International Journal Of Core Engineering & Management
Volume-4, Issue-3, June-2017, ISSN No: 2348-9510

VERIFYING INTEGRITY IN MULTI-CLOUD STORAGE USING EFFICIENT COOPERATIVE PROVABLE DATA POSSESSION

Roshanee Bopche
Research Scholer M.Tech ,Department of Computer Science & Engineering
Shri Ram Group Of Institution, Jabalpur (M.P), INDIA
rsbopche@gmail.com

Sapna Choudhary
Assistant Professor, Head of the Department, Department of Computer Science & Engineering
Shri Ram Group of Institution, Jabalpur(M.P.),INDIA
choudharysapnajain@gmail.com

Abstract

The term 'Cloud' is a network of remote servers hosted on the internet and used to Store, Manage, and Process data in place of local server or personal computer. Multi cloud storage is an tremendous technique using a collection of cloud to provide data storage and data sharing for clients cooperatively .Provable data possession (PDP) is a technique for ensuring the integrity of data in storage outsourcing .Construction of an efficient PDP scheme for distributed cloud storage to support the scalability of service and data migration .We present an efficient method for selecting optimal parameter values to minimize the computation costs of clients and storage service providers .We use Cooperative provable data possession scheme for based on interactive proof system(IPS).This Cooperative PDP scheme adopting Layered Index Hash Hierarchy(IHH).
Keywords: Cloud Storage , Data Integrity ,RSA ,HMAC, CPDP.

I. INTRODUCTION

The term Cloud is used as a metaphor for the Internet, it is a network of remote servers hosted on internet and used to store, manage, and process data in place of local servers or personal computer. The cloud makes it possible for you to access your information from anywhere at any time through web browser. While a traditional computer setup requires to be in the same location as your data storage device, on the other hand the cloud removes the need for you to be in the same physical location. The typical cloud computing providers offer common business online, which is accessible via a web browser or the Internet, while the software and data are stored on the server.

II. CLOUD COMPUTING

Cloud computing has become one of the most discussed computer IT paradigms in recent years. With the rapid development of processing and storage technologies and the success of the Internet, computing resources are cheaper, more powerful and ubiquitous than ever. This technological trend made possible the realization of a new computing model called cloud computing, in which resources (eg CPU and memory) are provided as general utility available that can be leased and

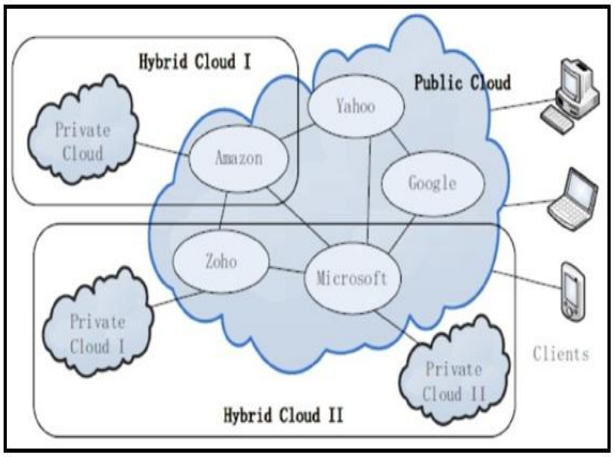
International Journal Of Core Engineering & Management
Volume-4, Issue-3, June-2017, ISSN No: 2348-9510

released by users through the Internet in an on-demand fashion.
Cloud computing provides an infrastructure, platform and software, services that are provided a subscription service for the consumer. These services include Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) Amazon Elastic Compute Cloud (EC2), Google App Engine and Force.com Are examples of IaaS, PaaS and SaaS respectively. IaaS is a very flexible option and the best choice to move applications to the cloud when there is no time to revise the application code for a cloud environment.]

