EasyChair Preprint

№ 6741

Cloud Computing Security Challenges And Issues

Akhilesh Saini

October 3, 2021

Cloud Computing Security Challenges And Issues

#Dr. Akhilesh Saini

* *Associate Professor (Computer Science), Ch. K.R.Godara Memorial College, Bashir,Tibbi, India*

***Abstract*—** All the major promises of the cloud -- improved IT efficiency, flexibility and scalability -- come with one major challenge: security.Many organizations can't delineate where cloud service provider (CSP) responsibilities end and their own responsibilities begin, opening them to numerous vulnerabilities. The increased expansiveness of the cloud also increases an organization's potential attack surface. To further complicate the matter, traditional security controls often don't fulfill cloud security needs. Cloud computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. Usually cloud computing services are delivered by a third party provider who owns the infrastructure. It advantages to mention but a few include scalability, resilience, flexibility, efficiency and outsourcing non-core activities. Cloud computing offers an innovative business model for organizations to adopt IT services without upfront investment. Despite the potential gains achieved from the cloud computing, the organizations are slow in accepting it due to security issues and challenges associated with it. Security is one of the major issues which hamper the growth of cloud.

I. INTRODUCTION

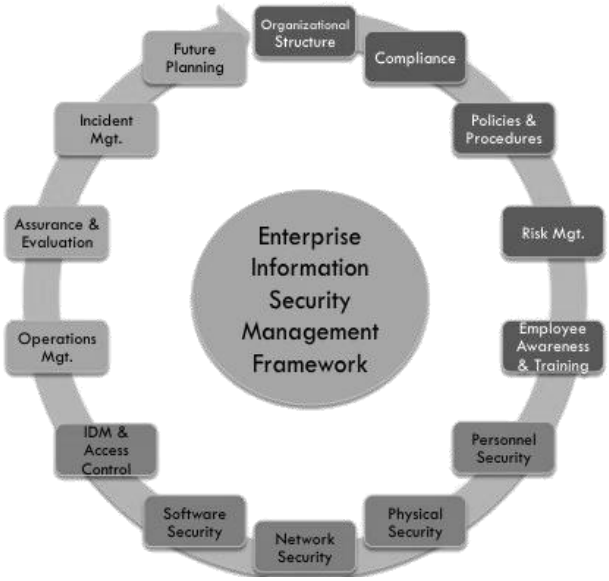
The cloud computing is a new computing model that provides the uniform access to wide area distributed resources on demand. The emergence of cloud computing has made a tremendous impact on the Information Technology (IT) industry over the past few years, where large companies such as Google, Amazon and Microsoft strive to provide more powerful, reliable and cost-efficient cloud platforms, and business enterprises seek to reshape their business models to gain benefit from this new paradigm[1]. However, there still exist many problems in cloud computing today. A recent survey by Cloud Security Alliance (CSA) shows that security have become the primary concern for people to shift to cloud computing.

For years the Internet has been represented on network diagrams by a cloud symbol until 2008 when a variety of new services started to emerge that permitted computing resources to be accessed over the Internet termed cloud computing. Cloud computing encompasses activities such as the use of social networking sites and other forms of interpersonal computing; however, most of the time cloud computing is concerned with accessing online software applications, data storage and processing power. Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It extends Information Technology's (IT) existing capabilities. In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Despite of all the hype surrounding the cloud, customers are still reluctant to deploy their business in the cloud.

EIS Security Solutions

Controlling access and utilization of shared assets are the most significant objectives of security models in a common system. With the extension of PC systems the mentality towards data security and other shared assets has entered another stage**.** Data security innovation arrangements can be named either proactive to forestall activities before the event of the issue (e.g., cryptography, computerized signature, hostile to infection) or receptive enough to react after the event of security issue (e.g., firewalls, passwords). They are actualized at the accompanying model levels: system, host and application levels**.**

A comprehensive methodology mulling over regions appeared in following just as a model point of view must be taken to guarantee security:-



Security Architecture for Cloud Computing

The NIST Cloud Computing reference engineering characterizes five significant entertainers in the cloud:

CLOUD CUSTOMER
CLOUD SUPPLIER
CLOUD TRANSPORTER
CLOUD REVIEWER
CLOUD INTERMEDIARY.

This part examines the standard systems **(RBAC, ABAC, TBAC)** and conventions (SAML and trust model) for the trading of verification, approval and quality information utilized in this theory. It likewise presents the arrangement language (XACML), and the theoretical order structure for recognizing cloud get to control necessities. XACML is utilized for the particular of approaches as a result of its expressiveness and adaptability in indicating access control arrangements.

Theoretical Classification Framework :-

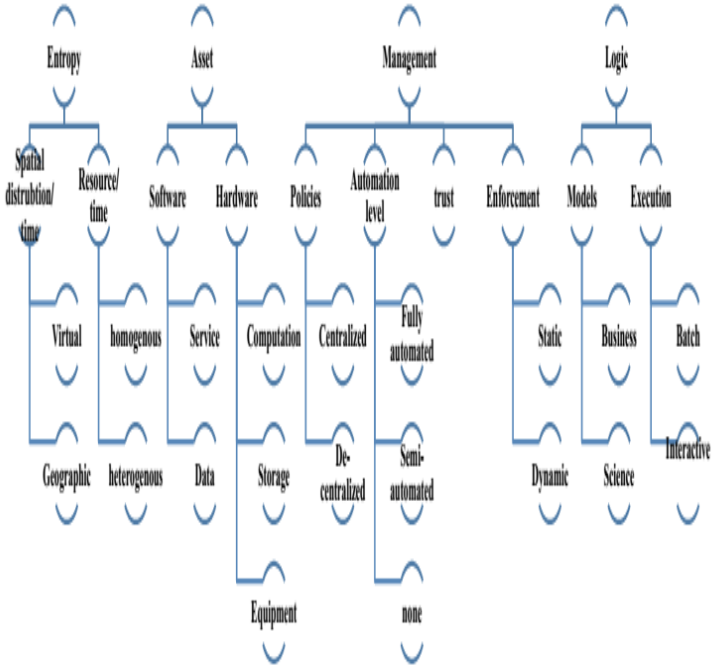
The conceptual categorization identifies and groups requirements into four different abstraction layers. Classification of the layers is as shown

Entropy layer: The entropy layer identifies requirements from the virtual and geographic dispersion of objects in a system.

