Improving Cloud Security Using Data Partitioning And Encryption Technique

Mr. Akash Kanade
Department of Computer Engineering
JSPM's JSCOE
Pune, India
akash.kanade1@gmail.com

Ms. Rohini Mule
Department of Computer Engineering
JSPM's JSCOE
Pune, India
rohinimule94@gmail.com

Mr. Mohammad Shuaib
Department of Computer Engineering
JSPM's JSCOE
Pune, India
mshuaibin@gmail.com

Ms. NamrataNagvekar
Department of Computer Engineering
JSPM's JSCOE
Pune, India
namratanagvekar27@gmail.com

Abstract- Cloud computing is Internet based computing where virtual shared servers provide software and other resources and hosting to customers on a pay-as-you-use basis. Cloud storage is nothing but the storing data on third party cloud servers. Advantages of cloud computing are almost unlimited storage and backup and recovery. Disadvantages of cloud computing are technical issues, cost and lack of support. But main disadvantage is security. As we store our data on third party cloud service providers our data is not completely safe. It impose a great risk. Many cloud servers are curious servers i.e., they try to read the data which is stored on it. In this paper our goal is to build an application for improving cloud security using partition and encryption method which will help to improve the cloud security. In this first we take file from client and divide it into number of parts. After partition we encrypt the all file parts. Then we send file parts to different cloud servers. When client want that data back we took that data from cloud servers and decrypt that data. After decryption we merge that data and give it to client. Our goal is that the application should have simple user interface for users flexibility.

***Keywords* -** AES, Cloud Computing, Data Partition, Decryption, Encryption, Security.

I. INTRODUCTION

In this era of technology, the Internet access becomes available in the recent years, Cloud computing is an internet based technology, being used widely nowadays to enable the end user to create and use software without worrying about the execution of the technical information from anywhere at any time.

In order to store the large volume of data, cloud storage systems use many small-scale independent storage systems. These systems together form the entire cloud storage. To store the data using cloud storage has multiple advantages. Few of them are data stored using an account can be synced in multiple devices using the same account. There are lot of conflicting replicas are available in cloud storage. Users can use minimal amount of storage space by avoiding the replicas. The cloud computing has many features to the users like communication media, file storage and computations, keep mirroring of highly important information, etc., Basically, user data are stored in various storage locations like local servers and cloud. An overview of cloud storage system is shownin Fig [1].

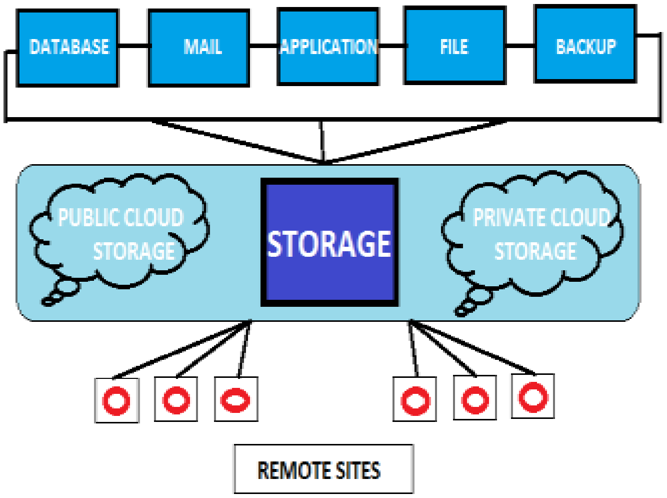


Fig. 1 Overview of cloud storage

Now computing technologies have attracted more and more people to store their private data on third party servereither for ease of sharing. When people enjoy the advantage of these new technologies and service, their concerns about data security also arise. Naturally, people would like to make their private data only accessible toauthorized users only. So we are trying to secure clients data using some algorithms.

II. LITERATURE SURVEY

In the Partitioning Technique literature review isdone for data integrity checking, data storagemechanisms and encryption mechanism. The dynamic data storage withtoken pre-computation and AES algorithm how it is storedin cloud is analyzed [1], [10] Integrity checking isused to detect and avoid misbehaving serverconsidering data correction and localizing errors.Distributed scheme is used to achieve theavailability, data quality,integrity of dependable storage services[2],[6]. Thedata storage using dynamic data operation method is usedto perform various operations. Security analysis is encode the data by RSA. Distributed storage system is alsoused to support the forwarded data in cloud.

