Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Data Partitioning: A Secured Data Storage on Cloud Environment

Archana G. Said
Department of Computer Engineering
Institute of Information Technology
All India Shri Shivaji Memorial Soceity's

Abstract— ***Cloud computing is a recently evolved computing terminology or allegory based on utility and consumption of different computing resources. Cloud computing is the competent way of computing services over the Internet. Cloud services allow persons and business to use software and hardware that are managed by third parties at remote locations. In cloud computing data security, integrity and access control are demanding issues, these issues remain the primary facts for adoption of cloud computing services. Existing solutions that use wholesome cryptographic techniques to tone down security and access control problems. In this paper, the proposed data partitioning technique with cryptography which ensure cloud storage security, integrity. Cloud storage integrity checking concept is used to enhance the integrity of cloud storage. System model constitutes of three layers namely client machine, trusted Third Party (TTP) and cloud storage servers. Partitioning method implemented at trusted third party. TTP performs operation like partition data, , Public key generation for each partition, Encrypt each partition using particular keys, storing each partition sequence of respective data, signature key and file attributes on its own server, sending partition at appropriate cloud server, retrieve as well merging of partitions, Decryption and integrity checking of data.***

Keywords — Cloud Model, Data Partitioning, Cloud Storage Integrity Checking, Encryption, Decryption

I. INTRODUCTION

Cloud computing enables companies to use compute resources as a service just like electricity -- rather than having to build and maintain computing infrastructures in-house.
Cloud computing promises several attractive benefits for businesses and end users. Three of the main advantage of cloud computing includes:

A. Self-service provisioning*:* End users can rotate up computing resources for almost any type of workload on-demand.
B. Flexibility*:* Companies can extent up as computing needs increase and then scale down again as demands decrease.
C. Pay per usage percentage*:* Computing resources are measured at a granular level, allowing users to pay only for the resources and workloads they use.

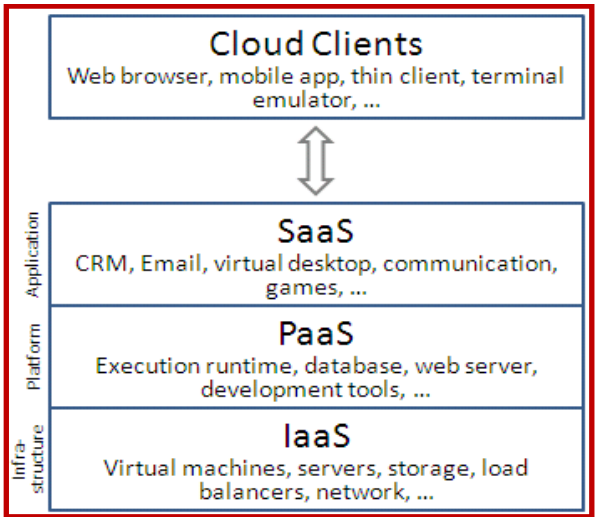

Figure1. Cloud Computing System

II. CLOUD COMPUTING SECURITY

Cloud computing security is the set of control-based technologies and policies designed to adhere to regulatory compliance rules and protection for the information, various data applications and infrastructure associated with cloud computing use. With employees, customers, business associates, supplier increasingly accessing corporate applications and data with mobile devices from the cloud system, protecting the edge of the network is no longer enough

A. Know who is accessing what

People within your organization who are privileged users, – such as DBA and employees with access to highly valuable intellectual property – should receive a higher level of analysis, receive training on securely handling data, and tight access control.

B. Limit data access based on user context

Change the level of access to data in the cloud depending on where the user is and what device they are using.

C. Take a risk-based approach to securing assets used in the cloud

Identify database with highly sensitive or valuable data and provide added protection, encryption mechanism and monitoring around the data.

D. Extend security to the device

Make sure that corporate data is isolated from personal data on the mobile devices. Install a patch management agent on the device so that it is always running the latest level of software. Scan mobile applications to check for threats.

E. Add intelligence to network protection

The network still needs to be protected. Network protection devices need to have the ability to provide massive control with analytics and insight into which users are accessing what content and applications.

