CONSISTENCY AND PRIVACY BASED REPLICATION SYSTEM IN SECURE SHARING FRAMEWORK

[*]N.Geetha, Assistant Professor, Department of Computer Science ,
Bharathiyar college of Engineering and Technology, Karaikal.
**M.Gayathri, II year M.Tech computer science,
Bharathiyar college of Engineering and Technology, Karaikal.

ABSTRACT

In Big data, users can outsource their computation and cost-effective manner to servers (also called clouds data storage) using Internet. Clouds can provide several types of services like applications infrastructures risk and platforms to help developers write applications (e.g., Amazon's S3, Windows Azure). Much of the data stored in clouds is highly sensitive. Security and privacy are thus very important issues in cloud data storage. In one hand, the user should authenticate itself before initiating any transaction, and on the other user, it must be ensured that the cloud accessing for cryptographic role-based access control (RBAC). The cloud can hold the user accountable for the data it outsources, and likewise, the cloud itself accountable for the services it provides. The validity of the user who stores the data is also verified. Cloud servers are prone to Hierarchical RBAC system, where a storage server can fail in arbitrary ways. The cloud is also prone to data modification and server colluding user behavior privileges'. In server colluding cloud storages, the adversary can compromise storage servers, so that it can modify data files as long as they are internally consistent. To provide secure data storage, the data needs to be encrypted. However, the data is often modified and this dynamic property needs to be taken into account while designing efficient secure storage techniques. So analyze efficient search on encrypted data is also an important concern in clouds. The clouds should not know the query but should be able to return the records that satisfy the query. This is achieved by means of searchable encryption. Access control in clouds is gaining attention because it is important that only authorized users have access to valid service. A huge amount of information is being stored in the cloud, and much of this is sensitive information. Care should be taken to ensure access control of this sensitive information which can often related to health, important documents. So we implement decentralized access control and user revocation schemes to improve security and privacy in real time cloud environments.

Keywords*: Big Data, Data Fragmentation, Node placement, User operation, RBAC*

1.INTRODUCTION

Big Data is an emerging technology which provider a lot of opportunities for online sharing of resources or services. One of the fundamental advantages of CC is pay-as you-go pricing model, where customers pay only according to their usage of the services. Cloud Computing is an internet oriented a computing. It dynamically delivers everything as a service over the internet base an on user demand, such as network, operating system, storage, hardware, software and resources. These are cloud services types: Infrastructure as a service (Iaas), Platform as a service (Paas), and Software as a Service (Saas). Cloud Computing is implementation as three models such as Public, Private and Hybrid Clouds. Cloud Storage system, is a also known as DAAS (Data storage as a service), is the abstract of storage last an interface where resources can be administered on demand. Cloud data resources works on sharing file systems because of its ability to handle an infinite volume of data effectively. Storage can be local or remote. Cloud computing is cost effective, secure and scalable but managing the load of random job available is a difficult work. Data availability means data is accessible

When never it is requested. Accessibility of data increases with increment in number of duplication of data. But after reaching a specific level of duplication, there occurs no development in availability. So it is better to find an optimum level of duplication. Availability and duplication ratio also depends on node failure ratio. If failure probability is high, more number of duplication of that data is required. So if node failure ratio is less, less duplication number is required for maximum file availability.

2. LITERATURE SURVEY

2.1 Role-based access controls

In this paper proposed According to the respective advantages of RBAC model and UCON model, Subject, Object, Role, Permission and Operation are all regarded as the instance of the class with attributes and methods on object-oriented programming, role-based access control model with the constraints of Temporal, spatial, attribute and workflow (TSAW-RBAC model) is proposed, the Observer Entity is introduced that assigns the operations to the Object according to the attributes of the Object and the Supervisor Entity is introduced that assigns the roles to the user according to the attributes of the user. It Can implement access control based on temporal and spatial constraints in the distributed computing environment, can implement user’s role-assign automatically based on Subject’s attributes and object’s attributes, can implement workflow based on the constraints of Subject’s attributes and object’s attributes, can implement the Digital Rights Management(DRM) and Trust Management.

