MJRET
Open Access
Multidisciplinary Journal of Research in Engineering and Technology
Journal homepage: www.mjret.in
ISSN:2348 - 6953

FILE FRAGMENTATION AND DUAL HOMOMORPHISM ENCRYPTION TECHNIQUE FOR SECURITY PUBLIC CLOUD

Priyanka Kamble[1], Jyoti Kamble[2]
[1]Department of Computer Engineering ,[2]Department of Information Technology
BVIT,Navi Mumbai,India

Abstract: *Outsourcing data which deploy over public cloud to an untouchable definitive control, as is done in circulated processing, offers climb to security concerns. The data exchange off might happen because of attacks by various customers and center points within the cloud. Thus, high endeavors to set up wellbeing are required to secure data within the cloud. Then again, the used security strategy ought to in like manner consider the headway of the data recuperation time. Proposed system performs fragmentation and replication of input data and loads it at each randomly selected data center. Each of the centers stores only a unitary part of a data record that ensures that even in the case of a productive strike, no imperative information is revealed to the attacker. Peer-to-Peer computing, highly available storage services, this P2P storage cloud storage can be formed to offer lowering the economic cost by increases as well as decreases the storage space of when participating users. Must been two cloud severs and users have trusted outside domain of data owners, P2P storage cloud brings becomes new challenges for data security and access control mechanism when that time data owners store sensitive information for sharing in the trusted domain. Moreover, there are number mechanisms for access control in P2P storage cloud. To this issue, we design a dual cipher text-policy attribute-based homomorphism encryption (ABHE)scheme.*

Keywords: *P2P, Cloud, DROPS, Nodes*

1. INTRODUCTION

Cloud computing and Peer-to-Peer (P2P) computing there are two of the node of internet peer to peer both of which are a form of distributed systems. Cloud computing is historically

storage data computer parameter is needed and provided as services over the Internet by cloud service providers. The multiple resources could be software, hardware, data storage, access with broadband internet access, users are able to acquire these services for application. Huge of data centres' consisting thousands of server application cloud computing processing and resources are centralized in data-canter's. P2P computing is a highly does not centralized decentralized cloud computing paradigm application. That resources of large number participating users to support efficient data according to the does not captained centralized application.

There are important differences between the two paradigms: the cloud sends multiple accesses the resources. In where P2P resources are free when that time cost was reduces. Indicates multiple related topics and needed projects term haveproposed P2P storage cloud systems. To combine the application that of both term, multiple access resources services based on the cloud while lowering the cost by pooling the storage space of all participating users to provide a substantially storage. This applications include backup and storage systems content distribution music or video streaming and online gaming In recent years, there are several actually, this times using pair connected computer in cloud system. companies such as security issues have been the top concerns in cloud computing. The advantages cloud data can be efficiently shared among a large number of users and the public verifier is able to handle the large number of auditing tasks simultaneously and efficiently. When users store important data in the cloud, maintaining confidentiality and privacy of the data to create one challenge Furthermore, users (i.e. data owners) publish data in the cloud and need terms of which users (i.e. data consumers) have the access privilege to which types of data. To achieve secure and flexible data sharing among a large number of users in P2P storage cloud, the security requirements are usually more complex. One more advantageIt follows protocol and does not pollute data integrity actively as a malicious adversary. The data owners need to keep data confidential against cloud servers and all the users two computers connected in peer that is big space create cloud in peer. For example, in a real-world application scenario, the data owners can be individual users and organization they may be publish their various articles, books and magazines online through P2P cloud.

A cloud must ensure throughput, enduring quality, and security. A key component choosing the throughput of a cloudthat stores data is the data recuperation time. In broad scale structures, the issues of data immovable quality, data availability, and response time are overseen data replication systems. In any case, putting duplicates data over different center points constructs the attack surface for that data. For example, securing m duplicates of an archive in a cloud as opposed to one generation constructs the probability of a center point

holding record to be picked as ambush loss, from 1 n to m n , where n is the total number of centers. From the above talk, we can find that both security and execution are fundamental for the forefront limitless scale structures, for instance, fogs. Thusly, in this paper, we all things considered methodology the issue of security and execution as a sheltered data replication issue. We present Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that judicially parts customer records into pieces and rehashes them at fundamental zones within the cloud. The division of an archive into parts is performed considering a given customer criteria such that the individual segments don't contain any imperative information.

