ISSN:0975-9646

Review of Cloud Storage Security and Cloud Computing Challenges

Pradnya B. Godhankar, Deepak Gupta

Computer Science and Engg Dept. Siddhant Collage of Engineering, Sudambare ,Chakan Talegaon Road,Taluka Maval, Disrtict Pune 412109

Abstract: Since from last decade most of organizations, individual end users are making use of online storage services in order to store their important information for the backup purpose. This data is stored on online storage system which is called as clouds. This stored data later accessed anywhere, anyplace and anytime in world using internet. This storage services is having main challenge of securing the information which is stored by different mankind. The security as well as privacy becomes the weakness of cloud services as the end users important data is stored on it and maintained by cloud service provider on behalf of end users. As advantage point of view cloud computing is nothing but the place for end user where end user can use the free resources for their own purpose on demand and share the information with their peers or mates through it over internet. This ultimately allows end user to access their important data from any geographical place at any time in less cost and time. Because this cloud storage services, use of many expensive software's avoided and hence requires less cost. In addition to this less personnel required, more scalability. However as the cloud servers present at different locations in which many end users information is stored and maintained, security becomes main issues of using it. Recently there are many methods presented over security of cloud storage by different researchers. Because of security issues in cloud computing, many big organizations worldwide enable to use cloud storage services. In this review paper we are aiming to present review of security issues in cloud storage systems, different methods, advantages, challenges etc.

Keywords: cloud computing, cloud storage, information security, data maintenance, cost, time.

I. INTRODUCTION

For all the online storage services, security is must for privacy preservation and information leakage avoidance, but security method should be strong enough to avoid different attacks of breaking it. Many customers as well as organizations are able to use online storage services only if there is strong security mechanism used by particular service provider. So to create a trusted environment for customers, we need to develop software, services, and processes with privacy in mind. Cloud computing is the biggest buzz in the computer world these days. Cloud computing is everywhere. The locality of physical resources and devices being accessed are in general not known to the end user. It also provides services for users to build up, deploy and manage their Applications on cloud ", that maintains and manages by itself [1] virtualization resources. NIST definition of cloud computing: cloud computing that can be rapidly provisioned and minimizing management effort or service provider interaction with configurable computing resources (e.g., networks, servers, Storage, applications, and services) to a shared pool of convenient, enabling on-demand network access to a model ".

The mechanism of cloud computing is based on concepts of grid computing, distributed computing as well as utility computing, but it is identified with their unique characteristics if its utilized properly. Cloud computing really is accessing resources and services needed to perform functions with dynamically changing needsAn application or service developer instead of a specific endpoint requests access or resources from the cloud name. What is Cloud manages several organizations across multiple infrastructures and overlaid on top of the infrastructures to tie them together one or more frameworks. Maintains that a virtualization cloud resources and manages itself has not been provided security in the cloud. Since, many companies adopt their unique security architecture [10]. For example Amazon is their own security infrastructure using encryption, cloud security here. Decryption, compression etc have a wide survey on different techniques.

In this review paper, we are aiming to present the review of privacy preservation and cloud storage security methods with their working approaches. In addition to this we are presenting challenges and issues of security in cloud computing. In below section II we are first discussing the different challenges of using cloud computing services. After that in section III we are discussing the different cloud storage security and privacy preservation methods reviewed. Finally conclusion is made on the basis of all discussions and future work.

II. CHALLENGES OF CLOUD COMPUTING

The current adoption of cloud computing is associated with numerous challenges because users are still skeptical about its authenticity. On a survey attended by IDC in 2008, the major challenges that prevent Cloud Computing from being adopted are recognized by organizations are as follows:

A. Security: it security issue cloud computing instrumental in obstructing the approval is clear. Appears without doubt, your data, your software and hard disk using a CPU and running on many security issues result in data loss. by the way, phishing, bot-NET (collection of machines running remotely) to serious threats of data and software Exchange. In addition Multi tenancy in the cloud computing model and computing resources to cope with novel technology requires that new security challenges. for example, hackers cloud clouds to start

an attack often makes them a relatively cheap cost and more reliable infrastructure services as the bot can use to organize the net. [9]

B. Costing Model: Cloud consumers must consider the tradeoffs amongst computation, communication, and integration. While migrating to cloud important can reduce infrastructure costs, increase data communications costs, meaning that is an organization's data and the cost of relocating public and community cloud and cost-per-use computing resources unit high. This problem if consumer hybrid cloud deployment model uses where the Organization's data public/private (in-house it infrastructure) among a number of Distributed especially Chief/community cloud makes sense Intuitively, CPU intensive on-demand computing. [9]