III. RELATED WORK

Collaborative Integrity Verification In Hybrid Clouds

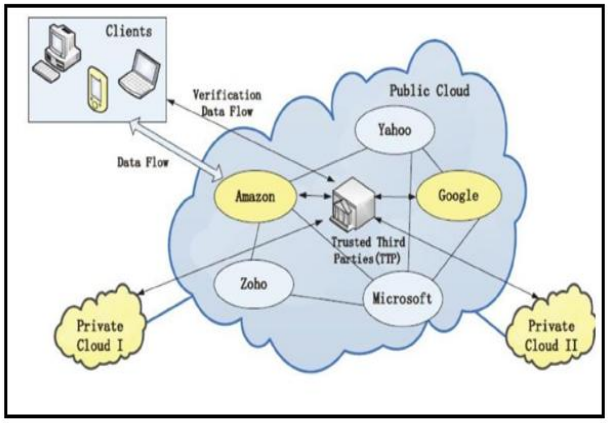
A hybrid cloud is a cloud computing environment in which an organization provides and manages some internal resources and the others provided externally. However, this new environment could cause irreparable losses to the customer due to the lack of a verification mechanism for the integrity of distributed data outsourcing. In this paper address
the construction of a collaborative integrity verification mechanism in hybrid clouds to support the scalable service and data migration, in which consider the existence of multiple cloud service providers to collaboratively store and maintain the clients' data. A hybrid cloud is a cloud computing environment in which an organization provides internal and external resources and manage it.



Figures: A1 Hybrid Cloud Diagram I[12]

Architecture considers a data storage service involving three different entities: Granted clients, a large amount of data to be stored in hybrid clouds and have the permissions to access and manipulate the stored data.

International Journal Of Core Engineering & Management
Volume-4, Issue-3, June-2017, ISSN No: 2348-9510



Figures: A2 Hybrid Cloud Diagram II[12]

Cloud Service Providers (CSPs), work together to provide data storage services and have enough storage spaces and computation resources; and Trusted Third Parties (TTPs), Trusted to store the verification parameters and offer the query services for these parameters.

Scalable and Efficient Provable Data Possession

Storage Outsourcing is an upward trend that requires a number of interesting integrity issues, many of which have been extensively studied in the past. However Provable Data Possession (PDP) scheme that has recently appeared in the research literature. The main problem is the frequency, efficiently and safely verifies that a storage server stores its customers (very large potential) reliably the outsourced data. It is assumed that the storage server in terms of integrity and reliability is not reliable.The problem is the customer of a small computer device is exacerbated with limited resources. The work has dealt with this problem above either public-key cryptography or requires the client to outsource its data in encrypted form. Build a very effective and proven PDP security technology, which relies exclusively on symmetric key cryptography, as you do not need bulk encryption.

Ensuring Data Storage Integrity In Cloud Computing

Cloud computing was introduced as the next generation of enterprise computing architecture. Unlike traditional solutions whose IT services are under the physical, logical and personnel controls, cloud computing moves application software and databases into large data centers where data management and services Are not quite trustworthy.

IV. PROBLEM STATEMENT AND PROPOSED SYSTEM

Problem description

Provable Data Possession (PDP) schemes evolved around public and single clouds offer a publicly accessible remote interface to check and manage the tremendous amount of data. The majority of existing PDP schemes is incapable of satisfying such an inherent requirement of hybrid clouds in terms of bandwidth and time. Although existing schemes can make a false or true decision for data possession without downloading data at untrusted stores, they are not suitable for a distributed cloud storage environment. In existing PDP scheme didn't have auto blocking mechanism to user

International Journal Of Core Engineering & Management
Volume-4, Issue-3, June-2017, ISSN No: 2348-9510

data which stored in to cloud server and did not useful for the large amount of data. In existing PDP scheme server can generate tag for multiple file blocks in term of single response value on client side, but the response from multiple cloud can be combined into single response value . For lack of homomorpic response the PDP protocol to check the integrity of file block stored in multi cloud server. Also client need to known exact position of file block stored into multi cloud so verification process in case will lead to high communication overhead and computation cost. Existing scheme RSA algorithm is used for key generation.

RSA Scheme

The RSA relies on the fact that it is easy to multiply two large prime number together but extremely hard to factor them back from the result. RSA is a block cipher in which the plain text and cipher text are integer between 0 ang n-1 . The RSA is public key cryptosystem that is based on the intricacy of integer factoring . The RSA public key encryption method is the first instance of a provably secure public key encryption method against preferred massege attecks. Assuming that the factoring trouble is computationally obstinate and it is rigid to uncover the prime factor of n = p * q. The RSA method is describe as:

Key generation algorithm

To generate the key entity A have to do the following :

1. by chance and secretly choose two large prime number p and q .
2. Compute the modulus p*q.
3. Compute ø(n) = (p-1) * (q-1).
4. Select chance integer e, 1 <e <n where gcd(e, ø) = 1.
5. Baghdad method[16] used to calculate the single decryption key d, 1<d< ø(n) where e*d = 1modø(n)
6. Determine public key and private key for entity A , the pair (e,n) as a public key (d,n) as private key .

