Research Journal of Applied Sciences, Engineering and Technology 9(8): 572-582, 2015
DOI:10.19026/rjaset.9.1441
ISSN: 2040-7459; e-ISSN: 2040-7467
© 2015 Maxwell Scientific Publication Corp.
Submitted: May 26, 2014 Accepted: July 19, 2014 Published: March 15, 2015

Research Article

Framework for Multilevel Privacy and Backup of Cloud Storage with CDMBackupSim

[1]C. Saravanakumar and [2]C. Arun
[1]Faculty of Computer Science and Engineering, St. Joseph's Institute of Technology, Sathyabama University, OMR, Chennai, Tamilnadu, India
[2]Department of Electronics and Communication Engineering, R.M.K College of Engineering and Technology, Chennai, Tamilnadu, India

Abstract: Cloud computing gives an enormous support to an individual and enterprise which can improve their needs in the global market. The customer's data are stored in different location in the cloud either in same or different region. These data should be handled securely from requester to provider end. The cloud security involves protecting and controlling the data, application and associated infrastructures by imposing the policies, technologies etc. The privacy is used to secure processing and handling the personal data in the cloud is not disclosed by the unauthorized parties. The cloud suffers a reliability issues due to lack of security and privacy over the data. The security levels are confined into a particular boundary which does not cover all access levels. The privacy information of various levels is handled by introducing a multilevel privacy technique for protecting user's data in various boundaries. The proposed framework gives an alert whenever the data are accessed by the Cloud Service Provider (CSP) or any other parties, so this will help the Cloud Service User (CSU) to know the status of data. The proposed work is simulated by introducing CDMBackupSim simulator which has various modules and it gives the simulated result for testing process.

Keywords: Cloud privacy, cloud security, cloud storage, deployment models, distributed systems

INTRODUCTION

Cloud computing evolves from desktop computing in which the data are not shared by other system. The client server model has to overcome the problem of sharing the data between the systems because all the data will depends upon only one system which is called the server. If the server get crashes which leads a severe problem in recovering of data. The Peer-to-Peer (P2P) computing is used to share the data without any master slave relationships. The grid computing holds a high end resources at one end and it solves the real world complex problem. The utility computing provides a way to access resources for the customer who will pay only what he actually consumed. The cloud computing is used to access any resources from the centralized location as a service which follows a pay-as-you-go basis model. There are different service models are available such as SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) and so on. These services are deployed into various deployment model in which the services are accessed through private cloud, public cloud, community cloud and hybrid cloud. The data are stored across the cloud can be protected by applying an effective security over the cloud communication. A single level of security is not suitable for reliable communication between the CSU and CSP. The multilevel security is imposed in various access level such as server access level security, Internet access level security, Database access level security, Program access level security and so on (Kanndukuri *et al*., 2009). The security policies are imposed in all level from CSU to CSP end. The protection of security is mainly focused on CSP because the CSP may misuse the service policies. The protection of data at the CSU level is kept confidential so that, misusing of services can be avoided. The growth rate of cloud services related to IT starts from 16 billion in 2008 to 42 billion in 2012 and also its share in the global market increases from 4.2 to 8.5% (Leavitt, 2009). The information exchange are also growing in high level which leads a high market demand, so the security and privacy management is necessary for the cloud service access. The conference management system such as EDAS and Easy Chair suffers because of the system administration which maintains a huge volume of data in submitting and reviewing the multiple conferences (Ryan, 2011). This data could be disclosed by any unauthorized parties, so the privacy should be imposed in order to conduct conferences properly. The cloud security is mainly used for data protection, data recovery and

Corresponding Author: C. Saravanakumar, Sathyabama University, Faculty of Computer Science and Engineering, St. Joseph's Institute of Technology, OMR, Chennai, Tamilnadu, India

enterprise continuity. The customer data are stored into the cloud data center which never violates the privacy policy of government regulations such as the FFIEC (Federal Financial Institutions Examination Council), HIPAA (Health Insurance Portability and Accountability Act) and PCI DSS (Payment Card Industry Data Security Standards) (Katzan, 2010). The existing cloud service suffers an interoperability and portability problem, because the CSU has locked into a single cloud infrastructures, platform or services. The big vendors such as Amazon, Google and Sales force etc., needs a common standard for eliminating the incompatible formats and feature from other CSP (Brian *et al*., Year). The multi core cloud computing maintains information for the data centers in an encrypted form with client security credentials. The client gets an impossible processing power due to the absence of multicore in the architecture (Hewitt, 2008). Virtual machine replication is used to provide an on demand cloud services and it causes data leakage problem in the cloud. Cloning is a technique for improving the customer service and cloud benefits in the global market level. It violates the privacy policies which also leads a data leakage problem. Amazon EC2 uses a template for virtual machine image which also suffers a privacy problem i.e., machine secrets are never disclosed to the public (for example host key, cryptographic salt value etc.,) (GroBauer *et al*., 2011). Cloud computing interoperability forum targeted the cloud infrastructure in a transparent platform for protecting the data by solving the security and privacy issues such as data privacy, resource privacy and content copyrights etc., (Pallis, 2010). Service Oriented Computing (SOC) mainly uses a message passing technique for realizing the workflow of services, message passed between services or between service and service container. The proprietary information with privacy is a biggest threat in the cloud security (Wei and Blake, 2010). The cloud computing suffers a major issues like privacy, security, anonymity, telecommunications capacity, liability, reliability, government surveillance and also it outpace information policy (Jaeger *et al*., 2008). The problem in privacy-preserving management of digital identity attribute with heterogeneous name could be eliminated by using privacy preserving multi-factor identity attribute verification protocol. This protocol supports matching technique based on look-up tables, dictionaries etc. Aggregate Zero Knowledge Proofs the Knowledge of cryptographic protocol (AGZKPK) which allows the user to interact with proof of knowledge and multiple identity attributes (Bertino *et al*., 2009). The data are stored into the cloud in a particular location would not be identified by the customer unless the request goes to the CSP. The privacy policies such as specific jurisdictions, contractual commitments and local privacy requirements are followed by the CSP without any violations (Brodkin, 2008). The vulnerability occurs in VM during the VM shutdown and starting a new virtual machine which uses the same memory space for storing sensitive information. This information suffers security and privacy implications such as identity theft, fraud and blackmail, stealing and so on. A secure shutdown and data destruction capabilities are proposed to eliminate any data which are available at the time of shutting down the VM (Krautheim, 2012). The deployment model such as private cloud, public cloud, community cloud and hybrid cloud does not offer the level of privacy and security over the cloud service. The privacy level is mainly based on the assurances, privacy policies, robustness of security and privacy control etc., (Jansen and Grance, 2011). The security and data privacy across the cloud services are IaaS, SaaS, PaaS which uses many standards such as Identity and Access Management (IAM), Data Encryption, Key Management, Records and Information Management, E-discovery EDRM (Electronic Discovery Reference Model) for maintaining a proper policies over the cloud access (Mell and Grance, 2010). The existing techniques are used to achieve the security and privacy over the customer's data which are available at the cloud. Nowadays the information grows enormously because of the demand in the cloud services so, some extra care must be taken to protect the data at maximum level in all data centers. Cloud service normally uses security standards and privacy policies within the boundary which leads an unauthorized disclosure of the data with backup mechanism. The proposed work focuses on the multilevel security and privacy for securing the data from unauthorized disclosure of data.