F. Build in the ability to see through the cloud

Security devices, such as those validating/authenticating user IDs and corresponding passwords, take security data to create the audit file needed for regulatory agreement and forensic investigation process. The trick is to find important/significant signals about a likely attack or security risks in the large amount of data.

III. CURRENT SCENARIO OF DATA STORAGE IN CLOUD

Cloud storage is a model of data storage where the digital data is stored in several logical pools, the physical storage distributed on multiple servers (and often locations), and the physical setting is typically owned and managed by a host company. People and organizations buy or lease storage capacity from the providers to store verity of data from user, organization, or some specific application data.

Cloud storage is based on highly virtualized infrastructure and is like broader cloud computing in terms of accessible interface, near-instant elasticity and scalability, multi-tenancy, and metered resources. Cloud storage services can be utilized from an off-premises service.

Cloud storage typically refers to a object storage service, but the term has expanded to include other types of data storage that are now available as a different services, like block storage and chunk storage.

IV. PROPOSED SYSTEM FOR DATA STORAGE ON CLOUD.

Now days many enterprises generate abundant amount of data that cannot be seated on local/desktop machines. For data storage and security cloud system is more advantageous.

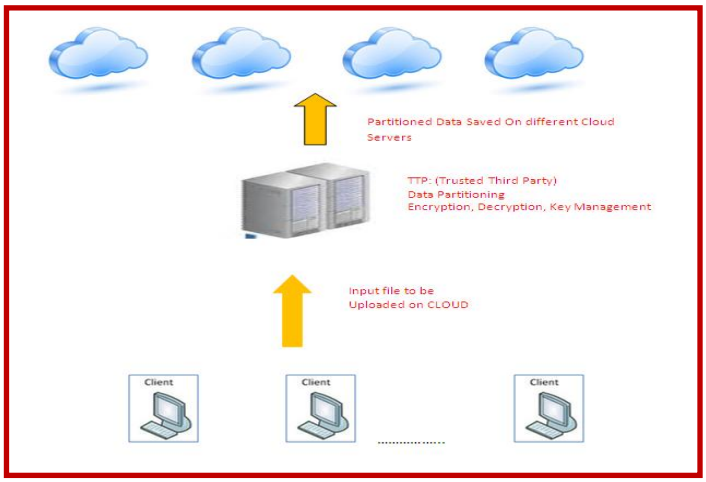

Figure 2. Proposed System Architecture

To store large quantity of data it will be first partitioned into number of chunks, each data chunk is then encrypted by Data Encryption Algorithm. Encrypted data is then stored on cloud.

V. DEFINITION OF PARTITIONING

A partition is a division of a logical database or its element into distinct non related parts. Database partitioning is normally done for easy manageability, effective performance.

Benefits of Data Partitioning

A popular and favorable application of partitioning is in a distributed database management system. Each partition may be loaded over multiple terminals, and users at the node/terminal can perform local transactions/manipulations on the partition. This increases performance for site that have regular transactions involving certain views of data, at the same time as maintaining availability and security

Advantages of Data Partitioning

1. Performance,
2. Maintenance, and
3. Availability.

1. Performance advantages

A data is partitioned based on criteria such as the value for a particular column. If a query requests data with a specified selection condition that would skip a complete partition.

2. Maintenance advantages

Most maintenance operations can be performed on a single partition. You can restore or recover a partition rather than the entire data table. In this way, you can considerably reduce the time required to do maintenance operations.

3. Availability

You can also use partitioning to place partitions into different tablespaces to improve availability. One tablespace can leave down without affecting the other tablespaces. If a tablespace is not available, the other tablespaces and their partitions are still available for data processing.

Splitting data into different partitions is also a time saving process. When you reduce the amount of data in each partition, it also reduces the amount of time required to recover the data from that partition.

VI. PARTITIONING CRITERIA

Now a days high end relational database management systems provide for different criteria to split the database. They take key parameter as a *partitioning key* and assign a partition based on some specific criteria. Common criteria for partitioning are as follows with country code zip code values:

A. Range partitioning

Selects a partition by determining if the partitioning key is inside a some specific range. An example could be a partition for all rows where the column zip code of a country has a value between 80000 and 89999.

