INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

ENSURE DATA SECURITY IN CLOUD STORAGE

PAVAN MUNDHARE

Computer Networking and Engineering Department, Khurana Sawant Institute of Engineering and Technology, Hingoli, Mah.

Accepted Date: 26/02/2015; Published Date: 01/03/2015

Abstract: Today's world relies on cloud computing to store their public as well as some personal information which is needed by the user. Cloud services offered to its users by cloud service providers. Clouds are generally implemented on cluster computers to provide the necessary scale and performance required by such services. As cloud computing have some advantages but also there are some drawbacks such as privacy of user's data, security of users data is very important aspects. The single database storage system is a less secure because data remain under a single database or better say data servers. This can lead to data loss due to different causes like hacking, server failure etc. If an attacker chooses to attack a specific user, then he can concentrate on a fixed cloud provider, try to have access to the client's information. This makes an easy job of the attackers, and gets the benefit of using data mining to a great extent. Thus single data server storage architecture is the biggest security threat concerning data mining on cloud, so in this paper present the secure approach that encrypt and replicate the data in distributed data server storage system. This approach involves the replication and storage of data.

Keywords: Computing, Cloud Storage, Cluster Computers, Replication, Security, Data Server.

Corresponding Author: MR. PAVAN MUNDHARE

Access Online On:

www.ijpret.com

How to Cite This Article:

Pavan Mundhare, IJPRET, 2015; Volume 3 (7): 138-145

PAPER-QR CODE

INTRODUCTION

The term cloud computing is used to capture vision of computing as a utility. A cloud is defined as a set of Internet-based application, storage and computing services sufficient to support most users' needs, thus enabling them to largely or totally dispense with local data storage and application software. Cloud computing is technology that provides the different services at very low cost. The different client stores data on Cloud storage. Cloud computing provides storage for storing the information and provides the security of that information. Cloud service models are infrastructure as a service, platform as a service, and software as a service and new for cloud is database as a service.

Cloud services are provided by different famous organizations like Google, Amazon and Microsoft etc. By using these services the client avoid the cost of buying extra resources. Cloud services provide the high computation capacity at low cost. The various data analysis techniques which are used for extracting valuable information from a large volume of data. These different techniques are used by Cloud service provider like Google uses the technique for identifying the user behaviour on the basis of search behaviour. In previous trend data to store on a single cloud the attacker applies an attack on it and accesses the information which is stored by the client on cloud storage. If the client is a field related to healthcare, shopping, insurance, banking, etc then there is big loss of information access by attackers, so distributed environment handles such kind of problem. The distributed data mart storage is service which is provided by cloud service provider. In Distributed Cloud storage, the information is stored from different kind of devices they only pay for storage as per usage.

Cloud Storage is a type of service that allow a user to save data on offsite storage system managed by third-party and is made accessible by a web services API. On cloud the data is stored at virtualized pools of storage. Hosting companies operate large space data centres and lease their storage. And companies, organizations and institutes who require their data to be hosted buy or lease storage capacity from hosting companies. The cloud storage system stores multiple copies of data on multiple servers and at different locations. If one system fails, then it only requires tracking the replicated data location.

Cloud Storage is a type of service that allow a user to save data on offsite storage system managed by third-party and is made accessible by a web services API. On cloud the data is stored at virtualized pools of storage. Hosting companies operate large space data centres and lease their storage. And companies, organizations and institutes who require their data to be hosted buy or lease storage capacity from hosting companies. The cloud storage system stores

multiple copies of data on multiple servers and at different locations. If one system fails, then it only requires to track the replicated data location.