Public key encryption algorithm

Message m encrypt by entity B for entity A which entity A decrypts to it.

Encryption : entity B should do following :

1. Obtain entity A public key (e,n).
2. Message m as an integer in the interval {0….n-1}.
3. Calculate c = m^e mod n .
4. Send the encrypted message c to A.

Decryption : To recover the message m fron the cipher text c. Entity A must do the following :

1. Get the cipher text c from entity B
2. recover the message m = c^d mod n

Disadvantages:

1) This algorithm has some limitation alongside certain attacks (i.e. Brute force , Mathematical attack ,Timing attacks and Chiper-text attacks) .
2) In the current system has no function to automatically block the cloud server.
3) The current system is less secure because no modern cryptographic technique.
4) There is no function to prove integrity based on a public key or any other key based on the file name.

5) The details of the attackers are not stored dynamically, but use the log file to store the details and data mining used to examine the concepts, which is time-staking and less secure..
6) Cloud user data store in untrusted cloud servers.
7) The data integrity is proving only based on the file name and not on the public key or any Other key.
8) For lack of homomorphic responses, the verification process in such a case will lead to high Communication overheads and computation costs at client sides as well.

Proposed System

To check the availability and integrity of outsourced data in cloud storages, researchers have proposed two basic approaches called Provable Data Possession and Proofs of Retrievability. Ateniese et al.I utilize Provable data possession (PDP), which is a cryptographic technique for verifying integrity of data without retrieving it at an untrusted server can be used to realize audit services. I first propose a verification framework for multi-cloud storage along with two fundamental techniques: hash index hierarchy (HIH) and homomorphic verifiable response (HVR). Then I constructed a lightweight PDP scheme based on cryptographic hash function and asymmetric key encryption and here I address the problem of provable data possession in distributed cloud environments from the following aspects: *high security*, *transparent verification*, and *high performance*. To achieve these goals, here I also proposed a publicly verifiable version (TTP), which allow anyone, not just owner to challenge the server from possession. Here the most important part is building the Trusted Third Party (TTP) server who is trusted to store the verification parameter and offer query service for these parameters. The number of updates and challenges is limited and fixed in advance, and users can not block insertions anywhere.

In this section we present efficient PDP scheme which is based on two fundamental parameter : hash index hierarchy(HIH) which the response of the client challenges computed from multiple CSP's can be combined in to single response and homomorphic verifiable response(HVR) which support multi cloud storage to generate tag for the particular file block.

To reduce these problem many algorithm have been designed and based on original RSA. Efficient RSA are the popular algorithm identified forb improving the main algorithm. To verify the integrity an d availability of outsourced data in cloud storage we have two basic method that's called Provable data Possession method and Proof of Irretrievability. PDP method are used for a static case and based on RSA scheme .But in this method owner or any one can challenge for possession. And no of updates are fixed previously and cloud user cannot insert block anywhere. So now we proposed a lightweight PDP for ensuring the availability and integrity of data in cloud server on the basis on homomorphic verifiable response and hash index hierarchy we projected a Efficient cooperative PDP (ECPDP) method. In these approach we use to Efficient RSA algorithm for key generation.

The RSA scheme to a scheme employs the general linear group of order of h*h matrix. The key range of efficient RSA is considerably momentous and can actually be used with hill cipher process. The difference of original RSA and efficient RSA is how to calculate ø(n) in key generation process . In Efficient RSA ø(n) was defined as:

Assume that n= p * q is the product of two large prime number and suppose g is the general linear group of h*h matrices then **g**:

International Journal Of Core Engineering & Management
Volume-4, Issue-3, June-2017, ISSN No: 2348-9510

$g = (ph - p0)*(ph - p1) \ldots (ph - ph - 1) + (qh - q0)*(qh - q1) \ldots (qh - qh - 1)$

here g(n,h) determine as a ø(n,h) wher h is the rank of linear matrices.