C. Charging Model: The elastic resource pool has made the cost analysis a lot more complicated than regular data centers, Often their cost calculates based on static computing consumption. in addition, the inherent physical server virtual machine instead of an instantiated cost analysis unit. SaaS cloud providers, their offering within the cost of developing the very substantial multitenancy. These include: the design and the software that originally was used for single-tenancy redevelopment of new features that thorough optimization to enhance security, performance and allow concurrent user access, and the cost of dealing with complications induced by the above changes as a result, SaaS providers need to trade between provision of multitenancy closed up by weight and cost savings through such overhead multi tenancy yielded less amortization, as licensed software on the site number, etc. so, SaaS providers charge a strategic and practical model for profitability is important to the stability of the cloud and SaaS Providers. [9]

D. Service Level Agreement (SLA): Although cloud consumers do not control the underlying computing resources, they entrusted their core business tasks when consumers migrate to cloud their quality, availability, reliability, and performance of these resources to make sure. in other words, the guarantee of or distribution providers to consumers. Usually, these service level agreements (SLAs) interactions between providers and consumers are provided through. the very first issue, so that they can cover most of consumer expectations such that granularity, expression and complicatedness, is an appropriate level for tradeoffs between SLA definition of specifications and relatively simple to be weighted, Verified, evaluated, and Kuyoro s. o., reinforced by Awodele o f & Ibikunle.

International Journal of computer networks (IJCN), (3) section: issues (5): 2011 253 on the cloud resource allocation mechanisms. In addition, various cloud offerings (annual, PaaS and SaaS) separate SLA will need to define the metaspecifications. Problems of implementation for cloud providers also have a number of raises. in addition, the user continuously advanced SLA system SLA evaluation framework feedback and optimization features to incorporate.[16]

E. What to migrate: Based on a survey (Sample size = 244) conducted by IDC in 2008 is the seven IT systems/applications being migrated to the cloud are: IT Management Applications (26.2%), Collaborative Applications (25.4%), Personal Applications (25%), Business Applications (23.4%), Applications Development and Deployment (16.8%), Server Capacity (15.6%), and Storage Capacity (15.5%). This result reveals that organizations still have security/privacy concerns in moving their data on to the Cloud. At present the easiest to move it systems management and personal applications such as peripheral. Organizations are conservative compared to annual SaaS employment. Because partly marginal is tasks are often outsourced to the cloud, and the main activities in the home. At the time of the three-year survey shows31.5% of their storage capacity, the Organization will move to the cloud. Although this number is still relatively low collaborative applications (46.3%) compared to that time. [1]

F. Cloud Interoperability issues: currently, each cloud offering how cloud applications/clients/users, leading to "blur the cloud" event has its own way to interact with it severely cloud vendor locking, development of the ecosystems which compels alternative and Ikretaon/offering side-by-side within an organization to optimize resources at different levels to opt users prohibits hinders ability. More importantly, the proprietary cloud APIs it inherited an organization's existing systems (for example a on-premise data center is a pharmaceutical company highly interactive modeling applications) to integrate cloud services with very hard across the clouds. And the clouds and local applications to realize seamless is interoperability between the primary fluid data. There is essential for interoperability level that clouds are a number of computing. First of all, to optimize it asset and computing resources, often sung Need home it and Sunnyvale CA marginal functions and activities (e.g. human resource system) on the cloud associated with their core competencies while outsourcing to keep. Second and more often than not the purpose of customization offered by different vendors, an organization of Familiar with a number is of marginal functions to the cloud to outsource. Standardized interoperability issues to be addressed would seem to be a good solution. Cloud computing just starts to take off, however, industry leading cloud vendors pressing interoperability issue has appeared on the agenda. [9]

III. Review Of Cloud Computing Storage Security Methods

3.1 Public Auditing with Complete Data Dynamics Support

Verification of data integrity at unreliable servers is the major concern in cloud storage. Proposed scheme first focused to discover the potential security threats and difficulties of preceding works and build a refined verification scheme Public auditing system with protocol that supports complete dynamic data operations is presented [3]. To accomplish dynamic data support, the existent proofread of PDP or PoR

scheme is improved by spoofing the basic Markle Hash Tree (MHT). Proposed system extended in the direction of allowing TPA to perform many auditing jobs by examining the bilinear aggregate signature technique.