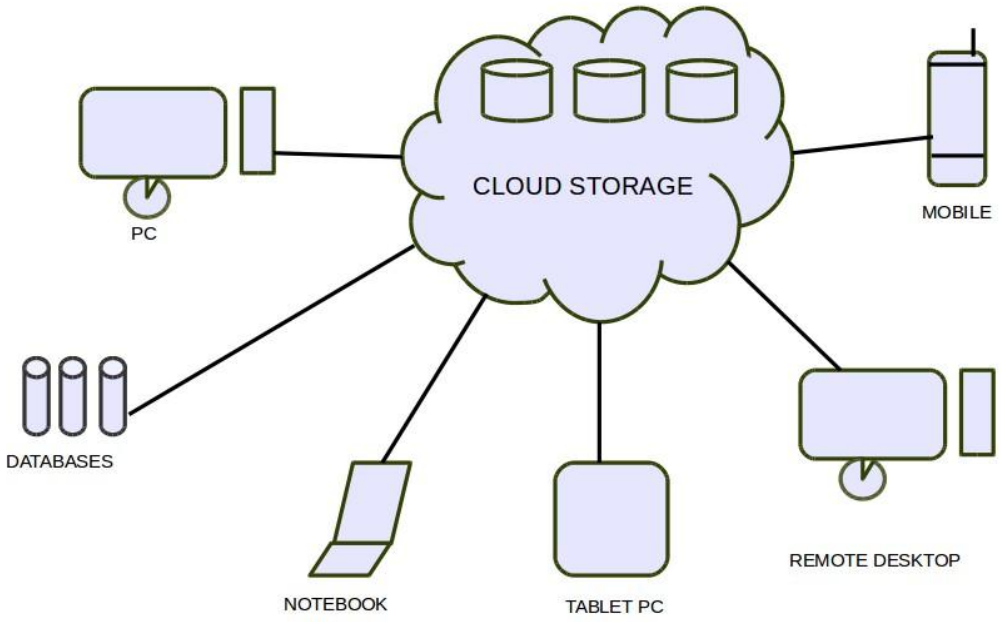

Figure 1: Cloud Storage System

The Figure [1] indicates cloud storage stores the information from different devices and these devices can access the information on demand at any time. Here purposes a secure approach that replicates the client's data and store on different data servers. Before replication, full copy of encrypted information stores on data warehouse for increasing the availability of information. It will increase the reliability and privacy of data. Storing the data in cloud is not that simple task. Apart from its flexibility and convenience, it also has several challenges faced by the consumers.

The consumers require ability to:

- Provision additional storage on demand.
- Know and restrict the physical location of the stored data.
- Verify- how data was erased
- Have access to a documented process for surely disposing of data storage hardware.

- Administrator access control over data.

2. LITERATURE REVIEW:

Cloud-based computing is an emerging practice that offers significantly more infrastructure and financial flexibility than traditional computing models. Cloud providers today offer everything from access to raw compute or storage capacity resources to full-blown application services in areas such as payroll and customer relationship management.

With cloud computing, all your data is stored on the cloud. That's all well and good, but how secure is the cloud? Can other, unauthorized users gain access to your confidential data? Theoretically, data stored in the cloud is unusually safe, replicated across multiple machines. But on the off chance that your data does go missing, you have no physical or local backup. Unless you methodically download all your cloud documents to your own desktop.

The data owner searches the data from encrypted data bases the search is based on rank keyword. The ranked keyword base search reduces the overhead of the data owner because there is no need to go through from each file. In this technique, the server site is only responsible for the search operation all other responsibilities are taken by the data owner [1].

Cloud Data Protection for Masses proposes a new cloud computing paradigm, data protection as a service. DPaaS is a suite of security primitives offered by a cloud platform, which enforces data security and privacy and offers evidence of privacy to data owners, even in the presence of potentially compromised or malicious applications. Data protection is provided by using three primitives they are access control, key management and logging. Also there is an auditor who audits all the transactions occurred in the system. Auditor finally provides an audit report based on all conversations.[2].

For the protection of data privacy, sensitive data usually have to be encrypted before outsourcing. This technique formalizes and solves the problem of effective fuzzy keyword search over encrypted cloud data while maintaining keyword privacy. Fuzzy keyword search greatly enhances system usability by returning the matching files when user's searching inputs exactly match the predefined keywords or the closest possible matching files based on keyword similarity semantics, when exact match fails. This idea exploit edit distance to quantify keywords similarity and develop an advanced technique on constructing fuzzy keyword sets, which greatly reduces the storage and representation overheads [3].