B. List partitioning

A partition is assigned a list of key values. If the partitioning key has one of these values, the partition is selected. For example all rows where the column Country is Iceland, Norway, Sweden, Finland or Denmark could build a partition for the Nordic countries.

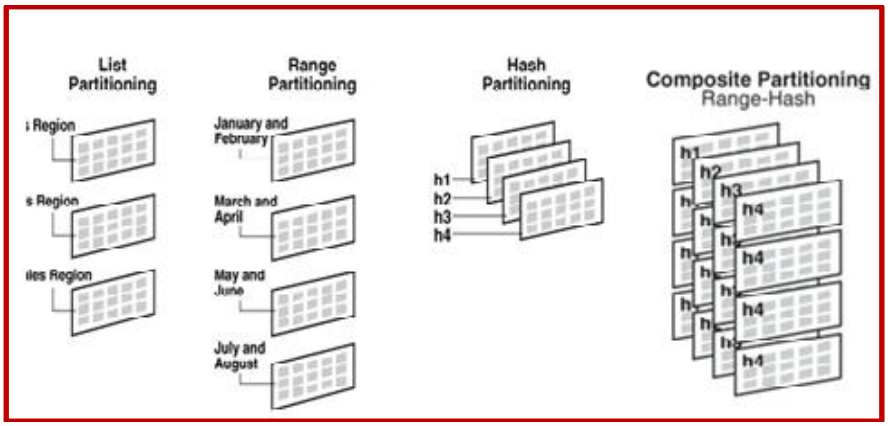

Figure 3. Partitioning Methods

C. Hash partitioning

The value of a hash function determines membership of a values in a particular partition. Assuming there are four partitions, the hash function could return a value among 0 to 3.

D. Composite partitioning

Composite partitioning is a partitioning technique that combines some of the other partitioning methods. The table is primarily partitioned by the first by range partitioning method and then each partition is sub-partitioned by the hash partitioning method.

Algorithm: Proposed system divided in 3 different modules as follow:

1. Client End: client machine is used by user who wants to store data on cloud nodes . Client machine browser enabled desk top machine

2. Cloud Storage Server: Machine which is going to Manage and provide storage space for the data chunks, computational resources and storage services by the cloud service provider (CSP).

3. Trusted Third Party (TTP): TTP, is the expertise and having capabilities to provide partitioning the data, encrypt data, store on the cloud servers and manage different resources among clients.

Encryption-Decryption Algorithm

For Encryption technique is used to encrypt the partitions of files for security and Integrity purpose. To encrypt data partitions RSA public key algorithm is used. Using Clients public key data is encrypted, stored on the cloud servers.

At the time data retrieval client is going to request data. TTP will search for the respective data partition and will return data to the client.

VII. CONCLUSION

In this paper we proposed data partitioning and storage technique for data storage security in cloud services. The partitioning of data enables storing of the data in easy and effective manner. It also gives way for easy access and there is less cost in data storage. Cloud storage integrity concept used to ensure integrity of stored data The space and time is also effectively reduced during storage. Integrity of data storage is achieved by applying encryption algorithm.

REFERENCES

[1] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou,"Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", IEEE INFOCOM 2010, San Diego, CA, March 2010

[2] Sunil Sanka, Chittaranjan Hota, Muttukrishnan Rajarajan," Secure Data Access in Cloud Computing", Computer Science and Information Systems Group, Birla Institute of Technology and Science-Pilani.

[3] Ayad F. Barsoum and M. Anwar Hasan," Enabling Data Dynamic and Indirect Mutual Trust for Cloud Computing Storage Systems", University of Waterloo, Ontario, Canada. IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSYEMS VOL: PP NO: 99 YEAR 2013

[4] M. Sudha, Dr.Bandaru Rama Krishna Rao, M. Monica," **A** Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment" International Journal of Computer Applications (0975 – 8887) Volume 12– No.8, December 2010