Key generation algorithm

To generate the keys entity A have to do the following :

1. Randomly chose two large prime number p and q .
2. Compute the modulus n = p * q.
3. Compute g = (n , h).
4. Chose the random integer e where gcd(e,g)= 1
5. Compute the inverse d where ed = 1mod g
6. Determine the entity A private key and public key . The pair (d , g) is private key while the pair (e , n) is the public key.

Public key encryption algorithm

Entity B encrypt a message m for entity A which entity A decrypts.

Encryption : entity B should do following :

5. Obtain entity A public key (n,e).
6. The message m as a h*h matrix X
7. Compute h*h matrix $c = m^e \bmod n$.
8. Send the encrypted message c to A.

Decryption : To recover the message m fron the cipher text c. Entity A must do the following :

3. Get the cipher text c from entity B
4. Convalesce the message $m = c^d \bmod n$

Advantage of the proposed scheme:

1) The key range of the proposed scheme is considerable. It means that it can be large enough to use by matrices of high level of ranks. The key range of RSA algorithm is ø(n) = (p-1)(q-1). But in the suggested scheme the key range is length g(n).
2) The intractability of the integer factoring of the modulus n in the propose scheme stay as same as a in RSA scheme:
3) The proposed scheme can be used as a digital signature by inserted in the matrix x as an item.

V. SYSTEM ARCHITECTURE

In this architecture, we consider the existence of multiple CSPs to cooperatively store and maintain the clients' data. Moreover, a cooperative PDP is used to verify the integrity and availability of their stored data in all CSPs. The verification procedure is described as follows:

International Journal Of Core Engineering & Management
Volume-4, Issue-3, June-2017, ISSN No: 2348-9510

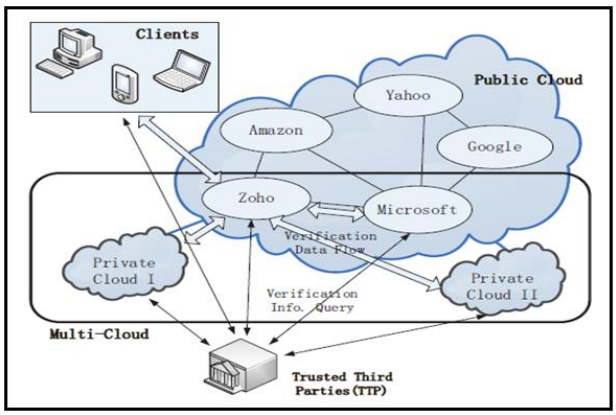


Figure: 5.1 Verification architecture for data integrity[12]

Firstly, a client (data owner) uses the secret key to pre-process a file which consists of a collection of n blocks, generates a set of public verification information that is stored in TTP, transmits the file and some verification tags to CSPs, and may delete its local copy; Then, by using a verification protocol, the clients can issue a challenge for one CSP to check the integrity and availability of outsourced data with respect to public information stored in TTP.

VI. RESULT AND ANALYSIS

The result of proposed method and existing method was implemented in java and according to 2.40 Ghz Intel Core i3 CPU and 2.00 gb ram . The compare result between the existing scheme and proposed scheme were carrid out according to the different size of file and execution thie in m/s. First we present the resulting time of Original RSA algorithm which are used to key generation in existing PDP scheme.

S.no	Size of file (kb)	Execution time of Original RSA (m/s)
1	1 kb	4.2
2	1.5 kb	5.1
3	2 kb	6.7
4	10 kb	7.3

Table no. 1 containing result of Original RSA algorithm

Now we present the resulting time of our scheme Efficient Cooperative provable Data Possession in this scheme to generate key pair used to Efficient RSA algorithm.

S.no	Size of file (kb)	Execution time of Original RSA (m/s)
1	1 kb	5.2
2	1.5 kb	5.5
3	2 kb	7.0
4	10 kb	9.9

Table no. 2 containing result of Efficient RSA algorithm

International Journal Of Core Engineering & Management
Volume-4, Issue-3, June-2017, ISSN No: 2348-9510

According to the result the key generation, encryption and decryption process time of the Efficient RSA increased then Original RSA scheme because the decryption key are higher then original RSA decryption key so to encrypt that massage will take longer time.