Comparison of online backup services: Online backup services are used to transmit data in a secure manner through an efficient data centre. The main objective of backup is to secure the data from fire, theft, crashes and disasters and so on. There are plenty of backup solutions in the market to achieve the backup of customer data. BackBlaze is one of the online backup services which has the ability to store 100 GB virtual files and 12 h 1080 p videos without file limit (Fisher, 2014). Crash Plan is an automotive backup service which supports various platforms like Windows, Mac OS X, Linux, Open Solaris and Solaris. The multi-layered security model for data security and privacy has been addressed but it is restricted only to the secure java virtual machines by applying cryptographic algorithms with industry standards (CrashPlan, 2014). Carbonite is a backup solution which has the unlimited automatic file encryption for protecting the privacy information features and also the files are accessed using computer or smartphones (Carbonite, 2014). Mozy is an online backup service which offers free storage of 2 GB with certain features like Military-Grade Security and 2X protect local backup (Mozy, 2014). SOS is a backup service which supports unlimited number of devices, unlimited versioning and

Table 1: Online backup service feature comparison (Online Backup Service Feature Comparison, 2014)

Feature	Crashplan	Backblaze	Mozy	Carbonite	SOS	Live drive	SugerSync	Bitcasa	SpiderOak	Acronis
Multi device syncing	No	No	Yes	Yes	Yes	No	Yes	No	No	No
Transfer encryption (128-bit)	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes
Transfer encryption (256-bit)	No	Yes	No	No	Yes	No	Yes	No	Yes	Yes
File encryption (128-bit)	No	Yes	No	Yes	No	No	No	Yes	Yes	No
File encryption (256-bit)	No	No	Yes	No	Yes	Yes	No	Yes	Yes	No
File encryption (448-bit)	Yes	No	Yes	No	No	No	No	No	No	No
Drive level backup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Folder level backup drive	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
File level Backup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Backup from mapped drive	Yes	No	No	No	Yes	Yes	Yes	Yes	No	No
Backup from attached drive	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
Continuous backup (= 1 min)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Backup frequency option (sec)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Idle backup option	Yes	Yes	Yes	Yes	No	No	No	Yes	No	No
File sharing	No	No	No	Yes	Yes	No	Yes	Yes	No	No

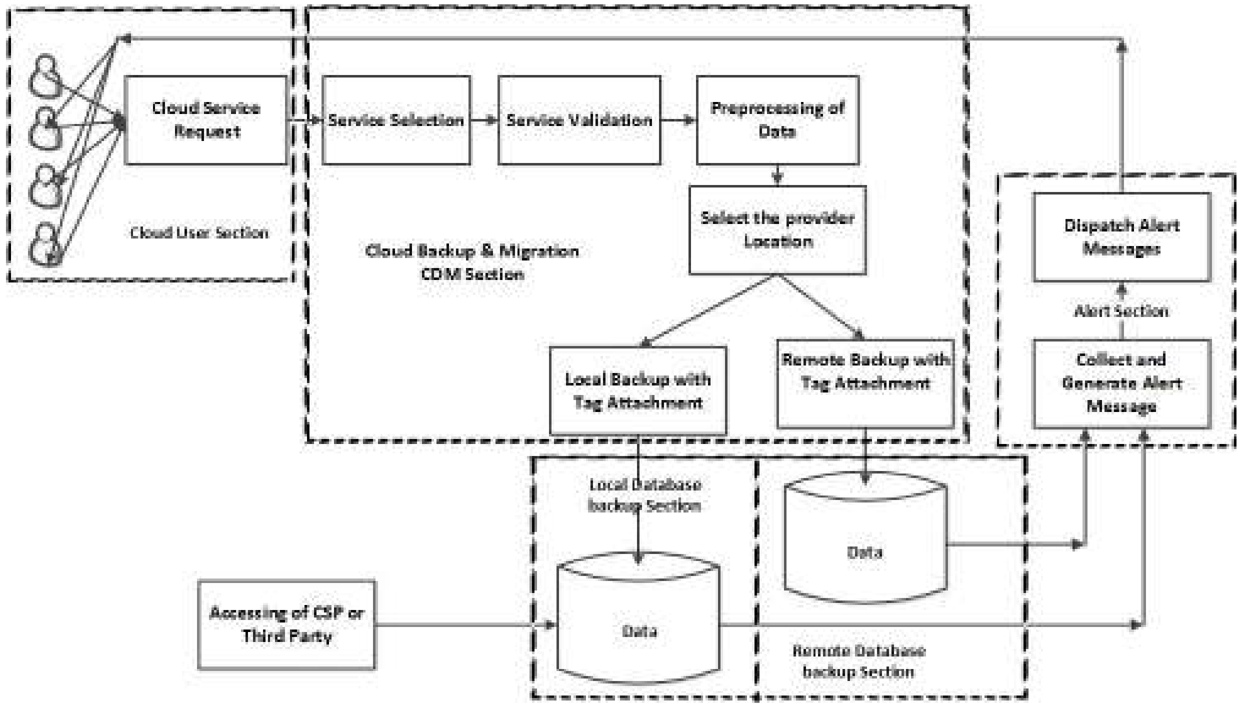

Cloud Service Request
Cloud User Section
Service Selection
Service Validation
Preprocessing of Data
Select the provider Location
Cloud Backup & Migration CDM Section
Local Backup with Tag Attachment
Remote Backup with Tag Attachment
Dispatch Alert Messages
Alert Section
Collect and Generate Alert Message
Local Database backup Section
Data
Data
Accessing of CSP or Third Party
Remote Database backup Section

