ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Sharing Of Large Scale Data in Corporate Network by Peer To Peer Based System

Bhavsar Harshada V.[1], Dr. S. V. Gumaste[2], Prof. Deokate Gajanan S.[3]

ME Student, Department of Computer Engineering, Sharadchandra Pawar College of Engineering, Dumbarwadi, Otur, Pune, India [1]

Professor, Department of Computer Engineering, Sharadchandra Pawar College of Engineering, Dumbarwadi, Otur, Pune, India[2]

Assistant Professor, Department of Computer Engineering, Sharadchandra Pawar College of Engineering, Dumbarwadi, Otur, Pune, India[3]

ABSTRACT: Recently, the amount of sensitive data produced by many administrations is out stepping their storage ability.The management of such large amount of data is quite expensive due to the requirements of high storage capacity and qualified recruits. Storage-as-a-Service (SaaS) offered by cloud service providers (CSPs) is a paid facility that enables organizations to outsource their data to be stored on remote servers. Thus, SaaS decreases the maintenance cost and mitigates the burden of large local data storage at the organization's end. A data owner pays for a desired level of security and must get some compensation in case of any difficulties dedicated by the CSP. On the other hand, the CSP needs a protection from any false accusation that may be claimed by the owner to get illegal damages. This paper, proposes a scheme that is used cloud storage system which has efficiency by the CSP and create trust among them. The proposed scheme shows two significant features: i) It allows the owner to outsource sensitive data to a CSP, and it ensures that only authorized users (i.e., Those who have the right to access the owner's file) receive the outsourced data i.e. It enforces the access control of the outsourced data can be done by sending a key through email to the registered users and ii) Allows indirect common belief between the owner and the CSP using Cheating detection module.

KEYWORDS: Cloud computing, Map Reduce, Network Security, Peer-to-peer systems, Query processing

I. INTRODUCTION

Cloud computing is playing an important role in current period, because of its flexibility, Immense Web-scale abstracted infrastructures, Dynamic allocations, Scaling, Movement of Applications, No long-term commitments and No hardware or software to install. So this results in Business and IT-aligned benefits are: Provides an effective and creative service delivery module, Delivery services in a less costly and higher quality business model while providing service access ubiquity, Rapidly deploy applications over the internet and leverage new technologies to deliver services When, Where and How your Clients needs them. Sharing Companies having common interest are always connected to a corporate network for sharing purposes [2]. A company creates its own website and shares a part of its business data with others which include supply chain networks such as supplier, manufacturer, and retailer who co-operate with each other to achieve their goals such as business planning, reducing production cost, developing business strategies and marketing solutions. Selecting right data sharing platform is very important task for sharing network. Usually, centralized data such as Data warehouse is used for data sharing, which extracts data from the internal production systems (e.g., ERP) of each company for following querying. Actually this data warehouse having some deficiency Such as [4], First, The share data network wants to scope up to support thousands of participants. Second, companies want to fully modify the access control rule to determine which business partners can see which part of their shared data. Most of them failed to overcome such problem. At last to increase the revenue; companies may change their business partners. Therefore, the participants may join and leave the share networks at resolve [1]. This situation cannot be handled by physical data warehouse, to overcome such problem this designs the system for Shared Network for data sharing. This system is the combination of cloud computing, databases

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

and peer to peer based technologies. This system gives the efficiency as pay as you go manner. This system has developed into its new stage of development as a cloud-enable System [3]. The structure of the system shows in Fig 1.

