Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 92 (2016) 128 – 135

Procedia Computer Science

2nd International Conference on Intelligent Computing, Communication & Convergence

(ICCC-2016)

Srikanta Patnaik, Editor in Chief

Conference Organized by Interscience Institute of Management and Technology

Bhubaneswar, Odisha, India

A Study on Data Storage Security Issues in Cloud Computing

Naresh vurukonda[1], B.Thirumala Rao[2]

[1,2]Department of CSE, KLUniversity, Vijayawada, A.P, INDIA

[1] naresh.vurukonda@gamil.com, [2] drbtrao@kluniversity.in

Abstract

Cloud computing is a revolutionary mechanism that changing way to enterprise hardware and software design and procurements. Because of cloud simplicity everyone is moving data and application software to cloud data centers. The Cloud service provider (CSP) should ensure integrity, availability, privacy and confidentiality but CSP is not providing reliable data services to customer and to stored customer data. This study identifies the issues related to the cloud data storage such as data breaches, data theft, and unavailability of cloud data. Finally, we are providing possible solutions to respective issues in cloud.

Peer-review under responsibility of the Organizing Committee of ICCC 2016

Keywords: Cloud service provider (CSP), cloud data storage, security issues, policies & protocols;

1. Introduction

Cloud computing is a revolutionary mechanism that changing way to enterprise hardware and software design and procurements. The cloud computing provides rich benefits to the cloud clients such as costless services, elasticity of resources, easy access through internet, etc. From small to large enterprises poignant towards cloud computing to increase their business and tie-ups with other enterprises [1]. Even though cloud computing has enormous benefits, cloud user are unwilling to place their confidential or sensitive data, it includes personal health records, emails and government sensitive files. Suppose once data are placed in cloud datacenter; the cloud client lost their direct control over their data sources. The Cloud Service Provider(CSPs) has promise to ensures the data

Peer-review under responsibility of the Organizing Committee of ICCC 2016

doi:10.1016/j.procs.2016.07.335

security over stored data of cloud clients by using methods like firewalls and virtualization. These mechanisms would not provide the complete data protection because of its vulnerabilities' over the network and CSPs have full command on cloud applications, hardware and client's data. Encrypting sensitive data before hosting can deserve data privacy and confidentiality against CSP. A typical problem with encryption scheme is that it is impractical because of huge amount communication overheads over the cloud access patterns. Therefore, cloud needs secure methods to storage and management to preserve the data confidentiality and privacy [2][5]. This paper mainly focuses on security vulnerabilities and issues in confidentiality and privacy over client data.

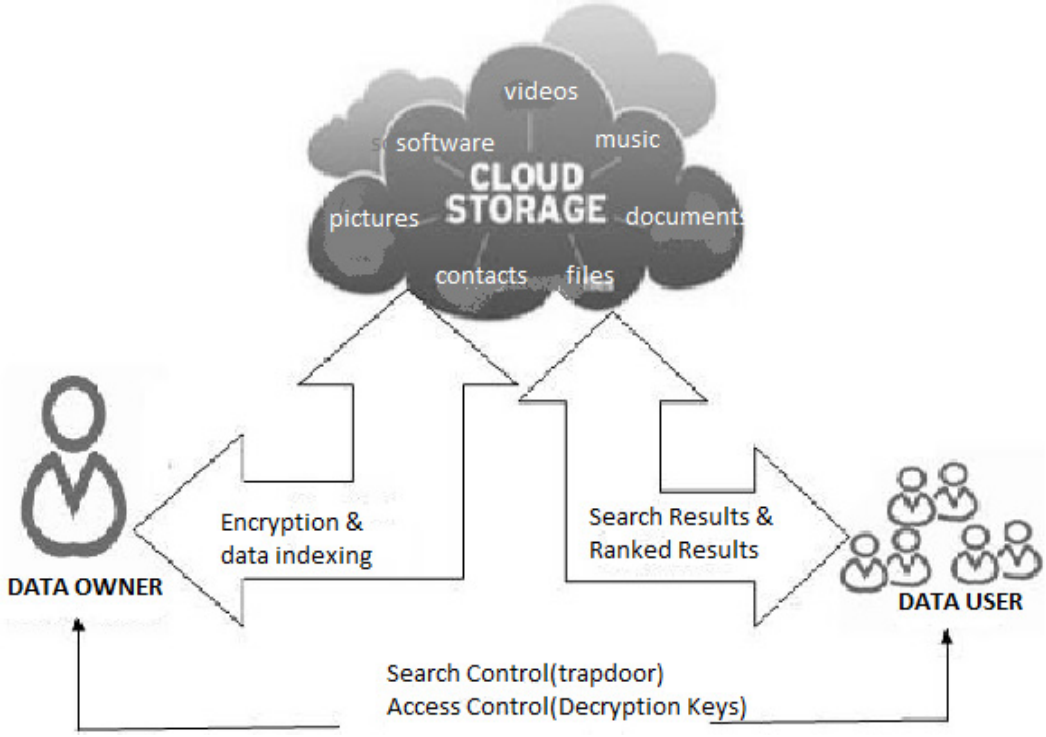

Figure 1: Cloud data storage model.

2. Cloud Data Storage Challenges & Issues

The cloud computing does not provide control over the stored data in cloud data centers. The cloud service providers have full of control over the data, they can perform any malicious tasks such as copy, destroying, modifying, etc. The cloud computing ensures certain level of control over the virtual machines. Due to this lack of control over the data leads in greater security issues than the generic cloud computing model as shown in figure 1. The only encryption doesn't give full control over the stored data but it gives somewhat better than plain data. The characteristics of cloud computing are virtualization and multi tenancy also has various possibilities of attacks than in the generic cloud model. The figure 2 has various issues those are discussed below in clearly.

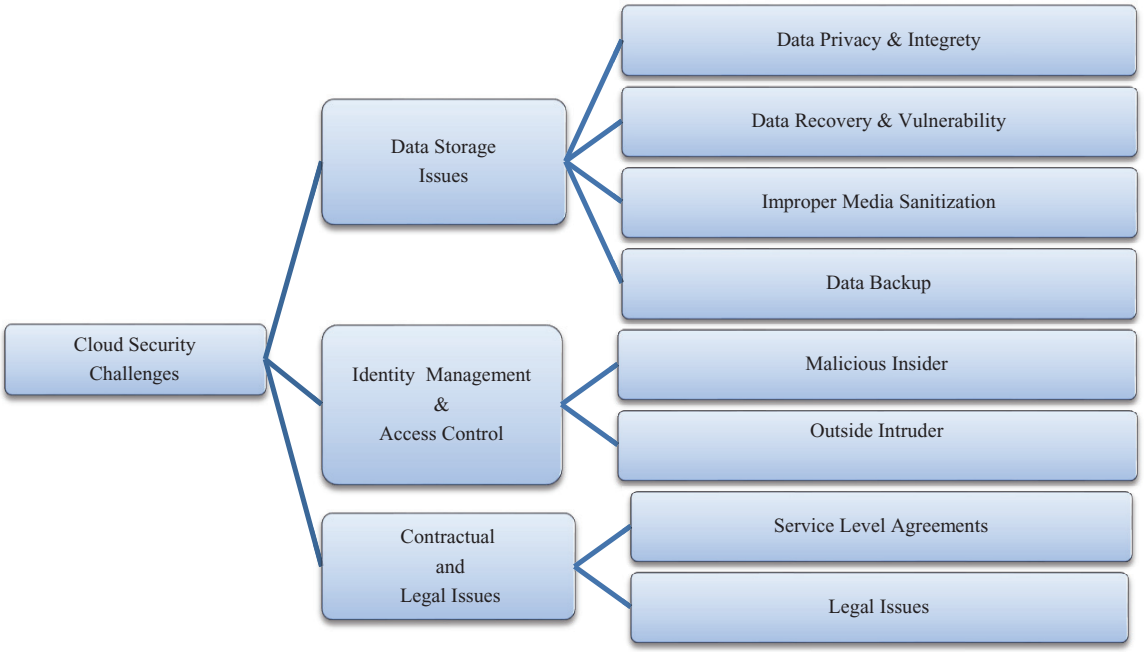

Figure 2. Cloud security Challenges

2.1 Cloud Storage issues

2.1.1 Data privacy and Integrity

Even though cloud computing provide less cost and less resource management, it has some security threats. As we discussed earlier cloud computing has to ensure integrity, confidentiality, privacy and availability of data in generic cloud computing model but the cloud computing model is more vulnerable to security threats in terms of above conditions. Because of simplicity cloud users are increasing exponentially and applications are hosted in cloud is very high. These situations lead to greater security threats to cloud clients. If any attack is successful on data entity will leads to data breach and takes an unauthorized access to data of all cloud users. Because of this integrity violation cloud data lost multi-tenant nature. Especially SaaS providers may also lost their technical data and they have great risk over data storage. Apart from these risks, data processing also has great risk while data being transformed among multiple tenants. Because of virtualization multiple physical resources are shared among the users. This leads to launch attacks by malicious insiders of the CSP and/or organization. These situations may allow the malicious user to perform attacks on stored data of other customer while processing their data. Other major risk is when data is outsourced to third party storage by the CSP [5]. The key generation and key management in cryptography for cloud computing is not standardized up to the mark. But without standard and secure key management for the cloud doesn't allow the standard cryptography algorithms to perform well in generic cloud computing model. Such that cryptography may also ensures the potential risks to cloud computing.

2.1.2 Data recoverability and vulnerability

Due to resource pooling and elasticity characteristics, the cloud ensures dynamic and on-demand Resource provisioning to the users. The resource allocated to a particular user may be assigned to the other user at some later point of time. In case of memory and storage resources, a malicious user can employ data recovery techniques to

obtain the data of previous users [13]. The authors in [13] were able to recover Amazon machine images files 98 % of the times. The data recovery vulnerability can pose major threats to the sensitive user data.

2.1.3 Improper media refinement.

The storage medias are sanitize because of following reasons (i) the disk may needs to replace with other disk (ii) No need to maintain the disk or no longer to maintain (iii) massacre of services. Improper refinement ensures great risk to stored data. In multi-tenant cloud it is not possible to refine as it is earlier tenant.

2.1.4 Data backup

The data backup is an important when accidental and/or intentional disasters. The CSP has to perform regular backups of stored to ensure the data availability. In fact, the backup data should be keeping with security guidelines to prevent malicious activities such as tampering and unauthorized access.

2.2. Identity Management and Access Control

The integrity and confidentiality of data and services are related with access control and identity management. It is important to maintain track record for user identity for avoiding unauthorized access to the stored data. The identity and access controls are complex in cloud computing because of that data owner and stored data are at different executive platforms. In cloud environment, different organizations use variety of authentication authorization agenda. By using different approaches for authentication and authorization gives a compound situation over a period of time. The cloud resources are dynamic and are elastic for cloud user and IP addresses are continuously changed when services are started or restarted in pay per usage model. That allows the cloud users to join and leave feature to cloud resources when they required i.e., on-demand access policy. All these features need efficient and effective access control and identity management. The cloud has to maintain quickly updating and managing identity management for joining and leaving users over cloud resources. There are many issues in access control and identity management, for example weak credentials may reset easily, denial of service attack to lock the account for a period of time, Weak logging and monitoring abilities, and XML wrapping attacks on web pages.

2.2.1 Malicious Insiders

An insider threat can be posed by employees, contractors and /or third party business partners of an organization. In cloud environment i.e., at Cloud Service Provider (CSP) side attacks leads to loss of user's information integrity, confidentiality, and security. This leads to information loss or breaches at both environments.. This attack is precious and it is well known to most of the organization [7].There is variety of attack patterns performed by insiders because of sophistication about internal structure of an organization data storage structure. Most organizations ignoring this attack because it is very hard to defend and impossible to find the complete solution for this attack. This attack ensures great risk in terms of data breaches and loss confidentiality at both organization and cloud level [8].

2.2.2 outside Intruder

Attacks that come from external origins are called outsider attacks [30]. Data security is one of the important issue in cloud computing. Since service providers does not have permission for access to the physical security system of data centers. But they must depend on the infrastructure provider to get full data security. In a virtual private cloud environment, the service provider can only specify the security setting remotely, and we don't know exactly those are fully implemented. In this Process, the infrastructure provider must reach the following objectives: (1) confidentiality, for secure data transfer and access, and (2) audit ability [31]. So that outside intruders can't access sensitive data which is stored in cloud.

2.3 Contractual and Legal issues

After moving to cloud computing environment, there are many issues in geographic jurisdictions, regulatory law, performance assurance, contract enforcements, etc. The above mentioned issues are comes under the legalities, Service Level Agreements and data location in data centers [9].