3.2 Implicit Storage Security to Data in Online

Providing implicit Storage Security to data in Online is more beneficial in a cloud environment. Presented implicit storage security architecture for storing data where security is disseminated among many entities [1] and also look at some common partitioning methods. So data partitioning scheme is proposed for online data storage that involves the finite field polynomial root. This strategy comprises of two partitioning scheme. Partitioned data are saved on cloud servers that are chosen in a random manner on network and these partitions are regained in order to renovate the master copy of data. Data pieces are accessible to one who has knowledge of passwords and storage locations of partitioned pieces.

3.3 Efficient Third Party Auditing (TPA)

Cloud consumers save data in cloud server so that security as well as data storage correctness is primary concern. A novel and homogeneous structure is introduced [4] to pro-vide security to different cloud types. To achieve data storage security, BLS (Boneh–Lynn–Shacham) algorithm is used to signing the data blocks before outsourcing data into cloud. BLS (Boneh–Lynn–Shacham) algorithm is efficient and safer than the former algorithms. Batch auditing is achieved by using bilinear aggregate signature technique simultaneously. Reed-Solomon technique is used for error correction and to ensure data storage correctness. Multiple batch auditing is an important feature of this proposed work. It allows TPA to perform multiple auditing tasks for different users at the same.

3.4 Identity-Based Authentication

In Cloud Computing, resources and services are distributed across numerous consumers. So there is a chance of various security risks. Therefore authentication of users as well as services is an important requirement for cloud security and trust. When SSL Authentication Protocol (SAP) was employed to cloud, it becomes very complex. As an alternative to SAP, proposed a new authentication protocol based on identity which is based on hierarchical model with corresponding signature and encryption schemes [2]. Signature and encryption schemes are proposed to achieve security in cloud communication. When comparing performance, authentication protocol based on identity is very weightless and more efficient and also weightless protocol for client side.

3.5 Way of Dynamically Storing Data in Cloud

Securely preserving all data in cloud is not an easy job when there is demand in numerous applications for clients in cloud. Data storage in cloud may not be completely trustable because the clients did not have local copy of data stored in cloud. To address these issues, proposed a new protocol system using the data reading protocol algorithm to check the data integrity [5]. Service -providers help the clients to check the data security by using the proposed effective automatic data reading algorithm. To recover data in future, also presented a multi server data comparison algorithm with overall data calculation in each update before outsourcing it to server's remote access point.

3.6 Effective and Secure Storage Protocol

Current trend is users outsourcing data into service provider who have enough area for storage with lower storage cost. A secure and efficient storage protocol is proposed that guarantees the data storage confidentiality and integrity [6]. This protocol is invented by using the construction of Elliptic curve cryptography and Sobol Sequence is used to confirm the data integrity arbitrarily. Cloud Server -challenges a random set of blocks that generates probabilistic proof of integrity. Challenge-Response protocol is credential so that it will not exposes the contents of data to outsiders. Data dynamic processes are used to keep the same security assurance and also provide relief to users from the difficulty of data leakage and corruptions problems.

3.7 Storage Security of Data

Resources are being shared across internet in public surroundings that creates severe troubles to data security in cloud. Transmitting data over internet is dangerous due to the intruder attack. So data encryption plays an important role in Cloud environment. Introduced a consistent and novel structure for providing security to cloud types and implemented a secure cross platform [7]. The proposed method includes some essential security services that are supplied to cloud system. A network framework is created which consists of three data backups for data recovery. These backups located in remote location from main server. This method used SHA Hash algorithm for encryption, GZIP algorithm for compression and SFSPL algorithm for splitting files. A secure crossed platform is reason for cloud computing.

3.8 Secure and Dependable Storage Services

Storage service of cloud permits consumers to place data in cloud as well as allowed to utilize the available well qualified applications with no worry about data storage maintenance. Although cloud provides benefits, such a service gives up the self-control of user's data that introduced fresh vulnerability hazards to cloud data correctness. To handle the novel security issue, defining a cloud data integrity and availability assurances, a pliable mechanism is proposed for auditing integrity in a dispersed manner [8]. Proposed mechanism allows users to auditing the cloud data storage and this auditing result utilized Homomorphism token with Reed-Solomon erasure correcting code technique that guarantee the correctness insurance and also identifying- misconduct servers rapidly. The proposed design is extended to support block-level data dynamic operations. If cloud consumer is not able to possess information, time and utility then the users can assign their job to an evaluator i.e. TPA for auditing process in safe manner.