Each of the cloud center points (we use the term center point to identify with handling, stockpiling, physical, and virtual machines) contains an unmistakable segment to assemble the data security. A productive attack on a single center must not reveal the territories of various pieces within the cloud. To keep an attacker unverifiable about the ranges of the record parts and to empower upgrade the security, we select the centers in a way that they are not adjacent and are at certain detachment from each other. The center point segment is ensured by the strategy for the T-shading. To improve data recuperation time, the center points are picked in light of the centrality measures that ensure an upgraded access time. To support improve the recuperation time, we judicially rehash parts over the centers that make the most vital read/form requests. The decision of the center points is performed in two stages. In the first stage, the center points are decided for the beginning circumstance of the segments considering the centrality measures. In the second stage, the center points are decided for replication.

2. LITERATURE SURVEY

Kashif Bilal [2], Described Data centers. These are being an architectural and functional block of cloud computing are integral to the Information and Communication Technology (ICT) sector. They analyzed robustness of the state-of-the-art DCNs. Their major contributions are: 1) presented multilayered graph modeling of various DCNs; 2) studied the classical robustness metrics considering various failure scenarios to perform a comparative analysis; 3) presented the inadequacy of the classical network robustness metrics to appropriately evaluate the DCN robustness; and 4) proposed new procedures to quantify the DCN robustness.

DejeneBoru [3], Described data replication, which brings data (e.g., databases) closer to data consumers (e.g., cloud applications),is seen as a promising solution. It allows minimizing

network delays and bandwidth usage. They have given data replication in cloud computing data centers. Unlike other approaches available in the literature, we consider both energy efficiency and bandwidth consumption of the system, in addition to the improved Quality of Service (QoS) because of the reduced communication delays.

Yves Deswarte [4], Describes an intrusion-tolerant distributed system. It is a system which is designed so that any intrusion into a part of the system will not endanger confidentiality, integrity and availability. This approach is suitable for distributed systems, because distribution enables isolation of elements so that an intrusion gives physical access to only a part of the system. By intrusion, we mean not only computer breakings by non-registered people, but also attempts by registered users to exceed or to abuse their privileges. In particular, possible malice of security administrators is taken into account. They described how some functions of distributed systems can be designed to tolerate intrusions, in particular security functions such as user authentication and authorization, and application functions such as file management.

Z. Yang, B. Zhao, and Y. Xing, S. [5,6] we have this overcome and it must be secure we further propose a secure, efficient and fine-grained data Access Control a feasible solution would be storing encrypted data and disclosing decryption keys only to authorized users. In the literature, related mechanisms can be found in the areas of cryptographic file systems and access control of outsourced data. However, these mechanisms either lack fine-grandness or scalability mechanism for P2P storage Cloud named ACPC. We enforce access policies based on user attributes, and integrate P2P reputation system in ACPC. Our security analysis demonstrates that ACPC is provably secure.

T. Maher, E. Bier sack, and P. Misheard in this paper we store the database in related data domain1 and domain 2 we discuss the some various problems with overcome using helpof public key and the master key. Cloud storage is made up of many distributed resources. If your internet connection is slow or unstable, you might have problems accessing of sharing your files. This data storage framework is able to combine and extend multiple databases Hadoop to store and manage diverse types of data collected by sensors and RFID readers. In addition, some components are developed to extend the Hadoop to realize a distributed file repository, which is able to process massive unstructured files efficiently.