Fig. 1: Multilevel privacy and backup model

continuous data backup, network drive support (SOS,2014). Sugar Sync is an online backup service which establishes the sync between all customer devices (SugarSync, 2014). Live drive is an online backup service which provides the support for mixing of backup plans in order to add cost effective interface over computer and mobile based applications (Livedrive, 2014). Bitcasa is an infinite external hard drive in the cloud which handle the out of space situation (Bitcasa, 2014). SpiderOak is a private online backup with sync and sharing functionality that offers 2GB free online backup to the customer (SpiderOak, 2014). Acronis is an online backup business services with the features like Disk Imaging, Incremental and Differential Backups, Free Online Storage, Nonstop PC Backup, Time Explorer, Automatic File Sync (Acronis, 2014). Table 1 describes that the comparison of online backup service in the cloud storage.

METHODOLOGY

Multilevel privacy and backup model: Figure 1 shows that the proposed model of multilevel cloud privacy and backup of the cloud storage. The cloud

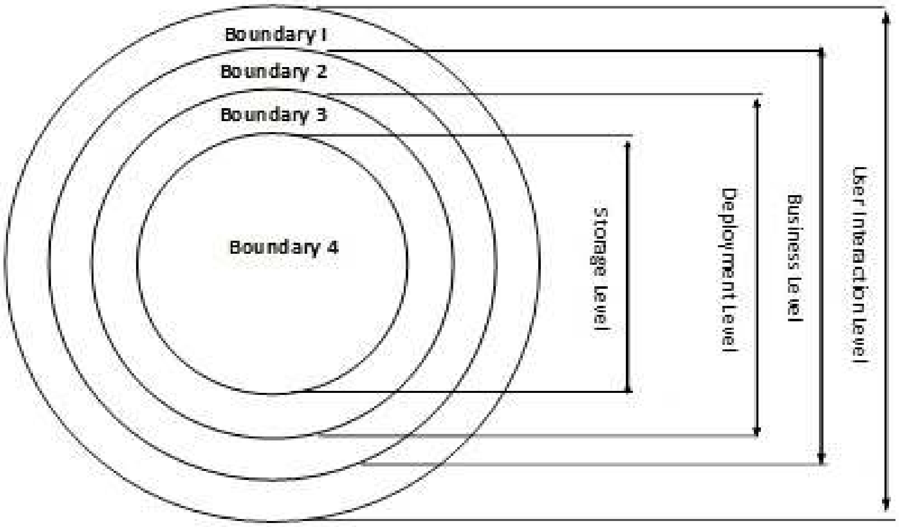


Fig. 2: Information boundary across various levels of cloud access

request section maintains the information which is related to the request from the user. This information is handled only by an authorized CSU so, the unauthorized requests are restricted at CSU end. The cloud backup and migration section selects the service, validates the service, preprocesses the data, selects the CSP and attach the tag for local as well as remote backup or migration. The information is handled with privacy so, unauthorized disclosure can be avoided. The local and remote backup of the data are handled in their own boundary which supports an efficient protection over the data. Suppose the CSP or third party needs to perform an operation or to access a data which triggers an alert message to the CSU. The CSU can able to know the status of the data and also know the reason for accessing the data, so that the data are protected from unauthorized disclosure. The alert section sends the status message to the CSU in order to achieve reliability at maximum level.

Privacy boundary levels for cloud service access: The privacy level depends upon the information which is protected in a particular boundary. Figure 2 shows that the privacy information level for overall cloud access from CSU level to the storage level. There is no disclosure of information from one level to another level and so on. For example, in cloud access the user authentication information (username and password) are used by the CSU interface level to storage level with an efficient manner. The information boundary at the business logic level needs the processing and accessing of data. For example the business logic information is kept confidential while processing and providing vital information to the CSU. The information boundary of private cloud is also kept confidential from unauthorized access of cloud data. Suppose the data is moved from private to public cloud some extra care should be taken in order to protect the data from unauthorized boundary. The sensitive data are kept confidential to make available within the cloud storage information boundary. The overall protection of information gives a reliable access for CSU and also it maintains the information in an appropriate boundary. Table 2 shows that the privacy information with various boundaries.

Table 2: Privacy information on cloud boundaries

Boundary	Privacy information
Cloud access level	
Customer level	Host information, credential information, location and purpose
Interface level	Network information, type of interface, process and kernel information
Data level	Data representation and specification, security policies
Storage level	Type of storage, location and server information
Business level	
Business level	Requested information, encryption policies
Processing level	Business logic information, method information, interaction level information
Data level	Input information, sub calculation information, response information
Access level	Access level information, authorization information
Deployment level	
Private level	Organization information and capacity, purpose
Public level	Information for sharing
Hybrid level	Exchange the information between cloud
Community level	Exchange the information between cloud
Storage level	
Migration level	
Local level	Storage information, representation information
Remote level	Location information, representation information
Backup level	
Local level	Storage information, representation information
Remote level	Location information, representation information

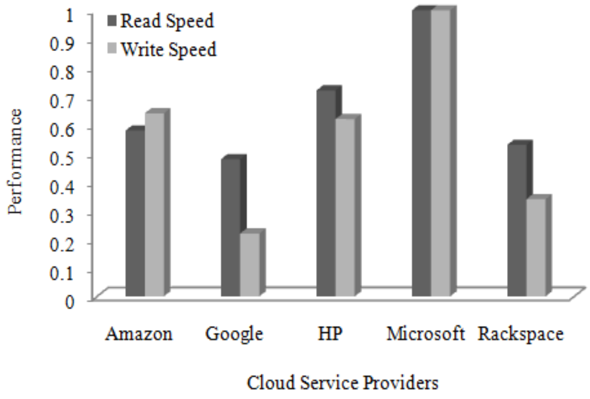


Fig. 3: Reading and writing speed of cloud storage with file size (< = 1 MB)