Assets layer: The asset layer identifies requirements from the type of shared objects within the boundary of the entropy layer.

Management layer: The management layer defines requirements from Plan management. It is used to fulfil the need for capturing security issues raised from the management of policies and trust relationships among objects.

Logic layer: The logic layer incorporates requirements that are not handled by the former layers.



a new architecture suitable for the cloud is proposed. We first define the access control requirements for a generic Cloud Computing scenario based on proposed conceptual categorization framework and then, make a comparison of existing access control models used for the cloud environment to determine their applicability. The results of our analysis are used to develop a System-Based Association Model suitable for the cloud.

Proposed Access Control Architecture

The following the proposed get to control design, which involves the accompanying structural segments:

•Context Handler goes about as a correspondence transport by making a common setting between segments,

•Policy Decision Point (PDP) settles on an entrance control choice by assessing the solicitation against the accessible

strategies,

•Policy Enforcement Point (PEP) advances they got solicitations to PDP and authorizes the commitments came back from PDP,

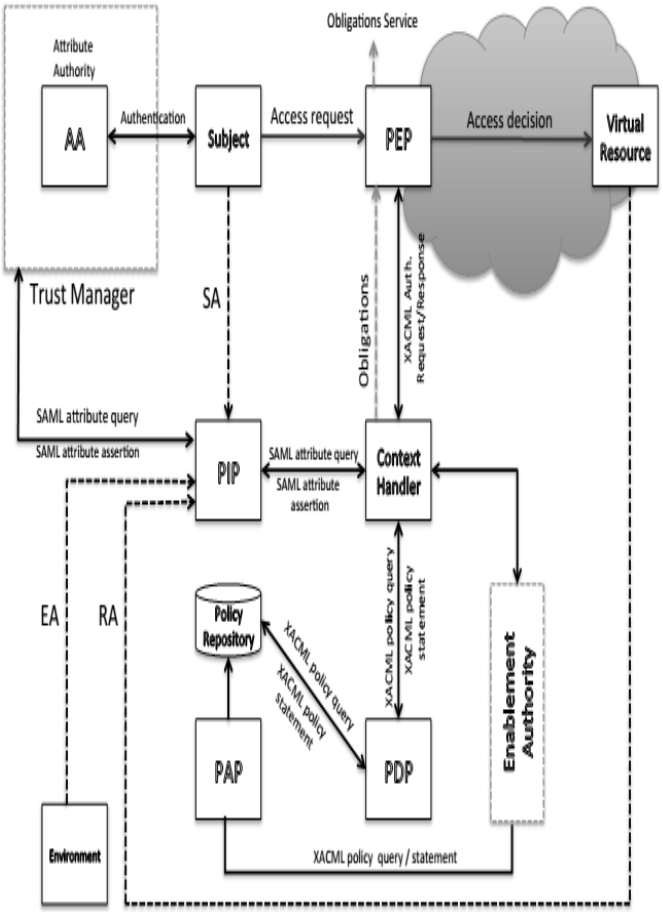
•Policy Administration Point (PAP) makes the strategies accessible to PDP

•Policy Information Point (PIP) recovers the quality qualities mentioned by setting handler.

•Trust Manager: This administration reacts to demands for characteristics in type of SAML quality questions.

•Role Enablement Authority: This is answerable for appointing jobs to clients and for empowering jobs for use inside a client's meeting, Policies are utilized to figure out which clients are permitted to empower which jobs and under which conditions. The jobs are communicated utilizing characteristics.

Among these segments, PEP and PDP are of specific significance as they are the segments where state data can be kept up.



Security Issues Based on the Delivery and Deployment Model of Cloud In SaaS, providers are more responsible for security. The clients have to depend on providers for security measures. As public cloud is less secure than private clouds, the stronger security measures are required in public cloud. Also in SaaS, it becomes difficult for the user to ensure that proper security is maintained or not. Private clouds could also demand more extensibility to accommodate customized requirements. The following key security elements [11] should be carefully considered as an integral part of the SaaS application development and deployment process: i) Data security

ii) Data locality

iii) Data integrity

iv) Data segregation

v) Data access

vi) Data confidentiality

vii) Network security

viii) Authentication and authorization

ix) Availability

x) Identity management and sign-on process In PaaS,

customers are able to build their own applications on top of the platforms provided. Thus it is the responsibility of the customers to protect their applications as providers are only responsible for isolating the customers' applications and workspaces from one another . So, maintaining the integrity of applications and enforcing the authentication checks are the fundamental security requirements in PaaS. IaaS is mainly used as a delivery model. The major security concern in IaaS is to maintain the control over the customer's data that is stored in provider's hardware. The consumers are responsible for securing the operating systems, applications, and content. The cloud provider must provide low-level data protection capabilities.Based upon the deployment model, public clouds are less secure than the other cloud models as it allows users to access the data across wide area network. In public cloud, additional security measurements like trust are required to ensure all applications and data accessed on the public cloud are not subjected to malicious attacks . Utilization on the private cloud can be much more secure than that of the public cloud because of it is specified for some particular organization. A hybrid cloud is a private cloud linked to one or more public clouds. Hybrid clouds provide more secure control of the data and applications

as each and everything is centrally managed. Each of the security requirements will be highlighted below in context of cloud computing:

A. Authorization:- Authorization is an important information security requirement in Cloud computing to ensure referential integrity is maintained. It follows on in exerting control and privileges over process flows within cloud computing. In case of public cloud, multiple customers share the computing resources provided by a single service provider. So proper authorization is required irrelevant of the delivery model used. In private cloud, authorization is maintained by the system administrator.

