ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

A Survey on Cloud Data Security and Integrity using Sack of Cryptographic Algorithms through Trusted Third Party (TTP)

Prof. Sonali A Patil, Pritam L Mahamane

Assistant Professor, Dept. of Computer Engineering, JSPM's BSIOTR College, Wagholi, Maharashtra, India

M.E Student, Dept. of Computer Engineering, JSPM's BSIOTR College, Wagholi, Maharashtra, India

ABSTRACT: In today's technological world, virtual resources and services are more demanded over the network and internet. For this cloud computing is the best solution in all terms like scalability, cost, flexibility, and efficiency. But the major factor affecting on cloud services is the poor security. Therefore in this paper, we propose sack of algorithms which are combine method of symmetric and asymmetric cryptographic algorithms encrypted for security and secure hash algorithm for data integrity.This ensures more data confidentiality with secure encryption of secret key using digital certificate through trusted third party(TTP).Trusted third party acts as substitute of cloud service user (CSU),by holding secret key and communicating with cloud service provider(CSP) , to reduce overhead of maintainability of data.We proposed the method for data integrity, which will enhance checking of data correctness with zero overhead to user.

KEYWORDS: TTP, Sack of algorithms, Virtual resources, symmetric, asymmetric cryptography, hash algorithm, cloud computing.

I. Introduction

Cloud computing is internet based computing where virtual shared service provides resources, software, infrastructure, platform and devices to customer located at any point without any infrastructure. When a Cloud is available in a pay-as-you-go manner to all the general public, it called as a Public Cloud. We use the term Private Cloud to refer to internal data centres or reserved locations of a business or other organization, not made available to the general public. Cloud computing enabling technologies are Grid computing, Utility computing, Virtualization and Service Oriented Architecture (SOA); the service being sold is Utility Computing.

Cloud computing has many benefits as it is location independent; it not needed to be installed on user's computer. Because of cloud, availability of information has increased, flexibility and market quick deployment also possible. Such growing technology just lack in the security issues. If the cloud service provider (CSP) does the security related actions that may create insider threats. However if cloud service user (CSU) does security related activities like encryption, sending key and performing necessary data integrations services as proposed in [2], it will increase overhead on user of performing all the computational operations and which is also contrast, to the service of cloud computing technology.

II. Related work

The author Syed Rizvi, Cover and Christopher proposed scheme for ensuring data confidentiality in cloud environment using third-party based encryption. In this paper the combination of symmetric and asymmetric algorithms are used, which highly helped us in our work. Here the data integrity should use the algorithm implemented at third party (TTP) side to reduce cloud service user (CSU) computational overhead[1]. The Muralikrishnan Ramane and Bharath Elangovan author proposed auditing, data verification request and response messages to introduce to someone third party, who will do security related activities and also verify data integrity. This proves the security of using (TTP)third party with increased efficiency by this we assume TTP is secure and trusted for handling secret key and computational

DOI: 10.15680/IJIRCCE.2016. 0412090

functions on behalf of cloud service user[3]. Priyadarshini Patil, Prashant Narayankar, and group proposed a survey of Cryptographic Algorithms: DES,3DES, AES, RSA and Blowfish. In this, these algorithms are analyzed on different parameters like memory size, time required for encryption, entropy, strength and then they conclude that AES algorithm is useful for the applications which demand confidentiality and integrity on the highest priority. Therefore if cryptographic strength is a most affecting factor in the application, then AES is the best algorithm suits for the application. [4].Qian Wang proposed paper specially focuses on dynamic data operation with integrity assurances. Data security over cloud with data integrity using multiple challenge-response messages between TTP and cloud user is proposed in this paper. This gives good result of checking data correctness with little overhead of workload on cloud service user (CSU)[5]. Dilli Ravilla, Chandra Shekar Reddy proposed new approach to the data integrity functions by using Hash algorithms. They find this as secure because, for any other algorithm, it is computationally infeasible to find a message that is very same message with the original and with the new arrival message [6].

III. PROPOSED ALGORITHM

A. *DESIGN CONSIDERATIONS:*

- All paths are highly secure.
- Previous used paths are keep in use.
- Data send in network is in block structure.
- Third Party uses database for storing key, certificate and hash value.
- Input data for cloud storage can be one line or a sentence.

B. *DESCRIPTION OF THE PROPOSED ALGORITHM:*

The proposed system for cloud data security, data is encrypting at cloud service user (CSU) side and communicated the secrete key with cloud service provider (CSP) through trusted third party which also monitoring the data alteration. The system can have the following steps.