Cloud security storage system is responsible for client's information. Sometimes the client's information is very sensitive then the cloud security storage system provides the security. The cloud security storage system is mostly adopted by different companies. Therefore, this project is supposed to create good social and economic benefits [4]. Song [5] presents an algorithm of search on encrypted data, uses an encryption information retrieval algorithm realizes adding authentication mechanism into encrypted result, the algorithm has a strong ability to resist the statistical analysis, but in cloud computing environment, complex validation process will consume too many resources.

A number of authentication techniques have been proposed in the recent times that are based upon graphical methods. Text based passwords are most commonly used for authentication; however they are highly vulnerable to several kinds of attacks. Graphical techniques are coming up as an attractive alternative to the conventional methods of authentication. In this paper proposed a graphical method of authentication that employs graphical coordinates along with a novel introduction of time interval between successive clicks. The user needs to recall the coordinates and the time interval of the successive clicks. This leads to the incorporation of the advantages of the recent graphical methods along with the added security achieved through the use of time interval. The proposed scheme has a much higher password space than the other contemporary graphical authentication schemes. The scheme is robust, secure and very convenient to use [3]. Both the administrator and the users should undergo the graphical password text. In view of the shortcomings of the traditional approach to authentication, i.e. alphanumeric passwords, Graphical techniques are gaining importance [6].

3. M ATERIAL AND METHODOLOGIES:

Clouds are generally implemented on cluster computers to provide the necessary scale and performance required by such services. A cluster computer is a set of interconnected computers that cooperate closely to provide a single, integrated high performance computing capability.

One cloud computing solution is to deploy the platform as a means for disaster recovery, business continuity, and extending the data center. With flexible "pay-as-you-grow" models, cloud computing can evolve with the needs of your business. In using the cloud, many organizations are still asking –When should I use the cloud for replication?

Replication is absolutely important for multiple people looking at the same data at the same time, depending on where they are, and it is very important for disaster recovery.

3.1 Working of Secure replication system architecture

The process is carried out as follows:-

- Step1: Client sends data to cloud service provider for storing.
- Step2: Cloud provides receive data and perform encryption.
- Step3: Full copy of encrypted data stores on data warehouse.
- Step4: After backup, performing replication and divide the data in parts according to the availability of data bucket (in our system use three data buckets B1,B2,B3)
- Step5: Storing the different part of information on different data bucket.
- Step6: Repeat Steps as per storing request.

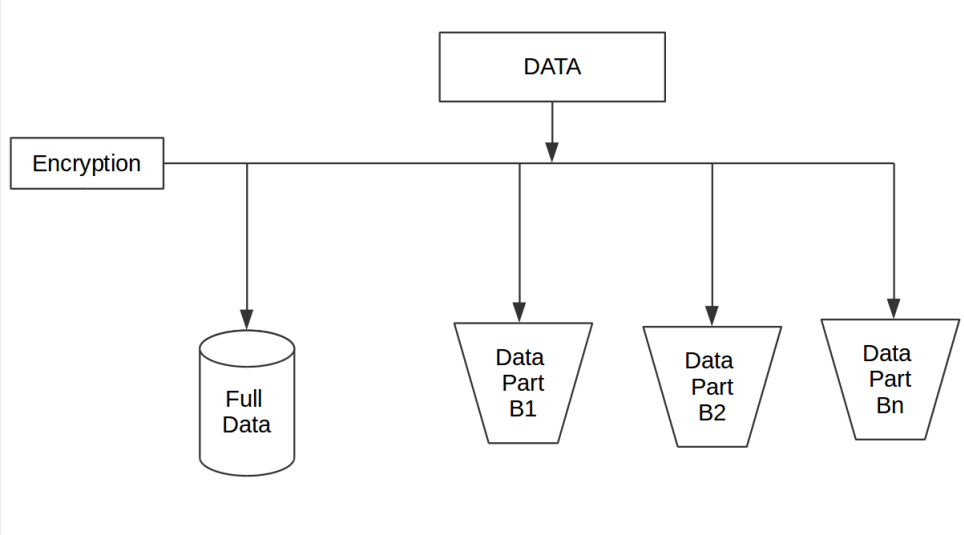

Figure 2: Secure replication system architecture

4. RESULT AND DISCUSSION:

In this system client send data to cloud service provider for storing it. The cloud receive data from client and perform encryption on it. After performing encryption full copy of data stores on data warehouse for backup. After full backup, performing replication divide the data in parts according to the availability of data bucket. In purposed system use three data buckets (B1, B2, B3) for increasing privacy and availability of client's data. The client's data store on backup warehouse and then divide the data in three parts and store on respective data buckets B1, B2,

B3. If any data bucket lost the part of client's data then it can reload from backup warehouse. In this way replication of client's data on different data buckets increase the availability of information as well as enhance the security of information.

