ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

Cost-Effective Data Sharing with Outsourced Revocation Using Forward Security in Cloud

Archana Shelke, Prof. Prashant Joshi

Dept. of Computer Engineering, GHRIET, Wagholi, Pune, India

ABSTRACT: Data sharing has never been easy with the advancement of cloud computing. The correct study on the shared data provides number of benefits to both the society and individuals. Storage-as-a-service obtainable by cloud service providers (CSPs) is paid ability that enables organizations to delegate their sensitive data to be stored on inaccessible servers. This paper proposes a cloud based storage method that allows the data proprietor to benefit from the convenien ces offered by the CSP and enables trust between them. Identity-bas- ed (ID-based) ring signature, which removes process of certificate verification, can be used as a alternate. In this paper, we proposed the security of ID-based ring signature by providing forward safety: If a top secret key of any user has been compromised, all preceding generated signatures that include this user still longer valid. This pro-perty is specially important to any large scale data distribution system, as it is not possible to ask all data owners to again authenticate their data even if a secret key of any user has been compromised. It allows the proprietor to funding or revoke admittance to the outsourced data

KEYWORDS: Forward Security; Identity-based signature; revocation; Outsourcing; Cloud computing.

I. INTRODUCTION

Nowadays, cloud computing is becoming more popular as an emerging technology. It provides number of computing resources to users. Many companies and people can outsource time-consuming computation workloads to cloud without spending the additional capital on deploying and maintaining hardware and software. Outsourcing computation has paying attention and researched widely. Cloud computing provides user with number of storage resources for storing data. Cloud Storage is one of the most important services of cloud computing [2].

Although this cloud computing provides number of benefits to users. It brings new security challenges. One of the most security challenges is how to check integrity of the data stored in cloud. When number of participants involved in data sharing, then we must take into account a number of issues, like efficiency, data integrity and privacy of data owner.

To construct an anonymous and authentic [1] data sharing system, ring signature is a relevant solution. Ring signature allows data owner to secretly confirm the data which is present in the cloud [1] [2].

The Certificate verification procedure has been removed by Identity-based (ID-based) ring signature. By providing forward security to the ID-based ring signature, the overall security can be improved i.e.: If a private key of the user has been compromised, all past exist signatures that include this user still applicable.

A. Motivation

ID-based ring signature is the best possible trade off among efficiency, data authenticity and anonymity. It provides a better solution on data sharing with a number of participants. To obtain a higher level protection, one can add more users in the ring. By doing this increases the possibility of key exposure.

Key exposure is the main drawback for normal digital signatures. If the secret key of a user is compromised, all signatures of that user become insignificant: future signatures are ineffective and no previously generated signatures can be trusted. When a key leakage is identified, key revocation schemes must be called instantly in order to avoid the generation of any signature using the compromised secret key. But this solution does not solve the problem of forgeability for past signatures.

To avoid this problem the idea of forward secure signature was suggested to maintain the validity of past signatures even if the current secret key is compromised.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

II. LITERATURE SURVEY

Following are the abstracts of the most relevant research works.

A. Forward Secure Digital Signature Scheme

In [3],authors have proposed the forward digital signature scheme in which, public key is kept fixed but secret key is updated is updated at regular intervals to provide forward security property: compromise of the current secret key does not enable an adversary to forge signatures of the past. This minimizes the harm caused by key exposure problem. Past signature remain secure even if exposure of the current secret key. In this scheme key redistribution is not required. This scheme is based on the Fiat Shamir identification scheme [4] and the Ong-Schnorr identification scheme [5]. This scheme is proven to be forward secured based on the hardness of factoring, in the random oracle model. The construction of this scheme is quite efficient.