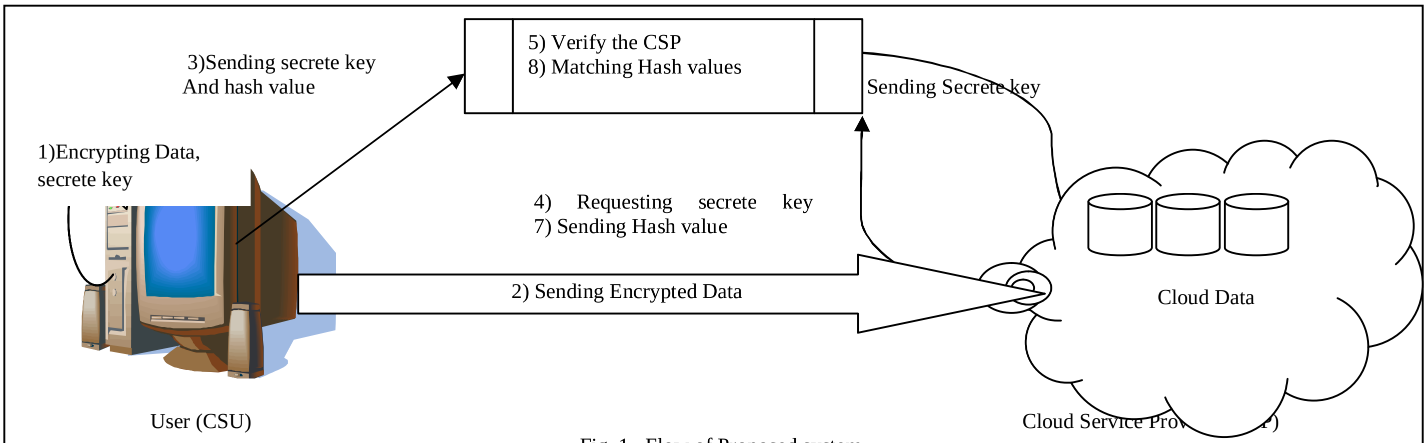

Fig. 1. Flow of Proposed system

Step 1: Encryption of Cloud Data And Secrete Key:

Cloud service user (CSU) encrypting the data which he/she want to upload on the cloud data storage with help of AES algorithm. Advanced Encryption Standard (AES) algorithm, is symmetric key cryptography algorithm, which proved as the best encryption algorithm [4]. The secrete key send to trusted third party (TTP) using RSA algorithm with user's signature attached.

$$C=E\ (PUB_{\ TTP}\ ,K_{\ S})$$

$$E_{\ PRI-CSU}\big(E\ (PUB_{\ TTP}\ ,K_{\ S})\big)$$

DOI: 10.15680/IJIRCCE.2016. 0412090

Where E is the Encryption Function, $PUB_{\ TTP}$ is the Public key of TTP, $K_{\ S}$ is the Secrete Key, $PRI_{\ CSU}$ is the Private Key of CSU (Cloud Service User).

Step 2: Transmitting Data and Requesting For Key:

Cloud Service User (CSU) sends the encrypted data to Cloud Service Provider (CSP) and encrypted secrete key to Trusted Third Party (TTP) using RSA algorithm with user's signature attached. Cloud Service Provider (CSP) when need to access user data, for decrypting data available on cloud, CSP request for secrete key to trusted third party (TTP).

Step 3: Functions Of Trusted Third-Party (TTP):

Trusted third party (TTP) is introduced for reducing user overhead of computational work and assure the security of data against insider or outsider threats [3]. Therefore TTP does many tasks while doing his role like as 1) Holding the secrete key and hash value, 2) creating Public Key Certificate, 3) on requesting the secrete key by CSP, the CSP is verified and secrete key has been exchanged, 4) verify the correctness of data.

1) Holding the Secrete Key and Hash Value

When the cloud service user send secrete key encrypted using user's signature, TTP decrypt the message and store the secrete key in database for that user. Along with it user send the hash value calculated for original data, which also stored for data verification at last.

.

2) Creating Digital Certificate (DC)

At the first, when TTP receive secrete key form cloud user, he verify the user by decrypting message using user's public key, as the user has send his signature with the encrypted secrete key. After verifying the cloud service user, TTP allocate public key certificate to user by acting Certificate Authority (CA) as itself.

$$D_{\ PUB-CSU}\left(E_{\ PRI-CSU}\left(E_{\ PUB-TTP}(K_{\ S})\right)\right) \ = \ E_{\ PUB-TTP}(K_{\ S})\ .$$

Where D is Decryption, $PUB - CSU$ is Public key of Cloud user.

3) Exchanging the Secrete Key

On the request of secrete key form cloud service provider (CSP), TTP authenticate the CSP by decrypting request. Then the secrete key for requested user_id is send by RSA algorithm.

$$D_{\ PUB-CSP}\left(E_{\ PRI-CSP}\left(MD_{comp}\right)\right) \text{…………Decryption of CSP's request}$$

$$E_{\ PUB-CSP}\ (Ks_{CSU1})\ \text{………………………..Sending secrete key by RSA}$$

Where $PRI - CSP$ is the Private key, $PUB - CSP$ is the Public key of CSP.

