Software as a Service in Cloud Computing

M. S. Kavitha & P. Damodharan

Department of Computer Science and Engineering, Akshaya College of Engineering and Technology
E-mail: shanmugam.kavitha@gmail.com

Abstract – Software as a Service (SaaS) is one of the delivery model of cloud computing in which service are provided by the service providers and client make use of it through Internet. Here we present a saas in pcloud. pcloud is a distributed system which contains a number of cooperated nodes. In pcloud, distribute the programming software to a number of nodes so that queries can be executed in parallel manner. In this distributed system, communication overhead between the co-operated nodes is very low. Programming code is send as a user queries to pcloud where it is processed and retrieved through PIR protocol. The concept used by the PIR protocol is the way that accesses of sequential segments are made to different physical storage devices. To minimize the effect of node failures, pCloud includes data replication. The Load Balancing can be achieved by loosely coupled and nearest neighbor property of clouds.

Key terms: pCloud, software as a service, PIR, Stripping technique, Load Balancing.

I. INTRODUCTION

Cloud computing is one of the recent trends that exists in the networking area. Cloud computing means utilization of resources that are available on Internet in the form of services. There are three different type of service models available which are termed as delivery models: Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS).

SaaS users have no hardware or software to buy, install, maintain, or update. Google Apps is one of the examples of SaaS which provide collaboration on various applications via internet.

A private cloud is a network or a data center that is owned by a company, group of people etc. Only those people can make use of resource. In this paper we present the software as a service in the pCloud. In order to so we need a protocol for retrieval purpose. We are using PIR protocol. PIR stands for Private Information Retrieval. Chor et al coined the word PIR. The practical implementation of computational PIR is used to retrieve the single page from the database.

All the aforesaid concept have been simulated using CloudSim simulator. We experimented using CloudSim which is implemented through org.cloudbus.cloudsim.* based on Java.Cloud.org. The Experimental result also examined. CloudSim is like a virtual machine which contains vmschedulers.

The remainder of this paper is organized as follows: Section 2 presents literature survey. Section 3 reviews the concepts used in this paper. Section 4 presents implementation part of this paper which can be viewed in the form of four sections. Section 5 gives experimental result of CloudSim. While Section 6 concludes the paper. And finally Section 7 gives idea for the future enhancements.

II. LITERATURE SURVEY

A survey on PIR protocol was studied.

2.1.1 Private Information Retrieval

Chor et al[3] show that n bits of communication are necessary to achieve information theoretic privacy, if only one database is available. In order to circumvent this bound the author propose using multiple non-interacting database. The advantage is that client queried information is kept secure. But major drawback is that query privacy is violated when the multiple single database is compromised.

2.1.2 Computational PIR

This computational PIR does not rely on multiple non-interacting database. Gasarch[5] shows cPIR require the database to compute modular addition for every bit of the database on each query, making them too computationally expensive to be practical. Here significantly reduces the amount of computation that must be done per query. It includes two protocols namely shortest vector problem and unique shortest vector problem. The query privacy guaranteed by cryptographic primitives. The limitation is that it is practically impossible to implement because of the high communication cost.
2.1.3 PIR using Trusted Hardware

PIR can also be treated as trusted hardware as secure hardware[7]. Here it acts as proxy between the client and the server. In this environment, PIR queries are processed as follows: 1) the client sends to the SC an encrypted version of the index of the desired bit (using public-key cryptography), 2) the SC processes the query on the raw data and extracts the result, without revealing what is actually being retrieved, and 3) the SC sends back to the client an encrypted version of the result, which is unreadable by the server. These methods have an optimal communication cost. The limitation is that client should trust secure hardware.

III CONCEPTS USED

The basic concepts used is described in this section. It includes section 3.1 as stripping technique, section 3.2 as Node failure, 3.3 as Load balancing and finally section 3.4 as PIR.

3.1 Stripping Technique:

In this paper we make use of the striping technique in order to retrieve the size of client output. The client is sending programming code as an input to the one of the node. The code is executed and the output is retrieved through the striping technique.

3.2 Node Failure

PIR protocols assumes the database to be non replicated if any node fails, the node cannot process the client request. In order overcome this, slightly modify pCloud to include data replication. The data replication is done here by distributing same programming software to two nodes.

3.3 Load Balancing

Load Balancing is a method to distribute queries across one or more co-operated peers. The Load Balancing can be achieved by nearest neighbor property of clouds. In the pcloud, the peers will collect the information about the neighboring peers. This information can be used to distribute the queries evenly among the peers.

3.4 PIR

The practical implementation of computational PIR is used to retrieve the single page from the database.

IV IMPLEMENTATION

The above concept can be implemented using four divisions. They are organized as section 4.1 as pcloud, section 4.2 as service provider, the service provider presented here is server, section 4.3 describes stripping technique and finally section 4.4 describes the saas.

4.1 pcloud

The group of peers forms the pcloud. In the private cloud I have included six co-operative peers. Each peer contains maximum of one programming language software such as Java, C#, Visual Basic, .net. The concept of Data replication is used such that any two nodes contain same programming language software. This data replication overcomes node failure.

4.2 Service Provider

The service provider is the server which handles the requests that cannot be processed by these nodes in pcloud. This is due to the fact that client’s queries are in different language other than the specified. The server contains the frequently used programs such as Fibonacci series, Factorial, Prime or not, Palindrome, Pyramid program, Armstrong number checking, Odd or Even, Quadratic equation solving, Complex roots, Matrix multiplication etc. If the client request is any one of the above mentioned programs, the query is processed and result is sent to the clients. Otherwise server informs the clients that the query cannot be processed.