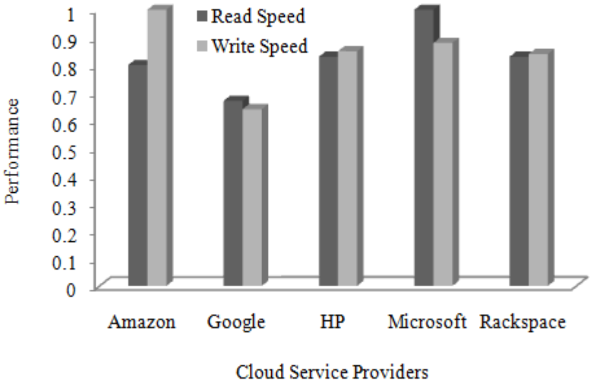


Fig. 4: Reading and writing speed of cloud storage with file size (>1 MB)

Performance comparison of various cloud storage: The performance of the cloud depends upon the scalability and stability for reading and writing cloud storage from small size to large file size. The following chart shows that the comparison of various cloud service provider which are related to the reading and writing operations of various file sizes (Cloud Performance, 2014). Figure 3 shows that the cloud storage of reading and writing speed over the file size less than 1 MB. Figure 4 shows that the reading and writing speed over the file size greater than 1 MB.

Organization of cloud backup and cloud access: Figure 5 describes that the taxonomy of cloud backup. The cloud backup has to follow various perspectives of access level in order to achieve maximum reliability. The cloud backup depends on the location in which the data are stored. The location is classified into two types namely local and remote. Local backup is to store the data in different places of storage in same machine or different storage in same location where as remote location backs up the data in different location irrespective of the region. The local backup first checks the capacity of the storage by following two methods which are used to check whether the threshold is reached or not. If it reached, then stores the data in storage otherwise it selects the replacement methods for identifying free slots for data backup. There are four replacement methods are proposed for efficient backup of data namely Long Time Ideal (LTI), Threshold Level Ideal (TLI), Time Stamp Based (TSB) and Priority

