to the world! Clearly, this is an application for P2P distributed data management systems for the same reasons as the health care application.

c) Data Caching: In the above two examples, each participant is actively involved in the process of consuming and supplying data. P2P distributed data management can also be deployed in passive nodes: nodes that are used to share resources (storage or computational power) on data that they may or may not be interested. Caching results from earlier queries is one such example - a node may have issued a query to some server (e.g., a data warehouse), the results of the query can be cached on the node (or some other neighbouring nodes). In this way, another node that requests for data that overlap the query result can potentially obtain partial answers quickly from this node, and the remainder from the original server. This also lightens the load on the original server. Indeed, Kalniset. al. [5] [8] [9] have shown how distributed caching can be deployed in P2P environments to speed up OLAP queries.

2.5. Query Processing

This system gives the two mode processing approach i.e parallel processing approach and adaptive processing approach [1]. Query is submitted over normal peer using fetching and processing. The normal peer remote the subquery and the results are shuffled to the query submitting peer P [11].

3. System Design

3.1 System Component

Figure 2 explains the system components and relationship between them.

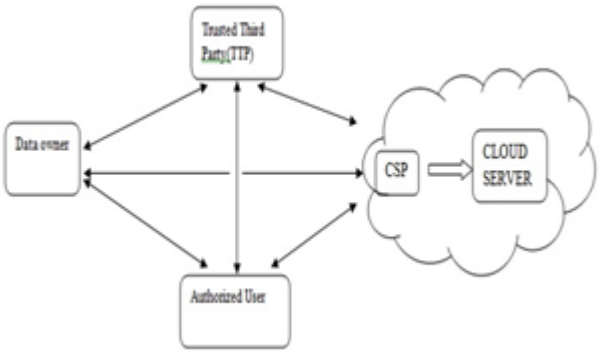

Figure 2: The System Component and their relationship

3.1.1 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.

3.1.2 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.

3.1.3. Authorized User

Authorized User is a client of owner who has right to access the remote data [12].

3.1.4. 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].

3.2 Working

This system is implemented using 4 types of module as explain following,

3.2.1. The Data Owner Module

The Owner module can perform 4 operations. In upload operation, the data owner selects file F and generates a secret key k for a file. To achieve privacy-preserving, the owner creates an encrypted file $F' = E_k(F)$. The owner sends encrypted file to the TTP. TTP computes hash value for file $H(F')$ and sends file F' to CSP. Key response operation is used by the data owner to grant or revoke access to the outsourced file [8] [10]. In this operation, the data owner checks key requests from authorized users and if data owner wants to grant access then sends key.

3.2.2. Cloud Service Provider Module

The Cloud Service Provider (CSP) module is used to store and retrieve data. The CSP stores encrypted files F' sent by Owner and sends file to authorized users on demand [10].

3.2.3. Trusted Third Party Module

The TTP module receives encrypted file F' from the data owner and computes hash value $H(F')$ using SHA-1 algorithm [8]. It stores $H(F')$ in its database which will be used during the dynamic operations and to determine the cheating party in the system (CSP or Owner). TTP send file F' to CSP module to store on cloud.

3.2.4. Authorized User Module

Authorized users are set of owner's clients who have the right to access the remote data. To access the data, the authorized user sends a data-access request to the CSP and TTP, and receives the data file in an encrypted form F' from CSP and hash value of encrypted file $H(F')$ from TTP [10]. To decrypt file authorized user requires secret key k generated by data owner. Authorized user sends key request to the data owner. The owner grants access to file by sending key k to user.

3.3 Updating and Access Control

The Outsourcing of the confidential data has been done by the data owner to the cloud storage servers in an encrypted Form [11]. When the authorized users request for data, they will get data in an encrypted form this data can be decrypted them using the secret key shared among the authorized users. It is assumed that the interaction between the owner and the authorized users to authenticate their identities has already been completed, and it is not considered in this work [10]. The TTP and CSP must be always online, while the owner is intermittently online. The authorized users able to access data file from CSP even when the owner is offline.

3.3 Cheating Model

The CSP resides in an untrusted domain and confidentiality and integrity of data in the cloud may be at risk. For economic incentives and maintaining a reputation, the CSP may hide data loss, or reclaim storage by discarding data that have not been or is rarely accessed [10]. On the other hand, a data owner and authorized users may scheme and falsely accuse the CSP to get a certain amount of settlement. They may dishonestly claim that data integrity over cloud servers has been violated.

3.4. Security Requirement

3.4.1 Confidentiality

Outsourced data must be protected from the TTP, the CSP, and users that are not granted access.

3.4.2 Integrity

Outsourced data are required to remain intact on cloud servers. The data owner and authorized users must be enabled to recognize data corruption over the CSP side.