Data integrity in cloud storage devices are analyzed in theresearch oriented works [8],[10]. PublicAuditability and dynamic data operation are used for supporting the integrity of data. Theobjective of this work is to havequality in services and independent perspective evaluating with the third partyauditor. Storage model is also devised here to supportmultiple auditing tasks to improve efficiency. In the works[3], [4], [5], author considers generating signature methodsfor ensuring the cloud storage security. Dynamic operationsare supported by using the RSA method supports dynamic operations[7]. This methoddiscussesdata correctness stored in cloud and data integrity.

III. PROPOSED SYSTEM

Our goal is to build a Java application for improving cloud security using partition method which will help to improve the cloud security. In this application we encrypt the client's data. After encryption we divide that data and send to different cloud servers. When client want that data back we took that data from cloud servers and decrypt that data. After decryption we merge that data and give it to client. The application should have simple user interface.

Concept :

We propose an efficient data storage security in cloud computing. The partitioning of data makes storing of the data in easy and effective. It also gives way for flexible access and there is less cost in data storage. The space and time is also effectively reduced during cloud storage. Dynamic operation is another important concept where, encryption and decryption process secures data, when storing into cloud. Also the remote data integrity checking detects the threats and misbehaving server while storing the data in cloud ensuring data security.

In this application the partitioning method is proposed for the data storage which avoids the local copy at the user side by using partitioning technique. This technique ensures high cloud storage integrity, improve error localization and identification of misbehaving server. In nature the data are dynamic. Hence in cloud this work aims to store the data in reduced space with less time and computational cost.

In this application we encrypt the client's data. After encryption we divide that data and send to different cloud servers. When client want that data back we took that data from cloud servers and decrypt that data. After decryption we merge that data and give it to client.

In this application we are providing a TPA [Third Party Administrator].

Actual flow of system:

- User selects file to upload on cloud server.
- Sends file to TPA.
- TPA receives file.
- TPA partitions file.
- TPA extracts digital signature of each file partition.
- TPA generates secrete keys for each partition.
- TPA encrypts each partition using respective secrete key.
- TPA stores partition sequence, signature, keys and file attributes on its own server.
- TPA sends partition to respective cloud storage.
- Storage server receive file partition.
- Storage server stores partition.

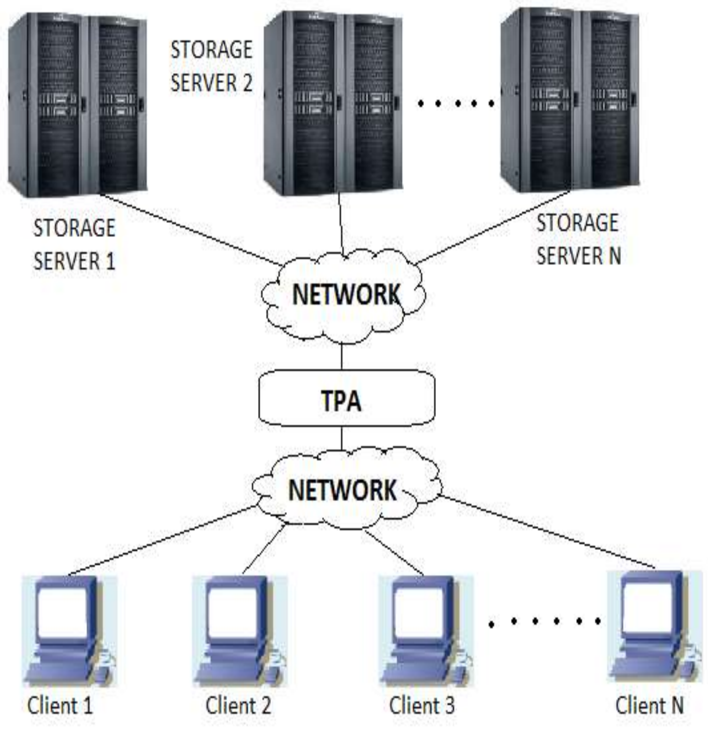


Fig. 2 Flow Of System

IV. METHODOLOGY

Partition Algorithm

- Load the Input file and size.
- Check size of file
- If file size is invalid then declare as Invalid size.