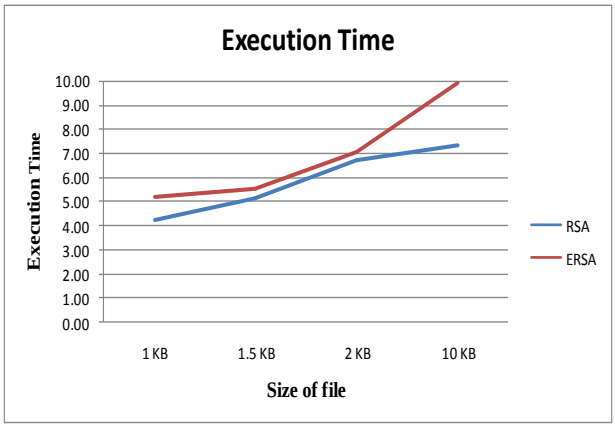


Figure 6.1 Comparison Graph RSA and Efficient RSA

The total execution time compare of efficient RSA and original RSA was increased means to creack encrypted massage are difficult as compare then original RSA algorithm . Now the second approach to finding the tag we use to MD5 algorithm that's generate hash value for specific data of file block . This is unique value and generate one time another time it will be change ,so compare to old and new generated tag , if both tag are same so no modification in to the stored data of server .

VII. SCREEN SHOTS OF IMPLEMANTATION

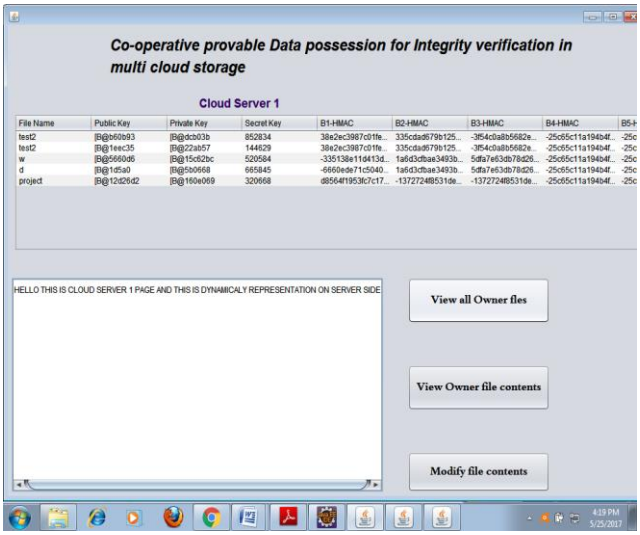


Figure 7.1 Data Representation On Cloud Server 1

International Journal Of Core Engineering & Management
Volume-4, Issue-3, June-2017, ISSN No: 2348-9510