4) Verification of User Data Integrity

In paper [5], the author used method of multiple challenge-responses between CSU and TTP for verifying data alteration, but this increase the overhead on user. By using Secure Hash Algorithm (SHA), which is best for data integrity also can be done at TTP side to decrease the overhead of user. Hash value calculated using SHA-512 gives more correct result for data integrity [6]. TTP takes hash value from both CSU, CSP and match it, to show any data alteration.

IV. Conclusion and Future Work

The objective of this paper, to give more data confidentiality along with the data integrity and zero overhead on user. According to that the algorithms and methods are chosen, it uses all cryptographic algorithms as, AES symmetric key algorithm, RSA asymmetric key algorithm, Digital Certificate (DC), Secure Hash Algorithm (SHA-512). At every stage these algorithms increases cloud data security and as it used through trusted third party (TTP), it also minimize cloud service user (CSU) burden. In future, the work can be done to replace RSA algorithm with Deffie Hellman (DH) algorithm which is more secure and specific for secrete key exchange.

REFERENCES

1. Syed Rizvi, Katie Cover, Christopher Gates, “A Trusted Third Party (TTP) based Encryption Scheme for Ensuring Data Confidentiality in Cloud Environment”, ScienceDirect ELSEVIER, journal Procedia Computer Science 36, pp. 381-386, 2014.
2. S. Arul Oli, L. Arockiam ,“A Novel Approach for Ensuring Data Confidentiality in Public Cloud Storage”, International Journal of Computer Applications (0975 – 8887).Advanced Computing and Communication Techniques for High Performance Applications (ICACCTHPA-2014).pp.1-5, 2014.
3. Muralikrishnan Ramane, Bharath Elangovan,“A Metadata Verification Scheme ForData Auditing In Cloud Environment”, International Journal on Cloud Computing: Services and Architecture(IJCCSA),Vol.2, No.4, pp. 1-10, August 2012.
4. Priyadarshini Patil, Prashant Narayankar, Narayan D G, Meena S M,“A Comprehensive Evaluation of Cryptographic Algorithms: DES,3DES, AES, RSA and Blowfish.”, ScienceDirect ELSEVIER, journal Procedia Computer Science 78, pp. 617-624, 2016.
5. Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, and Jin Li,“Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing”, IEEE Transactions on parallel and Distributed System,vol.22, no.5, pp.847-859, May2011.
6. Dilli Ravilla, Chandra Shekar Reddy Putta, “Enhancing the Security of MANETs Using Hash Algorithms”, ScienceDirect ELSEVIER, journal Procedia Computer Science 54, pp. 196-206, 2015.
7. Triveni A. Bhalerao, Prof. N. P. Kulkarni, “Survey on Secure Cloud Data Sharing Using Trusted Third Party”, International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 10, pp. 1-4, October 2016.
8. Mr. Manish M Potey, Dr C A Dhote, Mr Deepak H Sharma, “Homomorphic Encryption for Security of Cloud Data”, ScienceDirect ELSEVIER, journal Procedia Computer Science 79,pp. 175 – 181, 2016.
9. Naresh vurukonda, B.Thirumala Rao, “A Study on Data Storage Security Issues in Cloud Computing”, ScienceDirect ELSEVIER, journal Procedia Computer Science 92,pp. 128 – 135, 2016.
10. Akashdeep Bhardwaj, GVB Subrahmanyam, Vinay Avasthi, Hanumat Sastry, “Security Algorithms for Cloud Computing”, ScienceDirect ELSEVIER, journal Procedia Computer Science 85,pp. 535 – 542, 2016.
11. K.Devika, M.Jawahar, “ Review On: Cryptographic Algorithms for Data Integrity Proofs in Cloud Storage”, International Journal of Engineering Trends and Applications (IJETA) – Volume 2 Issue 1, pp. 14-19, Jan-Feb 2015.
12. Niels Ferguson, Richard Schroeppel, and Doug Whiting, “A simple algebraic representation of Rijndael”, Proceeding of Selected Areas in Cryptography, 2001, Lecture notes in computer science, Springer-Verlag, pp. 103-111, 2001.

BIOGRAPHY

Professor Sonali A Patil is an Assistant Professor in the Computer Engineering Department, College of JSPM’s Bhivarabai Sawant Institute of Technology and Research (B.S.I.O.T.R.), Wagholi, Pune University, Maharashtra, India. Her research interest is Cloud Computing.

Pritam Laxman Mahamane is a student of Master in Engineering (M.E.) in the Computer Engineering Department, College of JSPM’s Bhivarabai Sawant Institute of Technology and Research (B.S.I.O.T.R.),Wagholi, Pune University, Maharashtra, India.