2.3.1. Service level agreements

The Service Level Agreement (SLA) can be described as a protocol, it specifies set of conditions and terms among user and Cloud service provider. The SLA should specify the following: Actions that CSP will taken when data breach happened, remedial actions and performance level at minimum level [5]. The users should have clear view on security for their resources and all other requirements should be agreed upon the SLA. The contract enforcement becoming issues because statistics provided by CSP are totally unproven. Finally, the contracts are non-negotiable and pre-defined that has to be in friendly manner between CSP and user. The regulatory laws such as Sarbanes- Oxley and HIPAA become an open issue [10].

2.3.2. Legal issues

The legal issues arise because that the presence CSP resources in geographically conflicting various legal jurisdictions [11]. If the user is migrated to one geographical to other, an issue will occur because of different legal jurisdictions. For a movement data is distributed over a various data centers, those are owned by CSP those have different laws and security guidelines. This scenario may takes into the serious issue in cloud computing.

3. Literature Solutions

In this section, we explained the research work solutions and at the same time it also given the comprehensive discussion. Results presented in tables that make the reader understand easily The discussion can be made in several sub-chapters.

3.1 Data storage issues solutions

The SecCloud is presented by Wei et al. [12], it provides a storage security protocol for cloud customer's data and it not only secures the stored data but also provides security on computational data. The SecCloud protocol uses encryption for storing data in secure mode. The multiplicative groups and cyclic additive pairing is used for key generation for cloud customers, CSP, and other business partners or trusted third party. The encrypted data along with the verifiable signature is sent to cloud data center along with session key. The Diffie-Hellman algorithm is used for generation of session key for both bilinear groups. By receiving encrypted data the cloud decrypts the data, verifies the digital signature and stores the original data in specified location in cloud. The SecCloud verifies whether data is stored at specified location or not. The Merkle hash tree is used for computation security in SecCloud protocol. The verifying agency will verify the computational results that are building by using Merkle hash tree. The File Assured Deletion (FADE) protocol provides a key management with data integrity and privacy in [15].

The key management along with the data integrity and privacy are assured by File Assured Deletion protocol (FADE) proposed in [18].Because of FADE simplicity; it is a light weight protocol and uses both asymmetric and symmetric key encryption of data. The Shamir scheme protects symmetric and asymmetric keys to generous the trust in the key management. A group of key managers are used by FADE protocol, those acts as a trusted third party. The key k is used as encryption key for file F of the client and another key used for encryption of data key ($k.$). The policy file maintains the details that which files are accessible. So that, to upload data the user requests the key pair from the third party by sending policy file p. The key manager sends public and private keys to the user by using the policy file. The upload file encrypts with randomly generated k and k is encrypted with symmetric key. That encrypted file is decrypted with the public key of generated key pair and MAC is also generated for integrity check. The reverse process will be taken by the receiver to get back original data.

Liu et al.[15] proposed a scheme that has a time based re-encryption with ABE algorithm to support secure data

sharing among the group with access control. This scheme ensures that forwarded data safely reached to the group users and it maintains the user revocation. In this scheme, the time period is associated with every user and by expiration the revocation automatically by Cloud Service Provider (CSP). This time based encryption scheme allows users to share keys in prior with CSP and CSP generate re-encryption keys by taking request from user. The ABE protocol ensures an access control by examining the set of attributes rather than identity. This scheme ensures the privacy and availability of data among the group peoples but doesn't concentrate on data integrity.

The probabilistic sampling is used to reduce the computational redundancy instead of rebuilding the whole tree again. The below list are key recommendations by the Computer Security Alliances (CSA) [18] for the data security and effective key management. The scope of key should be maintained by group or individual. The standard encryption algorithms should be used and weak algorithms should discard.

The best guidelines for key management and encryption software products should be used, it is better to use legitimate software technology to ensure security on storage. The customer or organizations and/or trusted third party should maintain effective key management. If the improper auditing protocol is designed, encryption process may control the data flow to external parties during the auditing. But encryption itself does not prevent data flow to external parties but instead it can reduce it some minimal level. But it requires great range of key management process and overheads for key generation while storing data. But exposure of encryption key leads to data leakage and it still a problem in cloud environment. This problem is addressed by combining the homomorphic authenticator along with the random masking process [19]. Illustrated in the following Table 1.

Table 1. The Possible Solutions of Data storage issues

Authors	**Proposed Scheme**	**Services**	**Privacy**	**Integrity**	**Availability**	**Confidentiality**
L. Wei, H. Zhu[12]	SecCloud,for Securing cloud data	Encryption Bilinear pairing Signature verification Trusted third party	✓	✓	×	✓
Y. Tang, P.P. Lee, J.C.S. Lui[15]	FADE, a protocol for data privacy and integrity	Encryption Trusted third party Assured deletion Threshold secret sharing	✓	✓	×	✓
Q.Liu,G.Wang[16]	TimePRE, a scheme for secure data sharing in cloud	Proxy re-encryption Attribute based encryption	✓	×	×	✓
Z. Tari[17]	A methodology for security of resident data	Erasure correcting Code Data redundancy	×	✓	✓	✓

3.2 Identity management and Access control solutions

The authors proposed Simple Privacy preserving Identity Management for Cloud Environments (SPICE) in [20] for identity management systems. The SPICE ensures group signature for providing the unidentified authentication, access control, accountability, unlink ability, and user centric authorization. The SPICE provides above mentioned properties with only a single registration. After user registration with trusted third party they obtain unique credentials for all the services provided by CSP. By using the credentials, user generates authentication certificate. Different CSPs expecting variety attributes for authentication and user has to generate their required form of authentication certificate with same credentials.

The Role Based Multi-Tenancy Access Control (RB_MTAC) been proposed in [21]. The RB_MTAC merges the role based access control scheme along with identity management. This requires user registration with CSP and obtains single credential that should be unique. The user has to choose the password while registration with CSP portal. By using these credentials the user can enter into the cloud environment by passing through identity module that uniquely identifies the user and after that it will be redirected to role assignment module that establish a connection to the RB_MTAC database and assigns the roles to registered user based on enrolled information.

Dhungana et al. [22] proposed a scheme for the cloud networking infrastructure as identity management framework and it is maintained by User managed Access (UMA) protocol. Here CSP acts as a host, while the authorized used acts as service owner. The authorization manager handles the service management and service requesting users also managed by authorization manager. This scheme ensures the identity management and access control across multiple Cloud providers with the help of authorization management. Illustrated in the following Table 2.

Table 2. The Solutions of Identity management and Access control

Authors	Proposed Scheme	Services	Access control	Authentication	Identity management
S.M.S. Chow, et al.[23]	SPICE, identity management framework	Anonymous and delegatable Authentication Access control Accountability	✓	✓	×
Z.Yan,P. Zhang[24]	Role based access control scheme	Access control	✓	✓	×
R.D.Dhungana, A.Mohammad[22]	Identity management framework	Identity management Authentication Access control	✓	×	✓
S. Ruj, M. Stojmenovic[25]	Decentralized access control for cloud storage	Attribute based encryption Attribute based signature	×	✓	✓
Z. Wan, J. Liu[26]	HASBE	Access control for cloud Re-encryption Privacy	✓	✓	×

3.3 Contractual and legal Issue solutions

In cloud computing environment, the users have great benefits because of simplicity and poses great risk in case of violation of service level agreements. The authors in [27] proposed a scheme that reacts on Service Level Agreements (SLA) violations in order to reduce the security risks in cancellation / violation environment. This scheme concentrates on algorithm that performs renegotiation of risk awareness. The algorithm uses the scheme of [28] to determine a minimum risk service among levels of service to fulfill the users need. The algorithm performs the scrutinizes and renegotiation of services at runtime environment for the replacement or cancellation of services. Finally it updates the risk factors according to the SLA.

Table 3. The Possible Solutions for Contractual and legal Issues

Authors	Proposed Scheme	Services	Negotiation	Enforcement	Monitoring
M.L. Hale, R. Gamble[28]	SecAgreement	Embedding security parameters into SLA ws-agreement	✓	×	×
M. Rak, N. Suri[29]	SPECS, SLA-based	Embedding security Matchmaking	✓	✓	✓

Rak et al. [29] proposed a SPECS method that ensures architecture to provide a services termed as SLA-based security as a service. The proposed architecture mainly focused three aspects namely negotiation, enforcement, and monitoring. The SPEC recommends the enforcement activating factors by monitoring and reporting or system startup.

4. Conclusion

The cloud computing architecture stores data and application software with minimal management effort and provides on demand services to customers through internet. But with cloud management customer don't have trust worthy commitments or policies. This will lead to many security issues with data storage such as privacy, confidentiality, integrity and availability. In this study we focused on data storage security issues in cloud computing and we first provided service models of cloud, deployment models and variety of security issues in data storage in

cloud environment. In the final section, we addressed possible solutions for the data storage issues that provide privacy and confidentiality in cloud environment.

References

[1] A. Abbas, K. Bilal, L. Zhang, S.U. Khan, A cloud based health insurance plan recommendation system: a user centered approach, Future Gener. Comput. Syst. (2014)
[2] P. Mell, T. Grance, The NIST definition of cloud computing (draft), NIST Special Publ. 800 (145) (2011) 7.
[3] J. Che, Y. Duan, T. Zhang, J. Fan, Study on the security models and strategies of cloud computing, Proc. Eng. 23 (2011) 586–593.
[4] R. Chandramouli, M. Iorga, S. Chokhani, Cryptographic key management issues and challenges in cloud services, in: Secure Cloud Computing, Springer, New York, 2014, pp. 1–30.
[5] C. Wang, Q. Wang, K. Ren, N. Cao, W. Lou, Toward secure and dependable storage services in cloud computing, IEEE Trans. Services Comput. 5 (2)(2012) 220–232.
[6] M. Balduzzi, J. Zaddach, D. Balzarotti, E. Kirda, S. Loureiro, A security analysis of amazon's elastic compute cloud service, in: Proceedings of the 27th Annual ACM Symposium on Applied Computing, 2012, pp. 1427–1434.
[7] Duncan, Adrian, Sadie Creese, and Michael Goldsmith. "Insider attacks in cloud computing." Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE, 2012.
[8] Khorshed, Md Tanzim, ABM Shawkat Ali, and Saleh A. Wasimi. "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing." Future Generation computer systems 28.6 (2012): 833-851.
[9] A. Andrieux, K. Czajkowski, A. Dan, K. Keahey, H. Ludwig, T. Nakata, J. Pruyne, J. Rofrano, S. Tuecke, M. Xu, Web services agreement specification.
[10] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, A. Ghalsasi, Cloud computing the business perspective, Decis. Support Syst. 51 (1) (2011) 176–189.
[11] B. Hay, K. Nance, M. Bishop, Storm clouds rising: security challenges for IaaS cloud computing, in: 44th Hawaii International Conference on System Sciences (HICSS), IEEE, 2011, pp. 1–7.
[12] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, A.V. Vasilakos, Security and privacy for storage and computation in cloud computing, Inform. Sci. 258 (2014) 371–386.
[13] O.D. Alowolodu, B.K. Alese, A.O. Adetunmbi, O.S. Adewale, O.S. Ogundele, Elliptic curve cryptography for securing cloud computing applications, Int. J.Comput. Appl. 66 (2013).
[14] M. Aslam, C. Gehrmann, M. Bjorkman, Security and trust preserving VM migrations in public clouds, in: IEEE 11th International Conference on Trust,Security and Privacy in Computing and Communications (TrustCom), 2012, pp. 869–876.
[15] Y. Tang, P.P. Lee, J.C.S. Lui, R. Perlman, Secure overlay cloud storage with access control and assured deletion, IEEE Trans. Dependable Secure Comput.9 (6) (2012) 903–916.
[16] Q. Liu, G. Wang, J. Wu, Time-based proxy re-encryption scheme for secure data sharing in a cloud environment, Inform. Sci. 258 (2014) 355–370.
[17] Z. Tari, Security and privacy in cloud computing, IEEE Cloud Comput. 1 (1) (2014) 54–57.
[18] Cloud security alliance, security guidelines for critical areas of focus in cloud computing v3.0, 2011.
[19] Y. Fu, Z. Lin, Exterior: using a dual-vm based external shell for guest-os introspection, configuration, and recovery, in: Proceedings of the 9th ACMSIGPLAN/SIGOPS International Conference on Virtual Execution Environments, 2013, pp. 97–110.
[20] S.M.S. Chow, Y. He, L.C.K. Hui, S.M. Yiu, Spicesimple privacy-preserving identity-management for cloud environment, in: Applied Cryptography and Network Security, Springer, Berlin, Heidelberg, 2012, pp. 526–543.
[21] S. Yang, P. Lai, J. Lin, Design role-based multi-tenancy access control scheme for cloud services, in: IEEE International Symposium on Biometrics and Security Technologies (ISBAST), 2013, pp. 273–279.
[22] R.D. Dhungana, A. Mohammad, A. Sharma, I. Schoen, Identity management framework for cloud networking infrastructure, in: IEEE International Conference on Innovations in Information Technology (IIT), 2013, pp. 13–17.
[23] Boneh, Dan, and Matthew Franklin. "Identity-based encryption from the Weil pairing." SIAM Journal on Computing 32.3 (2003): 586-615.
[24] Z. Yan, P. Zhang, A.V. Vasilakos, A survey on trust management for Internet of things, J. Netw. Comput. Appl. 42 (2014) 120–134.
[25] S. Ruj, M. Stojmenovic, A. Nayak, Decentralized access control with anonymous authentication of data stored in clouds, IEEE Trans. Parallel Distrib. Syst. 25 (2) (2014) 384–394
[26] Z. Wan, J. Liu, R.H. Deng, HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing, IEEE Trans. Inform. Forensics Sec. 7 (2) (2012) 743–754.
[27] M.L. Hale, R. Gamble, Risk propagation of security SLAs in the cloud, in: IEEE Globecom Workshops (GC Wkshps), 2012, pp. 730–735.
[28] M.L. Hale, R. Gamble, Secagreement: advancing security risk calculations in cloud services, in: IEEE Eighth World Congress on Services (SERVICES), 2012, pp. 133–140.
[29] M. Rak, N. Suri, J. Luna, D. Petcu, V. Casola, U. Villano, Security as a service using an SLA-based approach via SPECS, in: IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom), vol. 2, 2013, pp. 1–6.
[30] Patel, Ahmed, et al. "An intrusion detection and prevention system in cloud computing: A systematic review." *Journal of Network and Computer Applications* 36.1 (2013): 25-41.
[31] Reddy, V. Krishna, B. Thirumala Rao, and L. S. S. Reddy. "Research issues in cloud computing." *Global Journal of Computer Science and Technology* 11.11 (2011).