A. Montresor and L. Abend in that papers we consider user revocation this mechanism reputation system in peer to peer computing. User revocation is an important issue in access

control systems. However, it is hard to execute user revocation efficiently in ABE schemes since each attribute is usually shared by multiple users. To revoke attributes from auser, the data owner has to re-encrypt all the files associated with revoked attributes and update the secret keys for all the remaining users who share these attributes. Those operations would introduce heavy computation overheads on the data owner and may also require the data owner to be always online.

G. Krietz and F. Niemela, we discuss that papers the performance evaluation shows that ACPC is highly efficient under practical settings, and it significantly reduces the computation overheads brought to data owners and cloud servers during user revocation The performance evaluation shows that ACPC is highly efficient under practical settings, and it significantly reduces the computation overheads brought to data owners and cloud servers during user revocationP2P reputation system was integrated into ACPC, which enables data owners to delegate most of the laborious user revocation tasks to cloud servers and reputable system peers. ACPC is provably secure, and is demonstrated to be more efficient and scalable than state-of-the art revocable ABE schemes.

3. PROPOSED SYSTEM

Above figure shows proposed system architecture, in which data owner upload data to cloud server, the cloud server performs data fragmentation, replication and data encryption and for dual encryption the re-encryption server is included which perform 2-level of encryption. When user first time registered as authorized user then key is generated which is used in encryption process. After data upload and fragmentation and encryption the data loaded to randomly selected note and replicated nodes.