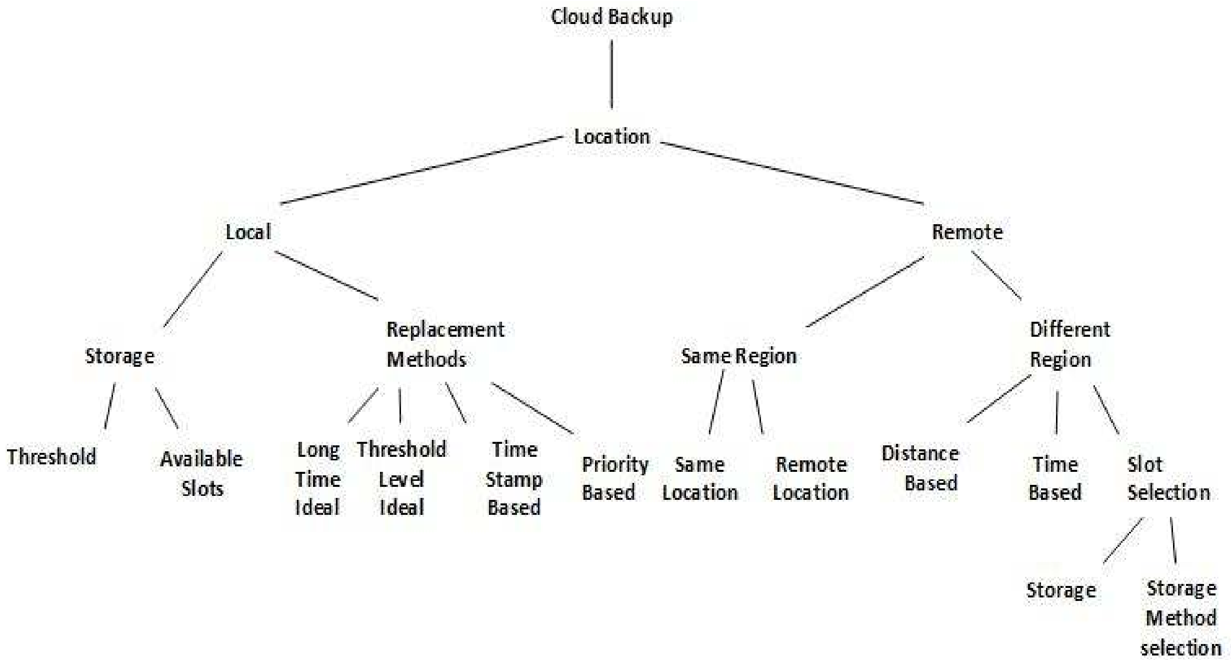


Fig. 5: Taxonomy of cloud backup

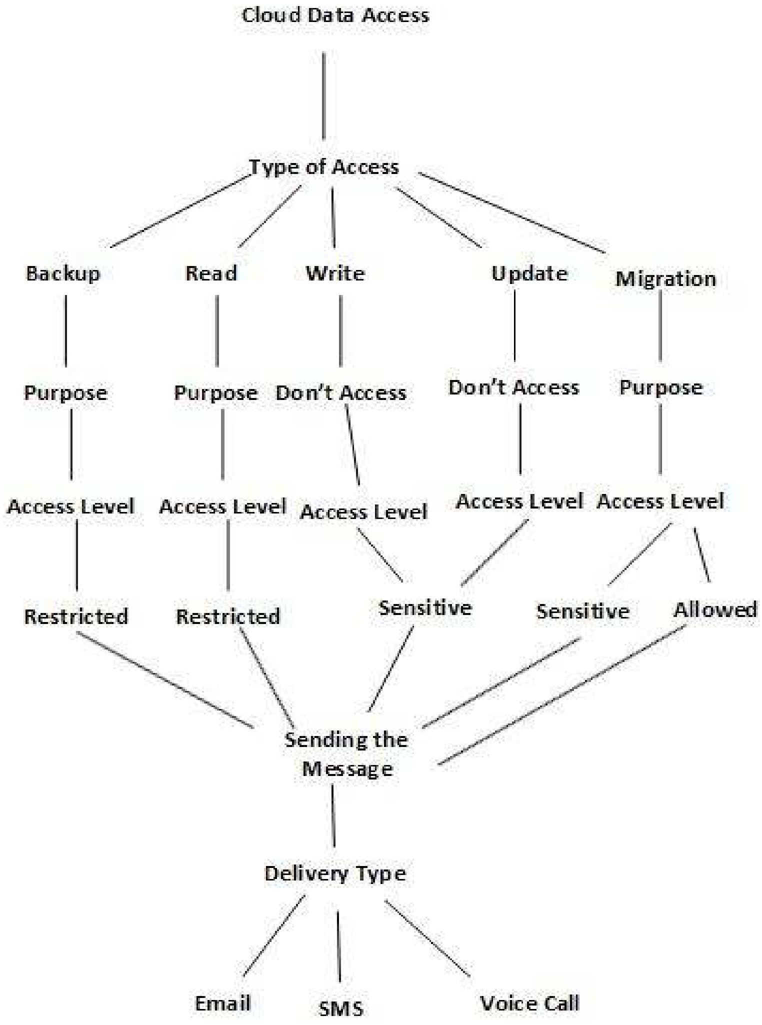
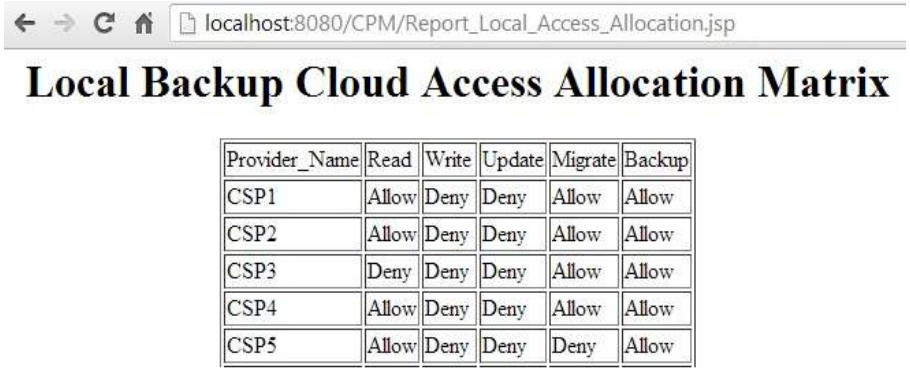


Fig. 6: Taxonomy of cloud access

Based (PB). These replacement methods will never remove the customer data from the storage instead it moves to some other location in the same region or other regions. LTI replacement method selects and replaces the data which are ideal in long time. TLI method checks the storage of threshold at the maximum level and selects the data using LTI method for moving the data to other location and fixing the slot. The TSB method replaces the data periodically and checks the access time with predefined time during storage of data in the cloud. PB method will replaces the data for backup by checking the priority assigned over the cloud data in the cloud storage. The remote backup is used to store the data either in same region or different region.

The data are backed up in the same region like as local backup technique. If it is different region the following methods are selected for effective cloud storage they are Distance Based (DB), Time Based (TB) and Selection Based (SB) cloud backup. DB selects the location based distance from the current data location. TB is used to back up the data based on time duration used by the cloud data. The organization of the cloud backup is proposed and verified by using CDMBackupSim simulator.

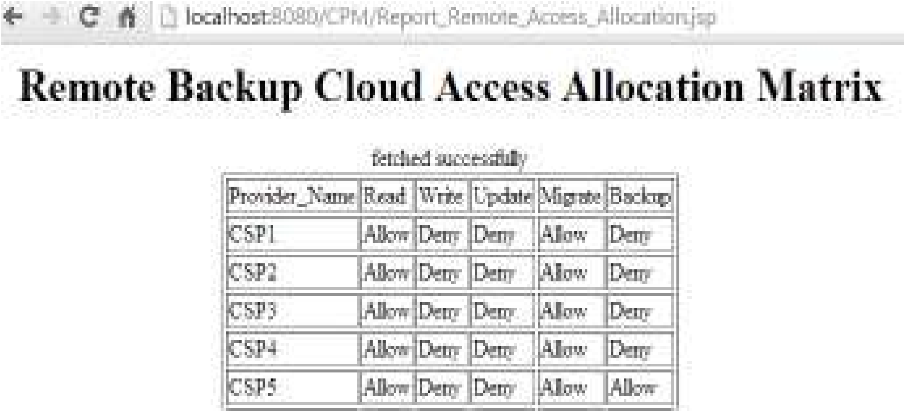
Figure 6 shows that the taxonomy of cloud data access. The provider may interact with the cloud storage for performing the backup and migrating the customer's data. The privacy information is protected in different levels so that the efficiency can be achieved over the cloud storage. The provider needs some level of access while handling the cloud storage performance processing. The type of accessing over the cloud storage is categorized into reading, writing, updating, migrating and backuping of data. CDMBackupSim provides the access level to various persons who use the cloud data. The necessities of particular access of data should be restricted then only the privacy information is protected from unauthorized disclosure. These access rights are assigned to the persons in three levels namely restricted, sensitive and allowed. The customer has to



Local Backup Cloud Access Allocation Matrix

Provider_Name	Read	Write	Update	Migrate	Backup
CSP1	Allow	Deny	Deny	Allow	Allow
CSP2	Allow	Deny	Deny	Allow	Allow
CSP3	Deny	Deny	Deny	Allow	Allow
CSP4	Allow	Deny	Deny	Allow	Allow
CSP5	Allow	Deny	Deny	Deny	Allow

Fig. 7: Local backup cloud access allocation matrix



Remote Backup Cloud Access Allocation Matrix

fetched successfully

Provider_Name	Read	Write	Update	Migrate	Backup
CSP1	Allow	Deny	Deny	Allow	Deny
CSP2	Allow	Deny	Deny	Allow	Deny
CSP3	Allow	Deny	Deny	Allow	Deny
CSP4	Allow	Deny	Deny	Allow	Deny
CSP5	Allow	Deny	Deny	Allow	Allow

Fig. 8: Remote backup cloud access allocation matrix

get a complete access rights then only the CSU can perform all the operations over the data. The traditional or existing online backup systems provide the services to CSU either local backup or remote backup, but this backup standard faces some issues like customer awareness and monitoring. Normally the customer doesn't know about how, where and what level of security available over the data. This proposed system provides a complete solution by implementing an alert mechanism over the cloud storage to satisfy the customer. If the providers or any users try to access the data, then the alert message will be delivered to the customer via SMS, Email or voice call. For every access of customer's data an alert will be generated. The main objective of the proposed system is to provide awareness among the customer to control their data and also retain the customer. Figure 7 and 8 shows the cloud backup access allocation matrix in CDMBackupSim Simulator.