An Approach for Data Storage Security in Cloud Computing

Deepanchakaravarthi Purushothaman[1]and Dr.Sunitha Abburu[2]

[1] Master of Computer Application ,Adhiyamaan College of Engineering Hosur, Tamilnadu-635109, India.

[2] Professor and Director, Master of Computer Application,Adhiyamaan College of Engineering Hosur, Tamilnadu-635109, India.

Abstract

Cloud computing is now days emerging field because of its performance, high availability, low cost. In the cloud many services are provided to the client by cloud. Data store is main future that cloud service provides to the companies to store huge amount of storage capacity. But still many companies are not ready to implement cloud computing technology due to lack of proper security control policy and weakness in protection which lead to many challenge in cloud computing.. The main objectives of this paper are, 1) To prevent Data access from unauthorized access, it propose a distributed scheme to provide security of the data in cloud .This could be achieved by using homomorphism token with distributed verification of erasure-coded data. 2) Proposed scheme perfectly stores the data and identifies the any tamper at the cloud server.3) And also performs some of the tasks like data updating, deleting, appending. This paper also provides a process to avoid Collusion attacks of server modification by unauthorized users. The proposed techniques is been implementation and results are shown at the below.

Keyword: *cloud computing, Authentication, homomorphism token, Collusion attacks.*

1. Introduction

Cloud computing is the most demanding and emerging technology throughout the world. Cloud computing is an Internet based computer technology. Some of the major firms like Amazon, Microsoft and google have implemented the "CLOUD" and have been using it to speed up their business. Cloud computing has given a new dimension to the complete outsourcing arena (SaaS, PaaS and IaaS) and they provide ever cheaper powerful processor with these computing architecture The major thing that a computer does is to store in the available space and retrieve information whenever requested by the authenticated user. The pioneer of Cloud Computing vendor,(example) Amazon S3 is storage for the Internet. Amazon S3 provides a simple web services interface that can be used to store and retrieve any amount of data, at any time, from anywhere on the web. It also allows developer to access the highly scalable, reliable, secure, fast, inexpensive infrastructure that Amazon uses to run its own global network of web sites. From the viewpoint of data security, which has always been an important aspect of quality of service, Cloud Computing unavoidably poses new challenging security threats for number of reasons.

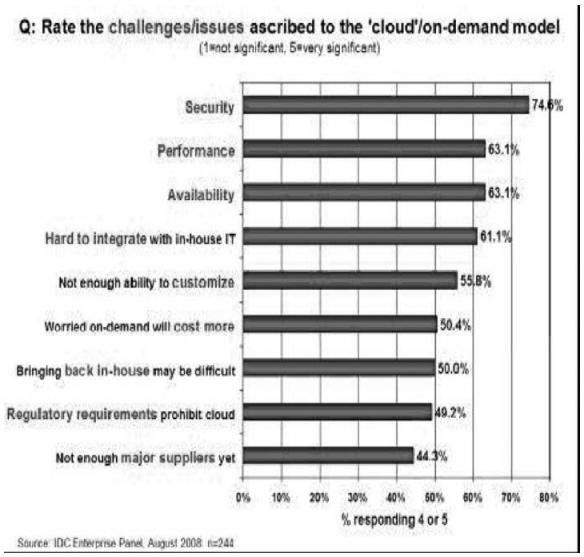

Fig.1. Results of IDC survey ranking security challenge[1]

- Unauthenticated person don't attack the authorized file
- Avoids Collusion attacks
- Malicious data modification attack

- Dynamic data operations
- Identification tamper server

2. Related Work

The Internet began to grow quickly in the 1990s and the increasingly sophisticated network infrastructure and increased bandwidth developed in recent years has dramatically enhanced the stability of various application services available to users through the Internet, thus marking the beginning of cloud computing network services. Many organizations tried to enhance for their security constraints, for their secure database, for their web application but they have not achieved a high-level security for their organizations. Data integrity quality of correctness, completeness, wholeness, soundness and compliance with the intention of the creator of the data. It is achieved by preventing accidental or deliberate but unauthorized insertion, modification or destruction of data in a database. Ensuring the integrity of the data really means that it changes only in response to authorized transactions.(see Fig.1) given stats confirm that the "Security" is the main Challenge in Cloud Computing For example IDC recently conducted a survey of 244 IT executives/CIOs and their line-of-business (LOB) colleagues to gauge their opinions and understand their companies' use of IT cloud services. Security ranked first as the greatest challenge or issue of cloud computing.

Shacham et al. [2] In a Compact proof-of-retrievability system, a data storage center must prove to a verifier that he is actually storing all of a client's data safely. The central challenge is to build systems that are both efficient and provably secure that is, it should be possible to extract the client's data from any prover that passes a verification.Juels and Kaliski [3] proposed a scheme called "provable data possession" (PDP) model for ensuring possession of file on untrusted storages. Their scheme utilized public key based homomorphic tags for auditing the data file, thus providing public verifiability. However, this scheme requires sufficient computation overhead that can be expensive for an entire file. Check.M.A Shah, M.Baker, J.C.Mogul;[4]proposed a scheme called "Auditing to Keep online Storage Services Honest" The need for auditing to support an online service-oriented economy. They highlight issues around both internal and external auditing. This paper [2][4][9],allows TPA to audit the cloud data storage without demanding user's time feasibity (or) resources. The proposed method provides public key verification for secured storage and investigate the problem of fine-grained data error Localization in the cloud.

3. Problem Statement

From the perspective of data security, which has always been an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for number of reasons.

- Data stored on cloud servers is not completely secure from infection**.** While popular cloud services such as Google Docs are equipped with virus scanning software, there is still the possibility of an internal or external attack affecting your data.
- The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, reordering, etc. To ensure storage correctness under dynamic data update, distributed protocol is used.

A descriptive architecture for secure data storage is illustrated in(see Fig .2) Data storage in a cloud is a process where the owner stores his data, files and applications through a Cloud Storage Provider (CSP) into a set of cloud servers. At the time of file storage, security key is used to secure the file from unauthorized access and then safely stored in the cloud. User who likes to access the file from cloud needs the security key to retrieve the file. User sends a key request to the owner and retrieves the file from the cloud after security key sent by the owner. File can't be accessed by any Unauthorized person or person who entering unmatching security key. For additional security, blocking IP address of the system those who illegally trying to access the file.

.

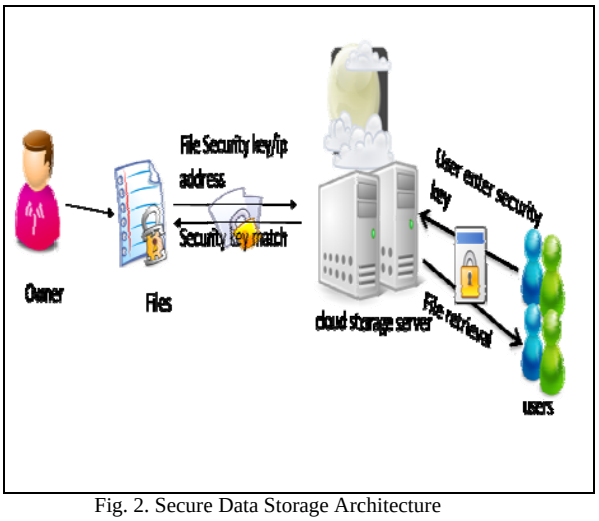

Fig. 2. Secure Data Storage Architecture

Data storage in a cloud is a process where the owner stores his data

This paper proposes using homomorphic token & verification of erasure-coded the current research provides cloud data security along with minimizes the redundancy.

- The distributed protocol in our work future provides the localization of data error. Which only provides binary results about the storage state across the distributed service in predecessors.
- Operations like Update, delete and integrity are also provided in the proposal methods.
- Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server Collusion attacks.

4. Secure Data Storage in Cloud

In cloud storage system, companies stores their data in the remotely located data server. Accordingly, correctness of the data is assured. Even though sometimes unauthorized person may modify or delete the data which leads to server compromise and/or random Byzantine failures. Because it can be the first step for fast recovery of the storage errors. The cloud storage systems propose an effective and flexible distributed scheme with explicit dynamic data support for file distribution across cloud servers. By computing homomorphic token using universal hash function [7] which can be perfectly integrated with the verification of erasure-coded data. As well as it identifies misbehaving servers. Finally, the procedure for file retrieval and error recovery based on erasure-correcting code is outlined.

4.1Token correctness

It achieves assurance for data storage correctness and data error localization, using pre-computed token. Before sharing file distribution using pre-computes a certain number of shortest verification token are generated that will ensure security for a block of data in a file in cloud storage. When the user wants to make sure the storage correctness for the data in the cloud, he challenges the cloud servers with a set of randomly generated block indices. After getting assurance of the user it again asks for authentication by which the user is confirmed to be the authenticated user. Upon receiving assurance, each cloud server computes a short “signature” over the specified blocks and returns them to the user. The values of these signatures should match the corresponding tokens pre-computed by the user. All servers operate over the same subset of the indices, the requested response values for integrity check must also be a valid codeword determined by a secret matrix. Suppose the user wants to challenge the cloud server’s t times to make sure the correctness of data storage. Then, he must pre-compute t verification tokens for each function, a challenge key and a master key are used. To generate the ith token for server j, the user acts as follows the details of token Generations are shown in Algorithm 1.

- Derive an arbitrary value i and a permutation key based on master permutation key.
- Calculate the set of randomly-chosen index.
- Calculate the token using encoded file and the arbitrary value derived.

Algorithm 1 Token Pre-computation

Block of data is represented as l;

No. of .blocks is denoted as n;

Let f be the function and t be the token ;

Index per proof is denoted as r;

Generate M_k and C_k;

For point G (j); j->1, n execute

/*j server position*/

For round i->1, t execute

/*i block index*/

Derive i = f (i) and k (i) from master key.Compute v(j)

End for

End for

Store all the vis locally.

End procedures

4.2. Correctness Verification and Error Localization

Error localization is a key requirement for eradicate errors in storage systems. However, many previous schemes do not explicitly consider the problem of data error localization.

The challenges response protocol in our work future provides the localization of data error. Which only provides binary results about the storage state across the distributed service in predecessors. The response values from servers for each challenge not only determine the correctness of the distributed storage, but also contain information to locate potential data error(s).
Specifically, the procedure of the ith challenge-response for a cross-check over the n servers is described as follows:

- The client reveals the i as well as the ith key k (i) to each servers
- The server storing vector G aggregates those r rows
- Specified by index k(i) into a linear combination R
- Upon receiving R is from all the servers, the user takes away values in R.
- Then the user verifies whether the received values remain a valid codeword determined by secret matrix.