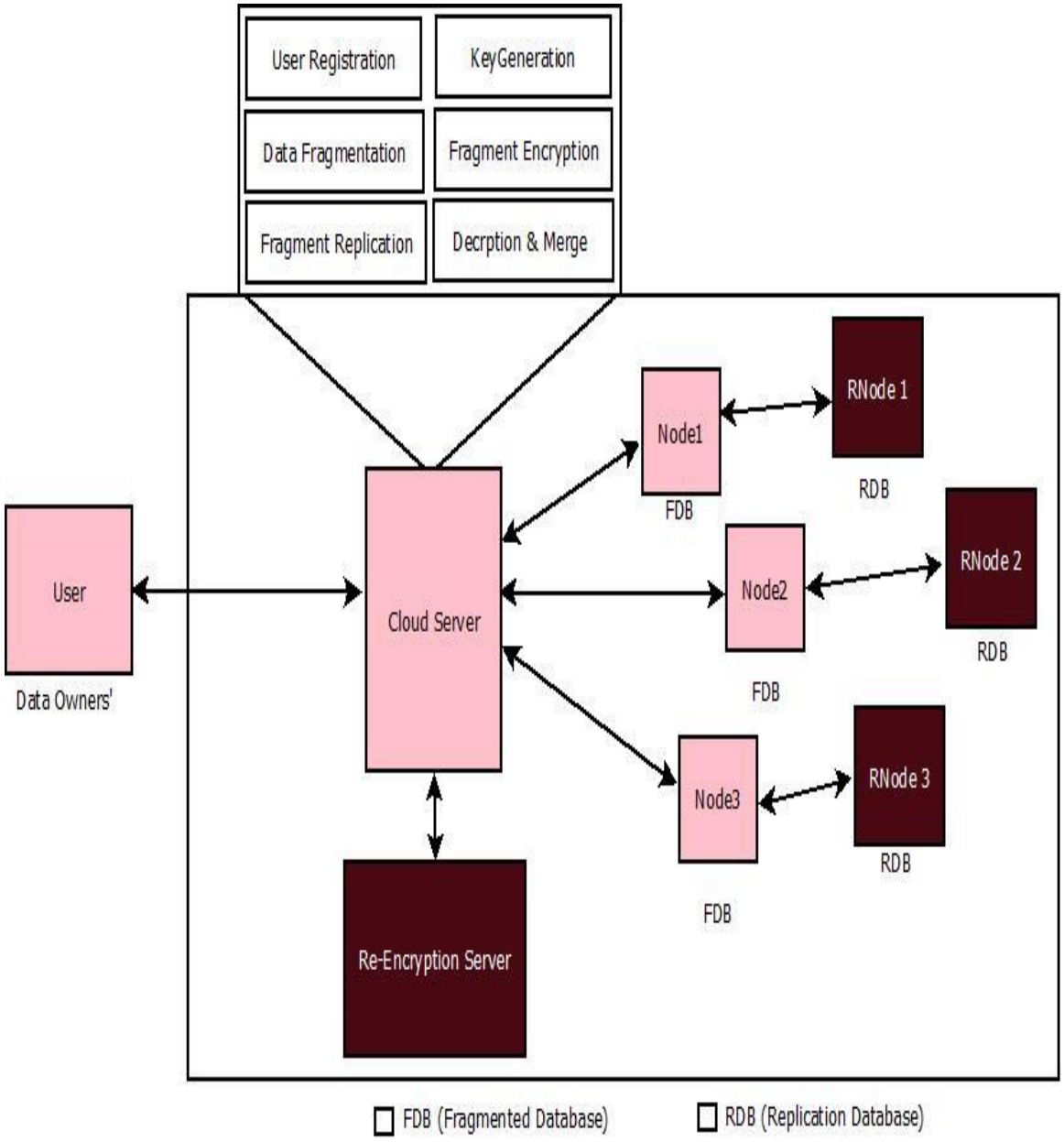

Figure 1: System Architecture

4. CONCLUSION

A distributed storage security plan, DROPS technique manages the security and execution as far as recovery time. The information record was divided, and the pieces are scattered over numerous hubs. The hubs were isolated by method for T-shading. The discontinuity and dispersal guaranteed that no noteworthy data was reachable by a foe if there should be an occurrence of a fruitful assault. No hub in the cloud put away more than a solitary section of the same document.

The aims at providing secure, efficient and data access control in P2P storage cloud, which is not supported by current works. To achieve this goal, we design an efficient dual encryption scheme and a corresponding then propose user revocation based on those schemes. To efficiently address the issue of user revocation, this verify peer to peer segments with the help of secret key and the master key.

REFERENCES

[1] *K. Bilal, S. U. Khan, L. Zhang, H. Li, K. Hayat, . A. Madani, N. Min-Allah, L. Wang, D. Chen, M. Iqbal, C. Z. Xu, and A. Y. Zomaya, "Division and Replication of data in cloud for optimal performance and security" IEEE Transaction for cloud computing DOI 10.1109/TCC.2015.2400460*

[2] *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.*

[3] *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.*

[4] *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.*

[5] *R. Ranjan, L. Zhao, Xu, A. Liao. Quiroz, and M. Preacher, "Peer to-peer cloud provisioning: Service discovery and load-balancing," in Cloud Compute.: Principles, Systems and Applications, Part 2,N.Antonopoulos,L.Gillam, Ed. London: Springer, pp. 195-217,May 2010.*

[6] *L. Bremer and K. Graffiti, "Symbiotic coupling of P2P and cloud systems: The Wikipedia case," in Proc. IEEE Int. Conf. Communed.,2013, pp. 3444 – 3449*

[7] *T. Maher, E. Bier sack, and P. Misheard, "A measurement study of the Wala on-line storage service," in Proc. 12th IEEE Int. Conf. Peer-to-Peer compute., 2012, pp. 237-248.*

[8] *A. Montresor and L. Arena, "Cloudy weather for P2P, with a chance of gossip," in Proc. 11th IEEE Int. Conf. Peer-to-Peer Compute.,2011, pp. 250-259.*

[9] *A. H. Payberah, H. Kavalionak, V. Kumaresan, A. Montresor, and S. Haridi, CLive: Cloud-assisted P2P live streaming, in Proc. 12th IEEE Int. Conf. Peer-to-Peer Comput.,2012, pp. 7990.*

B. Wang, B. Li, and H. Li, Certificate less Public Auditing for Data Integrity in the Cloud Proc. IEEE Conf. Comm. and Network Security (CNS13), pp. 276-284, 2013.