3.9 Optimal Cloud Storage Systems

Cloud data storage which requires no effort is acquiring more popularity for individual, enterprise and institutions data

backup and synchronization. A taxonomic approach to attain storage service optimality with resource provider, consumer's lifecycle is presented [9]. Proposed scheme contributes storage system definition, storage optimality, ontology for storage service and controller architecture for storage which is conscious of optimality. When compared with existing work, more general architecture is created that works as a pattern for storage controller. A new prototype Nubi Save is also proposed which is available freely and it implements almost all of RAOC concepts.

3.10 Process of access and Store Small Files with Storage

To support internet services extensively, Hadoop distributed file system (HDFS) is acquired. Several reasons are examined for small file trouble of native Hadoop distributed file system: Burden on Name Node of Hadoop distributed file system is enforced by large amount of small files, for data placement correlations are not considered, perfecting mechanism is not also presented. In order to overcome these small size problems, proposed an approach that improves the small files efficiency on Hadoop distributed file system [10]. Hadoop distributed file system is an Internet file -system representative, which functioning on clusters. The cut-off point is -measured in Hadoop distributed file system's circumstance in an experimental way, which helps to improve I/O performance. From taxonomic way, files are categorized as independent files, structurally and logically-related files. Finally perfecting technique is used to make -better access efficiency and considering correlations when files are stored.

3.11 File Storage Security Maintenance

To assure the security of stored data in cloud, presented a system which utilizes distributed scheme [11]. Proposed system consists of a master server and a set of slave -servers. There is no direct communication link between clients and slave servers in the proposed model. Master server is responsible to process the client's requests and at slave server chunking operation is carried out to store copies of files in order to provide data backup for file recovery in future. Users can also perform effective and dynamic data operations. Clients file is stored in the form of tokens on main server and files were chunked on slave servers for file recovery. Thus proposed scheme achieved storage correctness insurance and data availability by using Token generation algorithm with homomorphism token and merging algorithm were used.

3.12 File Assured Deletion (FADE) for Secure Storage

Proposed a file assured deletion scheme based on policy to dependably efface files of cancelled file access policies [12]. Working prototype of FADE is implemented at the top of Amazon S3. Performance overhead is also evaluated on Amazon S3.

3.12.1. File Assured Deletion Based on Policy

Data file format for logical file access policy is associated with a data key for each file access policy should be enclosed with the control key. Maintenance is the responsibility of the key managers control key when a policy is canceled, the policy control key manage from r. main idea is as follows: each file is saved with the data key and the control key data key is used to preserve. The key here is to keep the keys Manager is responsible for. Control key is deleted when a Microsoft Office policy cancelled. so that encrypted file and data key may not be not come. In the case of deleted file still exists, a copy of the file is encrypted and available to everyone. Coordinator and submit multiple policies such as voyage policies too. Conjunctive policies are used to recover file by satisfying all policies whereas disjunctive policies satisfying only one policy. Conclusion is FADE is executable in practice and this approach includes all dynamic data operations. Cryptographic operations are less and meta-data over-head are small.

3.13 Accessing Outsourced Data Efficiently

An approach is proposed to attain flexible access control and dynamic large-scale data in a safe and effective way. An Owner-write-user-read scenario is presented for accessing data [13]. Original data owner be only able to update/ modify- their data. Cloud users will be able to read information- with corresponding access rights. Proposed approach deals with key generation, dynamics handling and overhead analysis. In key generation part, a key derivation hierarchy is generated and Storage over-head is moderated. Dynamics handling part consists of dynamic data operations and access rights of user. Eavesdropping can be overcome by over-encryption and lazy revocation.

There is no direct communication link between clients and slave servers in the proposed model. Master server is responsible to process the client's requests and at slave server chunking operation is carried out to store copies of files in order to provide data backup for file recovery in future. Users can also perform effective and dynamic data operations. Clients file is stored in the form of tokens on main server and files were chunked on slave servers for file recovery. Thus proposed scheme achieved storage correctness insurance and data availability by using Token generation algorithm with homomorphism token and merging algorithm were used.

3.14 File Assured Deletion (FADE) for Secure Storage

Proposed a file assured deletion scheme based on policy to dependably efface files of cancelled file access policies [12]. Working prototype of FADE is implemented at the top of Amazon S3. Performance overhead is also evaluated on Amazon S3.