CDMBackupSim simulator: Cloud computing has various simulators which provide the result related to the cloud service models. CloudSim provides a generalized modelling simulation framework for cloud infrastructure with application services. CloudAnalyst analyses the working behavior of large scale internet application in the cloud. GreenCloud is used to analyses the energy efficiency of the data centres. GridSim is an event based simulator for grid and cloud based scientific environment. DCSim is used to evaluate and develop data centre management (Oujani, 2014). This simulator gives the simulation result with various parameters of the cloud computing, but does not concentrate on the disaster management of cloud data. The proposed CDMBackupSim simulator is used to backup the cloud data in local as well as remote location. The CDMBackupSim comprises of various modules such as provider selection, service selection, service validation, backup selection, tag attachment, access level allocation and alert generation. The provider selection is used to select a suitable provider who meets the customer's requirement. The services are selected by using service selection module then the selected services are validated over various parameters. The backup selection module is used to select the backup either in local or remote location. The tag is generated as soon as the backup selection gets completed. The tag contains all performance parameters such as data size, CID, CL, AL, capacity, current response size and identifies the free slots. The CID and CL are Client Identification and Client Location respectively. AL is an allocation of Access Level for

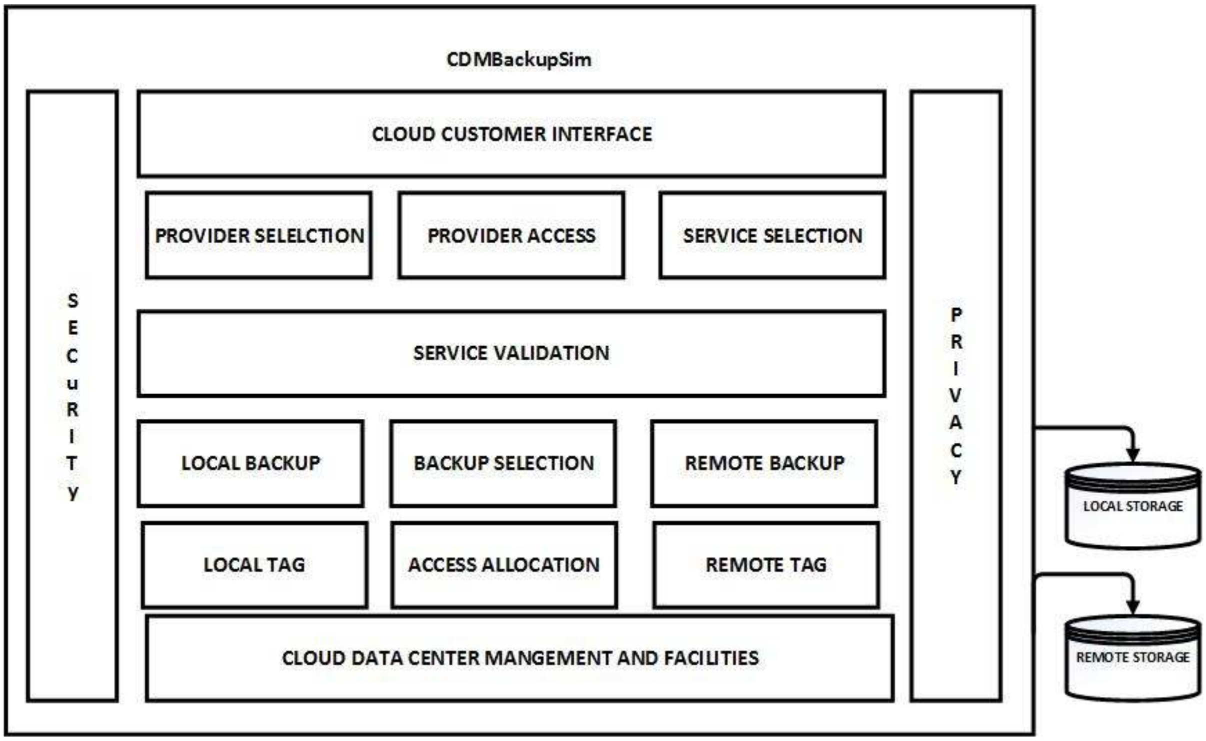


Fig. 9: Architecture of CDMBackupSim simulator

various users and providers. The capacity of the cloud storage and current expected response size is also fixed in a tag. The freeslots are identified for applying the replacement algorithms. In remote backup the location of the remote storage systems are identified either in the same region or different region. Figure 9 describes that the overall architecture of CDMBackupSim simulator.

Algorithm: The algorithms of CDMBackupSim for protecting the privacy information are as follows:

Algorithm for CDMBackupSim:

```
Input: CustomerData$_j$ = <Data$_j$, E$_j$, Size$_j$>
Output: Status backup of data or access violations
Request$_j$ = <Data$_j$, E$_{j+}$CustomerInfo$_j$>
Location$_j$ = getBackupLocation ();
If (Location$_j$ ='Local') then
    StorageMethod$_j$ = getStorageMethod ();
    Tag$_j$ = <Data$_j$, CID$_j$, CL$_j$, AL$_j$, Capacity$_j$, ResponseSize$_j$, FreeSlotCount$_j$>
    AccessAllocation$_j$ = <Backup$_j$, Read$_j$, Write$_j$, Update$_j$,
    Migrate$_j$>
    Data$_j$ = Data$_j$ + Tag$_j$ + AccessAllocation$_j$;
    FreeSlot$_j$ = freeSlotIdentification ();
    If (FreeSlot$_j$ = 'Yes') then
        BackupDataToStorage (Data$_j$);
    Else
        ReplacementSelection$_j$ = selectReplacementMethod ();
        Backup the data to the new location;
    End If; End If
Else If (Location = 'Remote') then
    Tag$_j$ = < Data$_j$, CIDj, CLj, ALj, Capacityj, ResponseSizej, FreeSlotCountj, Locationj>
    AccessAllocation$_j$ = <Backup$_j$, Read$_j$, Write$_j$, Update$_j$,
    Migrate$_j$>
    Data$_j$ = Data$_j$ + Tag$_j$ + AccessAllocation$_j$;
    Region$_j$ = regionSelection ();
    If (Region$_j$ = 'Same') then
        Backup to the new location in the current region;
        Use suitable replacement algorithms, if necessary;
    Else If (Region$_j$ = 'Different') then
        Free slots or Storage Verification;
        Backup the data to the new location in the particular region;
    End If; End If
Access$_j$ = <ProviderName$_j$, Purpose$_j$, AccessLevel$_j$, ToleranceLevel$_j$>
Access Allocation = get Access Allocation (Access Level$_j$, ToleranceLevel$_j$);
If (Access$_j$ = AccessAllocation$_{j)}$ then
    Access the data for specific purpose;
Else
    Alert = generateAlert ();
    Send the alert to the customer location for access violations;
End If
Return BackupStatus
```