Because all the servers operate over the same subset of indices, the linear aggregation of these r specified rows (R (1)i , . . . ,R(n)i) has to be a codeword in the encoded file matrix. If the above equation holds, the challenge is passed. Otherwise, it indicates that among those specified rows, there exist file block corruptions. Once the inconsistency among the storage has been successfully detected, we can rely on the pre-computed verification tokens to further determine where the potential data error(s) lies in. Note that each response R(j) i is computed exactly in the same way as token v(j) i , thus the user can simply find which server is misbehaving by verifying.

5. Implementation

5.1 Secure Software Development Life Cycle

The Security Development Lifecycle (SDL) is a software development security assurance process consisting of security practices grouped by seven phases Investigation, Analysis, Logical design, Physical design, Implementation, Maintenance.

Phase1.Investigation**:**Define project processes and goals, and document them in the program security policy.
Phase2.Analysis: Analyze existing security policies and programs, analyze current threats and controls, examine legal issues, and perform risk analysis.

Phase3.Logical design: Develop a security blueprint, plan incident response actions, plan business responses to disaster, and determine the feasibility of continuing and/or outsourcing the project.

Phase4.Physical design: Select technologies to support the security blueprint, develop a definition of a successful solution, design physical security measures to support technological solutions, and review and approve plans.

Phase5.Implementation: Buy or develop security solutions. At the end of this phase, present a tested package to management for approval.

Phase6.Maintenance: Constantly monitor, test, modify, update, and repair to respond to changing threats.

5.2 Main Modules

5.2.1 Client Module

The client sends the query to the server. Based on the query the server sends the corresponding file to the client. Before this process, the client authorization step is involved. In the server side, it checks the client name and its password for security process. If it is satisfied and then received the queries form the client and search the corresponding files in the database. Finally, find that file and send to the client. If the server finds the intruder means, it set the alternative Path to that intruder. Using screen shown in fig.3.

5.2.2 System Module

- User

Users, who have data to be stored in the cloud and rely on the cloud for data computation, consist of both individual consumers and organizations.

- Cloud Service Provider (CSP)

A CSP, who has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems.

- Third Party Auditor (TPA)

An optional TPA, who has expertise and capabilities that users may not have, is Trusted to assess and expose risk of cloud storage services on behalf of the users upon request.

5.2.3 Cloud Data Storage Module

Cloud data storage, a user stores his data through a CSP into a set of cloud servers, which are running in a simultaneous, the user interacts with the cloud servers via CSP to access or retrieve his data. In some cases, the user may need to perform block level operations on his data.users should be equipped with security means so that they can make continuous correctness assurance of their stored data even without the existence of local copies. In case that users do not necessarily have the time, feasibility or resources to monitor their data, they can delegate the tasks to an optional trusted TPA of their respective choices. In our model, we assume that the point-to-point communication channels between each cloud server and the user is authenticated and reliable, which can be achieved in practice with little overhead. Using screen shown in Fig.4.

5.2.4 Cloud Authentication Server

The Authentication Server (AS) functions as any AS would with a few additional behaviors added to the typical client-authentication protocol. The first addition is the sending of the client authentication information to the masquerading router. The AS in this model also functions as a ticketing authority, controlling permissions on the application network. The other optional function that should be supported by the AS is the updating of client lists, causing a reduction in authentication time or even the removal of the client as a valid client depending upon the request. Using screen shown in Fig.5.

5.2.5 Misbehaving server model

When the user enters into cloud server and the user will start to access the file, but at the same time an unauthorized user enters into the cloud server without the proper authentication to the cloud server the particular IP address will be noticed and it makes some attention to the cloud owner. Using screen shown in fig.6.

6. Conclusion

This paper briefly explained the problems of data security in cloud data storage. And also provided a way out to ensure user correctness. We propose a

7. Result

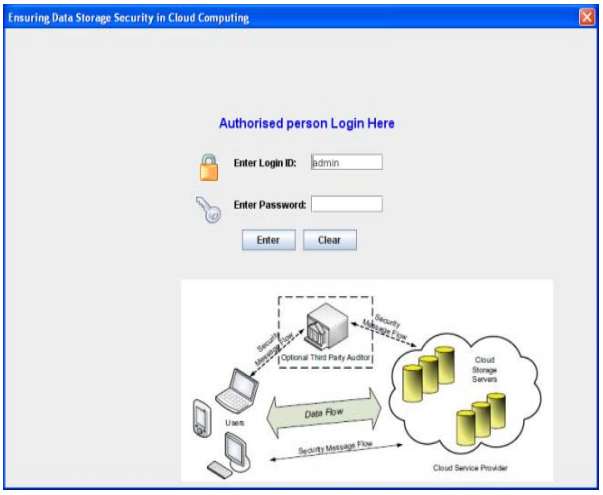

Fig-3: Authorized Person Login

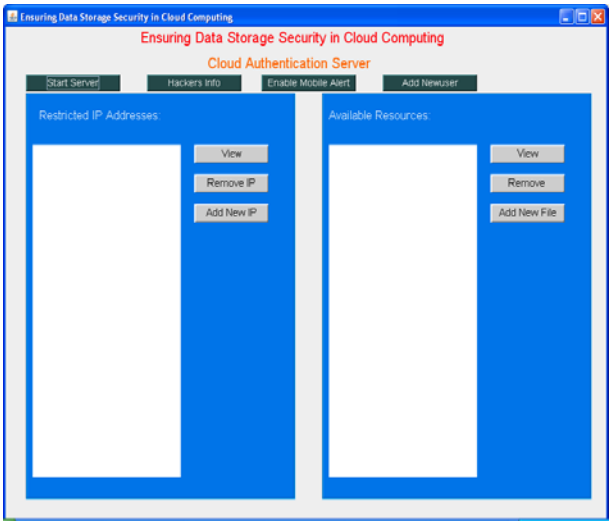

Fig-4: Cloud Data Storage

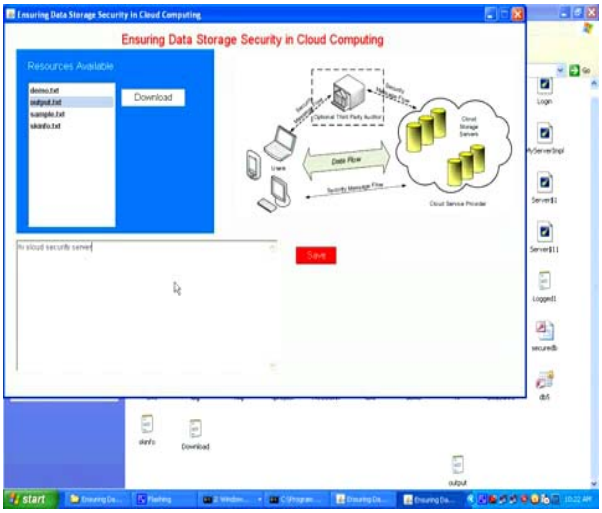

Fig-5: User Side Login

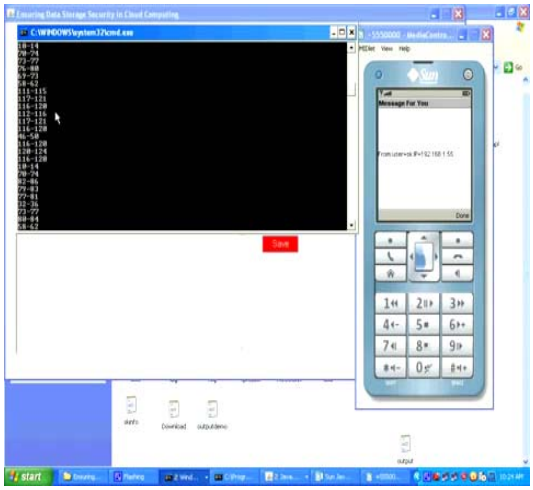

Fig-6: Misbehaving Server Model

distributed scheme through homomorphism token with distributed verification of erasure-coded data. Additionally, the technique provides a process to avoid colluding attacks of server modification by unauthorized users. We believe that data storage security in Cloud Computing, an area of challenges and of dominant significance, is still in its infancy to be identified. We envision several possible directions for future research on this area. It allows Third Parity Auditor to audit the cloud data storage without demanding users' time, probability.

References

[1] John W. Rittinghouse, James F. Ransome, "Cloud Computing Implementation, Management, Security", CRC Press 2009 by Taylor and Francis Group, LLC.

[2] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc.of Asiacrypt '08, Dec. 2008.

[3] G.Ateniese. R. D. Pietro ,L.V.Mancini and G. Tsudik, "Scalable and Efficient Provable Data Possession,"Proc of Securecomm'08.

[4] M.A Shah, M.Baker, J.C.Mogul, "Auditing to Keep Online storage services Honest,"Proc 11th USENIX Workshop on Hot Topics in Operating Systems(HOTOS'07). pp. 1–6, 2007.

[5] T.S.J.Schwarz and E.L.Millerds, "Store, Forget, and check: Using Algebraic Signatures to Check Remotely administered Storage,"proc.of ICDCS'06, pp. 12–12, 2006.

[6] Case study: http://eyeos.org/ cloud desktop

[7] L. Carter and M. Wegman, "Universal Hash Functions," *Journal of Computer and System Sciences*,

[8] http://searchcloudcomputing.techtarget.com/resources#parentTopic4

[9] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L.Kissner, Z. Peterson,and D. Song, "Provable Data Possession at Untrusted Stores," Proc. Of CCS '07, pp. 598–609, 2007.

[10] Cloud security Alliance"Top threats to Cloud *http://www.cloudSecurityalliance.org/topthreats/casthreats.v1.0.pdf*.

CONTEMPORARY RESEARCH IN INDIA
ISSN 2231 - 2137

RESEARCH PAPER ON CLOUD COMPUTING

Mrs. Ashwini Sheth[1], Mr. Sachin Bhosale[2], Mr. Harshad Kadam[3]

Asst. Prof.[1], Department of C.S., I.C.S. College, Khed, Ratnagiri

H.O.D.[2], Department of I.T., I.C.S. College, Khed, Ratnagiri

Student[3], M.Sc. I.T., I.C.S. College, Khed, Ratnagri

Abstract: *Cloud Computing has come of age later Amazons introduce the first of its kind of cloud services in2006. It is particularly suitable to Hong Kong because of the unbelievable amounts of the data that are being processed here daily in several sectors, and there are signs that subscription to cloud services by the local companies will soon be on a skyrocket course, despite a slow start in beginning years. As a research theme, cloud computing now easily tops any schedule of topics in a computer science because of its far-reaching suggestion in many sector in computing, especially a big data which without cloud computing is at the great concept. The current creation of a main cloud R&D centre in Hong Kong by Lenovo (January 2015) attests to this fact.*

Cloud computing, the life time dream of computing as a utility, has the capacity to convert a huge part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Developers with new invention ideas for new Internet services no longer require the huge capital outlays in hardware to deploy their service or the human expense to operate it. They need not be worried about overprovisioning for a service whose popularity does not meet their predictions, thus wasting costly resources, or under provisioning for one that becomes wildly popular, thus missing potential customers and revenue. In addition to, companies with huge batch-oriented tasks can get results as fastest as their programs can scale, since using 1,000 servers for one hour costs no more than using one server for 1,000 hours. Without paying a premium for large scale, is unprecedented in the history of IT, by this elasticity of resources.

Introduction

Joseph Carl Robnett Licklider in the 1960s developed Cloud Computing with his work on ARPSNET to interact with people and data from in any place at any time. In 1983, CompuServe presented its users as a little amount of disk space that could be used to accumulate any files they choose to upload.

Simply put, Cloud working out is the distribution of Computing services-including servers, database, networking, storage, software, analytics and intelligence-over the Internet ("the Cloud") to offer faster revolution, flexible resources, and economies of scale. Cloud working out is the delivery of computing services such as servers, storage, database, networking, software, analytics, intelligence, and more, over the Cloud (Internet). Cloud Computing gives a different to the on-premises datacentre.
Mobility.

One of the other largest outward uses of cloud calculating is the mobility that it brings, Both to the pleasurable user, as well as to the commercial and business user. Many of us are already conversant with some Cloud Computing services, like Google Docs, or even email services. The utmost popular Cloud Computing products include AWS Elastic Compute, Google Cloud Engine and AWS Lambda.

The most famous cloud computing services are including Amazon Web Services, Google Cloud platform and Microsoft Azure. Cloud Computing is flexible. Cloud-based services are model for businesses with increasing or changeable bandwidth demands. If your requirements increase, it's easy to ruler up your cloud capacity, drawing on the service's remote servers.