2.2 A data outsourcing architecture combining cryptography and access control

The outsourcing of data into the cloud inherently requires a mechanism to control the access capability of the users and the cloud providers. This mechanism requires efficient cryptographic primitives to achieve fine grained access control of data, proof of storage, and revocation of the authorization. In this paper, we present a secure cloud data storage architecture with the features of dynamic user construction, revocation of the authorization, and proof of storage. In the proposed architecture, we used attribute based broadcast encryption, attribute based access control, and proxy re-encryption to achieve an efficient solution.

2.3 Over-encryption: Management of access control evolution on outsourced data

In this paper proposed a flexible distributed storage integrity auditing mechanism, utilizing the homomorphism token and distributed erasure-coded data. The proposed design allows users to audit the cloud storage with very lightweight communication and computation cost. The ever cheaper and more powerful processors, together with the software as a service (SaaS) computing architecture, are transforming data centers into pools of computing service on a huge scale. In this paper, we propose an effective and flexible distributed storage verification scheme with explicit dynamic data support to ensure the correctness and availability of users’ data in the cloud. To ensure the security and dependability for cloud data storage under the aforementioned adversary model, we aim to design efficient mechanisms for dynamic data verification and operation and achieve the following goals: (1) Storage correctness (2) Fast localization of data error (3) Dynamic data support (4) Dependability (5) Lightweight. To achieve the assurances of cloud data integrity and availability and enforce the quality of dependable cloud storage service for users, we propose an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append.

2.4 Privacy Preserving Access Control with Authentication for Securing Data in Clouds

In this paper, we propose a new privacy preserving authenticated access control scheme for securing data in clouds. In the proposed scheme, the cloud verifies the authenticity of the user without knowing the user’s identity before storing information. We propose our privacy preserving authenticated access control scheme. According to our scheme an user can create a file and store it securely in the cloud. This scheme consists of use of the two protocols ABE and ABS. A trustee can be someone like the federal government who manages social insurance numbers etc. A creator on presenting the token to one or more KDCs receives keys for encryption/decryption and signing. The access policy decides who can access the data stored in the cloud. If the user has attributes matching with access policy, it can decrypt and get back original message. Write proceeds in the same way as file creation. By designating the verification process to the cloud, it relieves the individual users from time consuming verifications. We will show that our scheme authenticates an user who wants to write to the cloud. An user can only write provided the cloud is able to validate its access claim. An invalid user cannot receive attributes from a KDC, if it does not have the credentials from the trustee. If an user's credentials are revoked, then it cannot replace data with previous stale data, thus preventing replay attacks. Our scheme not only provides fine-grained access control but also authenticates users who store information in the cloud.

3. RELATED WORK

K. Bilal,et.al…,[1] presented a comparison of the major DCN architectures that address the issue of network scalability and oversubscription and simulated the performance of the major DCN architectures in various practical scenario under different network configurations. The presentation of the three-tier architecture is dependent on physical topology and oversubscription share at different network layers.

M. Manzano,et.al…,[2] represents the robustness analysis of the DCN topologies and various observations. The results provide the classical robustness metrics, such as average nodal degree, algebraic connectivity, and spectral radiuses are incapable to evaluate DCNs appropriately. Most of the metrics only regarded as the largest connected component for robustness evaluation.

D. Boru,et.al…,[3] projected a data duplication technique for cloud computing with datacenters which save the energy, network band width and communication delay both between geographically sharing data centers as well as inside each data center.

W. A. Jansen,et.al…, [4] formative the privacy of complex computer systems is also a ancient privacy problem that overshadows large scale computing in general. Attaining the high promise qualities in development has been an obscure goal of computer privacy researchers and practitioners, and is also a job in growth for cloud computing.

G. Kappes,et.al…,[5] analyze the privacy requirements in multi tenant data systems. Then we introduce the dike authentication architecture, which combines native access control with renter namespace isolation that is backwards compatible to object-based file systems.