This makes difficult job of the attackers. The insider attacker refers as employee that works under organization which is responsible securing and storing the client's information. If any data bucket hack by an attacker then it can access the only part of information, for full information there is need to apply attacks on other data buckets. The data bucket is crashes or down also impact on the availability of information. The purposed system also removes that drawback. If any data bucket is crashes or down then client's request also able to extract the data from backup warehouse. In this scenario data bucket B1 is fail and not responding the user request. In this case the part of information is lost.

The purposed system allow user to extract the information from backup ware house. The availability of data bucket also affect on security of information. In case of large no of data buckets the data divide in more parts and store different parts in different data buckets. Each data buckets have very small part of information. If any data bucket is hacked by attacker then it can take only small part of information.

5. CONCLUSION:

Many of cloud users think that cloud is secure and easier. However, most of the IT experts feel that the cloud has lots of problems in the field of data security and privacy issues towards the growth of cloud computing. No user will transfer their data to the cloud until the trust is built between the cloud service providers and consumers. In this paper, I have outlined the general principles of new approach to perform secure replication on stored data. This is a most influential technique which will provide better results for security and availability of information. This secure replication technique can be usefull in order to build a secure and reliable distributed storage. The enhancement done in this technique will increase the quality by different data server host with cloud provider and store information according to its sensitivity. This new technique can be applicable in different cloud providers companies and organizations etc.

6. REFERENCES

1. Gupta Sarika, Sangita Rani Satapathy, Mehta Piyush and Tripathy Anupam, "A Secure and Searchable Data Storage in Cloud Computing", 3rd IEEE International Advance Computing Conference (IACC), 2013, page 106-109.

2. Dawn Song, Elaine Shi, Ian Fischer, and Umesh Shankar. “Cloud data protection for the masses”, IEEE Transactions in Computer Society, 45(1):39–45, 2012.

3. Sunumol Cherian and Kavitha Murukezhan. “Providing data protection as a service in cloud computing”, International Journal of Scientific and Research Publications, Volume 3, Issue 6, June 2013 ,ISSN 2250-3153.

4. Liu Hao, Dezhi Han, “The study and design on secure-cloud storage system”, In IEEE society, 2011, page 5126-5129.

5. D. Song, D. Wagner and A. Perrig, “Practical techniques for searching on encrypted data”, IEEE Symp on Research in Security and Privacy. Los Alamitos, CA: IEEE Computer Society, (2000), pp. 44-55.

6. Ashwini G. Raut. “Slicing of graphical password for privacy preserving in cloud computing”, International Journal of Scientific & Engineering Research., 5(4):57– 59, 2014.

7. Taeho Jung, Xiang-Yang, Zhiguo Wan, Meng Wan, “Privacy Preserving Cloud Data Access With Multi- Authorities”, Proceedings IEEE INFOCOM, 2013, page 2625-2633.

8. Julian Jang-Jaccard, A vnish Manraj and Nepal Surya, “Portable Key Management Service for Cloud Storage”, 8th International Conference on Collaborative Computing: Networking, Applications and Worksharing, 2012, page 147-156.

9. Gupta Arjun Kumar, Byung Gook Lee, HoonJae Lee and Anu Kumari, “Secure Storage and Access of Data in Cloud Computing”, In IEEE society, 2012, page 336-339.

10. Shakeel Ahlam Ansari Ahmed and Devadkar Kailas Kisan, “Secure Cloud Mining”, IEEE International Conference on Computational Intelligence and Computing Research, 2012.

11. Jin Li, Qian Wang, Cong Wang, and Ning Cao. “Fuzzy keyword search over encrypted data in cloud computing”, IEEE Transactions on INFOCOM, 2010, 3, 2010.