INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SPECIAL ISSUE FOR INTERNATIONAL LEVEL CONFERENCE "ADVANCES IN SCIENCE, TECHNOLOGY & MANAGEMENT" (IC-ASTM)

AN APPROACH TO PARTITION AND MANAGE DATA SECURITY IN CLOUD COMPUTING

MISS. SONALI S. DHULE

College of engineering and Technology, Akola

Accepted Date: 05/09/2017; Published Date: 10/10/2017

Abstract: The advent of the cloud computing paradigm has given rise to many innovative and novel proposals for managing large-scale, fault-tolerant and highly available data management systems. It allows different service providers to distribute many applications as services in an economical way. Therefore, many users and companies have begun using cloud computing. However, they are concerned about their data when they store it on a third party, the cloud. Fears of leakage of sensitive data or loss of privacy make the adoption of cloud services less attractive for organizations. In this project an algorithm is presented to protect a table in a database from any leakage. We have developed a model with a view to offer secure data management capability in cloud databases. The model distributes and scatters the data over the Files in order to protect it from any leakage. In addition, to increase security, we design a genetic algorithm to perform the optimal partition. The results show that our method can achieve more than 2X better performance over the execution without partitioning.

Keywords: Data Partitioning, Cloud computing, Security, RSA , Encryption, Decryption

Corresponding Author: MISS. SONALI S. DHULE

Co Author: -

Access Online On:

www.ijpret.com

How to Cite This Article:

Sonali S. Dhule, IJPRET, 2017; Volume 6 (2): 491-496

PAPER-QR CODE

INTRODUCTION

Cloud Computing is the key driving force in many small, medium and large sized companies and as many cloud users seek the services of cloud computing, the major concern is the security of their data in the cloud. Securing data is always of vital importance and because of the critical nature of cloud computing and the large amounts of complex data it carries, the need is even more important. Hence forth, concerns regarding data privacy and security are proving to be a barrier to the broader uptake of cloud computing services. With the potential to significantly decrease costs through optimization and increased operating and economic efficiencies, cloud computing is a great invention. In addition, cloud computing could significantly improve its cooperation, agility, and scale, therefore enabling a truly global computing model over the Internet infrastructure.

1.1 Dimensions of cloud security

1 Identity management

Every enterprise will have its own identity management system to control access to information and computing resources. Cloud providers either integrate the customer's identity management system into their own infrastructure, using federation or SSO technology, or a biometric-based identification system,or provide an identity management solution of their own.

2 Physical security

Cloud service providers physically secure the IT hardware (servers, routers, cables etc.) against unauthorized access, interference, theft, fires, floods etc. and ensure that essential supplies (such as electricity) are sufficiently robust to minimize the possibility of disruption. This is normally achieved by serving cloud applications from 'world-class' (i.e. professionally specified, designed, constructed, managed, monitored and maintained) data centers.

3 Personnel security

Various information security concerns relating to the IT and other professionals associated with cloud services are typically handled through pre-, para- and post-employment activities such as security screening potential recruits, security awareness and training programs, proactive

4 Privacy

Providers ensure that all critical data (credit card numbers, for example) are masked or encrypted and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

1. PROPOSED WORK

In this paper we describe about System model of Privacy Maintaining using RSAwhich provides a complete solution of data files and also integrity checking. The cloud data storage service consists of following different Entities

1. Client (User): Who have to stores large amount files on Cloud server.

2. Cloud Service Provider (CSP): It is separate entity that provides major storage space, resources, and maintenance for user data files.

3. Third Party Auditor (TPA): TPA is another network entity that has knowledge capability that client does not have. This is checking the user outsourced data files without copy of those files.

Block of data files performed at User level. Block module accept user input file. When user Browse fileit divided into smaller parts. It helps to store the data effectively in quick manner enhancing easy access to data also when there is need. The original data is complex and there is difficulty in storing it in cloud, so blocking function is used to make the storage easy in cloud. The block of files are encrypted, that is encoded with the public key and stored in cloud.