4. DROPS FRAMEWORK

Duplicate can be used for maintaining availability in company any load conditions or failure situations. By improving the technique of duplicate, performance and availability of system can be improved. But excessive duplicate can also adverse effects like high level storage cost or degradation in systems overall Performance due to excessive use of bandwidth. So DROPS framework is better to use because it can understand fragments of the data. T-coloring algorithm can provide improved results in case when system is in model state. It is generally used when requests are of similar nature and distributed equally. In T-coloring, measure the distances of each data for placing data in cloud system. Distances are calculated using centrality measure. Centrality is measure of the relative importance of a node in the network. But in DROPS framework, data can be lost due to updation at the time of retrieving from cloud storage. This problem can be overcome by the following section and illustrated DROPS framework in fig 1.

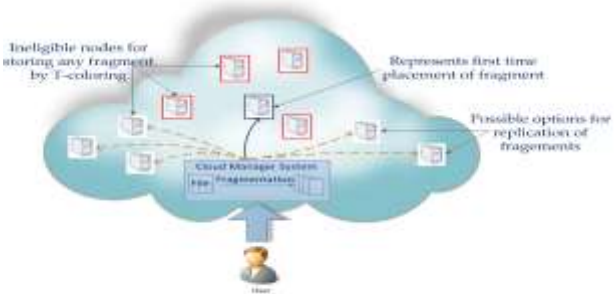

Ineligible nodes for storing any fragment by T-coloring
Represents first time placement of fragment
Possible options for replication of fragements
Cloud Manager System
Fragmentation
User

Fig- 1: DROPS Framework

5. IMPROVED TRUST MODELS

Big data service provider requires a system which can handle a large number of requests at a time. For processing the huge cloud of requests for data access permission, services need to be very available. System keeps many copies of the blocks of data on different nodes by duplicate. A large number of replication strategies for management of replicas have been implemented in traditional system. As a result of replication, data replications are stored on different data nodes for high reliability and availability. Duplication factor for each data block and replica placement sites need to be decided at first. In existing framework data can be lost so in this paper propose improved

DROPS framework that includes heuristic auditing strategy to protect the data from loss. It present efficient consistency as a service model, where a group of data owners that constitute service provider can verify whether the data cloud update the data or not and design user operation table to change status of fragmented files with different metrics and proposed framework in fig 2.

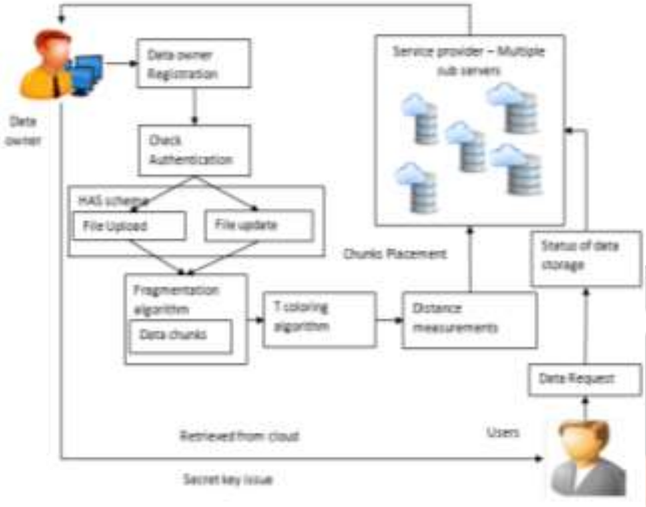
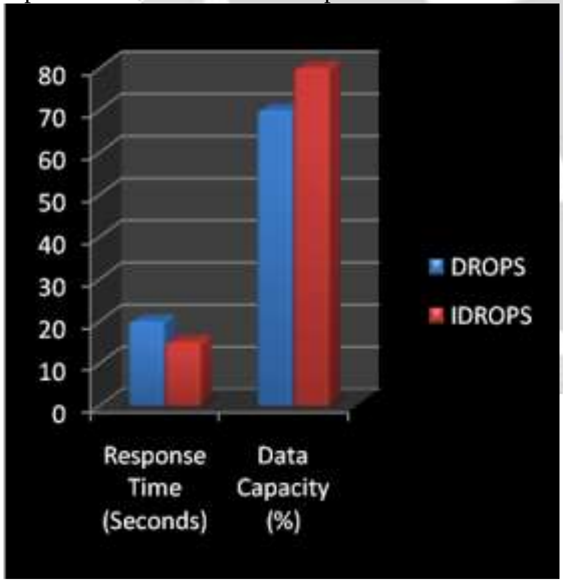