B. Forward secure Threshold signature scheme

In [6], authors have constructed forward-secure threshold signature schemes. This scheme is having following characteristics: even if more than the threshold number of players is compromised, it is not possible to fake signatures relating to the past. This characteristic is achieved while keeping the public key fixed and updating the secret keys at regular intervals. The schemes are rationally efficient in that the amount of secure storage, the signature size and the key lengths do not vary proportionally to the number of time periods during the lifetime of the public key.

Author has suggested two forward secure threshold signature schemes. These are Multiplicative secret sharing and Polynomial Secret Sharing. The disadvantage of the multiplicative secret sharing scheme is that n honest players are required to participate in the signing and the refreshing protocols. Both proposed schemes are depends on the Bellare-Miner forward-secure signature scheme [3]. This scheme uses multiplicative secret sharing and tolerates mobile eavesdropping adversaries. The second scheme is based on polynomial secret sharing. It suffers from mobile halting adversaries.

C. Security and Privacy-Enhancing Multicloud Architectures

The fundamental concept is to operate number of different clouds at the same time to lessen the threat of maleficent data manipulation and disclosure. By integrating number of different clouds, the trust assumption can be lowered to assumption of non-collaborating cloud accommodation providers. This setting makes it a lot of harder for an external attacker to retrieve hosted data. These approaches are operating on the different cloud accommodation level [7][9].

D. Identity-based Ring signature scheme

In [10],the need for validity checking of the certificates and the need for registering for a certificate are eliminated by identity based cryptosystems for getting the public key. For the efficiency and the authenticity of ring sig-nature, these two features are beneficial where a utilizer can secretly sign a message on behalf of a group of conscripted users and considering the authentic signer also.

III. PROBLEM STATEMENT

The Proposed system called forward secure ID-based ring signature, which is an essential tool for building cost-effective authentic and anonymous data sharing system [1].

a. The proposed system provides formal definitions on forward secure ID-based ring signatures.
b. The proposed system presents a concrete design of forward secure ID based ring signature like trustworthy third party authenticity of data by including key for validation.

IV. IMPLEMENTATION DETAILS

A. Proposed System Architecture

Forward secure identity based ring signature in the cloud suggests data sharing should be done in a well-organized manner. This architecture provides multiple cloud environments for enormous data sharing in secure way. Client in the figure represents individual cloud accommodation utilizer. The cloud servers may be residing in different physical locations. The storage of the data depending upon available spaces in the server is decided by CSP.The ring formation of users is offered by the identity based ring signature. The secure data transmission is performed by well organized encryption and decryption techniques.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

The components of the proposed system are CSP (Cloud Storage Service Provider), TTP (Trustworthy Third Party), Data Owner, Authenticate user.

The fig.1 shows the Proposed System architecture.

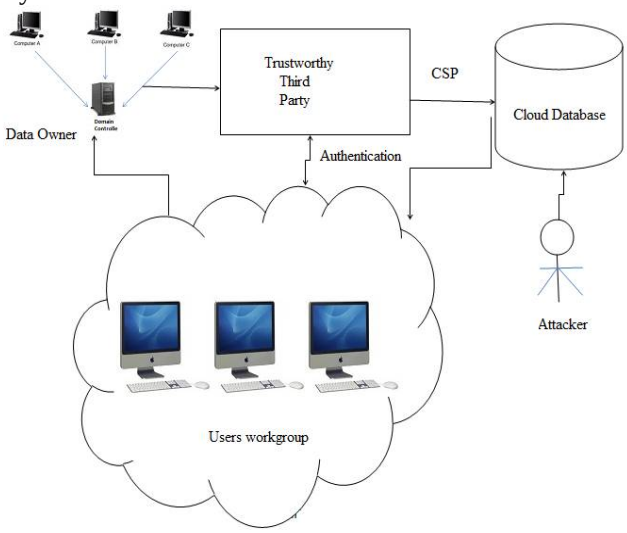

Fig 1: ***Proposed System Architecture***

a. Data Owner

Data Owner wishes to save and share data over cloud. Data owner does not know where his information will be stored by the CSP.