- Else
    - Count size = S
    - Split file into n partitions with extension and index value.
    - Return files.

Merging Algorithm

- Collect all decrypted file partitions
- Check file status
- If (file!) then File is missing.
- Else
    - Count the index value
    - Merge files.
    - Return file.

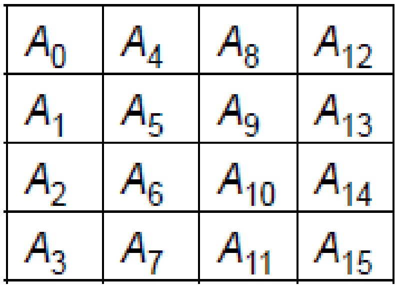
AES Algorithm

Advanced **E**ncryption **S**tandard (AES) is a symmetric key block cipher published by the NIST in December 2001. AES encrypts and decrypts a data block of 128 bits. The key size can be 128, 192, 256 bits.

The number of round: 10 rounds for 128 bits
12 rounds for 192 bits
14 rounds for 256 bits

Internal Structure of AES

AES is a byte-oriented cipher.
The state A (i.e., the 128-bit data path) can be arranged in a 4X4 matrix:



A_0	A_4	A_8	A_{12}
A_1	A_5	A_9	A_{13}
A_2	A_6	A_{10}	A_{14}
A_3	A_7	A_{11}	A_{15}

withA0,…, A15 denoting the 16-byte input of AES

Encryption

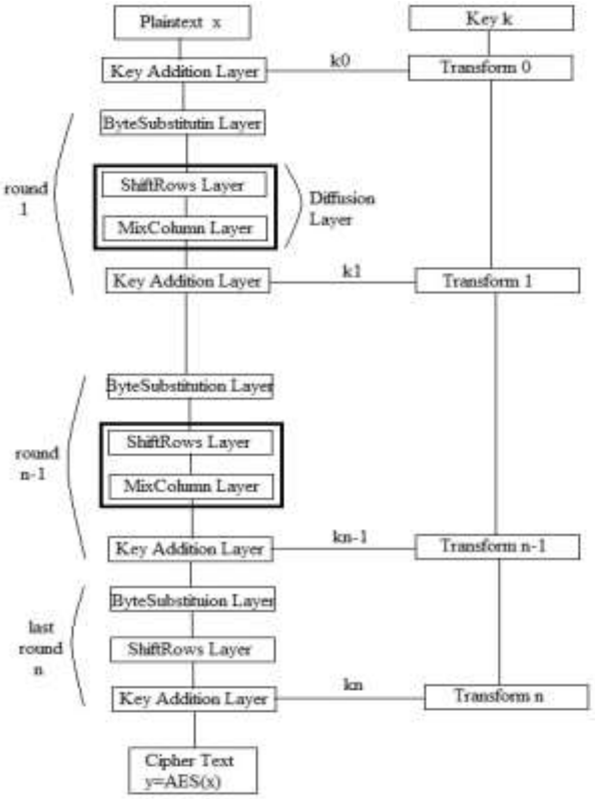


Fig. 3 Rounds of Encryption Process

For 128 bits AES each round contains four steps.

