# CLOUD ARCHITECTURE FOR EFFECTIVE COST TOWARDS DIFFERENTIAL QUERY SERVICES

**S Sayee Sreedhar[1], K Durga Prasad[2], Prof. S.V.Achutha Rao[3]**

*[1]M.Tech (CSE) Scholar, Vikas College of Engg and Tech., Nunna, Vijayawada, A.P, (India)*

*[2]Asst. Professor, Department of Computer Science Engg.,*

*Vikas College of Engg. and Tech., Nunna, AP, (India)*

*[3]Professor & Head, Department of CSE,*

*Vikas College of Engg and Tech., Nunna, Vijayawada, (India)*

## ABSTRACT

*Cloud computing as a developing technology trend is estimated to reshape the advances in info technology. In a cost-efficient cloud infrastructure, a user can tolerate a certain degree of interval while retrieving info from the cloud to decrease costs. In this paper, we address two major issues in such an environment: secrecy and efficiency. We first review a secretive keyword based file recovery scheme that was formerly proposed by Ostrovsky. Their structure allows a user to get files of interest from a not trusted server without disclosing any info. The main disadvantage is that it will cause a huge querying above incurred on the cloud, and thus goes opposite the novel intention of cost efficiency. In this paper, we present a scheme, termed efficient information retrieval for ranked query, and based on an aggregation and distribution layer, to decrease querying above incurred on the cloud. In efficient information retrieval for ranked query, queries are classified into many ranks, where a higher ranked query can get a higher ratio of matched files. A user can get files on demand by selecting queries of dissimilar ranks. Large number of matched files is useful in this feature, but the user only wants a small subset of them. Under dissimilar parameter settings, extensive estimations have been conducted together analytical models and on a real cloud infrastructure, in order to examine the usefulness of our schemes.*

***Index Terms: Cloud Computing, Single Cloud, Multi-Cloud, Cloud Storage.***

## I. INTRODUCTION

Cloud computing as an initial technology is estimated to reshape info technology processes in the near future. Due to the prodigious merits of cloud computing, e.g., scalability, flexibility and cost-effectiveness more and more companies choose to outsource their data for distribution in the cloud. As a classic cloud application, an companies subscribes the cloud services and permits its staff to share files in the cloud. Each file is described by a set of keywords, and the staff, as authorized users, can retrieve files of their interests by querying the cloud with certain keywords. In such an environment, how to protect *user privacy* from the cloud, which is a third party outside the security boundary of the organization, becomes a key problem. Now a days the usage of cloud computing is rapidly increased in many companies. For various reasons the small and medium companies are using cloud computing, to access their applications the services are fast and it also reduce their arrangement costs. Cloud service providers should indicate secrecy and safety issues as a matter of high and quick priority. Handling with “single cloud” service providers is becoming less popular with consumers due to potential harms such as service accessibility failure and the chance that there are misusing insiders in the single cloud. In this

year, there has been a move in the direction of "multiclouds", "intercloud" or "cloud-of-clouds". This paper emphases on the matters related to the data safety context of cloud computing. As data and info will be provided with a third party, cloud computing users want to avoid a not trusted cloud service provider. Guarding private and important info, such as credit card particulars or a patient's medical records from enemies or misusing insiders is of serious importance. In the addition of, the potential for movement from a single cloud to a multi-cloud atmosphere is studied and investigation related to safety issues in single and multi-clouds in cloud computing are measured. Remainder for this paper is ordered as follows. Section 2 defines the starting of cloud computing and its modules. In addition of, the current examples of cloud service providers and the profits of using their services. Section 3 tells safety risks in cloud computing. Section 4 examines the new era of cloud computing, i.e., multi-clouds and current solutions to point the safety of cloud computing, as well as probing their restrictions. Section 5 current proposals for future work. NIST defines cloud computing as "a model for allowing appropriate, on-demand network access to a shared pool of configurable computing assets (e.g., networks, storage, servers, services and applications) that can be quickly provisioned and released with nominal management strength or service provider interface". This model consists of five features, three distribution models, and four arrangement models. The five key features of cloud computing are: on-demand self-service, location-independent supply pooling, broad complex access, quick elasticity, and measured service. These five features represent the first layer in the cloud environment design (see Figure1).