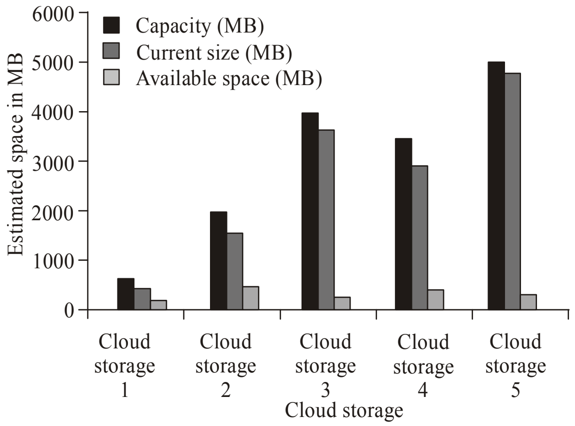


Fig. 10: Backup availability estimation

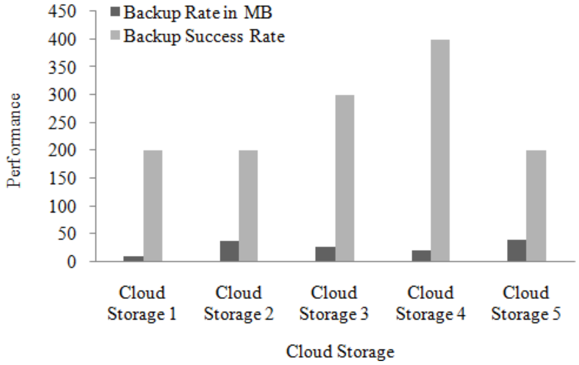


Fig. 11: Backup success rate estimation

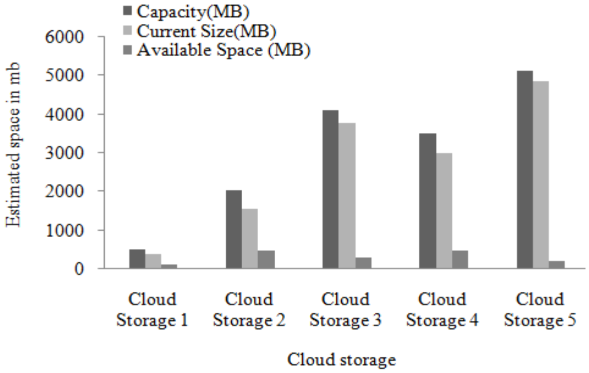


Fig. 12: Recovery availability estimation

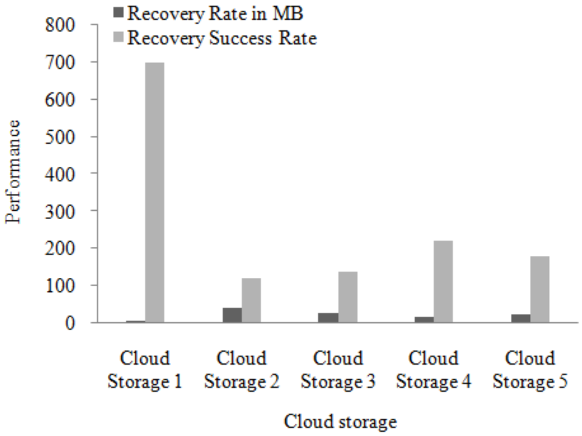


Fig. 13: Recovery success rate estimation

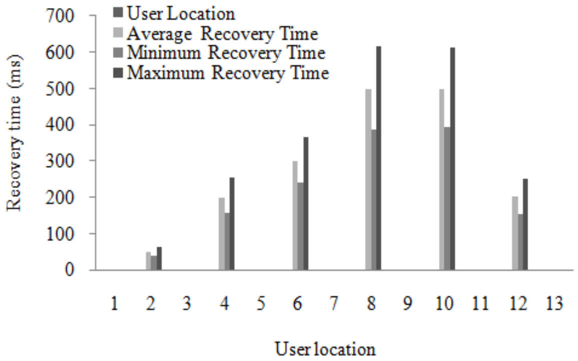


Fig. 14: User location vs. recovery time

SIMULATION RESULTS AND DISCUSSION

The CDM BackupSim simulator has been implemented using JSP as a front end, MySQL as a back end and server as a Tomcat 7.0 webserver. The data samples used in the simulator is ALL and AML data of the blood cancer. The main objective of this simulator is to achieve maximum reliability over customer data and protect the privacy information from unauthorized disclosure in all boundaries of the cloud access. It also provides awareness to the customer in order to know the level of security and the current location by using an alert mechanism. The backup availability estimation is calculated over cloud storage with storage space which is shown in Fig. 10.

The performance of the cloud backup is analyzed based on various cloud storage parameters such as backup rate and backup success rate shown in Fig. 11.

The recovery availability estimation is calculated with vaious performance parameters such as recovery Rate and cloud storage shown in Fig. 12.

The performance of the cloud recovery is analyzed based on various cloud storage parameters such as recovery rate and recovery success rate shown in Fig. 13.

The user recovery time with user location is analyzed based on the recovery time with various types shown in Fig. 14.