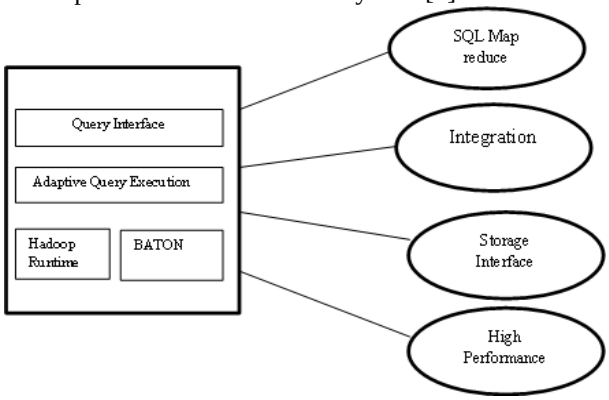

Fig.1: The Structure of System

The Data produced in the Association is Enormous and very Confidential and maintaining this data to the organization is challenging so they may go for outsourcing the data to CSP, This data may be Distributed and stored for a long time due to operational purposes and regulatory submission. The local management of such enormous amount of data is problematic and costly. While there is an observable drop in the cost of storage hardware, the management of storage has become more complex and represents approximately 75% of the total ownership cost. Since the data owner physically releases sensitive data to a remote CSP [5], there are some concerns regarding confidentiality, integrity, and access control of the data. The confidentiality feature can be guaranteed by the owner via encrypting the data before outsourcing to remote servers [9]. The proposed model provides trusted computing environment by addressing important issues related to outsourcing the storage of data, namely confidentiality, integrity, access control and mutual trust between the data owner and the CSP. This means that the remotely stored. In summary, this paper shows that designed system provides inexpensive, Flexible solutions for shared network. They evaluate the system against Hadoop DB [2], an approach for data sharing applications which shows that the proposed system is significantly better than Hadoop DB.

II. LITERATURE SURVEY

A. Existing System

A solution to detect cheating from owner side as well as CSP side is done through digital signatures. For each file owner attaches digital signature before outsourcing. The CSP first verifies digital signature of owner before storing data on cloud [7]. In case of failed verification, the CSP rejects to store data and asks the owner to resend the correct signature. If the signature is valid, both the file and signature are storedon the cloud servers. The digital signature achieves non-repudiation from the owner side. When an authorized user (the owner) requests to retrieve the data file, the CSP sends file, owner's signature and CSP's signature on (file || owner's signature). The authorized user first verifies the CSP's signature. In case of failed verification, the user asks CSP to re-perform the transmission process. If CSP's signature is valid, the user then verifies owner's signature. If verification fails, this indicates the corruption of data over the cloud servers [8]. The CSP cannot repudiate such corruption for the owner's signature is previously verified and stored by the CSP along with file. Since CSP's signature is attached with the received data, a dishonest owner cannot falsely accuse the CSP regarding data integrity. The above solution increases the storage overhead on cloud as owner's signature is stored along with the file on cloud servers. Moreover, there is an increased computation overhead, CSP has to verify signature of owner before storing file on cloud, and the authorized user verifies two signatures for each received file. If the CSP receives file from trusted entity other than the owner, the signature verification is not needed since the trusted entity has no incentive for repudiation or collusion [6]. Therefore, delegating small part of owner's work to the TTP reduces both the storage and computation overheads. However the outsourced data must be kept private and any leakage of data toward the TTP must be prevented Limitations are as follows,

1) The CSP is untrusted, and thus the confidentiality and integrity of data in the cloud may be at risk.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

2) Computation Overhead is more in owner side As well as CSP side
3) A data owner and authorized users may collude and falsely accuse the CSP to get a certain amount of reimbursement.
4) The Owner May Loss the direct control over the sensitive data.

III. PRAPOSED SYSTEM

A. System Architecture

This system uses the pay-as-you-go business model popularized by cloud computing. By combining cloud computing, database, and peer-to-peer (P2P) technologies [6] containing a cloud development of Best Peer. At the last stage of its development, this System is improved with distributed access control, multiple types of indexes and pay-as-you-go query processing for deliver elastic data sharing services in the cloud [5]. The software components of the system are separated into two parts: Core and Adapter. The Architecture is shown in Fig. 2. The core having all function of data sharing and it shows that it is platform independent.