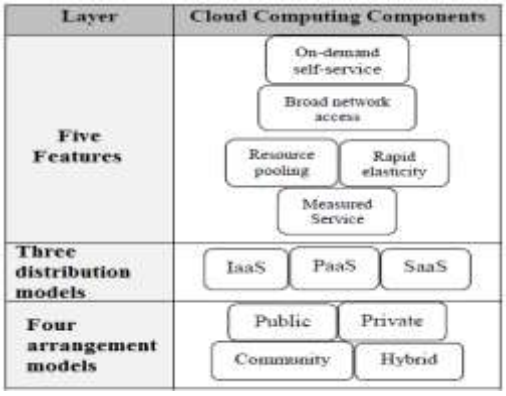


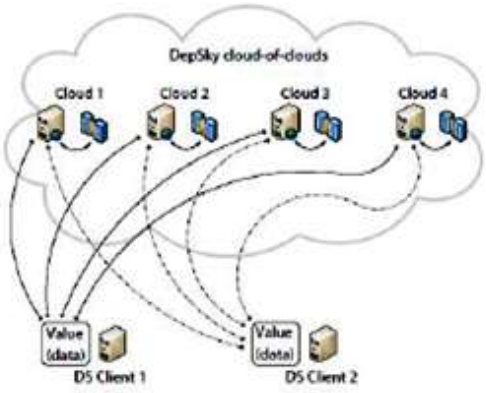

**Figure: Cloud Architecture**

The three key cloud transfer models are environment as a service (IaaS), software as a service (SaaS), and platform as a service (PaaS). In IaaS, the user can advantage from networking environment services, data storing and computing services. In other words, it is the distribution of computer environment as a service. Example of IaaS is the Amazon web service [25]. In PaaS, the operator runs custom applications using the service provider's assets. It is the distribution of a computing platform and solution as a service. The example of PaaS is GoogleApps. Running software on the service provider's environment and providing licensed applications to users to use services is known as SaaS. The example of SaaS is the Salesforce.com CRM application. This model denotes the second layer in the cloud architecture. Cloud placement models include public, community, private, and hybrid clouds. A cloud location that is accessible for multi-tenants and is existing to the public is called a open cloud. A secretive cloud is available for an exact group, while a community cloud is changed for an exact group of consumers. Hybrid cloud setup is an addition of two or more cloud (private, community, or public cloud) [51]. This model denotes the third layer in the cloud architecture. Only two types of cloud infrastructure are presented by Kamara and Lauter, namely public and private clouds. The infrastructure that is maintained and handle by users is in the private cloud. Data that is retrieved and controlled by trusted users is in a safe and protected secretive cloud, whereas the infrastructure that is handled and controlled by the cloud

service supplier is in an open cloud. In specific, this data cannot be handled with the user's control, and is handled and shared with not safe and not trusted servers.

## II. PROPOSED WORK

The DepSky design consists of four clouds and for each cloud uses its own specific interface. The algorithm DepSky exists in the clients' machines as a software library to interact with each cloud. These are the four clouds are storage clouds, so there are no codes to be implemented. The DepSky collection permits reading and writing actions with the cloud storage.




As the DepSky system pacts with unlike cloud service providers, the DepSky collection pacts with unlike cloud interface service providers and accordingly, each cloud accepts the data format. The data model DepSky consists of three different levels: a generic data unit, the data unit implementation and the conceptual data unit.

This model contains three parts: writers, readers and four cloud storage service providers, the client's tasks where readers and writers. Bessani et al. in cloud storage it explain the difference between readers and writers. Readers can fail (incase, they can flop by crashing, they can flop from time to time and then display any behavior) whereas, writers only fail by colliding. Changing from single clouds or multi-clouds to inner-clouds is perfect and important for many causes. Based on the Cachinet al. "Cloud Services of single clouds are still topic to outage". In the addition of, we presented that over 80% of the organization "fear safety threats and loss of control of data and techniques". Vukolic takes that the main purpose of changing to inter-clouds is to increase what was offered in single clouds by allocating reliability, trust, and safety among multiple cloud service providers. In the addition, dependable distributed storage which uses a subset of BFT methods was suggested by Vukolic to be used in different types of clouds. A number of current studies in this area have built protocols for inter-clouds. Redundant Array of Cloud Storage for instance, utilizes RAID-like methods that are normally used by CDs and file systems, but for several cloud storage. Abu-Libdeh et al. accept that to avoid "hawker lock-in", distributing a user's data among multiple service clouds is a helpful result. This repetition also reduces the cost of switching service providers and gives better fault tolerance. Therefore, the storing load will be spread among a number of providers as a result of the Redundant Array of Cloud Storage proxy. The High Accessibility and Integrity Layer is a different example of a protocol that controls multiple service clouds. High Accessibility and Integrity Layer is a spread cryptographic system that permits a number of servers to confirm that the client's stored data can be fetch and integral. High accessibility and integrity layer provides a software layer to address accessibility and truthfulness of the stored data in an inter-cloud. Cachin et al. current a design for inter-cloud storage, it is a step closer than RACS and High accessibility and integrity layer as a reliable service in multiple

