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

Data Authentication and Security Approach Using Ring Base Forward Security

Miss. Ashwini Ajinath Satpute, Prof.Rugraj Rajpurohit

Department of Computer Engineering, Alard College of Engineering, Marunji, Pune, India

ABSTRACT: Cloud Computing is ceaseless growing latest technology in IT industry, academia and business. The practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer. Cloud computing is highly accessible, flexible technology that puts hardware, software, and virtualized resources. Cloud computing infrastructure works over the internet on demand basis. Main features of cloud computing is that on-demand capabilities, broad network access, resource pooling, rapid elasticity ,measured service scalability and provides shared services to user on demand basis in distributed environment. Commonly available cloud computing service providers are Google, Yahoo, Microsoft, Amazon etc. The details of cloud services are abstracted from users. The most common issues of cloud computing as efficiency, integrity and authenticity. Moreover, users are unaware of location where machines which actually process and host their data. The motivation of this paper is to propose a secure data accessing and sharing scheme, for public clouds.

KEYWORDS: Cloud computing, IaaS, pricing scheme, utility function

I. INTRODUCTION

Data sharing system. By using this method an owner of the data anonymously authenticate his information which can be put into the Storage at different places along with identity information. In order to construct the cost-effective authentic and anonymous data sharing system Forward secure ID-based ring signature is an essential tool. ID-based ring signature seems to be an optimal factor which exchange among efficiency, data authenticity and anonymity. It provides a sound solution on data sharing between a large numbers of participants. One can add more users in the ring in order to obtain a higher level protection but doing this increases the opportunity of key exposure as well. Key exposure is the fundamental limitation of ordinary digital signatures. If the private key of a user is compromised and if the attacker knows partial or full key means all signatures of those users become worthless. By using this compromised signature future signatures also validated. The previously issued signatures also cannot be trusted. Once a key leakage is identified, key revocation mechanisms must be invoked immediately. By using this mechanism the generation of any password using the compromised secret key should be prevented. However, this mechanism does not solve the problem of forge ability for previously used signatures. In order to preserve the validity of past signatures the forward secure signature was proposed this mechanism works even though current secret key is compromised. First it calculates the total time of the validity of a public key and divides them into T time periods. A key compromise of the current time slot does not enable an adversary to produce valid signatures pertaining to past time slots. In a ring signature scheme the key exposure create more severe problem. If the secret key of one of the ring member's is exposed by the attacker means they can produce valid ring signatures of any documents belonging to that group. For doing this type of attack the attacker only needs to include the compromised user in the "group" and silently watch the transaction between the groups. The exposure of one user's secret key may discover all previously obtained ring signatures but the condition is that user is one of the ring members. Since the member cannot identify whether a ring signature is generated prior to the key exposure or not without using any mechanism. So the forward security is a necessary requirement in a big data sharing system. Otherwise, huge amount of time and resource will be waste. The forward-secure digital signatures should be designed in various fashions in order to add forward security on ring signature. Two types forward secure ring signature schemes they are discussed in [1], [2]. However they both work in the traditional public key setting. In this type of settings the signature verification involves expensive certificate check for every ring member. This will work for big ring also such as the more number of users in a smart grid. In order to summarize the design of ID-based ring signature with forward security the forward security is the fundamental tool .

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 key features of this forward security scheme is It is in ID-based setting so the elimination of the costly

- Certificate verification process makes it scalable for large number of users and especially suitable for big data analytic environment. The size of a secret key is just one integer
- Key update process only requires an exponentiation time. The pairing operation could not be used in any stage.

II. LITERATURE SURVEY

Problem Statement

There are few concerns involving because the information owner physically releases sensitive information to some distant CSP:

- Confidentiality - Outsourced information has to be protected from users which are not allowed access, the CSP, and the TTP.
- Integrity - Outsourced data must keep undamaged on cloud servers. Authorized users and the information owner should be empowered to recognize information corruption.
- Access control – Authorized users only have to be permitted to gain access to the information that was outsourced.
- The defense of CSP - The CSP has to be safeguarded against fake accusations that could be stated by owner/users
  that were dishonest, and this type of malicious conduct is needed to be disclose

III. PROPOSED SYSTEM

Forward secure identity predicated ring signature for data sharing in the cloud architecture that proposed data sharing in an efficient manner. This architecture, provide multiple cloud environment for astronomically immense data sharing in secure way. Client in the diagram represents individual cloud accommodation utilizer. The servers may reside in different physical locations. The CSP decides the servers to store the data depending upon available spaces. Identity predicated ring signature provide the ring formation of users. The authentic data sharing in multiple clouds to provide secure data sharing at sizably voluminous system. The encryption and decryption provide secure data transmission ID-based forward secure ring signature scheme are designed to following ways. The identities and user secret keys are valid into T periods and makes the time intervals public and also set the message space M= { 0,1 }*.