B. Identification & authentication:- As the major concerns in public and private cloud include internal and external threats, data collection, privacy and compliance, so, it is the cloud service provider's ability to have a secure infrastructure to protect customer data and guard against unauthorized access. We need to have some identification and authentication process to verifying and validating individual cloud users based upon their credentials before accessing any data over the cloud. That's why identification and authentication is mandatory security requirement in public and private cloud.

C. Integrity:- The integrity requirement lies in applying the due diligence within the cloud domain mainly when accessing data. Therefore ACID (atomicity, consistency, isolation and durability) properties of the cloud's data should without a doubt be robustly imposed across all Cloud computing delivery models.

D.- Confidentiality In Cloud computing, confidentiality plays a major part especially in maintaining control over organizations' data situated across multiple distributed databases. Asserting confidentiality of users' profiles and protecting their data, that is virtually accessed, allows for information security protocols to be enforced at various different layers of cloud applications. Cloud Computing Security Issues and Challenges: A Survey 451 Data confidentiality is one of the most difficult things to guarantee in a public cloud computing environment. There are several reasons for that: First, as public clouds grow, the number of people working for the cloud provider who actually have access to customer data (whether they are entitled to it or not) grows as well, thereby multiplying the number of potential sources for a confidentiality breach. Second, the needs for elasticity, performance, and fault-tolerance lead to massive data duplication and require aggressive data caching, which in turn multiply the number of targets a data thief can go after. Third, end-to-end data encryption is not yet available. So, data confidentiality will be maximized by using a large number of private clouds managed by trusted parties.

E. Availability:- Availability is one of the most critical information security requirements in Cloud computing because it is a key decision factor when deciding among private, public or hybrid cloud vendors as well as in the delivery models. The service level agreement is the most important document which highlights the trepidation of availability in cloud services and resources between the cloud provider and client. The goal of availability for Cloud Computing systems (including applications and its infrastructures) is to ensure its users can use them at any time, at any place. Many Cloud Computing system vendors provide Cloud infrastructures and platforms based on virtual machines. So availability is a mandatory security requirement for IaaS and PaaS whether the public cloud is used or private cloud. As in private cloud, all services are internal to the enterprise, so availability is also required when SaaS is to be used. F. Non-repudiation Non-repudiation in cloud computing can be obtained by applying the traditional ecommerce security protocols and token provisioning to data transmission within cloud applications such as digital signatures, timestamps and confirmation receipts services (digital receipting of messages confirming data sent/received).

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

A. **Security:** It is clear that the security issue has played the most important role in hindering Cloud computing acceptance. Without doubt, putting your data, running your software on someone

else's hard disk using someone else's CPU appears daunting to many. Well-known security issues such as data loss, phishing, botnet (running remotely on a collection of machines) pose serious threats to organization's data and software. Moreover, the multi-tenancy model and the pooled computing resources in cloud computing has introduced new security challenges that require novel techniques to tackle with. For example, hackers can use Cloud to organize botnet as Cloud often provides more reliable infrastructure services at a relatively cheaper price for them to start an attack.

B. Costing Model: Cloud consumers must consider the tradeoffs amongst computation, communication, and integration. While migrating to the Cloud can significantly reduce the infrastructure cost, it does raise the cost of data communication, i.e. the cost of transferring an organization's data to and from the public and community Cloud and the cost per unit of computing resource used is likely to be higher. This problem is particularly prominent if the consumer uses the hybrid cloud deployment model where the organization's data is distributed amongst a number of public/private (in-house IT infrastructure)/community clouds. Intuitively, ondemand computing makes sense only for CPU intensive jobs.

C. Charging Model: The elastic resource pool has made the cost analysis a lot more complicated than regular data centers, which often calculates their cost based on consumptions of static computing. Moreover, an instantiated virtual machine has become the unit of cost analysis rather than the underlying physical server. For SaaS cloud providers, the cost of developing multitenancy within their offering can be very substantial. These include: re-design and redevelopment of the software that was originally used for single-tenancy, cost of providing new features that allow for intensive customization, performance and security enhancement for concurrent user access, and dealing with complexities induced by the above changes. Consequently, SaaS providers need to weigh up the trade-off between the provision of multitenancy and the cost-savings yielded by multi-tenancy such as reduced overhead through amortization, reduced number of on-site software licenses, etc. Therefore, a strategic and viable charging model for SaaS provider is crucial for the profitability and sustainability of SaaS cloud providers.

D. Service Level Agreement (SLA): Although cloud consumers do not have control over the underlying computing resources, they do need to ensure the quality, availability, reliability, and performance of these resources when consumers have migrated their core business functions onto their entrusted cloud. In other words, it is vital for consumers to obtain guarantees from providers on service delivery. Typically, these are provided through Service Level Agreements (SLAs) negotiated between the providers and consumers. The very first issue is the definition of SLA specifications in such a way that has an appropriate level of granularity, namely the tradeoffs between expressiveness and complicatedness, so that they can cover most of the consumer expectations and is relatively simple to be weighted, verified, evaluated, and enforced by the resource allocation mechanism on the cloud. In addition, different cloud offerings (IaaS, PaaS, and SaaS) will need to define different SLA metaspecifications. This also raises a number of implementation problems for the cloud providers. Furthermore, advanced SLA mechanisms need to constantly incorporate user feedback and customization features into the SLA evaluation framework

E. What to migrate: Based on a survey (Sample size = 244) conducted by IDC in 2008, 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. Currently, peripheral functions such as IT management and personal applications are the easiest IT systems to move. Organizations are conservative in employing IaaS compared to SaaS. This is partly because marginal functions are often outsourced to the Cloud, and core activities are kept in-house. The survey also shows that in three years time, 31.5% of the organization will move their Storage Capacity to the cloud. However this number is still relatively low compared to Collaborative Applications (46.3%) at that time.