Accessibility; Cloud computing smooth's the entrance of implementation and data from any location worldwide and from any device with an internet connection. Cost savings; Cloud computing

proposals businesses with accessible computing resources hence saving them on the cost of obtaining and maintaining them. Examples of Cloud Computing Dropbox, Facebook, Gmail. Cloud can be used for storage of files. Banking, Financial Services.

Consumers accumulation financial information to cloud computing serviced providers. Health care. Education. Government. Big data Analytics. Communication. Business Process. Variety of Cloud Computing There are three important types of cloud environment, also known as cloud distribution models. Businesses can select to run applications on communal, personal or mixture clouds — depending on their definite requirements.

Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centres that gives those services. The services themselves have huge been referred to as Software as a Service (SaaS).a Some vendors use terms such as IaaS (Infrastructure as a Service) and PaaS (Platform as a Service) to reate their products, but we eschew these because accepted definitions for them still vary broadly. The line between "low-level" infrastructure and a higher-level "platform" is not crisp. We believe the two are more alike than different, and we examine them together. Likewise it is, the related term "grid computing," from the high-performance computing community, suggests protocols to offer shared computation and storage over long distances, but those protocols did not lead to a software environment that grew beyond its community.

We see three specifically compelling use cases that favour utility computing over conventional hosting. A opening case is when demand for a service varies with time. For example, provisioning a data centre for the peak load it must sustain a few days per month leads to underutilization at other times. rather, cloud computing lets an company pay by the hour for computing resources, potentially leading to cost savings even if the hourly rate to rent a machine from a cloud giver is larger than the rate to own one. A second case is when demand is unknown in advance. For example, a Web start up will need to support a spike in demand when it becomes famous, followed potentially by a reduction once some visitors turn away. Finally, company that perform batch analytics can use the "cost associativity" of cloud computing to finished computations faster: using 1,000 EC2 machines for one hour costs the same as using one machine for 1,000 hours.

While the economic appeal of cloud computing is often related as "converting capital expenses to operating expenses" (CapEx to OpEx), we believe the phrase "pay as you go" more directly captures the economic benefit to the buyer. Hours purchased via cloud computing can be distributed non-uniformly in time (for example, use 100 server-hours today and no server-hours tomorrow, and still pay only for 100); in the networking community, this way of selling bandwidth is since known as usage-based pricing's In extension, the absenteeism of up-front capital expense allows capital to be redirected to core business investment.

Therefore, even if Amazon's pay-as-you-go pricing was more expensive than buying and depreciating a comparable server over the same period, we argue that the cost is outweighed by the extremely main cloud computing economic advantage of elasticity and transference of risk, especially the risks of overprovisioning (underutilization) and under provisioning (saturation).

We start with elasticity. The key examination is that cloud computing's ability to add or remove resources at a fine grain (one server at a time with EC2) and with a lead time of minutes rather than weeks allows matching resources to workload much more closely. Real world estimates of average server used in data centres range from 5% to 20%.15,17 This may sound shockingly low, but it is consistent with the observation that for many services the peak workload beat the average by factors of 2 to 10. Since few users intentionally provision for less than

the expected peak, resources are idle at nonpeak times. The large pronounced the variation, the large the waste.

For a simplified example, assume that users of a hypothetical site fall into two classes: active users (those who use the site regularly) and defectors (those who abandon the site or are turned away from the site due to poor performance). Additionally, suppose that 10% of active users who receive poor service due to under provisioning are "permanently lost" opportunities (become defectors), that is, users who would have remained regular visitors with a better experience. The site is initially provisioned to handle an expected peak of 400,000 users (1,000 users per server × 400 servers), but unexpected positive press drives 500,000 users in the first hour. Of the 100,000 who are turned away or receive inferior service, by our assumption 10,000 of them are everlasting lost, leaving an active user base of 390,000. The next hour sees 250,000 new distinctive users.

From a hardware provisioning and pricing point of view, three aspects are new in cloud computing which are as follows:

- The arrival of unlimited computing resources available on demand, fatly enough to follow load surges, thereby eliminating the need for cloud computing users to plan far ahead for provisioning.
- The destruction of an up-front commitment by cloud users, thereby allowing companies to start little and rise hardware resources only when there is an rise in their needs'
- The ability to pay for use of computing resources on a short-term basis as needed (for example, processors by the hour and storage by the day) and release them as needed, thereby rewarding conservation by letting machines and storage go when they are no long time useful

For those deploying software out in the cloud, adaptability is a crucial issue—the need to marshal resources in such a way that a program continues running smoothly even as the number of users grows. It is not just that servers must respond to hundreds or thousands of requests per second; the system must also coordinate information coming from number of sources, not all of which are under the control of the same organization. The pattern of communication is many-to-many, with each server talking to number of clients and each client invoking programs on number of servers.

The another end of the cloud-computing transaction—the browser-based user interface—presents challenges of another kind. The intimate window-and-menu layer of modern operating systems has been fine-tuned over decades to meet user wants and belief. Duplicating this functionality inside a Web browser is a considerable feat. Besides, it has to be done in a similarly impoverished expansion of environment. A programmer creating a desktop application for Windows or one of the Unix variants can choose from a broad array of programming languages, code libraries, and application frameworks; major parts of the user interface can be gathered from pre-built components. The equivalent scaffolding for the Web computing platform is much extra primitive.

A major problem of moving applications to the cloud is the need to master number of languages and operating environments. In number of cloud applications a back-end process relies on a relational database, so part of the code is written in SQL or other query language. On the client side, program logic is likely to be execute in JavaScript embedded within HTML documents. Standing between the database and the client is a server application that might be written in a scripting language (such as PHP, Java, and Python). Information exchanged between the several layers is likely to be encoded in some variation of XML.

Al though the new model of remote computing seems to reverse the 1980s "liberation" movement that give individual users custody over programs and data, the shift does not necessarily restore control to managers in the corporate IT department.

To the expand that cloud computing succeeds, it constitute an obvious competitive challenge to vendors of shrink-wrap software. Ironically, the open-source motion could also have a tough time modifying to the new computing model. It's one thing to create and distribute an open-source word processor competing with Microsoft Word; not so obvious is how a consortium of volunteers would generate a Web service to compete with Google Docs.

Public Cloud

A public cloud environment is maintained by an outsourced cloud provider and is reachable to many businesses through the internet on a pay-per-use model. This distribution model provides services and organization to businesses who want to save money on IT operational costs, but it's the cloud provider who is responsible for the invention and safeguarding of the resources.

Public clouds are model aimed at minor with average magnitude businesses with a constricted budget requiring a quick and easy platform in which to deploy IT resources. Merits of a public cloud Easy scalability No geographical restrictions Cost effective Highly reliable Easy to manage Demerits of a public is Not examine the safest option for sensitive data

Private Cloud

This cloud distribution model is a modified infrastructure maintained by a single business. It offers a precise environment in which contact to IT resources is additionally centralized within the business. The present exemplary perhaps visibly introduced either obtainable handled internal. Even though secluded cloud introducing obtainable valuable, as largest productions it could be action a developed equal of safety and extra self-sufficiency to modify the storing, interacting and calculate mechanisms toward ensemble their IT necessities.

Merits of an isolated cloud

Better-quality level of safety Superior switch ended the slave Customizable benefit of an individual cloud firm to approach details out of isolated position Requires IT expertise Hybrid Cloud For businesses in search of the good of both secluded and communal cloud distribution copies, a mixture cloud atmosphere is a moral decision. By merging the two representations, a mixture cloud prototypical provides a more tailor-made IT solution that meets explicit business requirements.

Merits of a mixture cloud

Highly changeable and accessible Cost effective Enhanced security Scams of a mixture cloud Communication in network level may be disagreed as it's used in equally personally and publicly clouds.

Cloud Services

Following are three foremost service models of cloud computing —

Infrastructure as a Service (IaaS)

Platform as a Provision (PaaS)

Program as a Provision

There are pure changes among the three and what they can suggestion a occupational in rapports of storing and basis combining, then they can too cooperate through individually additional method of wide-ranging prototypical of cloud computing.

IaaS (Infrastructure as Service)

This is the most communal service method of cloud adding as it offers the fundamental infrastructure of virtual servers, network, operating systems and data storage drives. It consents for the flexibility, reliability and the scalability that many businesses pursue with the cloud, and remove the need for hardware in the office.

This makes it model for minor and average sized structuring observing for a charge virtual IT explanation to provision occupational development. IaaS is a entirely subcontracted recompense-for-custom facility and is obtainable as a communal, isolated or mixture organization.

This is where a cloud computing breadwinner array the infrastructure and the program substructure, but productions can grow and route their own appeal. Web use can be shaped rapidly and simply via PaaS, and the

service is supple and vigorous sufficient to provision them.

PaaS keys are ascendable and model for commercial surroundings where numerous designers are occupied on a only estimate It is also convenient for circumstances somewhere an current information basis (such as CRM tool) wants to be leveraged.

SaaS (Software as a Service)

This cloud calculating explanation includes the disposition of software over the internet to several productions who pay via contribution or a pay-per-use model. It is a valued tool for CRM and for requests that need a lot of web or mobile charge — such as a mobile sales organization software. SaaS is accomplished from a dominant position so trades don't have to concern about sustaining it themselves, and is model for short-term schemes.

Compensations of Cloud Computing

1) Back-up and bring back information Once the data is deposited in the cloud, it is calmer to get back-up and return that data using the cloud.
2) Improved collaboration Cloud applications expand association by allowing groups of people to rapidly and simply share information in the cloud via shared storage.
3) Outstanding convenience Cloud permits us to swiftly and simply access supply data anywhere, anytime in the entire world, with an internet assembly. An internet cloud substructure growths group output and competence by safeguarding that our information is constantly nearby.
4) Low preservation charge Cloud calculating reduce both hardware and software conservation costs for organizations.
5) Mobility Cloud adding allows us to simply entree all cloud information via mobile.
6) Unlimited storage capacity Cloud provide us a vast quantity of storage volume for storing our vital information such as pictures, pamphlets, auditory, audio-visual, etc. in one position
7) Data security Information safety is one of the main benefits of cloud computing.

Cloud suggestions several progressive structures connected to safety and confirms that information is firmly warehoused and felt.

Drawback of Cloud Calculating

1) Internet Connectivity In cloud computing, each facts (picture, audial, audio-visual, etc.) is stowed on the cloud, and we admittance these data concluded the cloud by means of the internet linking
2) Vendor lock-in Vendor lock-in is the main difficulty of cloud computing. Firm may face difficulties when relocating their facilities from one seller to a further As dissimilar vendors provide various stages, that can reason trouble affecting from one cloud to additional.
3) Imperfect Controller Cloud organization is entirely owned, accomplished, and checked by the provision source, so the cloud manipulators have fewer control concluded the purpose and implementation of facilities inside a cloud framework
4) Security though cloud facility workers expedient the greatest safety values to stock significant info. But, earlier accepting cloud skill, you should be attentive that you will be distribution all your association's data to a third party, i.e., a cloud calculating package earner. While distribution the information on the cloud, there may be a chance that your organizations data is chopped by programmer. Scope of Cloud Computing The possibility of cloud computing is an optimistic. According to a statement, the cloud computing marketplace is about $2 billion in India and is predictable to cultivate with a yearly progress rate of 30%.

By 2020, the cloud computing marketplace in India is made-up to influence $4 billion and generate extra than a the numbers of jobs in this country. Roles exact to this area, such as Cloud

Organization Engineer, Cloud Designer, Cloud Initiative Designer, and Cloud Software Plans, are in huge mandate rendering to a account.

Conclusion

Cloud computing marks the commencement of a new stage in the arena of data and communication technology as it carries with an development paradigm which has the possible to change the way in which computing was done. Users are still getting aware through this expertise and a change from conformist subtracting to cloud computing will ensue but progressively. Owed to this technology, developers with novel ideas about internet services will no longer need to spend large amounts of currency in structure their programs and tools substructure abilities.

References

1. https://www.bing.com/search?q=link+for+
2. https://www.ijsr.net INTERNET SOURCES
3. www.leadingedgetech.co.uk/it-services/it...
4. www.sam-solutions.com/blog/four-best-cloud...
5. myventurepad.com/the-pros-and-cons-of-hybrid
6. community.spiceworks.com/cloud/articles/2504
7. www.tutorialspoint.com/cIoud_computing/cloud...
8. www.coursehero.com/file/pvI9c3b/This-model-can...
9. www.branex.com/blog/cloud-service-models-saas-vs...

A Study on Cloud Computing Services

Dr. CH. V. Raghavendran
Associate Professor,
Ideal College of Arts & Sciences, Kakinada, India.