CONCLUSION AND RECOMMENDATIONS

The cloud computing plays an important role in IT field for providing the services which are needed by the cloud consumers. There are large number of service models and deployment models available to satisfy the demand request of the CSU. The customer's data are stored in the data centre which is located in the geographical location. The customer always has a problem in identifying the location of his data which is only known by the CSP. The location aware cloud computing is needed for an effective usage of data by the customer. The privacy over the cloud is an important factor which protects the information from unauthorized disclosure i.e., it keeps the information within the boundary. The existing security standards and privacy policies are restricted to a single CSP only. The proposed technique is used to impose a multilevel privacy over the cloud information in order to achieve a highest level of protection from unauthorized access. The levels are classified into cloud user level, cloud business level, cloud processing level, cloud storage level. These levels share some information outside the boundary for accessing the cloud service where as sensitive data are kept within their boundary. The proposed framework uses alert mechanism to provide an alert message to the cloud customer for every access of his data by the CSP or third parties. The privacy policies are imposed in various levels to keep track of information within the boundary i.e., whenever the violation occurs; the CSU gets the alert message. The overall objective of the proposed framework is to assess the privacy level over the cloud and also to develop a CDMBackupSim for implementing and testing the performance of the cloud storage. In future the privacy policies will be implemented over mobile cloud i.e. the mobile user can know his data location with maximum privacy level. This study can be extended with various replacement techniques over the cloud backup in the cloud storage.

REFERENCES

Acronis, 2014. Retrieved form: http:// www.acronis. com/homecomputing/trueimage/?utm_source = 6549527&utm_medium = affiliates&utm_cam paign = cj # add-cloud-storage #cloud-storage.

Bertino, E., F. Paci, R. Ferrini and N. Shang, 2009. Privacy-preserving digital identity management for cloud computing. Bull. IEEE Comput. Soc. Tech. Comm. Data Eng., pp: 1-7.

Bitcasa, 2014. Retrieved form: http://info.bitcasa.com /BCo re1.html?utm_source = cj&utm_medium = affiliate, 2014.

Brian, O., T. Brunschwiler, H. Dill, H. Christ and B. Falsafi *et al*., year. White Paper Cloud Computing. White Paper SATW, pp: 1-51.

Brodkin, J., 2008. Gartner: Seven cloud-computing security risks. Cloud computing is picking up traction with businesses, but before you jump into the cloud, you should know the unique security risks it entails. July 02, pp: 1-2.

Carbonite, 2014. Retrieved form: http://www. carbonite. com/lp/aff/cj-buy1.aspx?cm_mmc = affiliate-_-CJ-_-Non-Discount+Areyou +at+risk $%$3F-_-6549527&c3 ch = Affiliate &c3nid = 65495 27, 2014.

Cloud Performance, 2014. Retrieved form: http:// www. ektron. com/Blogs/Udaiappa-Ramachandran/ Which-Cloud-Compa ring Microsoft-Azure-and-Amazon-Web-Services/ (Accessed on: 13.4.14, 2014).

CrashPlan, 2014. Stepped-Up Security. Retrieved form: http:// www. code42.com/crashplan/, 2014.

Fisher, T., 2014. A Full Review of Backblaze, an Online Backup Service. Retrieved form: http://pcsupport. about.com/od/backup/fl/backblaze -review.htm.

Grobauer, B., T. Walloschek and E. Stöcker, 2011. Understanding cloud computing vulnerabilities. IEEE Secur. Priv., 9(2): 50-57.

Hewitt, C., 2008. ORGs for scalable, robust, privacy-friendly client cloud computing. IEEE Internet Comput., 12(5): 96-99.

Jaeger, P.T., J. Lin and J.M. Grimes, 2010. Cloud computing and information policy computing in a policy cloud? J. Inform. Technol. Pol., 5(3): 269-283.

Jansen, W. and T. Grance, 2011. Guidelines on Security and Privacy in Public Cloud Computing. NIST Special Publication 800-144, pp: 1-80.

Kanndukuri, B.R., R Paturi and A. Rakshit, 2009. Cloud security issues, advanced software technologies, IIIT, Pune, India. Proceeding of IEEE International Conference on Services Computing, pp: 527-520.

Katzan, H., 2010. On the privacy of cloud computing. Int. J. Manage. Inform. Syst., 14(2): 1-12.

Krautheim, F.J., 2009. Private virtual infrastructure for cloud computing. Proceedings of the 2009 Conference on Hot Topics in Cloud Computing, HotCloud'09, pp: 1-5.

Leavitt, N., 2009. Is cloud computing really ready for prime time? Computer, 42(1): 15-20.

Livedrive, 2014. Retrieved form: http://www.live drive.com/?AID = 10709106&PID=6549527 & tid = af filiatecj, 2014.

Mell, P. and T. Grance, 2010. Effectively and Securely Using the Cloud Computing Paradigm. NIST, Information Technology Laboratory 10-7-2009 With Minor comments by Dr. Yesha Sivan, (As part of the Cloud Panel in Web 2010), pp: 1-93.

Mozy, 2014. Retrieved form: https://mozy.com/ product/mozy/personal # frame_Free?ref = 451c76 aa, 2014.

Online Backup Service Feature Comparison, 2014. Retrieved form: http://pcsupport.about.com/od/ backup/a/online-backup-comparison.htm.

Oujani, A., 2014. A Survey on Cloud Computing Simulations and Cloud Testing. Retrieved form: http://students.cec.wustl.edu/~azinoujani/ (Accessed on: 15th April, 2014).

Pallis, G., 2010. Cloud computing-the new frontier of internet computing. IEEE Internet Comput., 14(5): 70-73.

Ryan, M.D., 2011. Cloud computing privacy concerns on our doorstep. Communi. ACM, 54(1): 36-38.

SOS, 2014. Retrieved form: http://www.sosonline backup.com/?AID = 10923174 and PID = 6549527 and src = CJ_6549527, 2014.

SpiderOak, 2014. Retrieved form: Available: https:// spideroak .com/, 2014.

SugarSync, 2014. Retrieved form: https://www. sugarsync. com/offers/affiliate1/index.2.html? utm_medium = Affiliate and utm_source = Commission Junction and utm_campaign = CommissionJunction_ Affiliatebannerlink.

Wei, Y. and M.B. Blake, 2010. Service-oriented computing and cloud computing: Challenges and opportunities. IEEE Internet Comput., 14(6):72-75.