- Byte Substitution
- Row shift
- Column Mixing
- Round Key Addition

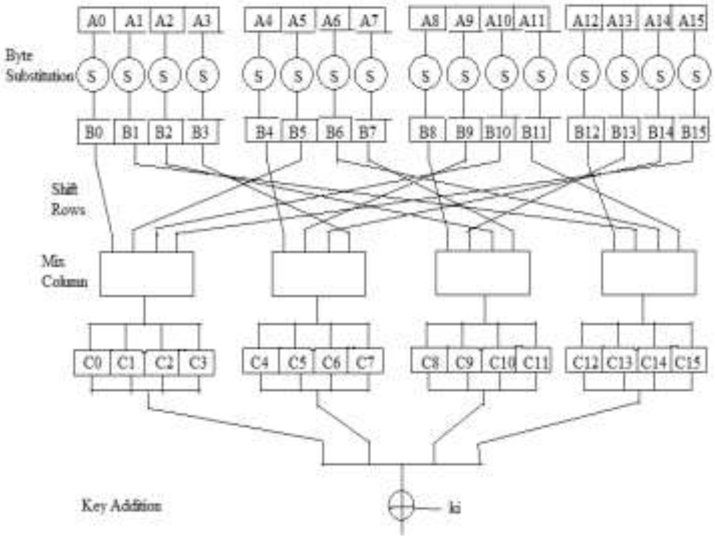

A0 A1 A2 A3 A4 A5 A6 A7 A8 A9 A10 A11 A12 A13 A14 A15
Byte Substitution
S
B0 B1 B2 B3 B4 B5 B6 B7 B8 B9 B10 B11 B12 B13 B14 B15
Shift Rows
Mix Column
C0 C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15
Key Addition
ki

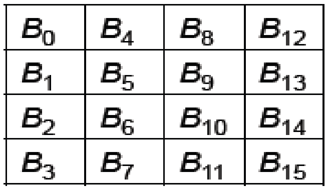
Fig. 4 Flow of algorithm

Byte Substitution

The Byte Substitution consists of 16 **S-Boxes**
In software implementations, the S-Box is usually realized as alookup table

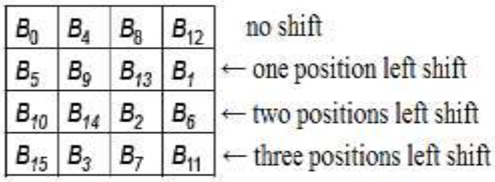
Row shift

Input matrix =>



B_0	B_4	B_8	B_{12}
B_1	B_5	B_9	B_{13}
B_2	B_6	B_{10}	B_{14}
B_3	B_7	B_{11}	B_{15}

Output matrix =>



B_0	B_4	B_8	B_{12}	no shift
B_5	B_9	B_{13}	B_1	← one position left shift
B_{10}	B_{14}	B_2	B_6	← two positions left shift
B_{15}	B_3	B_7	B_{11}	← three positions left shift

Column Mixing

Linear transformation mixes each column of thestate matrix.
In column mixing 4-byte column is considered as a vector and multiplied by a 4*4 matrix, e.g.

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{pmatrix}$$

where 01, 02 and 03 are given in hexadecimal notation

Round Key Addition

- In encryption the key is provided as input is expanded into an array of forty four 32 bit words, w(i).
- In AES four different stages are used, one of permutation and three of substitution.
- For encryption, the cipher begins with an AddRoundkey stage, followed by nine rounds that each includes all four stages, followed by a tenth round of three stages.
- Only the AddRoundkeystage make use of the key.