3.12.1. File Assured Deletion Based on Policy

Data file is logically connected with file access -policy and a data key. Each file access policy should be attached with control key. Maintenance of control key is the responsibility of key manager. When a policy is cancelled, control key of that policy will be dispatched from the key man-ager. The main idea is as follows: each file with data key is saved and control key is used to protect data key. Here key manager is responsible for retaining keys. The control key is deleted when a -policy is cancelled. So that the encrypted file and data key could not be regained. In case the file is removed

still a copy exists, that file is encrypted and unavailable to everyone. Multiple policies such as conjunctive and disjunctive policies are also presented. Conjunctive policies are used to recover file by satisfying all policies whereas disjunctive policies satisfying only one policy. Conclusion is FADE is executable in practice and this approach includes all dynamic data operations. Cryptographic operations are less and meta-data over-head are small.

3.13 Accessing Outsourced Data Efficiently

An approach is proposed to attain flexible access control and dynamic large-scale data in a safe and effective way. An Owner-write-user-read scenario is presented for accessing data [13]. Original data owner be only able to update/ modify- their data. Cloud users will be able to read information- with corresponding access rights. Proposed approach deals with key generation, dynamics handling and overhead analysis. In key generation part, a key derivation hierarchy is generated and Storage over-head is moderated. Dynamics handling part consists of dynamic data operations and access rights of user. Eavesdropping can be overcome by over-encryption and lazy revocation.

Table 1. Comparative analysis on advantage and limitations of existing storage techniques

Storage Scheme	Proposed Approach	Advantages	Restrictions
1. Implicit Storage Security to Online data	Data partitioning scheme for online data storage.	Partitioned data pieces cannot bring out any user information.	In case user forgot where the data stored, it will become difficult for users.
2. Identity-Based Authentication	New authentication protocol based on identity which is based on hierarchical model	Weightless and more expeditious.	Only certificate communication is taken into account.
3. Public Auditing with Complete Data Dynamics support	PKC-based homomorphic authenticator is used to outfit the verification protocol.	Basic Markle Hash Tree (MHT) is manipulated for block tag authentication.	Computation cost of BLS scheme is prominent.
4. Efficient Third Party Auditing (TPA)	Novel and uniform security structure. Storage security is accomplished by utilizing BLS algorithm.	Auditor performs auditing jobs for different users at the same.	Unable to support both public verification and dynamic data correctness.
5. Dynamic Storage way in Cloud Computing	New protocol system using the data reading protocol algorithm. Multi server data comparison algorithm to recover data.	Integrity can be verified before and after data insertion.	TPA is not considered for integrity checking process.
6. Effective and Secure Storage Protocol	Efficient and secure storage protocol is implemented by utilizing Elliptic curve cryptography and Sobol Sequence	Block level data dynamic operations are also used to maintain the same security assurance.	Elliptic Curve Cryptography scheme is only suitable for devices with restricted low power.
7. Storage Security of data	Uniform and modern structure of security for different cloud types. SHA Hash, GZIP algorithm and SFSPL algorithm.	Provided data backups for data recovery. Includes essential security services such as authentication, encryption and decryption and compression.	Data back ups are available at multiple servers. So there is a chance for servers to behave unreliably.
8. Secure and Dependable Storage Services	Homomorphic token with Reed-Solomon erasure correcting code.	Guaranteed the correctness insurance and also identified the immoral server behavior.	Gross overhead approximately stays equal with other.
9. Optimal Cloud Storage Systems	Taxonomic approach for achieving cloud storage service optimality. Proposed a new NubiSave prototype	Proposed generic architecture served as blueprint for optimal storage controller. NubiSave is available freely.	NubiSave is needs to integrate with frontends for future research.
10. Process of access and store small files with storage	Prefetching technique should be used to make better access efficiency.	Improves the access ability of small files. Cut-off point is measured to improve I/O performance	Formula for cut-off point not available. It will be identified in future.
11. File Storage Security Maintenance	Distributed scheme contains master server and a set of slave servers. Token generation algorithm and merging algorithm are used.	File chunking operation is carried out to provide data backup in case of server failure.	Data chunks are stored in slave server will lead to an opportunity of corrupting data by servers.
12. File Assured Deletion (FADE) for Secure Storage	Conjunctive and disjunctive policies are used for file recovering process.	Support for dynamic data operations and meta data overhead is less.	Time and Space are the major overhead of this scheme.
13. Accessing outsourced data efficiently	An Owner-write-user-read Scenario for accessing data.	Original data owner be only able to update/ modify their data.	Combination of multiple policies is not supported.