In our proposed system user will first encrypt data and then Encrypted file divided into block that encrypted block will store on cloud. For encrypting data we are using RSA

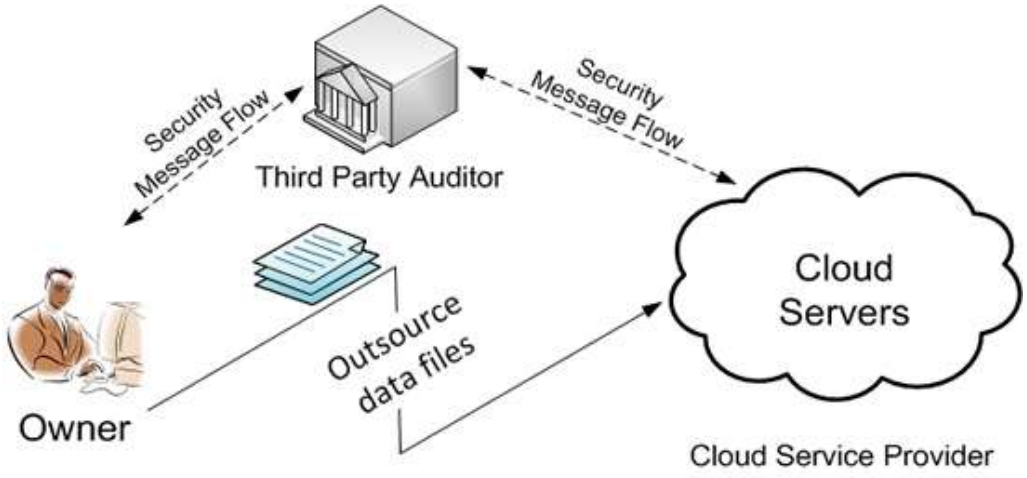

Figure 1: TPA in cloud computing for secure Transmission

2.1 Data Partitioning

Algorithm for Partitioning:

1. Select File from local system.
2. File_Name := Retrieve file name from selected file.
3. File_Extension := Retrieve File Extension from selected file.
4. If PARTITION_NOT_EXIST (File_Extension)
   - 4.1 Then CREATE_PARTITION (File_Extention)
5. Else Current_Partition:= NEW_PARTITION (File_Extention)
6. File_Name_Letter := FILE_NAME_ALPHABATE (File_Name)
7. If PARTITION_NOT_EXIST(File_Name-Letter)
   - 7.1 File_Count := COUNT_FILE_IN-PARTITION(Current-partition)
   - 7.2 If Threshold ≥ File_Count
     - 7.2.1 Then CREATE_PARTITION(File_Name_Letter)
     - 7.2.2 Current_Partition := NEW_PARTITION(File_Name_Letter)
   - 7.3 Else STORE_FILE (Current_Partition)
   - 7.4 Exit
8. Else Current_Partition:= NEW_PARTITION(File_Name_Letter)
9. File_Name_Letter:= NEXT_FILE_LETTER(File_Name_Letter)
10. GOTO Step 6

2.2 RSA algorithm

RSA algorithm involves three steps:

1. Key Generation
2. Encryption
3. Decryption

Key Generation:

Before the data is encrypted, Key generation should be done. This process is done between the Cloud service provider and the user.

Steps:

1. Choose two distinct prime numbers a and b. For security purposes, the integers a and b should be chosen at random and should be of similar bit length.
2. Compute n = a * b.
3. Compute Euler's totient function, Ø(n) = (a-1) * (b-1).
4. Chose an integer e, such that 1 < e < Ø(n) and greatest common divisor of e , Ø(n) is 1.

Now e is released as Public-Key exponent.

5. Now determine d as follows: d = e-1(mod Ø(n)) i.e., d is multiplicate inverse of e mod Ø(n).
6. d is kept as Private-Key component, so that d * e = 1 mod Ø(n).
7. The Public-Key consists of modulus n and the public exponent e i.e, (e, n).
8. The Private-Key consists of modulus n and the private exponent d, which must be kept secret i.e, (d, n).

2.2.1 Encryption:

Encryption is the process of converting original plain text (data) into cipher text (data).