Fig- 2: Improved Cloud storage Framework

6. EXPERIMENTAL RESULTS

We can evaluate the performance of the system using the parameters such as (i) increasing the number of nodes in the system, (ii) increasing the number of objects keeping number of nodes constant, (iii) changing the nodes storage capacity, and (iv) varying the read/write ratio. These measurements are consolidated as capacity of replication node and time of updation. And it can be plotted as graph in fig 3.



7. CONCLUSION

In this paper, we present enabling data integrity proof and consistency services over multi cloud system using Heuristic auditing strategy which helps in revealing violations as much as possible. The cloud consistency model and local auditing, global auditing that helps users to verify the cloud service provider (CSP) provides the promised consistency or not and quantify the severity of the violations. Therefore system monitors consistency service model as well as level of data upload which helps the user to get the data in updated version. User can understand various sub servers in trust models. It is a considered to provide regular update mechanism to authenticate fragments simply and provide the data to users after updating only.

8.REFERENCES

[1] K. Bilal, S. U. Khan, L. Zhang, H. Li, K. Hayat, S. A. Madani, N. Min-Allah, L. Wang, D. Chen, M. Iqbal, C. Z. Xu, and A. Y. Zomaya, “Quantitative comparisons of the state of the art data center architectures,” Concurrency and Computation: Practice and Experience, Vol. 25, No. 12, 2013, pp. 1771-1783.
[2] K. Bilal, M. Manzano, S. U. Khan, E. Calle, K. Li, and A. Zomaya, “On the characterization of the structural robustness of data center networks,” IEEE Transactions on Cloud Computing,
Vol. 1, No. 1, 2013, pp. 64-77.
[3] D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya, “Energy-efficient data replication in cloud computing datacenters,” In IEEE Globecom Workshops, 2013, pp. 446-451.
[4] Y. Deswarte, L. Blain, and J-C. Fabre, “Intrusion tolerance in distributed computing systems,” In Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy, Oakland CA, pp. 110-121, 1991.
[5] B. Grobauer, T.Walloschek, and E. Stocker, “Understanding cloud computing vulnerabilities,” IEEE Security and Privacy, Vol. 9, No. 2, 2011, pp. 50-57.
[6] W. K. Hale, “Frequency assignment: Theory and applications,” Proceedings of the IEEE, Vol. 68, No. 12, 1980, pp. 1497-1514.
[7] K. Hashizume, D. G. Rosado, E. Fernndez-Medina, and E. B. Fernandez, “An analysis of security issues for cloud computing,” Journal of Internet Services and Applications, Vol. 4, No. 1, 2013, pp. 1-13.
[8] M. Hogan, F. Liu, A.Sokol, and J. Tong, “NIST cloud computing standards roadmap,” NIST Special Publication, July 2011.
[9] W. A. Jansen, “Cloud hooks: Security and privacy issues in cloud computing,” In 44th Hawaii IEEE International Conference onSystem Sciences (HICSS), 2011, pp. 1-10.
[10] G. Kappes, A. Hatzieleftheriou, and S. V. Anastasiadis, “Dike: Virtualization-aware Access Control for Multitenant F
ile systems,” University of Ioannina, Greece, Technical Report No. DCS2013-1, 2013.