IV. CONCLUSION AND FUTURE WORK

Over the any kind of Internet worldwide, cloud storage services offered wide range of storage services and resources to use for any individual or big organizations. Even if this cloud services delivers many advantages to end users, on other hand it is vulnerable to many challenges. Security is one of them which are major as compared to others. The current research problem of cloud computing is privacy preservation and security. In this review paper we have presented the study over different methods presented so far for the cloud storage security as well as discussed the different challenges of cloud computing. For the future work we further suggest to work improved security solution for security of storage in cloud computing.

V. REFERENCES

1. Parakh A and Kak S (2009). Online data storage using implicit security Information Sciences, vol 179(19), 3323–3331.
2. Li H, Dai Y et al. (2009), Identity-Based Authentication for Cloud Computing, M. G. Jaatun, G. Zhao, and C. Rong (Eds.): Cloud Computing, Lecture Notes in Computer Science, vol 5931, 157–166.
3. Wang Q, Wang C et al. (2011). Enabling Public Audit ability and Data Dynamics for Storage Security in Cloud Computing, IEEE Transactions on Parallel and Distributed Systems, vol 22(5), 847–859.
4. Balakrishnan S, Saranya G, et al. (2011). Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud, International Journal of Computer Science and Technology, vol 2(2), 397–400. 5. Dinesh C (2011). Data Integrity and Dynamic Storage Way in Cloud Computing, Distributed, Parallel, and Cluster Computing.
5. Kumar S P, Subramanian R (2011)**.** An efficient and secure protocol for ensuring data storage security in Cloud Computing, International Journal of Computer Science Issues, vol 8(6), No 1, 261–274.
6. Sajithabanu S, Raj E G P (2011). Data Storage Security in Cloud, International Journal of Computer Science and Technology, vol 2(4), 436–440.
7. Wang C, Wang Q et al. (2012), Toward Secure and Dependable Storage Services in Cloud Computing, IEEE Transactions on Services Computing, vol 5(2), 220–232.
8. Spillner J, Müller J et al. (2012), Creating optimal cloud storage systems, Future Generation Computer Systems, vol 29(4), 1062–1072. Dong B Zheng Q et al. (2012). An optimized approach for storing and accessing small files on cloud storage, Journal of Network and Computer Applications, 35 (6), 1847–1862.
9. Deshmukh P M, Gughane A S et al. (2012). Maintaining File Storage Security in Cloud Computing International Journal of Emerging Technology and Advanced Engineering, vol 2(10), 2250–2459.
10. Tang Y, Lee P C et al (2010). FADE: a secure overlay cloud storage system with File Assured Deletion, 6th International ICST Conference, and Secure Comm.
11. Wang W, Li Z et al. (2009). Secure and Efficient Access to Outsourced Data, CCSW '09 Proceedings of the 2009 ACM workshop on Cloud computing security, 55–66.
12. A Platform Computing Whitepaper. "Enterprise Cloud Computing: Transforming IT."$ *Platform Computing*, pp6, 2010.
13. Global Netoptex Incorporated. "Demystifying the cloud. Important opportunities, crucial choices." pp4-14. Available: http://www.gni.com [Dec. 13, 2009].
14. M. Klems, A. Lenk, J. Nimis, T. Sandholm and S. Tai. "What's Inside the Cloud? An Architectural Map of the Cloud Landscape." *IEEE Explore*, pp 23-31, Jun. 2009.
15. C. Weinhardt, A. Anandasivam, B. Blau, and J. Stosser. "Business Models in the Service World." *IT'S Professional*, vol. 11, pp. 28-33, 2009.
16. N. Gruschka, L. L. Iancono, M. Jensen and J. Schwenk. "On Technical Security Issues in Cloud Computing" In PROC 09 IEEE International Conference on Cloud Computing, 2009 pp 110-112.
17. N. Leavitt. "Is Cloud Computing Really Ready for Prime Time?" *Computer*, vol. 42, pp. 15-20, 2009.
18. M. Jensen, J. Schwenk, N. Gruschka and L. L. Iacono, "On Technical Security Issues in Cloud Computing." in PROC IEEE ICCC, Bangalore 2009, pp. 109-116.
19. C. Soghoian. "Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era" The Berkman Center for Internet & Society Research Publication Series. Available: http://cyber.law.harvard.edu/publications [Aug.22, 2009].