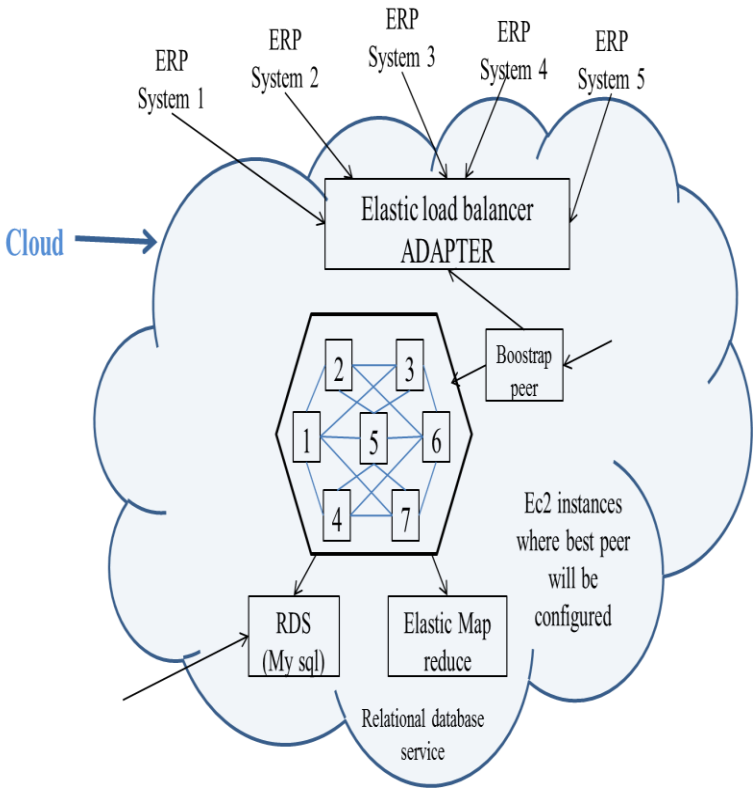

Fig. 2. The System Architecture

The adapter contains one abstract adapter for getting portable service edge and a set of real adapter components which by specific cloud service providers (e.g., Amazon). To achieve portability it build two level design, With appropriate adapters, this System can be portable to any cloud environments (public and private) or even non-cloud environment (e.g., on-premise data centre) [7]. The System can be implemented an adapter for Amazon cloud platform.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

B. Component of System

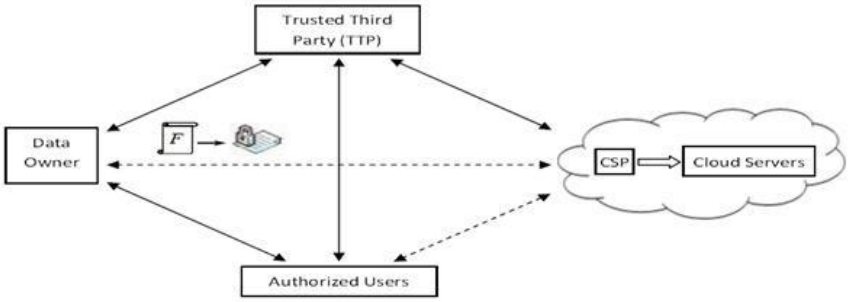

Fig. 3 Component of Cloud Computing Storage System

Fig. 3explainsthe system components and relationship between them.

1) *Data Owner:* Information Owner of the device component is the nothing the user of craving to save and share data over cloud. Information owner isn't having any idea where my information will be stored by the CSP and there is trust shortfall on CSP [10] [11].As data is most important for info owner and the data owner do not desire that his information is observable to the CSP [12]. To fix the preceding issue set trustworthy third party and before uploading the data, it's encrypted / auditor which are set to keep watch.
2) *Trusted Third Party / Auditor:* Database auditing involves a database to not be unaware of the actions of the database users. Database administrators and consultants frequently set up auditing for the security purposes. For example to ensure that advice to be accessed by those without the permission do not access it.Auditing is the monitoring and recording of user database activities that are selected. It might be based on groupings of variables that can include user name, program, time, and so on, including the kind of SQL statement executed, or on individual activities [10] [12]. Auditing can be triggered by security policies when specified components including, within an Oracle database are obtained or altered the contents within a given object.