Data owner wants that his information should not be observable to the CSP, as data is most significant for him. To fix this issue, the TTP is available. Before uploading the data, it's encrypted and TTP is set to keep watch.

b. Trustworthy Third Party(TTP)

Database auditing involves the actions of the database users. Database administrators (DBA) regularly set up auditing for the security purposes.

Auditing is associated with monitoring and recording of user selected database activities. Auditing might be based on combinations of variables that can include user name, program, time, etc. For example when specified components within an Oracle database are obtained or changed the contents within a given object, then auditing can be triggered by security policies.

The DBA can collect data about which tables are being updated, how many logical I/Os are performed, or how many concurrent users can be connected at peak times.DBA also finds information related with an authorization and access control execution.

c. Authenticate User

Authenticate User is a client of data owner who has all rights to access the remote data.

d. Cloud Storage Service Provider (CSP)

Cloud Storage Services Provider provides database. It allows data owner to keep any kind of information. CSP also allows to the user to make the user defined database schema. According to user requirement the space for the user instance will be allocated by CSP.

B. ALGORITHMS

Algorithms for the proposed system are as follows:

a. AES128 16-bit Algorithm

Generate user u1 ID; Set of users u1's attribute -> Domain B;
All Attribute check in Domain manager;
Now, Generate RandomValue[unique] attribute = j;
Generate Random value [user] = r1;

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

Secret key= (j+r1).user u1's ID;
Encrypting user data along with ID
Encrypt (user ID. (j+r1)+data)
Decrypting user data along with ID
Decrypt (user ID. (j+r1)+data)

b. SHA 256 Algorithm

Input: string required to calculate the SHA score.
Output: SHA score of string
Step 1: Padded with the length in such way that the result is multiple in minimum 512 bit long.
Step 2: Parse into 512 bit message blocks M(1),M(2)…….. M(n) the message block can process at one time using the initial hash values H(0).
Step 3: Then compute the sequence
H(i) = H(i1)+ CM(i) (H(i1));
Step 4: return the H(i) SHA score of given string.

c. User level Access Control Algorithm

Domain A1= {user m1, user m2, user m3….user mn}
Domain B1= {user n1, user n2, user n3…user nn}
Domain C1= {user u1, user u2, user u3…. user un}
Roles = {Domain Manager, Domain Provider, Data owner}
Permissions = {R, W, RW}
For user m2 request resource in Domain A1

```
 {
   if (user m2 attribute ID matches)
      {
         Data owner checks user m2 ID;
      //user m2 attribute ID has been stored in DO1
           Grants Access;
       }
    Else Access forbidden;
 }
Else if (user m2 attribute not matches)
{
   Data Owner checks for the user m2 roles & permission
   If (Authorized person in Domain A1)

{  Domain A1 saying that Resource not available; }
 }
}
```

d. Cross domain achieving access Algorithm

For user u1 request resource in Domain B1

```
  {
     if ( user u1's ID==TRUE)
       {   user u1's ID available in Domain C1;
           Domain C1== user u1's ID;
           Domain B1 checks user ID in Domain Manager;
           Grant access to user u1;
        }
Else {
```

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

Access forbidden; }}

C. MATHEMATICAL MODEL

Let, Parties (l_1, l_2,..., l_t) can compute a (t, n)-ring signature, σ, on a message, m, on input (m, SK_{l1}, SK_{l2}, ..., SK_{lt}, PK_1, ..., PK_n).

A Signature scheme is a triple of probabilistic polynomial time algorithms, (G, S, V), satisfying:

G (key-generator): generates a public key, pk, and a corresponding private key, sk, on input 1^n, where n is the security parameter.

S (signing) : returns a tag, t, on the inputs: the private key, sk, and a string, x.

V (verifying) : outputs *accepted* or *rejected* on the inputs: the public key, pk, a string, x, and a tag, t.