Dr. G. Naga Satish
Associate Professor,
Aditya Engineering College, Surampalem, India.

Dr. P. Suresh Varma
Professor, University College of Engineering,
Adikavi Nannaya University, Rajahmundry, India.

Dr. G. Jose Moses
Associate Professor,
Raghu Engineering College, Visakhapatnam, India.

***Abstract*—Cloud computing is a computing model of providing IT resources, such as application, infrastructure, and platform in the form of service by using Internet. Cloud Computing provides infrastructure for computing and processing of all types of data resources and adopted to deal with the large amounts of data. This Internet based current technology has brought flexibility, capacity and power of processing. This technology has recognized service- oriented idea and has formed a new system in the computing world with its influence and benefits. The capabilities of Cloud computing have been able to move IT industry one step forward. Nowadays, huge and prominent enterprises have migrated to cloud computing and have relocated their processing and storage to it. In this paper, we provide an overall perception on cloud computing and draw attention to its services.**

Keywords*—Cloud Computing, Services, Cloud providers.

I. INTRODUCTION

Cloud computing is on demand network access to computing resources which are often provided by an outside entity and require slight management. Those resources include servers, storage space, network, applications and services [1] [2]. A number of architectures and useful models are present for cloud computing, and these are able to be used with other technologies and design approaches [3].

According to Gartner's list, Cloud computing is on the top of the ten most disruptive technologies of the next coming years [4]. It stand for the long-held dream of visualizing computing as a service [5] where the economy of scale principles help to drive the cost of computing infrastructure effectively down. Big players such as Sun Microsystems, Google, IBM, Amazon and Microsoft have initiated to establish new data centers for hosting Cloud computing applications in different locations around the world to provide redundancy and make sure consistency due to site collapse or failure.

Nowadays, cloud is the most excellent solution for those who are looking for quick implementation techniques [6]. Cloud computing is a kind of configurable, parallel, distributed, virtual, and flexible systems that refers to provision of applications such as hardware and software in virtual data centers via internet [7]. Cloud computing services are configurable and customers pay fees based on the use of resources and services [8-12]. Rest of the paper is structured as follows. Section 2 discusses the history of cloud computing. Section 3 explains the characteristics of cloud computing. Section 4 explains the types of clouds. In section 5, the paper give details of main cloud service models. The section 6 discusses opportunities and challenges in cloud computing. Finally, the paper is concluded in section 7.

II. HISTORY OF CLOUD COMPUTING

Since the sixties, cloud computing has developed along a number of lines, with Web 2.0 being the most recent evolution. However, since the Internet only started to offer significant bandwidth in the nineties, cloud computing for the masses has been something of a late developer. One of the first milestones in cloud computing history was the arrival of Salesforce.com in 1999, which pioneered the concept of delivering enterprise applications via a simple website. The services firm paved the way for both specialist and mainstream software firms to deliver applications over the internet. The next development was Amazon Web Services (AWS) in 2002, which provided a suite of cloud-based services including storage, computation and even human intelligence through the Amazon Mechanical Turk. Then in 2006, Amazon launched its Elastic Compute cloud (EC2) as a commercial web service that allows small companies and individuals to rent computers on which to run their own computer applications. "Amazon EC2/S3 was the first widely accessible cloud computing infrastructure service," which provide its SaaS online video platform to UK TV stations and newspapers.

Another big milestone came in 2009, as Web 2.0 hit its stride, and Google and others started to offer browser-based enterprise applications, though services such as Google Apps. The most important contribution to cloud computing has been the emergence of "killer apps" from leading technology giants such as Microsoft and Google. When these companies deliver services in a way that is reliable and easy to consume, the knock-on effect to the industry as a whole is a wider general acceptance of online services. Other key factors that have enabled cloud computing to evolve include the maturing of virtualization technology, the development of universal high-speed bandwidth, and universal software interoperability standards.

III. CHARACTERISTICS OF CLOUD COMPUTING

There has been much discussion in industry and academia about what cloud computing actually means [13], [14], [15]. The US National Institute of Standards and Technology (NIST) has developed a working definition that covers the commonly agreed aspects of cloud computing [16]. It summarizes cloud computing as: "*a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers,*

storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". According to this definition, cloud computing has the five essential characteristics,

1) *On-demand self-service*.
2) *Broad network access*.
3) *Resource pooling*.
4) *Rapid elasticity*.
5) *Measured Service*.

Cloud computing is an emerging distributed computing paradigm that promises to offer cost-effective scalable on demand services to users, without the need for large up-front infrastructure investments [17]. One of the main reasons for the success of cloud computing is the role it has played in eliminating the size of an enterprise as a critical factor in its economic success. An excellent example of this change is the notion of *data centers* which eliminate the need for small companies to make a large capital expenditure in building an infrastructure to create a global customer base [18].

IV. TYPES OF CLOUDS

Cloud computing comes in three forms: public clouds, private clouds, and hybrids clouds. A recent study conducted by KPMG [19] found that 81% of businesses were either evaluating cloud services, planned a cloud implementation or had already implemented a cloud strategy. Businesses can choose to deploy applications on Public, Private, Hybrid clouds or the newer Community Cloud.

A. *Public Clouds*

Public clouds are owned and operated by companies that use them to offer rapid access to affordable computing resources to other organizations or individuals. With public cloud services, users don't need to purchase hardware, software or supporting infrastructure, which is owned and managed by providers. Public clouds are made available to the general public by a service provider who hosts the cloud infrastructure. Examples of public clouds include Amazon Elastic Compute Cloud (EC2), IBM's Blue Cloud, Sun Cloud, Google AppEngine and Windows Azure Services Platform. A public cloud is the obvious choice when:

- Your standardized workload for applications is used by lots of people, such as e-mail.
- You need to test and develop application code.
- You need incremental capacity.
- You're doing collaboration projects.

B. *Private Clouds*

Private clouds are data center architectures owned by a particular organization that provides flexibility, scalability, provisioning, automation and monitoring. The goal of a private cloud is not sell "as-a-service" offerings to external customers but instead to gain the benefits of cloud architecture without giving up the control of maintaining your own data center. Private clouds are more expensive but also more secure when compared to public clouds. Private cloud is needed in the following cases:

- You need data sovereignty but want cloud efficiencies
- You want consistency across services
- Your data center must become more efficient
- You want to provide private cloud services

C. *Hybrid Clouds*

Hybrid Clouds are a composition of two or more clouds (private, community or public) that remain unique entities but are bound together offering the advantages of multiple deployment models. In a hybrid cloud, you can control third party cloud providers in either a full or partial manner; increasing the flexibility of computing. For instance during peak periods individual applications, or portions of applications can be migrated to the Public Cloud. Here are situations where a hybrid environment is suitable:

- Your company wants to use a SaaS application but is concerned about security.
- Your company offers services that are tailored for different vertical markets.
- You can provide public cloud to your customers while using a private cloud for internal IT.

D. *Community Clouds*

A Community Cloud is designed to meet the needs of a community. Such communities involve people or organization that has shared interests. This includes industrial groups, research groups, standards groups, and so on. Community clouds are a hybrid form of private clouds built and operated specifically for a targeted group. These communities have similar cloud requirements and their ultimate goal is to work together to achieve their business objectives. The goal of these clouds is to have participating organizations realize the benefits of a public cloud with the added level of privacy, security, and policy compliance usually associated with a private cloud. Situations where a community cloud is best:

- Government organizations within a state that need to share resources
- A private HIPAA compliant cloud for a group of hospitals or clinics
- Telco community cloud for Telco DR to meet specific FCC regulations

V. SERVICES OF CLOUD COMPUTING

Nowadays Cloud computing has become a well-known buzzword. As a brand new infrastructure to offer services, Cloud Computing has many advantages in comparing to those existing conventional service providers, such as tremendous fault-tolerance capability, high availability, reduced investment, infinite scalability, probable performance and so on and therefore followed by most of the IT companies, such as Google, Microsoft, Salesforce, Amazon [20]. Cloud computing services are used by government and companies to deal with a variety of application and infrastructure needs such as database, CRM, data storage, and compute. Cloud computing services have several common attributes like – *Multi-tenancy, Elastic, Network-access, On demand, Virtualization and Metering/chargeback.*

Big companies like Microsoft in software industry, Google and Amazon in Internet technology field are joining

to develop cloud services [21], [22]. The most common cloud computing services offered internally or by third party providers are: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

A. Software-as-a-Service (SaaS)

A software that is deployed over the Internet is considered as Software as a Service (SaaS). In SaaS, a provider licenses an application to customers either as a service on demand, through a subscription, charged as per their usage, or at no charge when there is a chance to make income from streams other than the user, such as from advertisement or user list sales. This minimizes the support and maintenance cost effectively. Recent reports show that SaaS will soon become common in every organization and it is important that buyers and users of technology understand what SaaS is and where it is suitable. Some defining characteristics of SaaS include

- Software delivered in a "one to many" model
- Users not required to handle software upgrades and
- Web access to commercial software
- Software is managed from a central location
- APIs allow integration between pieces of software

B. Platform-as-a-Service (PaaS)

A computing platform that allow the designing of web applications quickly and easily without the complexity of buying and maintaining the software and infrastructure is defined as Platform as a Service. PaaS is comparable to SaaS except that, rather than being software delivered over the web, it is a platform for the creation of software, delivered over the web. Here the service provided by the company includes basic standards of development and how you can distribute them effectively. Here the environment would contain an OS, a database, an environment where programming language can be executed and a web server. This let the developer to design, test and implement their own software on the same platform that their end-user clients operate to run the application. The Google App Engine and the Microsoft Azure is a good example of this service model. Some basic characteristics of PaaS include

- Built in scalability of deployed software including load balancing and failover
- Web based user interface creation tools help to create, modify, test and deploy different UI scenarios
- Integration with web services and databases via common standards
- Support for development team collaboration

C. Infrastructure-as-a-Service (IaaS)

Infrastructure as a Service (IaaS) is a way of distributing Cloud computing infrastructure – servers, storage, network and operating systems – as an on-demand service. Instead of buying servers, software, datacenter space or network equipment, clients instead buy those resources as a fully outsourced service on demand [23]. Internet Engineering Task –Force(IETF) has defined the IaaS model to be the most basic service model. This model is related with a virtual engine [24] and users can access to infrastructures with virtual machine [25]. The line between PaaS and IaaS is becoming more blurred as vendors introduce tools as part of IaaS that help with deployment including the ability to deploy multiple types of clouds [26]. IaaS is generally accepted to comply with the following;

- Resources are distributed as a service
- Includes multiple users on a single piece of hardware
- Has a variable cost, utility pricing model
- Allows for dynamic scaling

D. Big-Data-as-a-Service (BDaaS)

BDaaS provides a cloud based structure that presents end-to-end big data solutions to companies. It is a combined structure of Hadoop as a Service (HDaaS), Data-as-a-Service (DaaS) and Data Analytics as a Service (DAaaS). The extensive growth of data is one of the key drivers prevailing in this space. The global Big-Data-as-a-Service (BDaaS) market is likely to grow from $1.8 billion in 2015 to $7 billion by 2020, at a CAGR of 31.5 % during the forecast period. On the basis of type of solutions, BDaaS to follow submarkets:

- Hadoop-as-a-Service (HaaS/HDaaS)
- Data-as-a-Service (DaaS)
- Data Analytics-as-a-Service (DAaaS)

E. Hadoop-as-a-Service (HaaS)

Hadoop is a keystone technology for many big data projects and applications. This is a data storage processing system that enables data storage, file sharing, data analytics etc. With growing of social media and Internet communication, Hadoop is being largely used by companies ranging from Facebook to Yahoo. According to Research and Markets, the Hadoop-as-a-service market will grow approximately by 85% year by year from 2014 to 2019. HaaS has emerged as a replacement to On-premises Hadoop. The following points help distinguish the variety of HaaS options.

- Data Scientists and Data Center Administrators needs must be satisfied
- HaaS Should Store "Data at Rest" in HDFS
- HaaS Should Provide Elasticity
- HaaS Should Support Non-stop Operations
- HaaS Should Be Self-Configuring

HaaS companies offer a "fully baked" version of Hadoop. It is usually their own version of Hadoop that follows closely to the original Apache Hadoop version. Following is a list of benefits of HaaS.