Decryption

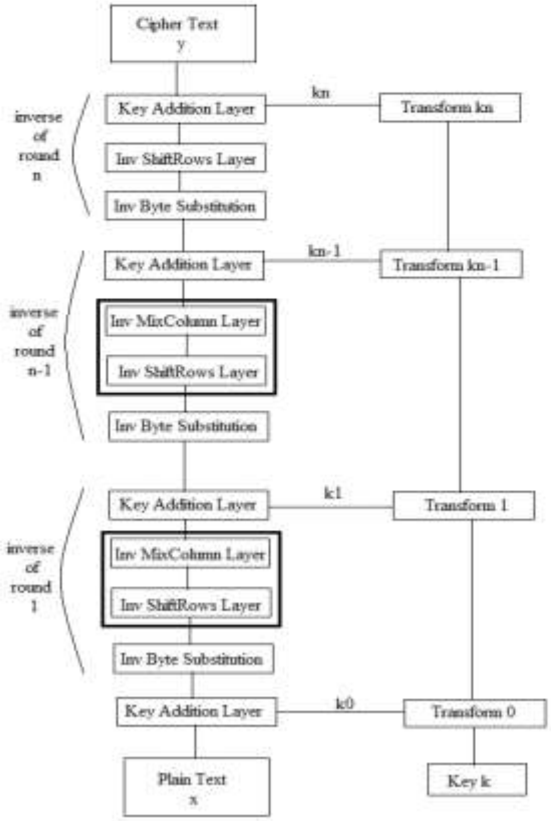


Fig. 5 Rounds of Decryption Process

InvMixColumn

$$\begin{pmatrix} B_0 \\ B_1 \\ B_2 \\ B_3 \end{pmatrix} = \begin{pmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{pmatrix} \cdot \begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix}$$

InvShiftRows

Input matrix =>

B_0	B_4	B_8	B_{12}
B_1	B_5	B_9	B_{13}
B_2	B_6	B_{10}	B_{14}
B_3	B_7	B_{11}	B_{15}

Output matrix =>

B_0	B_4	B_8	B_{12}	no shift
B_{13}	B_1	B_5	B_9	→ one position right shift
B_{10}	B_{14}	B_2	B_6	→ two positions right shift
B_7	B_{11}	B_{15}	B_3	→ three positions right shift

V. CONCLUSION AND FUTURE WORK

The proposed work aims in the design of secured data storage and error tolerance in cloud storage. The data storage security is provided by the way of storing data using partitioning technique and encryption decryption technique. The small units of files that are split is encrypted which provides more security. The data loss analysis has taken care during this process by proctor. It also gives way for flexible access and there is less cost in cloud data storage. The space and time is also effectively reduced during cloud storage. Dynamic operation is another important concept where, encryption and decryption process secures data, when storing into cloud. Also the remote data integrity checking detects the threats and misbehaving server.

In Future we planned to provide higher level of security by using advanced encryption and decryption algorithm and searching mechanisms for outsourced computations in cloud services.

REFERENCES:

1) Wang Qian, RenKui, Cao Ning and Lou Wenjing , "Toward Secure and Dependable Storage Services in Cloud Computing," Services Computing, IEEE Transactions on , vol.5, no.2, pp.220-232, April-June 2012.

2) Hsiao-Ying Lin; Tzeng, W.-G.; , "A Secure Erasure Code-Based Cloud Storage System with Secure Data," IEEE Transactions on , vol.23, no.6, pp.995-1003, June 2012.

3) Zhiguo Wan; Deng, R.H.; , "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control inCloud Computing," Information Forensics and Security, IEEE Transactions on , vol.7, no.2, pp.743-754, April 2012.

4) Zorzo, S.D.; "Privacy Mechanism for Applications in Cloud Computing," IEEE (Revise IEEE America Latina) , vol.10, no.1, pp.1402-1407, Jan. 2012.

5) C. Wang, S.S.M. Chow and W. Lou, “Privacy- Preserving Public Auditing for Secure Cloud computing Storage,” IEEE Trans.Computers, preprint, 2012.

6) ZhuoHao, "A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability" IEEE Transactions on Knowledge and Data Engineering, Vol. 23, No. 9, pp. 1432-1437, September 2011.

7) FlorinaAlmenares, Patricia Arias, Daniel Díaz-Sanchez and Andres Marín, "Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing" IEEE Transactions on Consumer Electronics, Vol. 58, No. 1, pp. 95-103, February 2012.

8) Cong Wang; KuiRen; Wenjing Lou; Jin Li; , "Enabling Public Auditability and Data Dynamics for Storage Security inCloud Computing," Parallel and Distributed Systems, IEEE Transactions on, vol.22, no.5, pp.847-859, May 2011.

9) Ravi Jhawar, Vincenzo Piuri and Marco Santambrogio, "Fault Tolerance Management in Cloud Computing:A System-Level Perspective" IEEE Systems Journal, Vol. 7, No. 2, pp. 288-297, June 2013.

10) C. Wang and W. Lou, “Ensuring Data Storage Security in Cloud Computing,” Proc. 17th Int’l Workshop Quality ofService (IWQoS ’09), pp. 1-9, July 2009