IV. SYSTEM ARCHITECTURE

Forward secure identity predicated ring signature for data sharing in the cloud architecture that proposed data sharing in an efficient manner. This architecture, provide multiple cloud environment for astronomically immense data sharing in secure way. Client in the diagram represents individual cloud accommodation utilizer. The servers may exist in different physical locations. The CSP takes decision of the servers to store the data depending upon available spaces. Identity predicated ring signature provide the ring formation of users. The authentic data sharing in multiple clouds to provide secure data sharing at sizably voluminous system. The encryption and decryption provide secure data transmission.

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

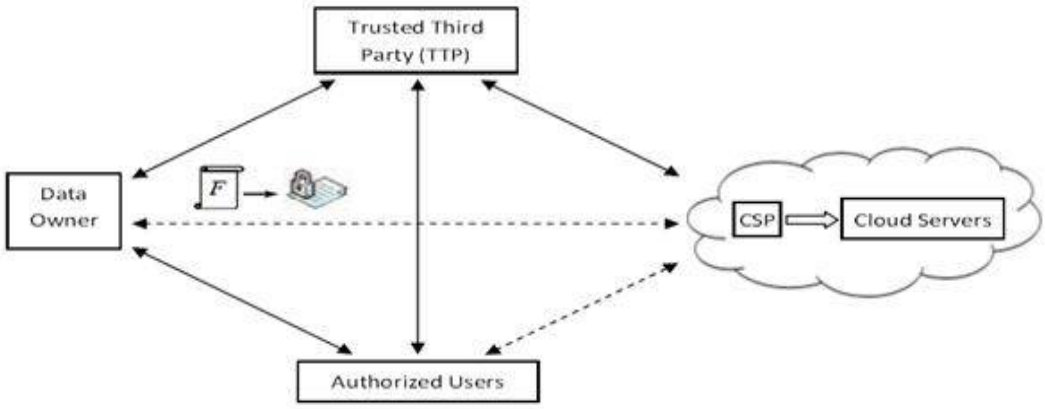

Figure 1: Proposed System Architecture

Data Owner

Information Owner of the device component is the nothing the user of desire to save and share data over cloud. Information owner isn't having any idea where my information will be stored by the CSP and there is trust shortfall on CSP.

As data is most important for info owner and the data owner do not desire that his information is observable to the CSP. To fix the preceding issue set trustworthy third party and before uploading the data, it's encrypted / auditor which are set to keep watch.

Trusted Third Party / Auditor

Database reviewing includes a database to not be uninformed of the activities of the database clients. Database heads and advisors every now and again set up evaluating for the security purposes. For instance to guarantee that exhortation to be gotten to by those without the consent don't get to it. Reviewing is the observing and recording of client database exercises that are chosen. It may be founded on blends of variables that can incorporate client name, system, time, etc, including the sort of SQL articulation executed, or on individual exercises. Reviewing can be activated by security approaches when indicated parts including, inside of an Oracle database are acquired or modified the substance inside of a given article.

For instance, the database executive can gather information about which tables are being redesigned, what number of coherent I/Os are performed, or what number of simultaneous clients unite at top times. Find issues with an authorization or access control execution

Authorized User

A client who has right to access the remote data is a Authorized User.

Cloud Storage Service Provider (CSP)

Database is provided by cloud Storage Services Provider. It permits information owner to keep any kind of information and also able to make the user define database schema. It can be Non SQL / SQL form of database instance. According to user requirement CSP will allocated the space for the user instance.

Algorithm

- Step 1: First data owner upload the text data like text file
- Then apply the AES 128 16 bit encryption and signature generation using secure hash function.
- Once data owner send the data to server it first receives to TTP it means Trusted Third Party, so it will generate the hash values using SHA-256 algorithm.
- Then send to service provider.
- Service provider store all the data into database.
- Client first login to system, and calculate SHA-256 keys
- If client SHA keys and TTP SHA keys are same then the client is validate for data accessing.

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

- Then he can generate the request to data owner for decryption keys. Once client generate the request to owner it will reflect on data owner's dashboard.
- Data owner can send the decryption keys to client.
- Data owner having control to grant and revocation for client.
- When data owner revoke the particular client then system will automatically change the existing keys.

AES 128

Generate user m1 ID; Set of users m1's attribute -> Domain B; element checks in Domain manager; Now, Generate Random Value[unique] attribute = ran;
Generate Random value [user] = r;
Secret key= (ran +r).user m1's ID; }
Encrypting user data along with ID
Encrypt (user ID. (rab+r)+data)
Decrypting user data n long with ID
Decrypt (user ID. (ran+r)+data)

SHA 256 Algorithms

Information: string required to ascertain the SHA score.
Yield: SHA score of string
Step 1: Padded with the length in such way that the outcome is numerous in least 512 piece long.
Step 2: Parse into 512 piece message squares M(1),M(2.. M(n) the message square can prepare at one time.
utilizing the beginning hash values H(0).
Step 3: Then process the succession
H(i) = H(i1)+ CM(i) (H(i1));
Step 4: give back the H(i) SHA score of given string.