System S = {Ts, DataOw, Ttp,CSP,Usr, F(i)}
Where
Ts= Current timestamp
DataOw= Data owner
Ttp= Trusted third party
CSP =Cloud service provider
Usr=end user
F(i)= ith file uploaded by user.

DataOw ∑ F(i)

Ttp ∞ Usr (including all users verification)

V. RESULT AND DISCUSSION

For the proposed system performance evaluation, we calculate matrices for accuracy. We implement the system on java 3-tier MVC architecture framework with INTEL 3.0 GHz i7 processor and 8 GB RAM. Here each graph shows the system performance with different experiments that has been classified in graphs. Finally system deploys on Amazon EC2 public cloud [16] with single virtual machine (VM) and got the results as below.

Here in graphs, X axis shows the total number of user and Y shows the time required in milliseconds for performing such operation.T is the transactions.

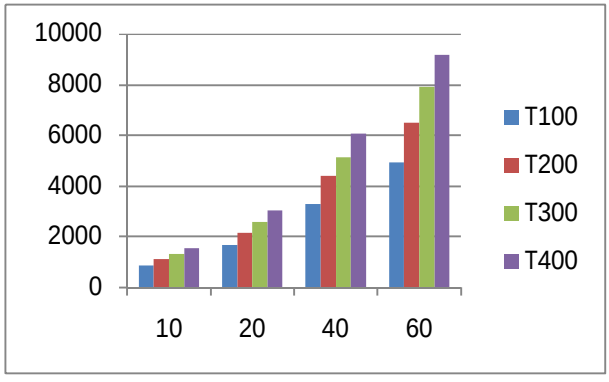

Fig 2. ***The average time for the data owner to create signature, when key size 512 bit***

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

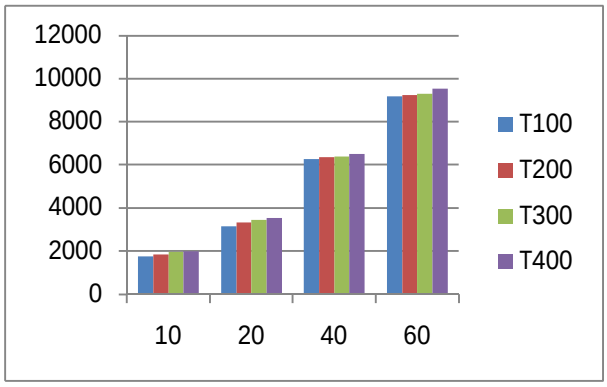

Fig 3. ***The average time for the service provider to verify the ring signature***

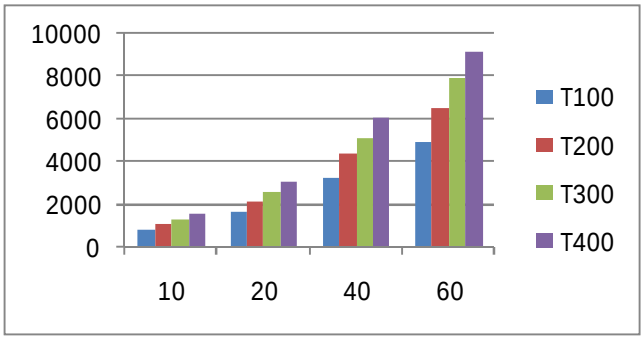

Fig 4. ***The average time for the TTP to verify the SHA score from end user***

VI. CONCLUSION AND FUTURE WORK

The Forward Secure ID-based Ring Signature supports an ID-based ring plan to prove forward security. For this plan any matching operation is not required. The period of mystery key is only one whole number, while the key upgrade handle just requires an exponentiation. This will be tremendously utilized in many applications, particularly to those need more security, for example, e-business exercises, e-contract signing and e-auction. The framework with multi-cloud framework [9] improves the effectiveness, sizably voluminous capacity and information sharing framework. For this experiment, it requires less space and less time. This property minimizes the cost factor.