Steps:

1. Cloud service provider should give or transmit the Public- Key (n, e) to the user who want to store the data with him or her.
2. User data is now mapped to an integer by using an agreed upon reversible protocol, known as padding scheme.
3. Data is encrypted and the resultant cipher text(data) C is C = me (mod n).
4. This cipher text or encrypted data is now stored with the Cloud service provider.

2.4 Decryption:

Decryption is the process of converting the cipher text(data) to the original plain text(data).

Steps:

1. The cloud user requests the Cloud service provider for the data.
2. Cloud service provider verify's the authenticity of the user and gives the encrypted data i.e, C.
3. The Cloud user then decrypts the data by computing, m = Cd (mod n).
4. Once m is obtained, the user can get back the original data by reversing the padding scheme.

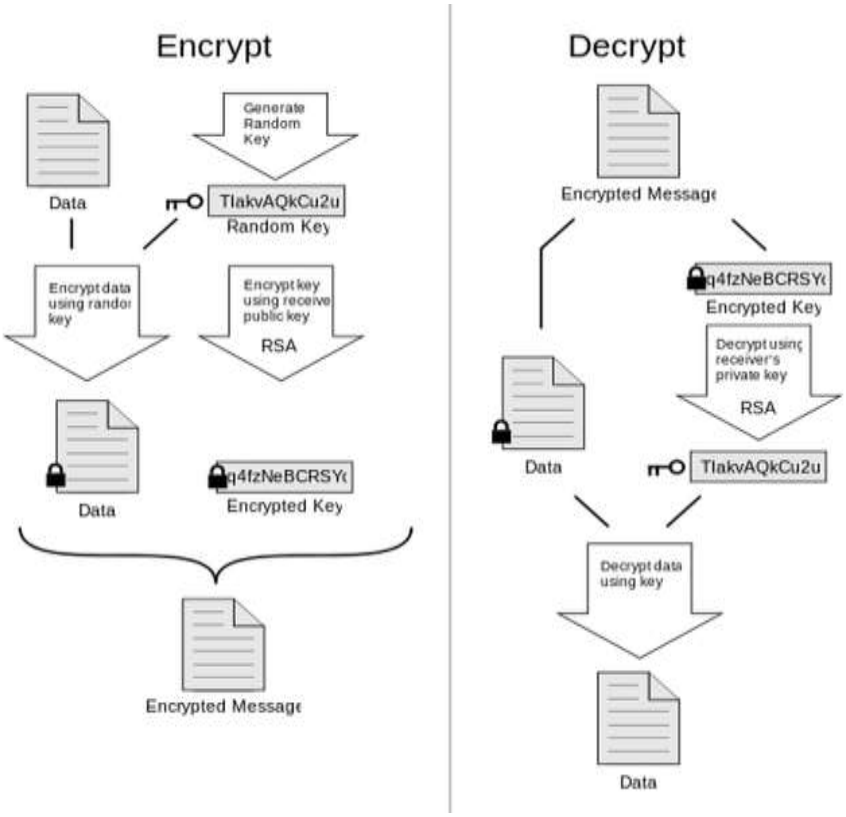

Figure 2: RSA Algorithm work flow

2. SYSTEM MODEL

Cloud Data are retrieved from the storage service as per the end user request. Data Storage architecture the end user can also decide what data need to be accessed and shared by the other users in cloud. Data accessed from

cloud service enables the services in secured manner. The data is partitioned into smaller blocks with file name before encryption for security by generating the public key to encode the data before storage. During the retrieval, the data are decrypted by generating the private key. Remote data integrity checking is used to maintain the data from threats. It also manages the effective storage and retrieval processes.