Mathematical Model
Let's,
D is denoted by dataset which includes the n number of paragraphs in file
D= {Ci1,Ci2,Ci3…..Cin}
Here, C is the intermediate module which holds the data processing for security as well as data privacy.
C= {C1,C2,C3…Cn}
C1= key generation
C2= encryption of data
C3= Authentication and TTP verification phase
C4 = decryption of data
C5=Revocation phase
C6=Resign key generation
Here R is web base approach which handles the parallel searching, the result of query classified into n number of result pages. All R instances might be virtual machine on cloud which will holds the data and when intermediate module generate the requirement it will execute parallel.

R= {R1,R2,R3….Rn}

V. RESULT AND DISCUSSION

After implementing some part of system we got system performance on satisfactory level. The below table shows the first algorithm performance for user plain data conversion as well encryption decryption.

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

Data Size in MB	Encryption time (Milliseconds)	Decryption time (Milliseconds)
5	515	612
10	1026	1033
15	1547	1556
20	2064	2033

Table 1: System performance

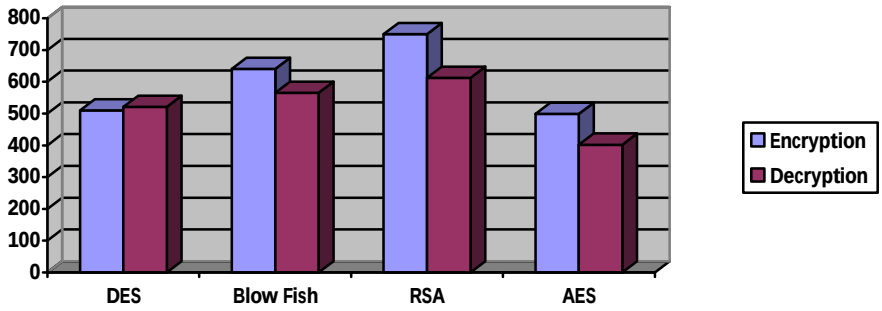

Table 2: System performance with proposed vs Existing

VI. CONCLUSION AND FUTURE WORK

The Forward Secure ID-Predicated Ring Signature sanctions an ID-predicated ring signature scheme to have forward security. It is the first in the literature to have this feature for ring signature in ID-predicated setting. The scheme provides unconditional anonymity and can be proven forward-secure unforgeable in the desultory oracle model. The scheme is very efficient and does not require any pairing operations. The size of utilizer secret key is just one integer, while the key update process only requires an exponentiation. This will be very utilizable in many other practical applications, especially to those require utilizer privacy and authentication, such as ad-hoc network, e-commerce activities and perspicacious grid. The system withal implemented in multi-cloud system to ameliorate the efficiency, sizably voluminous storage and data sharing system. Thus Reduce computation involution of designation and verify. Reduce space and time requisites ameliorate the cost efficient mechanism. The current scheme relies on the arbitrary oracle postulation to prove its security. Consider a provably secure scheme with the same features in the standard model as an open quandary and our future research work

REFERENCES

1) A. Shamir. Identity-Based Cryptosystems and Signature Schemes. In CRYPTO 1984, volume 196 of Lecture Notes in Computer Science ,pages 47–53. Springer, 1984.
2) R. L. Rivest, A. Shamir, and Y. Tauman. How to Leak a Secret. In ASIACRYPT 2001, volume 2248 of Lecture Notes in Computer Science, pages 552–565. Springer, 2001.
3) E. Bresson, J. Stern, and M. Szydlo. Threshold ring signatures and applications to ad-hoc groups. In M. Yung, editor, CRYPTO 2002, volume 2442 of Lecture Notes in Computer Science, pages 465–480. Springer, 2002.
4) J. K. Liu and D. S. Wong. On the Security Models of (Threshold) Ring Signature Schemes. In ICISC 2004, Lecture Notes in Computer Science. Springer, 2004.
5)F. Zhang and K. Kim. ID-Based Blind Signature and Ring Signature from Pairings. In ASIACRYPT 2002, volume 2501 of Lecture Notes in Computer Science, pages 533–547. Springer, 2002.
6) J. Han, Q. Xu, and G. Chen. Efficient id-based threshold ring signature scheme. In EUC (2), pages 437–442. IEEE Computer Society, 2008.
7) 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.
8) "Amazon.com," Amazon Web Services (AWS), 2008. [Online]. Available: http://aws.amazon.com.
9) P. P. Tsang, M. H. Au, J. K. Liu, W. Susilo, and D. S. Wong. A suite of non-pairing id-based threshold ring signature schemes with different levels of anonymity (extended abstract). In ProvSec, volume 6402 of Lecture Notes in Computer Science, pages 166–183. Springer, 2010.