REFERENCES

[1] Xinyi Huang, Joseph K. Liu+, Shaohua Tang, Yang Xiang, Kaitai Liang, Li Xu, Jianying Zhou,"Cost-Effective Authentic and Anonymous Data Sharing with Forward Security" IEEE TRANSACTIONS ON COMPUTERS VOL: 64 NO: 6 YEAR 2015

[2] Jia Yu, Kui Ren, Senior Member, IEEE, and Cong Wang, Member, IEEE," Enabling Cloud Storage Auditing with Verifiable Outsourcing of Key Updates" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. , NO. , 2015

[3] M. Bellare and S. Miner. A forward-secure digital signature scheme. In Crypto'99, volume 1666 of Lecture Notes in ComputerScience, pages 431–448. Springer-Verlag, 1999.

[4] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," Advances in Cryptology { Crypto 86 Proceedings, Lec. Notes in Comp.Sci. Vol. 263, A. Odlyzko ed., Springer-Verlag, 1986.

[5] H. Ong and C. Schnorr, "Fast signature generation with a Fiat-Shamir like scheme,"Advances in Cryptology { Eurocrypt 90 Proceedings, Lec. Notes in Comp. Sci. Vol. 473,Damgfiard ed., Springer-Verlag, 1990.

[6] Forward-Secure Threshold Signature Schemes Michel Abdalla Sara Miner Chanathip Namprempre The extended abstract of this work appears in D. Naccache, editor, Topics in Cryptology {CT-RSA 2001, Volume 2020 of Lectures Notes in Computer Science, San Francisco, CA, USA,Apr. 8{12, 2001. Springer-Verlag, Berlin, Germany.

[7] J.-M. Bohli, N. Gruschka, M. Jensen, L. L. Iacono, and N. Marnau, Security and privacy-enhancing multicloud architectures," IEEE Trans. Dependable Sec. Comput., vol. 10, no. 4, pp. 212–224, Jul. \Aug. 2013.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

[8] J. Yu, F. Kong, H. Zhao, X. Cheng, R. Hao, and X.-F. Guo. "Noninteractive forward-secure threshold signature without random oracles." J. Inf. Sci. Eng., 28(3):571–586, 2012.
[9] X. Liu, Y. Zhang, B. Wang, and J. Yan. Mona: Secure multi-owner data sharing for dynamic groups in the cloud. IEEE Trans. Parallel Distrib. Syst., 24(6):1182–1191, 2013.
[10] Javier Herranz IIIA,Identity-Based Ring Signatures from RSA Artificial Intelligence Research Institute, Spanish Na-tional Research Council, Campus UAB s/n, E-08193 Bel-laterra, Spain
[11] E.-J. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage", in Proceedings of the Network and Distributed System Security Symposium, 2003.
[12] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proceedings of the Network and Distributed System Security Symposium,, 2005.
[13] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks, 2008.
[14] Javier Herranz IIIA, "Identity-Based Ring Signatures from RSA" Artificial Intelligence Research Institute, Spanish National Research Council, Campus UAB s/n, E-08193 Bellaterra, SpaM. Bellare and S. Miner, "A forward-secure digital signature scheme," in Proc. 19th Annu. Int. Cryptol. Conf., 1999, vol. 1666, pp. 431–448.
[15] Li, Jin, Jingwei Li, Xiaofeng Chen, Chunfu Jia,and Wenjing Lou. "Identity-Based Encryption with Outsourced Revocation in Cloud Computing", IEEE Transactions on Computers,2015.Publicat ion
[15] J. Yu, R. Hao, F. Kong, X. Cheng, J. Fan, and Y. Chen. Forward secure identity-based signature: Security notions and construction. Inf. Sci., 181(3):648–660, 2011.
[16] "Amazon.com," Amazon Web Services (AWS), 2008. [Online]. Available: http://aws.amazon.com.