Auditing is usually used to:

a. Enable future responsibility for current actions moving unique content, or taken in a certain schema, table, or row.
b. Deter users (or others) from improper actions according to that responsibility.
c. Find out problematic action,For example, if some user is deleting data then the security administrator might decide to audit all connections to all successful and unsuccessful deletions of rows and the database from all tables in the database.
d. Notify an auditor the user has more honors than expected which can lead to reconsidering user authorizations and an unauthorized user deleting or is manipulating information.
e. Monitor and collect information about database activities that are specific, For example, the database administrator can collect data about which tables are being upgraded, how many logical I/Os are performed, or how many concurrent users connect at peak times.
f. Find issues with an authorization or access control execution.

3) *Authorized User:* Authorized User is a client of owner who has right to access the remote data [12] [13].
4) *Cloud Storage Service Provider (CSP):* Database is provided by cloud Storage Services Provider. It permits information owner to keep any kind of information and also able to make the user define database schema. It can be Non SQL / SQL form of database instance. According to user requirement CSP will allocated the space for the user instance [12][13].

C. Mathematical Model

1) *Problem Description:*

Let S be a system which do analysis and read documents; such that S = {S1, S2, S3, S4} where S1 represents data owner with encryption.S2 represents TTP for generate hashing with data chunks. S3 represents Access control and

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

decryption by CSP. S4 user downloading and verification.
Result: S holds list of modules in the system

2) Activity:

2.1 Activity I : Data Encryption & selection

Let S1 be a set of clients nodes which are connected to server

S1= {U1,U2.U3……..Un}

Where,

S1is the set of users which are registered.

Results: If User encrypted data success proceed Else discard t

2.2*Activity II:* User Authentication phase

Let's S2 define user authenticate or not

Where

Ui ={UI1,UI2.UI3……UIn}

Ui is the set of database users.

Results: If user provided d and password in database then authenticated

2.3 Activity III: S3 and S4

S3 ={Au1,Au2,Au3……Aun} Role base Accessible users

S4={Dec1,Dec2……Decn) final decrypted data

Where

Algorithms required private keys.

Results: If(keys are match) then proceed Else discard.

D. Implementation

The proposed scheme is executed using HTML, JSP and Java i.e Web Application. The proposed scheme contains of six modules: User Registration, Owner Registration, User Login, Owner Login, TTP Module, TTP Alert Module and CSP Module. The User Registration Module will take the required information from the User i.e. Name, email-id, Password, Employee code and Mobile Number and Stores in Database. The Owner Registration Module will take the required information from the Owner i.e. Name, email-id, Password, Employee code and Mobile Number and Stores in Database [14]. The User Login Module Accepts the Email-id and Password from the User and Validate These Credentials with the Database if These Information is correct Then it will allow them to Login. The Owner Login Module Accepts the Email-id and Password fromthe Owner and Validate These Credentials with the Database if These Information is correct Then it will allow them to Login. The TTP Module also had a TTP Login it will ask them to enter Valid User Name and Password, After Login the TTP module will have the Files which are uploaded by the Owner. The TTP Alert Module Will check for the Dishonest Party (i.e. Owner or CSP) by comparing File which is stored in its database as well as File sent from the Authorized User if they want [15]. The CSP Module also had a CSP Login it will ask them to enter Valid User Name and Password, After Login the CSP module will have the Files which are uploaded by the TTP will validate the credentials given by the each entity. (i) Data Confidentiality is attained using the encryption algorithms. (ii) Detection of Dishonest Owner/CSP Using the TTP alert module.