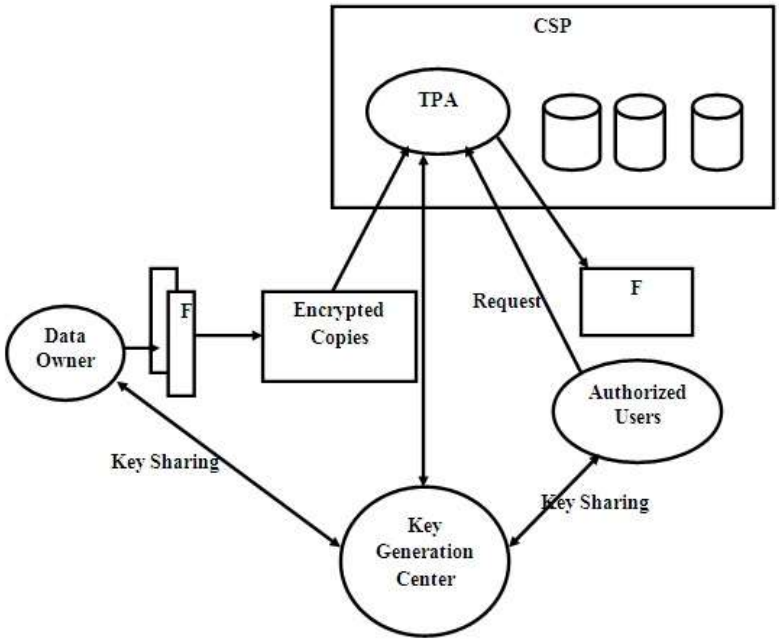

Figure 3: System Model

To get file list will return file list of a sub domain to cloud client check if sub domain is present or not if not present then return blank else return file list separated by comas. UDP File Store it will receive a file from cloud client and will store at a specified location on datacenter. UDP File Send it will send a file to cloud client at a specified IP address and Port number from specified location on datacenter.

3. CONCLUSION

In the current scenario, Cloud Computing is being emerged as one of the most powerful and developing networking system which is utilised by developers as well as users. Cloud computing is well suited for the persons who are interested to mould in networking environment. As security is one of the key challenging factor in network platform, providing security in cloud computing also plays a prime concern for its effective utilization.

Thus, in our paper, we given solution to the problem as only the registered user can access the data. Even if some intruder (unauthorized user) gets the data accidentally or intentionally if he captures the data also, he can't decrypt it and get back the original data from it. Hence forth, data security is provided by implementing RSA algorithm.

REFERENCES

1. Rongxing et al, —Secure Provenance: The Essential Bread and Butter of Data Forensics in Cloud Computing‖, ASIACCS'10, Beijing, China..
2. R. La'Quata Sumter, —Cloud Computing: Security Risk Classification‖, ACMSE 2010, Oxford, USA
3. Mladen A. Vouch, —Cloud Computing Issues, Research and Implementations‖, Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246
4. Wenchaoet al, —Towards a Data-centric View of Cloud Security‖, CloudDB 2010, Toronto, Canada

5. Soren Bleikertz et al, —Security Audits of Multi-tier Virtual Infrastructures in Public Infrastructure Clouds‖, CCSW 2010, Chicago, USA.
6. Flavio Lombardi& Roberto Di Pietro, —Transparent Security for Cloud‖, SAC'10 March 22-26, 2010, Sierre, Switzerland.
7. Wayne A. Jansen, —Cloud Hooks: Security and Privacy Issues in Cloud Computing‖, 44th Hawaii International Conference on System Sciesnces 2011.
8. Jinpeng et al, —Managing Security of Virtual Machine Images in a Cloud Environment‖, CCSW, 2009, Chicago, USA
9. Miranda & Siani, —A Client-Based Privacy Manager for Cloud Computing‖, COMSWARE'09, 2009, Dublin, Ireland
10. Dan Lin & Anna Squicciarini, —Data Protection Models for Service Provisioning in the Cloud‖, SACMAT'10, 2010, Pittsburgh, Pennsylvania, USA
11. en.wikipedia.org/wiki/Locality_of_reference.
12. informationweek.com/news/storage/security/228300050 219
13. Farhan Bashir Shaikh, Sajjad Haider __ Security Threats in Cloud Computing 11-14 December 2011, Abu Dhabi, United Arab Emirates
14. Osama M Ben Omran, Brajendra Panda-A New Technique to Partition and Manage Data Security in Cloud Databases The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)