F. Cloud Interoperability Issue: Currently, each cloud offering has its own way on how cloud clients/applications/users interact with the cloud, leading to the "Hazy Cloud" phenomenon. This severely hinders the development of cloud ecosystems by forcing vendor locking, which prohibits the ability of users to choose from alternative vendors/offering simultaneously in order to optimize resources at different levels within an organization. More importantly, proprietary cloud APIs makes it very difficult to integrate cloud services with an organization's own existing legacy systems (e.g. an on-premise data centre for highly interactive modeling applications in a pharmaceutical company).The primary goal of interoperability is to realize the seamless fluid data across clouds and between cloud and local applications. There are a number of levels that interoperability is essential for cloud computing. First, to optimize the IT asset and computing resources, an organization often needs to keep in-house IT assets and capabilities associated with their core competencies while outsourcing marginal functions and activities (e.g. the human resource system) on to the cloud. Second, more often than not, for the purpose of optimization, an organization may need to outsource a number of marginal functions to cloud services offered by different vendors. Standardization appears to be a good solution to address the interoperability issue. However, as cloud computing just starts to take off, the interoperability problem has not appeared on the pressing agenda of major industry cloud vendors.

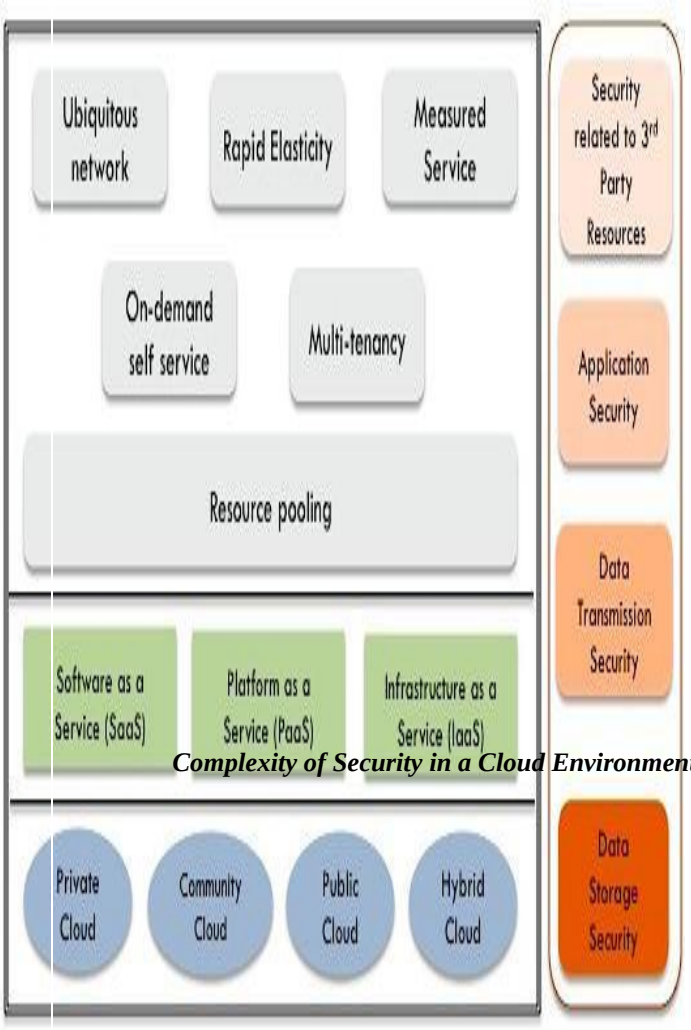
CLOUD COMPUTING SAFETY MEASURES

Cloud computing security is an emerging sub-area of PC security, security management, and much more comprehensively, data security. This refers to a comprehensive collection of techniques, developments, and controls conveyed to secure information, applications, and the associated Cloud Computing environment ***(Reeja, 2012)***. With regard to this research, it involves understanding how approaches can be applied in the cloud to resolve interesting dangers and challenges along these lines, affirming data protection. This section discusses Cloud Computing, its security issues and benefits. It presents Cloud Computing protection to be controlled as a response and presents models that have been recognised for use within the cloud situation to be controlled.

Cloud computing is progressing as an aid. It helps businesses to scale assets all over as they require (i.e., the "pay-more only as costs occur" model of figuring), making data protection an important requirement for cloud-based administrations. As problems acquired from virtualization and SOA progresses, the multitenant definition of the cloud is powerless against data gaps, dangers and tackles ***(Grundy and Miller, 2010)*** and in this way, it is imperative to have strong access control approaches set up to preserve the confidentiality, trustworthiness and accessibility of information.

Figure 3.1 ***(Subashini and Kavitha, 2011)*** demonstrates the difficulty of protection in the cloud domain. The lower layer refers to the various cloud organisation models, especially private, network, open and half and half cloud. The following layer speaks to the unique SaaS, PaaS, and IaaS conveyance models. The conveyance models

structure the cloud core, showing certain characteristics, such as quick versatility, estimated administration, on-demand self-administration, multi-tenure and asset pooling, each layer has different security needs ***(Subashini and Kavitha, 2011)***. The cloud system can be ensured by illuminating the security problems of SaaS, PaaS and IaaS by implication, as indicated by Asma, Chaurasia & Mokhtar (2012), and adequate security can be achieved by understanding the data, virtualized state and security issues of correspondence.



Complexity of Security in a Cloud Environment

CONCLUSION:- Although Cloud computing can be seen as a new phenomenon which is set to revolutionise the way we use the Internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human's lives easier. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. Cloud computing is no exception. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future. Many enhancements in existing solutions as well as more mature and newer solutions are urgently needed to ensure that cloud computing benefits are fully realized as its adoption accelerates. Cloud computing is still in its infancy, and how the security and privacy landscape changes will impact its successful, widespread adoption.