- Managed Hadoop – No need to hire a system admin
- Ease of use – Built to get started quickly
- No hardware/infrastructure – Just add/remove servers as you need it
- Support – Each company has a team of Hadoop experts to help when needed

F. Data-as-a-Service (DaaS)

As SaaS continues to triumph the technology world with innovative products and innovative software platforms, DaaS, its identical twin brother, helps infuse quality data into business and marketing campaigns. Technology based DaaS solutions provide real time market information and customer

data. Without considering the platform or location DaaS separate data from its related applications to bring meaningful information to users. DaaS brings together the technologies necessary to retrieve data from heterogeneous sources such as transactional databases, data warehouses, enterprise resource planning (ERP) systems, and customer relationship management (CRM) solutions. The DaaS approach delivers the following benefits:

- Ability to move data easily from one platform to another
- Preservation of data integrity by implementing access control measures
- Ease of administration and collaboration
- Compatibility among diverse platforms
- Global accessibility

G. Data-Analytics-as-a-Service (DAaaS)

Data Analytics as a Service (DAaaS) or Analytics as a Service (DAaaS) uses the cloud based delivery model and provides the extensible analytical tools [27]. In this service, different analytical tools are available and able to analyze the heterogeneous data. The service users uploads their enterprise data over the cloud and gets the analyzed data useful for business purpose via cloud which consists of the analytical algorithms of machine learning concepts. DAaaS combines the two trends – Big data and Cloud. It represents an approach to the extensible platform that provides cloud based analytical capabilities and covers wide ranging functionalities from data acquirement to end user visualization, reporting and interaction. Analytics as a service allows personalized access of information data sets for knowledge workers. This means that information consumers like business analysts and data scientists, can explore information in an interactive manner and get richer insights rapidly. The advantage of DAaaS is to lower the hurdle of entry to higher analytical capacity, without demanding that the user commits to large internal infrastructures and human resources to the project. Instead of a complex custom project the customer follows simpler steps:

- Data Scientists working for the organization explore the AppStore for an Analytical App that fits the problem
- They rent the Analytical App for a specific time or quantity of data
- They configure the Analytical App to its needs
- Then the data is fed from the internal systems to the Analytical App
- Outcomes are available for all other uses

H. Database-as-a-Service (DBaaS)

Database-as-a-service (DBaaS) is a cloud computing service model that provides users with some form of access to a database without the need for setting up physical hardware, installing software or configuring for performance. In DBaas, customers are charged based on the used features; capacities used and use of database administration tools. Database manager module of DBaas controls all underlying database instances via an Application Program Interface (API). This API is available to the user by management console – Web application, which the user may use to manage and configure the database and even provision or de-provision database instances. Markets and Markets forecast the cloud database and DBaaS market to rise from $1.07 billion in 2014 to $14.05 billion by 2019, at a Compound Annual Growth Rate (CAGR) of 67.30% in the projected period of 2014-2019 [28]. With the DBaaS market projected to reach $1.8 billion by 2016 [29], the need for an agile data tier in the cloud has become paramount.

I. Information-as-a-Service (INaaS)

Information as a Service (INaaS) is the facility to present consistent and secure methods to create, manage, exchange, and extract meaningful information from all available data in the right format at the right time. This allows any application to access any type of information using API, and refers to the ability to use any type of remotely hosted information. Enterprises use information from many different sources through a single application or mash up [30]. The concept of INaaS is "to decouple the information consumer from the underlying complexity of the data landscape". It is a mechanism to organize the transformation of data to information and derive actionable business insights in a structured and modernized manner, despite of the type or place of data.

J. Business-Process-as-a-Service (BPaaS)

Businesses are embracing process optimization, to improve their performance and define clear business outcomes. Business process such as payroll, printing, ecommerce distributed as a service over the Internet and accessible by one or more web enabled interfaces like PC, smart devices and phones can be considered as a Business Process as a Service (BPaaS). Advertising services such as Google Adsense, IBM Blueworks Live for business process management are some of the numerous publicly available services, whereas there are number of other services that today IT departments provide to their users within the firewall or to the trusted partners. The BPaaS market contains a variety of business solutions that help clients and companies effectively adapt to the new changing business circumstances and reduce labor costs. The most popular services offered under the BPaaS umbrella include – Customer service, HR functions (payroll, incentive compensation), Procurement, Sales operations, Industry operation processes. The BPaaS market range is likely to raise from $1.62 Billion in 2015 to $4.71 Billion by 2020, at a CAGR of 23.7% from 2015 to 2020 [31]. More BPaaS providers are embarking on this exciting journey in the cloud. The market annual growth by 2016 is projected to reach 10.7%, according to Gartner, and strong demand is anticipated for all types of cloud services offerings [32].

K. Integration-as-a-Service (INaaS)

Integration as a Service (INaaS) is a cloud service delivery model for integration. Integration-as-a-Service bring an integrated solution that presents connectivity to backend systems, sources, files, and operational applications through the implementation of well-defined interfaces, web services, and calls between applications and data sources. Top

organizations are providing Integration as a service such as Dell Boomi, CloudSwitch, and MuleSoft and so on.

L. Security-as-a-Service (SECaaS)

The users are exposed to security attacks, as they access the Internet through relatively unsecured highways. This is where SECaaS comes in; serving as a buffer against the most unrelenting online threats [33]. SECaaS is based on the Software as a Service (SaaS) model but restricted to particular information security services. This is an outsourcing model for security management. SECaaS involves applications such as anti-virus software delivered over the Internet but the term can also refer to security management provided in-house by an external organization. The goal of SECaaS is to offer security for the information systems while still allowing the achievement of business goal and preserving the integrity, availability and confidentiality of the information resources. Security-as-a-Service offers a number of advantages, which include:

- Regular updates of virus definitions that are not dependent on user compliance
- Faster user provisioning
- Greater security expertise than is typically available within an organization
- Outsourcing of administrative tasks, such as log management
- Using a cloud-based security product also bypasses the need for costly security experts and analysts

Security as a Service product vendors include Cisco, McAfee, Panda Software, Symantec, Trend Micro and VeriSign. In the coming next four years cloud-based SECaaS implementation is expected to increase significantly and likely to double in growth by 2017 [34]. Gartner is forecasting the cloud-based security services market, which includes secure email or web gateways, Identity and Access Management (IAM), remote vulnerability assessment, security information and event management to raise to $4.13 billion by 2017 [35].

M. Testing-as-a-Service (TaaS)

Cloud computing leads a chance in presenting Testing as a Service (TaaS) for SaaS, clouds, and cloud-based applications. TaaS is an outsourcing model in which testing activities associated with an organization's business activities are outsourced to a third party that specializes in simulating real world testing environments as per client requirements. TaaS may engage experts to help and advise employees or simply outsourcing an area of testing to a service provider. This brings new business opportunities, challenges, and demands in innovative service models, testing techniques, QoS standards, and requirements [36]. There are four key factors which govern the process of taking an existing application requirement to the cloud. These provide the appropriate framework for delivering enterprise ready testing on the cloud – People, Process, Governance and Infrastructure.

N. Anything-as-a-Service (XaaS)

XaaS is a combined term said to stand for a number of things including "X as a service," "anything as a service" or "everything as a service." The term XaaS describes a wide class of services related to cloud computing and remote access. XaaS is the next generation of cloud computing services. This combines the online delivery of separate private or public cloud services to users. With so many diverse classes of IT resources now delivered this way, XaaS is a somewhat ironic term for the propagation of cloud services. The most common examples of XaaS are Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). The combined use of these three is referred as the SPI model (SaaS, PaaS, IaaS). Other examples of XaaS include Storage as a Service, Communications as a Service, Network as a Service, Desktop as a Service, Disaster recovery as a Service, Monitoring as a Service and even emerging services such as Marketing as a Service and Healthcare as a Service.

VI. CONCLUSION

Today cloud computing is top of mind with IT companies around the world. Cloud computing has the potential of offering enormous benefits for companies that use it for the deployment and scaling of IT for business processes. More and more industries, from accountancy firms to zoological societies, are adopting cloud computing services. Every day, millions of customers are using online cloud services viz., Apple iCloud, Gmail and Dropbox across desktop and mobile devices. But competition between cloud and outsourcing providers is increasing as new start-ups continue to enter the $80 billion global cloud computing market. We expect that the cloud computing will rise, so developers should take it into account. In spite of whether a cloud provider sells services at a low level of concept or a higher level, we believe computing, storage, and networking must all focus on horizontal scalability of virtualized resources rather than on single node performance.

REFERENCES

[1] N. Sadashiv and S. D. Kumar, "Cluster, grid and cloud computing: A detailed comparison," 2011 IEEE 6th International Conference on Computer Science & Education (ICCSE), pp. 477–482, 2011.
[2] N. I. of Standards and Technology, "NIST Cloud Computing Program," http://www.nist.gov/itl/cloud/, 2011.
[3] IOS Press, "Guidelines on security and privacy in public cloud computing," Journal of EGovernance, 34, pp. 149-151. DOI: 10.3233/GOV-2011-0271, 2011.
[4] Gartner, "Gartner top ten disruptive technologies for 2008 to 2012. Emerging trends and technologies roadshow," 2008.
[5] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California at Berkeley Technical Report No. UCB/EECS-2009-28, Feb 2009.
[6] Mohammed Alhamad, "A Trust-Evaluation Metric for Cloud applications", International Journal of Machine Learning and Computing, Vol. 1, No. 4, 2011.
[7] Nezih Yigitbasi, "C-Meter: A Framework for Performance Analysis of Computing Clouds", IEEE/ACM International Symposium on Cluster Computing and the Grid, 2009.
[8] Borko Furht and Armando Escalante, "Handbook of Cloud Computing", Springer, 2010.
[9] Abah Joshua & Francisca N. Ogwueleka, "Cloud Computing with Related Enabling Technologies," International Journal of Cloud Computing and Services Science (IJ-CLOSER), Vol.2, No.1, pp. 40~49, 2013.
[10] NIST Advisory Working Group, "NIST Cloud Computing Standards Roadmap", NIST Special Publication, 2011.

[11] Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing", NIST Special Publication, 2011.
[12] M. Malathi, "Cloud Computing Concepts", IEEE, 2011.
[13] L. Gonzalez, L. Merino, J. Caceres, and M. Lindner, "A Break in the Clouds: Towards a Cloud Definition", Computer Communication Review, 39(1), 2009.
[14] D. Plummer, T. Bittman, T. Austin, D. Cearley, and D. Smith, "Cloud computing: Defining and describing an emerging phenomenon", Technical report, Gartner, 2008.
[15] J. Staten, S. Yates, F. Gillett, W. Saleh, and R. Dines, "Is cloud computing ready for the enterprise?", Technical report, Forrester Research, March 2008.
[16] P. Mell and T. Grance, "Definition of cloud computing," Technical report, National Institute of Standard and Technology (NIST), July 2009.
[17] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Commun. ACM, 53:50–58, April 2010.
[18] D. Agrawal, A. El Abbadi, F. Emekci, and A. Metwally, "Database Management as a Service: Challenges and Opportunities," In ICDE, 1709–1716, 2009.
[19] http://www.appcore.com/types-cloud-computing-private-public-hybrid-clouds/
[20] Minqi Zhou; Rong Zhang; Dadan Zeng; Weining Qian, "Services in the Cloud Computing era: A survey," 4th International Universal Communication Symposium (IUCS), pp.40–46, 2010.
[21] L. Qian, Z. Luo, Y. Du, and L. Guo, "Cloud Computing: An Overview," in CloudCom '09: Proceedings of the 1st International Conference on Cloud Computing. Springer-Verlag, pp. 626–631, 2009.
[22] G. Lin, D. Fu, J. Zhu, and G. Dasmalchi, "Cloud Computing: IT as a Service," IT Professional, vol. 11, no. 2, pp. 10–13, 2009.
[23] http:// diversity.net.nz/ wp-content/ uploads/ 2011/ 01/ Moving -to-the-Clouds .pdf
[24] Kaiqi Xiong, "Service Performance and Analysis in Cloud Computing", IEEE, 2009.
[25] Ioannis A. Moschakis & Helen D. Karatza , "Performance and Cost evaluation of Gang Scheduling in a Cloud Computing System with Job Migrations and Starvation Handling", IEEE, 2011.
[26] http:// m.zdnet.com/ blog/ forrester /is- the- iaaspaas- line-beginning-to-blur/583
[27] "Data Analytics as a Service: unleashing the power of Cloud and Big Data", Ascent white paper, March 2013.
[28] http:// www.marketsandmarkets.com/PressReleases/ cloud-database-as-a-service-dbaas.asp(accessed in December'15)
[29] Matt Aslett, DBaaS poised to drive next-generation database growth, 451 Research, Aug 2013.
[30] D.S. Linthicum, Addison-Wesley information technology series: "Cloud Computing and SOA Convergence in your Enterprise, A step-by-step guide", India: 2010, first Ed.
[31] http:// www.marketsandmarkets.com/ Market - Reports /business-process-as-a-service-bpaas-market-986.html, Publishing Date: November 2015.
[32] Gartner Says Worldwide Public Cloud Services Market to Total $131 Billion, http://www. gartner.com/ newsroom/id /2352816, February 2013.
[33] www.cloudbric.com/ blog/ 2015 /09 /the- newbies- guide -to-security-as-a-service-secaas/
[34] http:// www.cloudcomputingadmin.com/ articles -tutorials/ security/security-service-cloud-based -rise-part1.html
[35] Ruggero Contu, Kelly M. Kavanagh, Market Trends: Cloud-Based Security Services Market, Worldwide, 2014, 2013.
[36] Gao, J. ; Xiaoying Bai ; Wei-Tek Tsai ; Uehara, T., Testing as a Service (TaaS) on Clouds, IEEE 7th International Symposium on Service Oriented System Engineering (SOSE), 2013, pg. 212 – 223.

Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 38 (2012) 2222 – 2227

Procedia Engineering

www.elsevier.com/locate/procedia

International Conference on Modeling Optimisation and Computing

Cloud Computing: possibilities, challenges and opportunities with special reference to its emerging need in the academic and working area of Information Science.

Prantosh kumar Paul(a*),Mrinal K Ghose (b)

*Resrearch Scholar,EIILM University,Jorethang,Sikkim,India.
Senior Scientist ISRO [Retried], Dean,R & D - Sikkim Manipal University,Tadong,Gangtok.

Abstract

Cloud computing is actually a model for enabling convenient, limitless, on demand network access to a shared pool of computing resource. This paper describes some aspect of cloud architecture including cloud based information mechanism, especially useful in information system. Paper mention about the challenges and opportunities of cloud based model. At last we mental the main SWOT in respect of information delivery mechanism.

Keywords:-computing, cloud computing, cloud model, virtualization, information science, computer science, information mechanism.

*Prantosh Kumar Paul, M-+917797700765 / M- +919851036765, apexpgi@rediffmail.com , prantoshkpaul@gmail.com

1877-7058 © 2012 Published by Elsevier Ltd. Open access under CC BY-NC-ND license.
doi:10.1016/j.proeng.2012.06.267

1. Introduction:-

Cloud computing is actually a mechanism or model for enabling easy,convenient,on demand network access to a shared pool of devices like server,networks,storage devices, application, services and other advance computing devices which are configurable another important feature of cloud computing is the minimum efforts and management cloud model gives us rapid services. It is consider as model and services rather than product or computing devices. Information is the processed data and information mechanism is the way or standard by which collection, selection, organization and dissemination of content and information is possible through scientific mechanism and procedure. Cloud computing model in the field of information and content mechanism provide us easy and convenient information and recourses to the entire information sector.

2. Cloud computing: meaning:-

In simplify manner define cloud is too hard. Many people, technologist, information scientist, researcher defines cloud computing various way and perspective. As Wikipedia define cloud computing as the delivery of computing as a services rather than a product, where by shared resources, software and information are provided to the computer and other devices. Let us check some definition of cloud computing:-

- NIST define cloud computing as “a model for enabling ubiquitous, convenient on demand network access to a shared pool of configurable computing recourses (e.g. Networks,Servers,Storage,Application and services) that can be rapidly provisioned and realized with minimal management effort or services provider interaction.[21]

- According to Frank Osafo, “a key element of cloud computing is that “services operate consistently regardless of the underlying systems”.

So from the above definition it is clear that cloud computing is actually nothing but the consumption model required for convenient recourses and content sharing.

3. Cloud computing: Contemporary uses:-

Due to various advancement Cloud Computing model is using in several places like:-

- Today many e-mail service provider using this model for convenient content delivery like- g mail.
- Cloud Computing is useful in web based document management.
- In the field of web-storage, editing and collaboration tools.
- In the e-commerce, e-governance, e-business cloud model is widely used.
- Today in many website the aliveness is the gift of cloud computing.
- Internet and web engineering is the field where application of cloud computing is possible.

4. Cloud computing: advantages:-

There are several advantages possible through the cloud computing such as:-

- It creates a healthy information technology infrastructure.
- Useful to provide and maximize flexibility and efficiency.
- It is possible quick IT delivery through cloud computing.
- It helps to integrate user and company personnel.
- It is provide hassle free maintenance of software and hardware.
- Cloud computing reduction in IT and computing cost.
- Cloud computing gives opportunities to harness the power technologies in the new and creative way without over spending on IT budget. [11]
- It creates wonderful platform for service, technology.
- It provides a new kind of user experience.
- It is reliable and user convenient

5. Cloud computing means cloud society: opportunities:-

Due to several advantage like flexibility, efficiency, green benefits, convenience cloud computing provides a wonderful opportunities to the following entries.

The developing countries like India, China, South Africa may get wonderful benefit from cloud computing for several reasons like-

- Money saving.
- Doing several works through cloud is possible. So ultimately it needs less manpower and technological support:-
- It enables and maximizes the capacity of small and medium business.
- Without large IT infrastructure, cloud computing provides big facilities for small organization.
- The government offices, universities, NGO, bank, hospital provides reduction in IT cost.
- It is provides efficient, reliable, convenient digital and online content and information management.
- The user using internet from low capacity may use this for fastest service.
- Using internet from mobile phones is also helpful from cloud computing.
- Through the distributed infrastructure and server the web service will grow significantly.
- It needs cheaper devices low storage capacity as well as processing power.

- The information technology infrastructure and market growing rapidly with the help of cloud computing.
- Computer users became less dependent on specific and needed software as the cloud model provide many applications through the network.
- Ultimately the economically poor countries, less information and computing countries may choose the cloud computing model for their efficient and fast data delivery.
- Due to transformation and inter exchange of information the availability and easy access of information helps to move on information society from the traditional society.
- The cloud computing model helps to up-lift of the states and countries.
- The cloud computing model also helps to create knowledge economy.
- The social networking sites also take the help of cloud computing in generally.
- The dynamic provisioning is possible through the cloud computing.

6. Cloud computing and its integration with Information Science: possibilities and Indian scenario-

According to *Information Scientist Broko*, Information Science is an interdisciplinary science that investigates the properties and behavior of information, the forces that govern the flow and use of information, and the technique, both manual and mechanical, of processing information for optimal storage, retrieval and dissemination.
Information science is actually a field of fields many subjects have great influence to make a separate discipline called information science. Information science mistakenly consider as computer science or library science or information technology. However this subject practically an interdisciplinary academic area which is constituent with Information Technology, Computer Science, Management Science and information perspective of library science or documentation. So it is full-fledged interdisciplinary subject with its own recognition. The cloud computing approach or model may apply in diverse academic field of information science and many working and institutional areas like:-

- Information Networks.
- Information System.
- Knowledge Grid and Networks.
- Information Centre and Data Centre.
- Information Analysis Centre, Documentation Centre and so on.

India has thousand of information and computer network for the purpose of institute, enterprise, foundation, academic institute or universities. As a full-fledged information system and network the following are giving their best like-

- National information System for Science and Technology.
- Education and Research Network.
- National Information Centre Network and so on.

But still during our literature survey and questionnaire review it is observed that there is a unwillingness towards application of cloud model in Information System and Network and similar. Some of the area where cloud model can use in ISN and Similar foundation such as:-

- To coordinate between one information centre to another or their apex body.
- To coordinate and sharing of information, book, document and even other recourses including hardware, software and so on.
- To work with the approaches of Top Level Management to Lower Level Management or vice versa

Now let us see some probable area of traditional area of Information Science, where cloud or virtualization model is applicable like:-

- For preparing auto indexing and auto abstracting, fuzzy based IRS.
- In document delivery Services, Current Awareness, Selective Dissemination of Information.
- To interact and designing website of Information Science school, college and Information Networks.
- In GUI based search engines it can be used.
- In auto classification and proper class number distribution this model useful.
- In the journal and consortium it may be used.
- In collection, selection, organization of knowledge.

7. Cloud computing: challenges:-

Though cloud computing gives wonderful benefit and limitless information mechanism but it has several issue and problems like-

- Government grant and assistance towards cloud based model is an emerging issue.
- Many foundation, establishment, government agencies are not aware about the cloud benefit.
- In many services cloud performance is an important issue.
- Unwillingness to changes, funding and finance is important challenges.
- Cloud computing needs high quality broadband connection other wise the whole efforts will be value less.
- In many website cloud based system may not work properly.
- Connection and speed in MB and GB format is an emerging issue.
- Delay of processing information that means latency is challenging fact as far as cloud computing is concerned.
- It needs front and backbone infrastructure and appropriate quality of services.
- Appropriate cyber law, act and policy should be frame for correct and right cloud model.
- Many cloud services are costly so for developing countries like India this is an emerging issue.

Cloud divide is also challenging because in many developing and developed countries are still not able to provide high speed broad band connection

8. Conclusion:-

No doubt cloud computing provide us cheaper, greener, faster, flexible, efficient environment. Apart from government, the NGO's, universities, higher educational institute, research centre can get benefit from this model. Though in many undeveloped countries cloud computing interest is minimum due to availability of foreign cloud service provider. But it is essential in the age of globalization that either a country should pay faith on Foreign Service provider or countries should try to develop a shelf sufficient cloud services of their own. But the actual service benefit should also need to keep in mind. So no doubt with the help of cloud computing we can create a healthy cloud based knowledge economy and healthy informatics practice through advancement of Information Science.

References:-

[1] http://cloudcomputing.blogspot.com

[2] http://cloudcomputing.sys-con.com/node/1528536

[3] ftp://public.dhe.ibm.com/common/ssi/sa/wh/n/ciw03067usen/CIW03067USEN.PDF

[4] http://en.wikipedia.org/wiki/Cloud_client

[5] Danielson, Krissi (2008-03-26). "Distinguishing Cloud Computing from Utility Computing". Ebizq.net. http://www.ebizq.net/blogs/saasweek/2008/03/distinguishing_cloud_computing/. Retrieved 2010-08-22.

[6] "Cloud Computing: Clash of the clouds". The Economist. 2009-10-15. http://www.economist.com/displaystory.cfm?story_id=14637206. Retrieved 2009-11-03.

[7] "National Science Foundation press release. September 2008. "National Science Foundation Awards Millions to Fourteen Universities for Cloud Computing Research." Retrieved 2010-03-01". Nsf.gov. http://www.nsf.gov/news/news_summ.jsp?cntn_id=114686. Retrieved 2010-08-22.

[8] Myslewski, Rik (2009-12-02). "Intel puts cloud on single megachip". Theregister.co.uk. http://www.theregister.co.uk/2009/12/02/intel_scc/. Retrieved 2010-08-22.

[9] "Nicholas Carr on 'The Big Switch' to cloud computing". Computerworlduk.com. http://www.computerworlduk.com/technology/internet/applications/instant-expert/index.cfm?articleid=1610. Retrieved 2010-08-22.

[10] "IEEE Technical Committee on Services Computing". Tab.computer.org. http://tab.computer.org/tcsc. Retrieved 2010-08-22.

[11] "Cloud Computing : the future of computing is here" Microsoft Interface | April - June 2010

[12] Abdul Azeez, T.A. "How to Design A Digital Library" SRELS Journal of Information Management Vol. 40, No. 3 September 2003 Paper Z. p267-273.

[13] Adhikary, Madhabmohan, And Amitava Nandi "Ideas of Ranganathan's Classification Theory Pervaded by Oriental Philosophy" SRELS Journal of Information management Vol. 40, No 3 September 2003. Paper AA. P275-284.

[14] Agarwal, Ritu and viswanath venkatesh. "Assessing a firms web presence: A Heuristic Evaluation Procedure for the measurement of usability" information systems research 13, no 3 (September 2002)

[15] Aladwani, Adel M "An integrated performance model of information systems projects" journal of management information systems 19 no 1 (September 2002).

[16] Alleman, James "Real options real opportunities" Optimize magazine (January 2002)

[17] Aparajita, "Virtual Information Center: How Close To Reality." SRELS Journal of information Management, Vol. 42, No. 4, December 2005, Paper A.E. p419-426.

[18] A P J Abdul Kalam"IT Strategy in Defense Environment." DESIDOC Bulletin of Information Technology, Vol. 20, Nos. 1&2 2003. P 7-12

[19] Aries, James A Subhankar Banerjee, Marc S Brittan, Eric Dillon, janusz s. kowalik and john p. lixvar. "Capacity and performance analysis of distributed enterprise system" communication of the ACM 45, no 6. 2002.

[20] www.en.wikipedia.org

[21] The NIST Definition of Cloud Computing (Draft), accessible:csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145 Cloud-definition.pdf