IV. RESULTS AND ANALYSIS

A. Security Analysis

1) Detection of dishonest owner/user :

If the owner/user falsely faults the CSP regarding data integrity, the TTP performs cheating detection procedure. In this procedure, TTP retrieves encrypted file from CSP and computes the temporary hash value F1Htemp and compares F1HTTP and F1Htemp. If F1HTT =F1Htemp then F1 has not been corrupted on the server and owner/ user is dishonest.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

2) Detection of dishonest CSP:

During the data access phase of the proposed scheme, the authorized user receives the encrypted file F1 from the CSP and F1HTTP from the TTP. The authorized user computes hash of encrypted file F1Hu and associates F1HTTP and F1Hu.
If F1HTP /= F1Hu, a report is issued to TTP to determine the dishonest party. The TTP retrieves encrypted file from CSP and computes the temporary hash value F1Htemp and compares F1HTTP and F1Hu.If F1HTTP ≠F1Htemp, thenF1 has been corrupted on the server and CSP is dishonest.

B. Performance Analysis:

The time performance of this paper was analysed under various file sizes. At first the time performance of this paper is evolved for different file sizes as shown in Table 1 and in Fig 4. Then the security operation time was evolved.

Table 1: Time Performance for file upload/download process.

File Size	Upload(sec)	Download(sec)
1kb	3	2
10 kb	9	4
50 kb	10	6
150 kb	20	9
200 kb	25	13

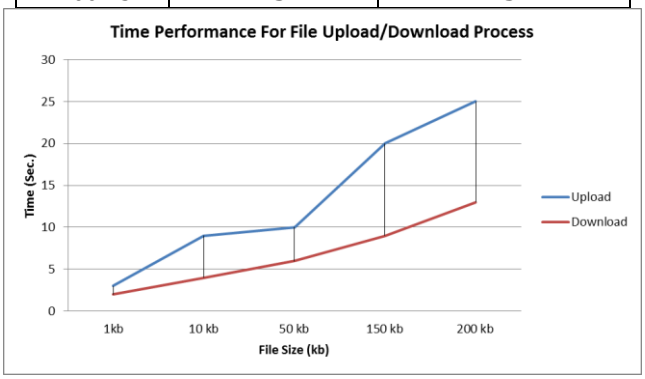

Fig. 4 Time performance of Upload/Download Processes

V. CONCLUSION

The part of cloud computing has brought many researchers from different fields; yet, much effort remains to reach use and the broad acceptance of cloud computing technology. The further work can be extent to study the data error localization, which is nothing but whenever data corruption has been detected during the storage correctness verification, Proposed scheme guarantees the simultaneous localization of data errors, i.e., the identification of the misbehaving server(s). The CSP needs a protection from any false accusation that may be claimed by the owner to get illegal compensations. In this paper, a cloud-based storage scheme is proposed that allows the data owner to benefit from the facilities offered by the CSP and enables indirect mutual trust between them.

VI. FUTURE SCOPE

The area of cloud computing has attracted many researchers from diverse fields; however, much effort remains to achieve the wide acceptance and usage of cloud computing technology. A number of future research directions stem from our current research. Problems to address during future research are summarized below:
Storage Overhead in TTP: The files which are outsourced to the CSP from the data owner all these files has to store in the TTP, This is necessary in detection of Dishonest party, But the storage space required to store the data is huge and

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

it will take sustainable cost as well and also the maintenance of that particular data, The research may be proceeded to minimize the data stored in the TTP.