References

1. Mell P, Grance T. The NIST definition of cloud computing. *Commun ACM.* 2010;53(6):50. [Google Scholar]
2. Brown A, Weihl B. *Official Google Blog.* 2011. Jun 24, [2011-08-05]. *webcite* An Update on Google Health and Google PowerMeter http://googleblog.blogspot.com/2011/06/update-on-google-health-and-google.html.
3. Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M. A view of cloud computing. *Commun ACM.* 2010;53(4):50–58. doi: 10.1145/1721654.1721672. [CrossRef] [Google Scholar]
4. Technology firms and health care: heads in the cloud: digitising America's health records could be a huge business Will it? *The Economist (US)* 2011;399(8727):63. [Google Scholar]
5. Li ZJ, Chen C, Wang K. Cloud computing for agent-based urban transportation systems. *IEEE Intell Syst.* 2011;26(1):73–79. [Google Scholar]
6. Behrend TS, Wiebe EN, London JE, Johnson EC. Cloud computing adoption and usage in community colleges. *Behav Inf Technol.* 2011;30(2):231–240. doi: 10.1080/0144929X.2010.489118. [CrossRef] [Google Scholar]
7. *DarkGovernment.* 2009. Jul 23, [2011-07-11]. *webcite* NSA Embraces Cloud Computing http://www.darkgovernment.com/news/nsa-embraces-cloud-computing.
8. Chatman C. How cloud computing is changing the face of health care information technology. *J Health Care Compliance.* 2010 Jun;12(3):37–70. [Google Scholar]
9. Dudley JT, Pouliot Y, Chen R, Morgan AA, Butte AJ. Translational bioinformatics in the cloud: an affordable alternative. *Genome Med.* 2010;2(8):51. doi: 10.1186/gm172. http://www.genomemedicine.com/content/2/8/51.gm172 [PMC free article] [PubMed] [CrossRef] [Google Scholar]
10. Schweitzer EJ. Reconciliation of the cloud computing model with US federal electronic health record regulations. *J Am Med Inform Assoc.* 2011 Jul 4; doi: 10.1136/amiajnl-2011-000162.amiajnl-2011-000162 [PMC free article] [PubMed] [CrossRef] [Google Scholar]
11. Haughton J. Year of the underdog: Cloud-based EHRs. *Health Manag Technol.* 2011;32(1):9. [Google Scholar]
12. Kabachinski J. What's the forecast for cloud computing in healthcare? *Biomed Instrum Technol.* 2011;45(2):146–50. doi: 10.2345/0899-8205-45.2.146. [PubMed] [CrossRef] [Google Scholar]
13. Rosenthal A, Mork P, Li MH, Stanford J, Koester D, Reynolds P. Cloud computing: a new business paradigm for biomedical information sharing. *J Biomed Inform.* 2010 Apr;43(2):342–53. doi: 10.1016/j.jbi.2009.08.014.S1532-0464(09)00115-4 [PubMed] [CrossRef] [Google Scholar]
14. Anderson NR, Lee ES, Brockenbrough JS, Minie ME, Fuller S, Brinkley J, Tarczy-Hornoch P. Issues in biomedical research data management and analysis: needs and barriers. *J Am Med Inform Assoc.* 2007;14(4):478–88. doi: 10.1197/jamia.M2114. http://jamia.bmj.com/cgi/pmidlookup?view=long&pmid=17460139.M2114 [PMC free article] [PubMed] [CrossRef] [Google Scholar]
15. Dudley JT, Butte AJ. In silico research in the era of cloud computing. *Nat Biotechnol.* 2010 Nov;28(11):1181–5. doi: 10.1038/nbt1110-1181.nbt1110-1181 [PMC free article] [PubMed] [CrossRef] [Google Scholar]
16. Wall DP, Kudtarkar P, Fusaro VA, Pivovarov R, Patil P, Tonellato PJ. Cloud computing for comparative genomics. *BMC Bioinformatics.* 2010;11:259. doi: 10.1186/1471-2105-11-259. http://www.biomedcentral.com/1471-2105/11/259.1471-2105-11-259 [PMC free article] [PubMed] [CrossRef] [Google Scholar]
17. Schatz MC, Langmead B, Salzberg SL. Cloud computing and the DNA data race. *Nat Biotechnol.* 2010 Jul;28(7):691–3. doi: 10.1038/nbt0710-691.nbt0710-691 [PMC free article] [PubMed] [CrossRef] [Google Scholar]
18. Avila-Garcia MS, Trefethen AE, Brady M, Gleeson F, Goodman D. Lowering the barriers to cancer imaging. eScience 2008: IEEE 4th International Conference on eScience; The 4th IEEE International Conference on eScience; December 8-12, 2008; Indiana, USA. New York, NY: IEEE; 2008. [CrossRef] [Google Scholar]
19. Bateman A, Wood M. Cloud computing. *Bioinformatics.* 2009 Jun 15;25(12):1475. doi: 10.1093/bioinformatics/btp274. http://bioinformatics.oxfordjournals.org/cgi/pmidlookup?view=long&pmid=19435745.btp274 [PubMed] [CrossRef] [Google Scholar]
20. Kudtarkar P, Deluca TF, Fusaro VA, Tonellato PJ, Wall DP. Cost-effective cloud computing: a case study using the comparative genomics tool, roundup. *Evol Bioinform Online.* 2010;6:197–203. doi: 10.4137/EBO.S6259. http://www.la-press.com/article.php?article_id=2422. [PMC free article] [PubMed] [CrossRef] [Google Scholar]
21. Memon FN, Owen AM, Sanchez-Graillet O, Upton GJ, Harrison AP. Identifying the impact of G-quadruplexes on Affymetrix 3' arrays using cloud computing. *J Integr Bioinform.* 2010;7(2):111. doi: 10.2390/biecoll-jib-2010-111.421 [PubMed] [CrossRef] [Google Scholar]