clouds. Cachin et al. improves the theories and protocols to address the CIRC aspects of the storing the data in clouds. As we revealed earlier, Bessani et al. current a practical storage cloud system called DepSky consisting of a mixture of various clouds to build a cloud of- clouds. Bessani et al. discuss some limits of the High accessibility and integrity layer protocol and RACS system when compared with DepSky. High accessibility and integrity layer does not assurance data privacy, it needs code execution in their servers, and it does not deal with various versions of data. None of these limits are found in DepSky, whereas the RACS system varies from the DepSky system in that it deals with "economic failures" and service provider lock-in and does not address the issue of cloud service storage safety problems. In the addition, it also does not deliver any technique to ensure data privacy or to provide updates of the data storage. At last, the DepSky system grants an experimental evaluation with several clouds, which is not similar from other earlier work on multi-clouds. Here the number of studies on gaining stability from not trusted clouds. For instance, it is similar to DepSky, Depot improves the performance of cloud storage, as Mahajan et al. believe that the cloud storages face several risks. However, Depot offers a solution that is inexpensive due to using single clouds, but it doesn't tolerate losses of data and its service accessibility depends on cloud accessibility. In some another work which develops the services on top of not trusted service clouds are studies such as SPORC and Venus. These studies are different from the DepSky system because they accept a single cloud (not a cloud-of-clouds). In the addition, they need code implementation in their servers. Moreover, they offer limited support for the inaccessibility of cloud services in contrast to DepSky. In order to decrease the danger in cloud service storage, users can use cryptographic methods to care for the stored data in the cloud. By using a hash function is a good solution for data truthfulness by storing a short hash in local memory. By this way, validation of the server replies is done by recalculating the hash of the received data which is related with the local stored data. Some amount of data is huge, and then a hash tree is the answer. Many cloud storage system prototypes have applied hash tree functions, such as TDB and SiRiUS. Papamanthou et al. and Mykletun et al. claim that this is an active space in research on cryptographic techniques for stored data validation. Cachinet al. discuss that although the earlier methods allow user to ensure the truthfulness of their data which has been reverted by servers, they do not assurance that the server will response a question without knowing what that question is and whether the data is stored correctly in the cloud server or not. PORs (Proofs of Retrievability) and PDP (Proofs of Data Possession) are protocols developed by Kaliski and Juels and Ateniese et al. to confirm high chance for the fetching of the user's data. Cachinet al. recommends using several cloud service providers to ensure data reliability in service cloud storage and running Byzantine-fault-tolerant procedures on them where each cloud keeps a single replica. Cloud computing resources are need in this approach and not only storage in the cloud service, such a cloud service provided in Amazon EC2, whereas if only storage cloud service is available, Cachin et al. advise of working with Byzantine Quorum Systems by using Byzantine Disk Paxos and using at least four different clouds in order to ensure users' automatic operations and to avoid the danger of one cloud failure. For future work, we aim to offer a structure to supply safe cloud databases that will assurance to prevent safety risks facing the cloud computing community. This structure will apply multi-clouds and the confidential sharing algorithm to reduce the danger of data interruption and the damage of service accessibility in the cloud and ensure data truthfulness. In relation to data interruption and data truthfulness, assume we want to allocate the data into three different cloud service providers, and we apply the confidential sharing algorithm on the kept data in the cloud service provider. A visitor needs to recover at least three values to be able to find out the real value that we want to hide from the visitor. This works on a Shamir's confidential sharing algorithm with polynomial functions method

which states that even with full facts of (k – 1) clouds, the service provider will not have any facts of vs (vs is the secret value). We have used this technique in earlier databases-as-a-serves research. We can say in other words, data thefter need to reclaim all the info from the cloud service providers to know the genuine value of the data in the cloud. Therefore, if the enemy hacked one cloud service provider's password or even two cloud service provider's secret code, they still need to theft the third cloud service provider (in the case where k = 3) to know the confidential which is the bad case situation. Hence, redoing data into multi-clouds by using a multi-share method may decrease the risk of data interruption and increase data integrity. We can say in other words, it will reduce the risk of the Hyper-Visor being theft and Byzantine problem-tolerant data being taken from the Cloud service provider. This is about service accessibility danger or loss of data, if we repeat the data into various cloud service providers, we could discuss that the data loss risk will be decrease. If the cloud service provider fails, we can still get our data live in other cloud service providers. The main aspect has been discovered from this survey and we will explore dealing with various cloud service provider interfaces and the network traffic between cloud service providers.