REFERENCES

1. Gang Chen, Tianlei Hu, Dawei Jiang, Peng Lu, Kian-Lee Tan, Hoang Tam Vo, and Sai Wu, "Extended BestPeer: A Peer-to-Peer Based Large-Scale Data Processing Platform",VOL. 26,NO. 6, JUNE 2014.
2. Gang Chen, Tianlei Hu, Dawei Jiang, Peng Lu, Kian-Lee Tan, Hoang Tam Vo, and Sai Wu, "BestPeer++: A Peer-to-Peer Based Large-Scale Data Processing Platform", VOL. 26,NO. 6, JUNE 2014.
3. H.V. Jagadish, B.C. Ooi, and Q.H. Vu, "BATON: A Balanced Tree Structure for Peer-to-Peer Networks," *Proc. 31st Int'l Conf. Very Large Data Bases (VLDB '05)*, pp. 661-672, 2005.
4. W.S. Ng, B.C. Ooi, K.-L. Tan, and A. Zhou, "PeerDB: A P2P-Based System for Distributed Data Sharing," *Proc. 19th Int'l Conf. Data Eng*., pp. 633-644, 2003.
5. S. Wu, S. Jiang, B.C. Ooi, and K.-L. Tan, "Distributed Online Aggregation," *Proc. VLDB Endowment*, vol. 2, no. 1, pp. 443-454, 2009.
6. S. Wu, J. Li, B.C. Ooi, and K.-L. Tan, "Just-in-Time Query Retrieval over Partially Indexed Data on Structured P2P Overlays," *Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD '08*), pp. 279-290, 2008.
7. S. Wu, Q.H. Vu, J. Li, and K.-L. Tan, "Adaptive Multi-Join Query Processing in PDBMS," *Proc. IEEE Int'l Conf. Data Eng. (ICDE '09*), pp. 1239-1242, 2009.
8. Beng Chin Ooi, YanfengShu, "Relational Data Sharing in Peer-based Data Management Systems." Kian-Lee Tan Sigmod Record special issue on P2P, 2003.
9. B.C. Ooi, K.L. Tan, A.Y. Zhou, C.H. Goh, Y.G. Li, C.Y. Liau, B. Ling, W.S. Ng, Y.F. Shu, X.Y. Wang, M. Zhang " PeerDB: Peering into Personal Databases." *The 2003 ACM SIGMOD Intl. Conf. on Management of Data (Demo*). (SIGMOD 2003).
10. Heng Tao Shen, YanfengShu, and Bei Yu IEEE Trans. Knowl. "Efficient Semantic-Based Content Search in P2P Network." Data Eng. 16(7): 813-826(2004)
11. Amazon.com, "Amazon Web Services (AWS)," Online at http://aws.amazon.com, 2008.
12. K. E. Fu, "Group sharing and random access in cryptographic storage file systems," *Master's thesis, MIT, Tech. Rep*., 1999
13. R. A. Popa, J. R. Lorch, D. Molnar, H. J. Wang, and L. Zhuang, "Enabling security in cloud storage SLAs with cloud proof," in *Proceedings of the 2011 USENIX conference*, 2011.
14. Fu,"Plutus: Scalable secure file sharing on untrusted storage," *in Proceedings of the FAST 03: File and Storage Technologies*, 2003.
15. D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short cipher texts and private keys," *in Advances in Cryptology - CRYPTO*, 2005, pp. 258–275.

BIOGRAPHY

Miss. BhavsarHarshada V completed her B.E. in Information Technology from Babasaheb Ambedkakar MaratWadaUniversity, Pune and doing M.E. from SharadachandraPawar College of Engineering, Dumberwadi.

Prof. G. D Deokate currently working as an assistant professor in SPCOE, Dumbarwadi.

Dr. S.V.Gumaste, currently working as Professor and Head, Department of Computer Engineering, SPCOE-Dumberwadi, Otur. Graduated from BLDE Association's College of Engineering, Bijapur, Karnataka University, Dharwar in 1992 and completed Post- graduation in CSE from SGBAU, Amravati in 2007. Completed Ph.D (CSE) in Engineerng& Faculty at SGBAU, Amravati. Has around 22 years of Teaching Experience.