4.3 Stripping Technique

The Stripping Technique is one of the concepts of PIR. The final result is retrieved through PIR protocol. The page size of the result is fixed used stripping.

4.4 Software as a service

The Software as a service indicates the query processing. The query processing is carried out under two phases; Query propagation and Result propagation. During the query propagation phase, the query is forwarded to neighbor nodes. The node which match programming software for the query will be processed by the same node. If no nodes match the query is forwarded to the server. During result propagation, result for client program is obtained.

V. EXPERIMENTAL RESULT

The experiment is carried out through the CloudSim and the result also obtained.

Datacenter represents the nodes of the private cloud. In this private cloud, list of four nodes is created. Each node is assigned with two files, i.e list of 8 files is created. Storage space namely storage 0-3 are created for each node. Server contains 3 files namely, file 9, file 10, file 11. 3 users are created, where user1 request for file1, while user2 request for file5 and the other request for file11. The files 1 and 5 will be available locally in...
the private cloud itself while user3 request goes to the server. Thus file 11 is retrieved from the server. Finally cloud simulation can be viewed.

Fig: simulation result

The above graph gives the total response time taken to execute the query of three users namely user1, user2, user3.

VI. CONCLUSION

The clients can submit their queries through any one of the four nodes. The node will process these requests and retrieves through PIR protocol. By utilizing a novel striping technique, pCloud can retrieve arbitrarily large blocks of information with a single query. Thus Saas presents the environment that client machine can have no hardware or software to buy, install, maintain, or update. Any number of clients queries can be submitted is handled by the concept of Load Balancing. The results can be analyzed by comparing with the other algorithms.

VII. FUTURE ENHANCEMENT

This paper implement the concept of Load Balancing using loosely coupled property. When pcloud based on the above concept is implemented it yields low response time. But when middleware is installed, it will reduce response time further.

The striping technique is not effective for multi-user query at a time. "Multi-casting routing” can be used which is to be implemented.

VIII. REFERENCES

[1] A. Ambainis, “Upper Bound on Communication Complexity of Private Information Retrieval,” Proc. Int’l Colloquium on Automata, Languages, and Programming (ICALP ’97), 1997.

[2] C. Cachin, S. Micali, and M. Stadler, “Computationally Private Information Retrieval with Polylogarithmic Communication,” Proc. Int’l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT ’99), 1999.

[3] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, “Private Information Retrieval,” Proc. Symp. Foundations of Computer Science (FOCS ’95), 1995.

[4] W. Gasarch, “A Survey on Private Information Retrieval (Column: Computational Complexity),” Bull. of the European Assoc. for Theoretical Computer Science (EATCS), vol. 82, pp. 72-107, 2004.

[5] W. Gasarch and A. Yerukhimovich, “Computationally Inexpensive cPIR,” Unpublished Draft, 2006.

[6] C. Gentry and Z. Ramzan, “Single-Database Private Information Retrieval with Constant Communication Rate,” Proc. Int’l Colloquium on Automata, Languages, and Programming (ICALP ’05), 2005.

[7] A. Iliev and S.W. Smith, “Private Information Storage with Logarithm-Space Secure Hardware,” Proc. Workshop Information Security, Management, Education, and Privacy, 2004.

[8] A. Khoshgozaran, H. Shirani-Mehr, and C. Shahabi, “SPIRAL: A Scalable Private Information Retrieval Approach to Location Privacy,” Proc. Workshop Privacy-Aware Location-Based Mobile Services (PALMS ’08), 2008.

[9] E. Kushilevitz and R. Ostrovsky, “Replication Is Not Needed: Single Database, Computationally-Private Information Retrieval,” Proc. Symp. Foundations of Computer Science (FOCS ’07), 1997.

[10] C.A. Melchor and P. Gaborit, “A Fast Private Information Retrieval Protocol,” Proc. IEEE Int’l Symp. Information Theory (ISIT ’08), 2008.

[11] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone, Handbook of Applied Cryptography. CRC Press, 1997.

[12] R. Ostrovsky and W.E. Skeith III, “A Survey of Single-Database Private Information Retrieval: Techniques and Applications,” Proc. Int’l Conf. Practice and Theory in Public-Key Cryptography (PKC ’07), 2007.
[13] D.A. Patterson, G.A. Gibson, and R.H. Katz, “A Case for Redundant Arrays of Inexpensive Disks (RAID),” Proc. ACM SIGMOD ’88, 1988.

[14] L. Sassaman, B. Cohen, and N. Mathewson, “The Pynchon Gate: A Secure Method of Pseudonymous Mail Retrieval,” Proc. Workshop Privacy in the Electronic Soc. (WPES ’05), 2005.

[15] R. Sion and B. Carbunar, “On the Computational Practicality of Private Information Retrieval,” Proc. Symp. Network and Distributed System Security (NDSS ’07), 2007.

[16] “pCloud: A Distributed System for Practical PIR .”, Stavros Papadopoulos, Spiridon Bakiras, Member, IEEE, and Dimitris Papadis.

[17] I. Stoica, R. Morris, D.R. Karger, M.F. Kaashoek, and H. Balakrishnan, “Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications,” Proc. ACM SIGCOMM ’01, 2001.

[18] S. Wang, X. Ding, R.H. Deng, and F. Bao, “Private Information Retrieval Using Trusted Hardware,” Proc. European Symp. Research in Computer Security (ESORICS ’06), 2006.

[19] P. Williams and R. Sion, “Usable PIR,” Proc. Symp. Network and Distributed System Security (NDSS ’08), 2008.

[20] S. Yekhanin, “Towards 3-Query Locally Decodable Codes of Subexponential Length,” J. ACM, vol. 55, no. 1, pp. 1-16, 2008.