22. Vaquero LM, Rodero-Merino L, Caceres J, Lindner M. A break in the clouds: towards a cloud definition. *ACM SIGCOMM Comput Commun Rev.* 2008 Jan;39(1):50–55. doi: 10.1145/1496091.1496100. [CrossRef] [Google Scholar]
23. Iyer B, Henderson JC. Preparing for the future: understanding the seven capabilities of cloud computing. *MIS Q Exec.* 2010;9(2):117–131. [Google Scholar]
24. Vouk MA. Cloud computing: issues, research and implementations. *J Comput Inf Technol.* 2008;16(4):235–246. doi: 10.2498/cit.1001391. [CrossRef] [Google Scholar]
25. Han Y. On the clouds: a new way of computing. *Inf Technol Libr 2010 June; 87-92.* 2010 Jun 1;29(2) [Google Scholar]
26. Cervone HF. An overview of virtual and cloud computing. *OCLC Syst Serv.* 2010;26(3):162–165. doi: 10.1108/10650751011073607. [CrossRef] [Google Scholar]
27. IBM and Juniper Networks Solutions Brief *IBM Global Services.* 2009. [2011-07-25]. *webcite* IBM and Juniper Networks: Delivering Solutions That Transform Your Networking
Infrastructure ftp://public.dhe.ibm.com/common/ssi/ecm/en/jns03002usen/JNS03002USEN.PDF.
28. Sittig DF, Singh H. Eight rights of safe electronic health record use. *JAMA.* 2009 Sep 9;302(10):1111–3. doi: 10.1001/jama.2009.1311.302/10/1111 [PubMed] [CrossRef] [Google Scholar]
29. Wang X, Tan Y. Application of cloud computing in the health information system. Proceedings of the 2010 International Conference on Computer Application and System Modeling (ICCASM); International Conference on Computer Application and System Modeling; October 22-24, 2010; Taiyuan, China. New York, NY: IEEE; 2010. [CrossRef] [Google Scholar]
30. He C, Jin X, Zhao Z, Xiang T. A cloud computing solution for hospital information system. Proceedings of the 2010 IEEE International Conference on Intelligent Computing and Intelligent Systems (ICIS); IEEE International Conference on Intelligent Computing and Intelligent Systems (ICIS 2010); October 29-31, 2010; Xiamen, China. New York, NY: IEEE; 2010. [CrossRef] [Google Scholar]
31. Botts N, Thoms B, Noamani A, Horan TA. Cloud computing architectures for the underserved: public health cyberinfrastructures through a network of healthATMs. Proceedings of the 2010 43rd Hawaii International Conference on System Sciences (HICSS); The 43rd Hawaii International Conference on System Sciences; January 5-8 , 2010; Hawaii, USA. New York, NY: IEEE; 2010. [CrossRef] [Google Scholar]
32. Yang CT, Chen LT, Chou WL, Wang KC. Implementation of a medical image file accessing system on cloud computing. Proceedings of the 2010 IEEE 13th International Conference on Computational Science and Engineering (CSE); The 13th IEEE International Conference on Computational Science and Engineering; December 11-13, 2010; Hong Kong, China. New York, NY: IEEE; 2010. [CrossRef] [Google Scholar]
33. Hoang DB, Chen L. Mobile cloud for assistive healthcare (MoCAsH). Proceedings of the; the IEEE Asia-Pacific Services Computing Conference; December 6-10 , 2010; Hangzhou, China. Asia-Pacific: :; 2010. [CrossRef] [Google Scholar]
34. Guo L, Chen F, Chen L, Tang X. The building of cloud computing environment for e-health. Proceedings of the 2010 International Conference on E-Health Networking, Digital Ecosystems and Technologies (EDT); The IEEE International Conference on E-Health Networking; July 1-3, 2010; Lyon, France. New York, NY: IEEE; 2010. [CrossRef] [Google Scholar]
35. Alagoz F, Valdez AC, Wilkowska W, Ziefle M, Dorner S, Holzinger A. From cloud computing to mobile Internet, from user focus to culture and hedonism: the crucible of mobile health care and wellness applications. Proceedings of the 2010 5th International Conference on Pervasive Computing and Applications (ICPCA); The 5th International Conference on pervasive Computing and Applications (ICPCA); December 1-3, 2010; Maribor, Slovenia. New York, NY: IEEE; 2010. [CrossRef] [Google Scholar]
36. Rolim CO, Koch FL, Westphall CB, Werner J, Fracalossi A, Salvador GS. A cloud computing solution for patient's data collection in health care institutions. In: Proceedings of the 2nd International Conference on eHealth, Telemedicine, and Social Medicine; February 10-16, 2010; New York, NY: IEEE. 2010. Feb 10, [CrossRef] [Google Scholar]
37. Nkosi MT, Mekuria F. Cloud computing for enhanced mobile health applications. Proceedings of the 2010 IEEE 2nd International Conference on Cloud Computing Technology and Science (CloudCom); The 2nd IEEE International Conference on Cloud Computing Technology and Science; Nov 30- Dec 3, 2010; Indianapolis, USA. New York, NY: IEEE; 2010. [CrossRef] [Google Scholar]
38. Rao GSVRK. Sundararaman K, Parthasarathi J. Dhatri: a pervasive cloud initiative for primary healthcare services. Proceedings of the 2010 14th International Conference on Intelligence in Next Generation Networks (ICIN); The 14th IEEE International Conference on Intelligence in Next Generation Networks (ICIN); October 11-14, 2010; Berlin, Germany. New York, NY: IEEE; 2010. [CrossRef] [Google Scholar]
39. Koufi V, Malamateniou F, Vassilacopoulos G. Ubiquitous access to cloud emergency medical services. Proceedings of the 2010 10th IEEE International Conference on Information