## III. CONCLUSION

In this paper, we proposed three EIRQ schemes based on an ADL to provide differential query services while protecting user privacy. By using our schemes, a user can retrieve different percentages of matched files by specifying queries of different ranks. By further reducing the communication cost incurred on the cloud, the EIRQ schemes make the private searching technique more applicable to a cost-efficient cloud environment. However, in the EIRQ schemes, we simply determine the rank of each file by the highest rank of queries it matches. For our future work, we will try to design a flexible ranking mechanism for the EIRQ schemes.

## REFERENCES

[1] P. Mell and T. Grance, "The nist definition of cloud computing (draft)," *NIST Special Publication*, 2011.

[2] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in *Proc. of ACM CCS*, 2006.

[3] R. Ostrovsky and W. Skeith, "Private searching on streaming data," in *Proc. of CRYPTO*, 2005.

[4] "Private searching on streaming data," *Journal of Cryptology*, 2007.

[5] J. Bethencourt, D. Song, and B. Waters, "New constructions and practical applications for private stream searching," in *Proc. Of IEEE S&P*, 2006.

[6] "New techniques for private stream searching," *ACM Transactions on Information and System Security*, 2009.

[7] Q. Liu, C. Tan, J. Wu, and G. Wang, "Cooperative private searching in clouds," *Journal of Parallel and Distributed Computing*, 2012.

[8] G. Danezis and C. Diaz, "Improving the decoding efficiency of private search," in *IACR Eprint archive number 024*, 2006.

[9] "Space-efficient private search with applications to rateless codes," *Financial Cryptography and Data Security*, 2007.

[10] M. Finiasz and K. Ramchandran, "Private stream search at the same communication cost as a regular search: Role of ldpc codes," in *Proc. of IEEE ISIT*, 2012.

[11] X. Yi and E. Bertino, "Private searching for single and conjunctive keywords on streaming data," in *Proc. of ACM Workshop on Privacy in the Electronic Society*, 2011.

[12] B. Hore, E.-C. Chang, M. H. Diallo, and S. Mehrotra, "Indexing encrypted documents for supporting efficient keyword search," in *Secure Data Management*, 2012.

[13] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. of EUROCRYPT*, 1999.

[14] Q. Liu, C. C. Tan, J. Wu, and G. Wang, "Efficient information retrieval for ranked queries in cost-effective cloud environments," in *Proc. of IEEE INFOCOM*, 2012.

[15] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Proc. of IEEE INFOCOM*, 2010.

[16] G. Wang, Q. Liu, J. Wu, and M. Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers," *Computers & Security*, 2011.

[17] M. Mitzenmacher, "Compressed bloom filters," *IEEE/ACM Transactions on Networking*, 2002.

[18] D. Guo, J. Wu, H. Chen, and X. Luo, "Theory and network applications of dynamic bloom filters," in *Proc. of IEEE INFOCOM*, 2006.

[19] A. Berl, E. Gelenbe, M. Di Girolamo, G. Giuliani, H. De Meer, M. Q. Dang, and K. Pentikousis, "Energy-efficient cloud computing," *The Computer Journal*, 2010.

[20] E. Gelenbe, R. Lent, and M. Douratsos, "Choosing a local or remote cloud," in *Proc. of IEEE NCCA*, 2012.

## AUTHOR PROFILE

**S Sayee Sreedhar**, pursuing M.Tech(CSE) Vikas College of Engineering and Technology, Nunna, Vijayawada. Affiliated to JNTU, Kakinada, A.P., India

**K Durga Prasad,** working as an Asst. Professor at Vikas College of Engineering and Technology, Nunna, Vijayawada, Affiliated to JNTU, Kakinada, A.P., India

**Prof S.V.Achutha Rao,** is working as a HOD of CSE at Vikas College of Engineering and Technology, Nunna, Vijayawada, Affiliated to JNTU, Kakinada, A.P., India