3.4.3 Access control

Only authorized users are allowed to access the outsourced data.

3.4.4 CSP's Defense

The CSP must be safeguarded against false accusations that may be claimed by dishonest owner/users, and such a malicious behavior is required to be revealed.

3.5 Algorithm

3.3.1. Algorithm for Creation of Bootstrap Peer

This algorithm is used for the building of this system using bootstrap peer node of having component of core use for building this system.

Algorithm 1 BootStrapDaemon ()
1: While true do
2: Status S = invokeCloudWatch ()
3: Array List PeerList = BootStrap.getAllPeer ()
4: Array List new Peer = New Array List ()
5: do i = 0 to PeerList. Size ()
6: if Peerlist.get (i).fails () then
7: Peer.loadMySQLBackUpFromRDS (PeerListget (i))
8: newPeer.add (peer)
9: BootStrap.setBlackList (PeerList.get (i))
10: else
11: if Peerlist.get (i).overloaded () then
12: Peer Peer = new Peer ()
13: BootStrap.removeAllNewPeer (Black List)
14: Sleep T second

3.3.2. Algorithm for Encryption

The encryption process consists of 10 rounds of processing for 128-bit keys. For encryption, each round consists of these four measures: SubBytes (), ShiftRows (), MixColumns (), AddRoundKey ()

Algorithm 2 Encrypt ()
1: Cipher(byte[] input, byte[] output)
2: {
3: byte[4,4] State;
4: copy input[] into State[] AddRoundKey
5: for (round = 1; round < Nr-1; ++round)
6: {
7: SubBytes ShiftRows MixColumns AddRoundKey
8: }
9: SubBytes ShiftRows AddRoundKey
10: Copy State[] to output[]
11: }

4. Results and Analysis

4.1. Security Analysis

4.1.1 Detection of Dishonest Owner/User

If the owner/user falsely faults the CSP regarding data integrity, the TTP performs cheating detection procedure.

4.1.2 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.

4.2. 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 Figure 3.

Table 1: Time Performance for file upload/download process

File Size	*Upload(sec)*	*Download(sec)*
10kb	5	3
15 kb	11	6
20 kb	14	9
50 kb	22	11
60 kb	25	16

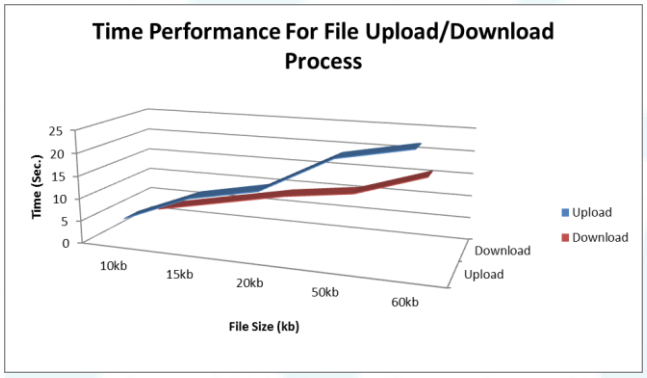

Figure 3: Time performance of Upload/Download Processes

5. Conclusion

This paper defines the business model for storage of large scale date in shared network due to cloud computing storage system. Cloud computing storage system provide efficient way to access large scale data securely using encryption algorithm and provide credential security while access data in shared network. This system make portable using the combination of cloud computing storage system, database, and peer-to-peer technologies. This is created on Amazon EC2 cloud platform which can powerfully handle typical workloads in a shared network and can move near linear query throughput as the number of normal peers grows.

6. Future Scope

A number of future research directions from our current research. Problems to address during future research are Storage Overhead in TTP, In this work 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, the storage space required to store the data is huge and 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, ”BestPeer++: A Peer-to-Peer Based Large-Scale Data Processing Platform”, VOL. 26,NO. 6, JUNE 2014.
[2] 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.
[3] 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.
[4] 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.
[5] 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.
[6] 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.
[7] Beng Chin Ooi, YanfengShu, “Relational Data Sharing in Peer-based Data Management Systems.” Kian-Lee Tan Sigmod Record special issue on P2P, 2003.
[8] 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).
[9] 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)
[10] K. E. Fu, “Group sharing and random access in cryptographic storage file systems,” Master’s thesis, MIT, Tech. Rep., 1999
[11] 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.
[12] Fu,“Plutus: Scalable secure file sharing on untrusted storage,” in Proceedings of the FAST 03: File and Storage Technologies, 2003.

Author Profile

Miss. Bhavsar Harshada V completed her B.E. in Information Technology from Babasaheb Ambedkar Marat Wada University, Pune and doing M.E. from Sharadachandra Pawar 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 Engineering & Faculty at SGBAU, Amravati. Has around 22 years of Teaching Experience.