Technology and Applications in Biomedicine (ITAB); The 10th IEEE International Conference on Information Technology and Applications in Biomedicine (ITAB); November 3-5, 2010; Corfu, Greece. New York, NY: IEEE; 2010. [CrossRef] [Google Scholar]
40. Arrais JP, Oliveira JL. On the exploitation of cloud computing in bioinformatics. Proceedings of the 2010 10th IEEE International Conference on Information Technology and Applications in Biomedicine (ITAB); The IEEE 10th International Conference on Information Technology and Applications in Biomedicine (ITAB); November 3-5, 2010; Corfu, Greece. New York, NY: IEEE; 2010. [CrossRef] [Google Scholar]
41. *Amazon Web Services.* 2011. [2011-07-20]. *webcite* AWS Case Study: Harvard Medical School http://aws.amazon.com/solutions/case-studies/harvard/
42. Business Wire *The Free Library.* 2008. [2011-07-25]. *webcite* DiskAgent Launches New Remote Backup and Loss Protection Software as a Service Offering http://www.thefreelibrary.com/DiskAgent(TM)+Launches+New+Remote+Backup+and+Loss+Protection+Software...-a0182194404.
43. Strukhoff R, O'Gara M, Moon N, Romanski P, White E. *SYS-CON Media, Inc.* 2009. Mar 20, [2011-07-18]. *webcite* Cloud Expo: Healthcare Clients Adopt Electronic Health Records with Cloud-Based Services http://cloudcomputing.sys-con.com/node/886530.
44. Editorial Staff *HealthImaging.com.* 2010. Feb 16, [2011-07-19]. *webcite* Acumen Nabs ONC Cloud Computing Contract http://www.healthimaging.com/index.php?option=com_articles&view=article&id=20648:acumen-nabs-onc-cloud-computing-contract&division=hiit.
45. Korea IT Times *IT Times.* 2010. Jul 20, [2011-08-05]. *webcite* Telstra Plans Launch of E-Health Cloud Services, Tip of the Iceberg for Opportunity http://www.koreaittimes.com/story/9826/telstra-plans-launch-e-health-cloud-services-tip-iceberg-opportunity.
46. IBM Press Room *IBM.* 2010. Nov 22, [2011-08-05]. *webcite* European Union Consortium Launches Advanced Cloud Computing Project With Hospital and Smart Power Grid Provider http://www-03.ibm.com/press/us/en/pressrelease/33067.wss.
47. Danek J. *Public Works Government Services Canada.* 2009. Oct 6, [2011-08-05]. *webcite* Cloud Computing and the Canadian Environment http://www.scribd.com/doc/20818613/Cloud-Computing-and-the-Canadian-Environment.
48. Avery P. *IT Business Edge.* 2009. Aug 26, [2011-08-05]. *webcite* Research Indicates Increase in Cloud Computing http://www.itbusinessedge.com/cm/community/kn/blog/research-indicates-increase-in-cloud-computing/?cs=35256.
49. Cherry S. Forecast for cloud computing: up, up, and away. *IEEE Spectrum.* 2009 Oct;46(10):68. [Google Scholar]
50. Bannerman PL. *Proceedings of the 17th Asia Pacific Software Engineering Conference Cloud Workshop.* New York, NY: IEEE; 2010. Cloud Computing Adoption Risks: State of Play; pp. 10–16. [Google Scholar]
51. Armbrust M, Fox A, Griffith R, Joseph AD, Katz RH, Konwinski A, Lee G, Patterson DA, Rabkin A, Stoica I, Zaharia M. *EECS Department, UC Berkeley.* 2009. [2011-09-08]. *webcite* Above the Clouds: A Berkeley View of Cloud Computing. Technical Report http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf.
52. Everett C. Cloud computing: a question of trust. *Comput Fraud Secur.* 2009 Jun 10;(6):5–7. doi: 10.1016/S1361-3723(09)70071-5. [CrossRef] [Google Scholar]
53. Jansen W, Grance T. *National Institute of Standards and Technology, US Department of Commerce.* 2011. Jan, [2011-09-08]. *webcite* Guidelines on Security and Privacy in Public Cloud Computing http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf.
54. European Network and Information Security Agency *ENISA.* 2009. [2011-09-08]. *webcite* Cloud Computing: Benefits, Risks and Recommendations for Information Security http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.
55. Zhang R, Liu L. Security models and requirements for healthcare application clouds. Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing (CLOUD); The 3rd IEEE International Conference on Cloud; July 5-10, 2010; Miami, FL, USA. New York, NY: IEEE; 2010. [CrossRef] [Google Scholar]
56. Baliga J, Ayre RWA, Hinton K, Tucker RS. Green cloud computing: balancing energy in processing, storage, and transport. *Proc IEEE.* 2011;99(1):149–167. doi: 10.1109/JPROC.2010.2060451. [CrossRef] [Google Scholar]
57. Durkee D. Why cloud computing will never be free. *Commun ACM.* 2010;53(5):70–69. doi: 10.1145/1735223.1735243. [CrossRef] [Google Scholar]
58. European Network and Information Security Agency *ENISA.* 2009. Nov, [2011-07-23]. *webcite* An SME Perspective on Cloud Computing: Survey http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-sme-survey/
59. *Microscoft Corp.* 2010. Nov, [2011-09-07]. *webcite* Privacy in the Cloud: A Microsoft Perspective http://www.microsoft.com/privacy/cloudcomputing