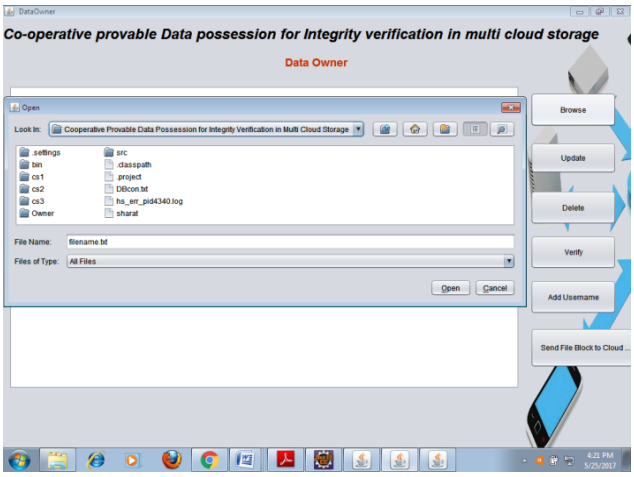


Figure 7.2 Data Owners representation

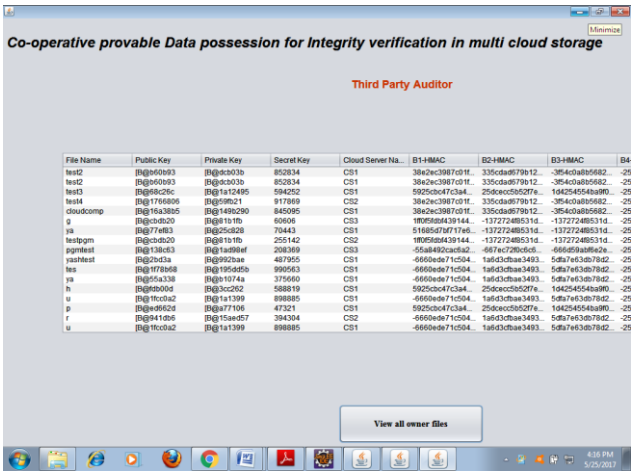


Figure 7.3 Third Party Auditor Representation

VIII. CONCLUSION

We proposed the implementation of an efficient method for distributed cloud PDP. Based on the hash index hierarchy and the verifiable homomorphic response we have projected an efficient cooperative PDP (ECPDP) method, supporting the dynamic query as insertion, deletion and modification Append, etc. On the storage servers. We also said that our method all security assets to track the interactive evidence system to zero knowledge so that it can withstand various attacks that used in the clouds as a public audit service. In addition, we optimized the probabilistic uncertainty and interval verification to restore audit performance. These experiments have clearly established that our approaches to present only a small amount of communication and calculation/computation. This method is more suitable for storing large amounts of data in the multi-cloud server. An Efficient Cooperative provable Data Possession scheme to support dynamically scalability on multiple storage server .

IX. FUTURE WORK

In our Efficient CPDP scheme Efficient RSA algorithm are used to key generation and MD5 algorithm for tag generation . Some one used to more effective algorithm to improve it. Trusted Third Party are used to monitoring all this process it should be able to make regular check on the integrity and availability of these delegated data at appropriate interval and should be able to organize, manage and maintain the outsourcing data.

References

[1] Rajkumar Buyya, Christian Vecchiola and S. Thamarai Selvi " Mastering Cloud Computing".

[2] G. Joon Ahn, Y.Zun, H. Hu, "Cooprative provable data possession for Intrigrity verification in multi cloud storage," IEEE Transaction on parallel and distributed system , vol: PP, issue 99, 14-02-2012.

[3] I. M. Llorente, I. T. Foster, R. S. Montero, B. Sotomayor, "Virtual infrastructure management in private and hybrid clouds," IEEE Internet Computing, vol.13, no. 5, pp. 14-22- 2009.

[4] J. Herring, L. Kissner, Z. N. J. Peterson, G. Ateniese, R. C. Burns, R. Curtmola, and D. X. Song, "Provable data possession at untrusted stores," ACM Conference on Computer andCommunications Security, P. Ning, S.D.C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 598-609.

[5] P. Ning, S. D. C. di Vimercati, A. Juels and B. S. K. Jr., "Proofs of retrievability for large files," ACMConference on Computer and CommunicationsSecurity P. F. Syverson, Eds. ACM, 2007, pp. 584-597.

[6] Pankaj Sareen " Cloud Computing: Types, Architecture, Applications, Concerns and Virtualization and Role of IT Governance in cloud", IJACCSSE, Volume-03, issue-03 pp. 533-538, March 2013.

[7] B. Waters, H. Shacham "Compact proofs of retrievability," ASIACRYPT, ser. Lecture Notes in Computer Science, J. Pieprzyk, Ed., vol. 5350. Springer, 2008, pp. 90-107.

[8] C.Wang and W. Lou, Q. Wang, J. Li, K. Ren, "Enabling public verifiability and data dynamics for storage security in cloud computing," ESORICS, ser. Lecture Notes in Computer Science, M. Backes and P. Ning, Eds., vol. 5789. Springer, 2009, pp. 355-370.

[9] S. P. Vadhan, and D. Wichs, Y. Dodis, "Proofs of retrievability via hardness amplification," TCC, ser. Lecture Notes in Computer Science, O. Reingold, Ed., vol. 5444. Springer, 2009, pp. 109-127.

[10] Trilok Singh Pardhi, Dr. Rajeev Pandey and Prof. Uday Chourasia " Survey of Integrity Verification in Multi-Cloud Storage by Efficient Cooperative Provable Data Possession", International Journal of Computer Application *(0975 – 8887) Volume 102– No.8, September 2014.*

[11] G.-J. Ahn, Y. Zhu, H. Hu, Y. Han, and S. Chen, "Collaborative integrity verification in hybrid clouds," in IEEE Conference onthe 7th International Conference on Collaborative Computing*: October 15-18*, 2011, pp. 197-206

[12] https://www.google.co.in/images