid shares of the same polynomial to reconstruct the secret. This has been proved[1]. According to our studies, Blundo scheme can be made more secure by selecting coefficients of the symmetric polynomial $F(x_1, \ldots, x_m)$ in *m* variables of degree t uniformly from F_p.

6.3 Correctness Proof for User Access Revocation

To revoke the access of a user from a file, owner associates a new polynomial (constructed from remaining shares using Lagrange interpolation) to that file such that revoked user cannot access the file with his share.

Proof:

For a polynomial $f(y_1, y_2, ..., y_k)$, the partial degree of y_i is defined as the maximum partial degree of y_i among all its monomials. Then the interpolation formula for symmetric functions is as follows:

Let x_1 , x_2 , ..., x_n be n distinct points, and let f(y_1 , y_2 , ..., y_k) be a symmetric function whose partial degrees are not greater than n - k. Then, for $1 \leq k < n$, we have

$$f(y_1, y_2, \ldots, y_k) = \sum_{I<n,\ |I|=K} f(x_{i1}, x_{i2}, \ldots, x_{ik}) \prod_{y \in Y,\ j \in J} (y - x_j) \Big/ \prod_{i \in I,\ j \in J} (x_i - x_j) \quad (4)$$

for k=1 the above equation reduces to the classical Lagrange interpolation formula:

$$f(x) = \sum_{i=1}^{n} f(x_i) \prod_{j \neq I} x - x_j / x_I - x_j,$$

where f (x) is a polynomial of degree not greater than n-1. Because the numerator in (4), $\prod_{y,\ j}$ (y-x_j) is symmetric in y_1 , y_2 , ..., y_k , this interpolation formula can hold only for symmetric functions. Since f (y1 , y2 , ..., yk) is symmetric, the summand in (4) is symmetric both in x_{i1} , x_{i2} , ..., x_{ik} , and in x_{j1} , x_{j2} , ..., x_{jn-r}. We can also say that for any subset i1<i2< … <ik of [n], (4) holds for (y_1 , y_2 , ..., y_k)=(x_{i1} , x_{i2} , ..., x_{ik}), just like the classical Lagrange interpolation formula.

Thus it is proved that, applying the Lagrange interpolation to F(x_1, x_2, …, x_m) for i = 1, 2, …, k + 1, the m-variate symmetric polynomial defined by (1) can be recovered by:

$$F(x_1, x_2, \ldots, x_m) = \sum_{i=1}^{k+1} F(i, x_2, \ldots, x_m) \prod_{j=1\ j \neq I}^{k+1} X_I - j / i - j.$$

7. Conclusion

This paper proposed a simple and secure framework for storing user's data in the cloud. For implementing pulverized access control, Blundo polynomial sharing scheme is implemented which is proven to be λ- collusion resistant. The framework allows flexible access revocation capability also. Revocation is achieved using interpolation which does not require any change in other user's shares. Security analysis of our system shows that the method is secure as well as correct while creating new polynomials after user access revocation. Modifying Blundo scheme with grid based implementation can reduce the communication overhead in identifying the polynomial to which a user is associated. This is a part of our future work.

References

1. C. Blundo, U. Vaccaro, A. Herzberg, M. Yung, A. De Santis and S. Kutten , Perfectly-Secure Key Distribution for Dynamic Conferences, 12th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO '92), pp. 471-486, 1993.
2. A.Behl, Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation, 2011 World Congress on Information and Communication Technologies (WICT), Page(s): 217 – 222.
3. F.B. Shaikh, Security threats in cloud computing, 2011 IEEE International Conference for Internet Technology and Secured Transactions (ICITST), Pages 214 – 219.
4. Wentao Liu, Research on cloud computing security problem and strategy, 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 2012 .
5. Yasin Akhtar Raja & Shaftab Ahmed, Tackling Cloud Security Issues and Forensics Model, IEEE, 2010, pp. 190-196.
6. Somani U., Lakhani K., Mundra, M., Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing, 1st International Conference on Parallel Distributed and Grid Computing (PDGC), 2010.
7. Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, Wenjing Lou, Scalable and Secure Sharing of Personal HealthRecords in Cloud Computing Using Attribute-Based Encryption, IEEE Transactions on Parallel and Distributed Systems, Volume: 24, 2013.
8. Rasheed A, Mahapatra R.N, The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks, IEEE Transactions on Parallel and Distributed Systems, Volume: 23, 2013.
9. Taub, H.; Gutman, S. , A symmetric matrix criterion for polynomial root clustering, Page(s): 243 – 248, 1990.
10. Rui Zhang, PeiShuai Chen, A dynamic cryptographic access control scheme in cloud storage services, 8th International Conference on Computing and Networking Technology (ICCNT), 2012 .