.aspx.
60. Google Privacy Center *Google.* 2010. Oct 3, [2011-08-06]. *webcite* Privacy Policy http://www.google.com/google-d-s/intl/en/privacy.html.
61. *Amazon Web Services.* 2008. Oct 01, [2011-08-05]. *webcite* AWS Privacy Notice http://aws.amazon.com/privacy/
62. *Cloud Security Alliance.* 2009. Dec, [2011-07-25]. *webcite* Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 http://www.cloudsecurityalliance.org/csaguide.pdf.
63. *US Department of Health & Human Services.* 1996. [2011-07-26]. *webcite* The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules http://www.hhs.gov/ocr/privacy/
64. *Minister of Justice, Canada.* 2011. Jan 1, [2011-08-05]. *webcite* Personal Information Protection and Electronic Documents Act (PIPEDA) http://laws.justice.gc.ca/PDF/Readability/P-8.6.pdf.
65. *European Commission.* [2011-08-06]. *webcite* EuroPriSe: The European Privacy Seal for IT Products and IT-Based Services https://www.european-privacy-seal.eu/
66. United Nations *United Nations Commission on International Trade Law.* 2010. [2011-08-05]. *webcite* UNCITRAL Legislative Guide on Secured Transactions http://www.uncitral.org/pdf/english/texts/security-lg/e/09-82670_Ebook-Guide_09-04-10English.pdf.
67. Pearson S. Taking account of privacy when designing cloud computing services. Proceedings of the ICSE Workshop on Software Engineering Challenges of Cloud Computing (CLOUD'09); the IEEE First international workshop on software engineering challenges for Cloud Computing (ICSE); May 16-24, 2009; Vancouver, BC, Canada. New York, NY: IEEE; 2009. [CrossRef] [Google Scholar]
68. Svantesson D, Clarke R. Privacy and consumer risks in cloud computing. *Comput Law Secur Rev.* 2010;26(4):391–397. doi: 10.1016/j.clsr.2010.05.005. [CrossRef] [Google Scholar]
69. Mather T, Kumaraswamy S, Latif S. *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice)* Sebastopol, CA: O'Reilly Media, Inc.; 2009. [Google Scholar]
70. Kuner C. Data protection law and international jurisdiction on the Internet (part 1) *Int J Law Inf Technol.* 2010;18(2):176–201. doi: 10.1093/ijlit/eaq002. [CrossRef] [Google Scholar]
71. Ward BT, Sipior JC. The Internet jurisdiction risk of cloud computing. *Inf Syst Manag.* 2010;27(4):334–339. doi: 10.1080/10580530.2010.514248. [CrossRef] [Google Scholar]
72. Financial Crimes Enforcement Network. US Department of Treasury *FinCEN.* [2011-07-13]. *webcite* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001. no date http://www.fincen.gov/statutes_regs/patriot/index.html.
73. Cavoukian A. *Information and Privacy Commissioner, Ontario, Canada.* 2009. Nov, [2011-07-13]. *webcite* A Discussion Paper on Privacy Externalities, Security Breach Notification and the Role of Independent Oversight http://www.ipc.on.ca/images/Resources/privacy_externalities.pdf.
74. *Javelin Strategy & Research.* 2011. [2011-07-23]. *webcite* Data Breach Notifications: Victims Face Four Times Higher Risk of Fraud https://www.javelinstrategy.com/brochure-158.
75. Marks EA, Lozano B. *Executive's Guide to Cloud Computing.* Hoboken, NJ: Wiley; 2010. [Google Scholar]
76. White Paper *Project Management Institute (PMI)* 2011. [2011-07-23]. *webcite* Cloud Computing: The New Strategic Weapon http://www.pmi.org/~/media/PDF/Home/CloudComputing_FINAL.ashx.
77. Stanoevska-Slabeva K, Wozniak T, Hoyer V. Practical guidelines for evolving IT infrastructure towards grids and clouds. In: Stanoevska-Slabeva K, Wozniak T, Ristol S, editors. *Stanoevska- Slabeva K, Wozniak T, Ristol S. editors. Grid and Cloud Computing: A Business Perspective on Technology and Applications.* Berlin: Springer; 2010. pp. 225–243. [Google Scholar]
78. US Department of Health & Human Services. Office of the National Coordinator for Health Information Technology . *The ONC-Coordinated Federal Health IT Strategic Plan: 2008-2012.* Washington, DC: ONC-HIT; 2008. [Google Scholar]
79. Kuo AM, Borycki E, Kushniruk A, Lee TS. A healthcare Lean Six Sigma System for postanesthesia care unit workflow improvement. *Qual Manag Health Care.* 2011;20(1):4–14. doi: 10.1097/QMH.0b013e3182033791.00019514-201101000-00004 [PubMed] [CrossRef] [Google Scholar]
80. Lee TS, Kuo MH. Toyota A3 report: a tool for process improvement in healthcare. *Stud Health Technol Inform.* 2009;143:235–40. [PubMed] [Google Scholar]
81. Marston S, Li Z, Bandyopadhyay S, Zhang J, Ghalsasi A. Cloud computing: the business perspective. *Decis Support Syst.* 2011;51(1):176–189. doi: 10.1016/j.dss.2010.12.006. [CrossRef] [Google Scholar]
82. Buyya R, Ranjan R. Special section: Federated resource management in grid and cloud computing systems. *Future Generation Comput Syst.* 2010;26(8):1189–1191. doi: 10.1016/j.future.2010.06.003. [CrossRef] [Google Scholar]
83. Kuo MH, Kushniruk AW, Borycki EM. Design and implementation of a health data interoperability mediator. *Stud*

Health Technol Inform. 2010;155:101–7. [PubMed] [Google Scholar]
84. Gagliardi F, Muscella S. Cloud computing: data confidentiality and interoperability challenges. In: Antonopoulos N, Gillam L, editors. *Antonopoulos N, Gillam L. editors. Cloud Computing: Principles, Systems and Applications (Computer Communications and Networks)* London: Springer; 2010. pp. 257–270. [Google Scholar]
85. Knowledge@Wharton *Wharton Business School, University of Pennsylvania.* 2009. Apr 1, [2011-07-15]. *webcite* No Man Is an Island: The Promise of Cloud Computing http://knowledge.wharton.upenn.edu/article.cfm?articleid=2190.
86. Creeger M. CTO roundtable: cloud computing. *Commun ACM.* 2009;52(8):50–56. doi: 10.1145/1536616.1536633. [CrossRef] [Google Scholar]
87. Fox A. Computer science. Cloud computing: what's in it for me as a scientist? *Science.* 2011 Jan 28;331(6016):406–7. doi: 10.1126/science.1198981.331/6016/406 [PubMed] [CrossRef] [Google Scholar]
88. Gartner Newsroom *Gartner, Inc.* 2011. Jan 21, [2011-07-14]. *webcite* Gartner Executive Programs Worldwide Survey of More Than 2,000 CIOs Identifies Cloud Computing as Top Technology Priority for CIOs in 2011 http://www.gartner.com/it/page.jsp?id=1526414.