International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-7, Issue-9, September 2021
ISSN: 2395-3470
www.ijseas.com

Opportunities and Challenges of Cloud Computing to Improve Security

#Mr. Akhilesh Saini

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

Abstract— The cloud computing is emerging and developing rapidly both conceptually and in reality, the legal/contractual, economic, service quality, interoperability, security and privacy issues still pose significant challenges. In this chapter, we describe various service and deployment models of cloud computing and identify major challenges. In particular, we discuss three critical challenges: regulatory, security and privacy issues in cloud computing. Some solutions to mitigate these challenges are also proposed along with a brief presentation on the future trends in cloud computing deployment. Cloud computing is a new way of delivering computing resources and services. Many managers and experts believe that it can improve health care services, benefit health care research, and change the face of health information technology. However, as with any innovation, cloud computing should be rigorously evaluated before its widespread adoption.

I. INTRODUCTION

Cloud computing refers to an on-demand, self-service Internet infrastructure that enables the user to access computing resources anytime from anywhere. It is a new model of delivering computing resources, not a new technology. Examples of commonly used non-health care applications include Microsoft Hotmail and Google Docs, while some better known applications in health care include Microsoft HealthVault and Google Health platform (recently discontinued). However, compared with conventional computing, this model provides three new advantages: massive computing resources available on demand, elimination of an up-front commitment by users, and payment for use on a short-term basis as needed . Several articles, forums, and blogs have reported its applications in industry, business, transportation, education, and national security.

Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. There are four basic cloud delivery models, as outlined by NIST (Badger et al., 2011), based on who provides the cloud services. The agencies may employ one model or a combination of different models for efficient and optimized delivery of applications and business services. These four delivery models are: (i) Private cloud in which cloud services are provided solely for an organization and are managed by the organization or a third party. These services may exist off-site. (ii) Public cloud in which cloud services are available to the public and owned by an organization selling the cloud services, for example, Amazon cloud service. (iii) Community cloud in which cloud services are shared by several organizations for supporting a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). These services may be managed by the organizations or a third party and may exist offsite. A special case of community cloud is the Government or G-Cloud. This type of cloud computing is provided by one or more agencies (service provider role), for use by all, or most, government agencies (user role). (iv) Hybrid cloud which is a composition of different cloud computing infrastructure (public, private or community). An example for hybrid cloud is the data stored in private cloud of a travel agency that is manipulated by a program running in the public cloud.

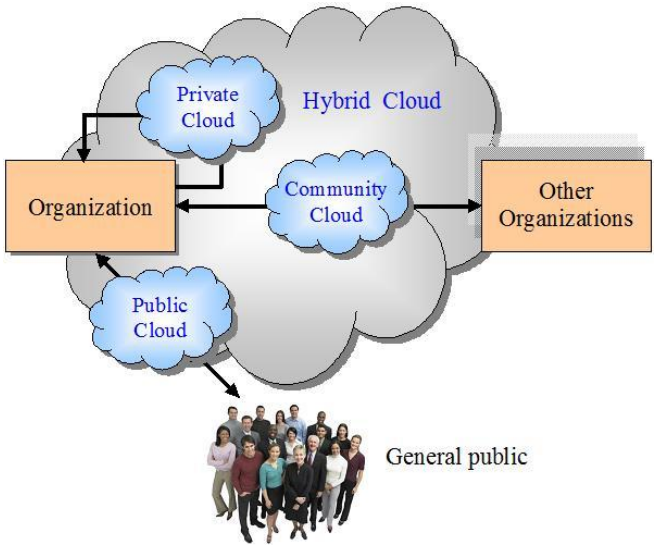
Cloud Computing: A New Economic Computing Model

Cloud computing is still a developing paradigm, and its definition, attributes, and characteristics will evolve over time. Vaquero et al studied more than 20 definitions and tried to extract a consensus definition as well as a minimum definition containing the essential characteristics.

(1) *Software as a service (SaaS):* The applications (eg, EHRs) are hosted by a cloud service provider and made available to customers over a network, typically the Internet.

(2) *Platform as a service (PaaS):* The development tools (eg, operation systems) are hosted in the cloud and accessed through a browser. With PaaS, developers can build Web applications without installing any tools on their computer, and then deploy those applications without any specialized administrative skills.

(3) *Infrastructure as a service (IaaS):* The cloud user outsources the equipment used to support operations, including storage, hardware, servers, and networking components. The provider owns the equipment and is responsible for housing, running, and maintaining it. The user typically pays on a per-use basis.



The cloud computing deployment models.

(1) *Public cloud:* A cloud service provider makes resources (applications and storage) available to the general public over the Internet on a pay-as-you-go basis. For example, the Amazon Elastic Compute Cloud (EC2) allows users to rent virtual computers on which to run their own applications. EC2 runs within Amazon's network infrastructure and data centers and allows customers to pay only for what they use with no minimum fee.

(2) *Private cloud:* A cloud infrastructure is operated solely for a single organization. In other words, the proprietary network or the data center supplies hosted services to a certain group of people. For example, Microsoft Azure enables customers to build the foundation for a private cloud infrastructure using Windows Server and System Center family of products with the Dynamic Data Center Toolkit.

(3) *Community cloud:* The cloud infrastructure is shared by several organizations with common concerns (eg, mission, security requirements, policy, and compliance considerations). For example, the Google GovCloud provides the Los Angeles City Council with a segregated data environment to store its applications and data that are accessible only to the city's agencies.

(4) *Hybrid cloud:* The cloud infrastructure comprises 2 or more clouds (private, public, or community). In this infrastructure, an organization provides and manages some resources within its own data center and has others provided externally. For example, IBM collaborates with Juniper Networks to provide a hybrid cloud infrastructure to enterprises to seamlessly extend their private clouds to remote servers in a secure public cloud

• **Software as a Service (SaaS):** deals with the virtualized and pay-per-use costing model whereby programming applications are leased to contracted relationship by specific SaaS dealer, e.g., Sales power (Zargar, Takabi, and Joshi, 2011).

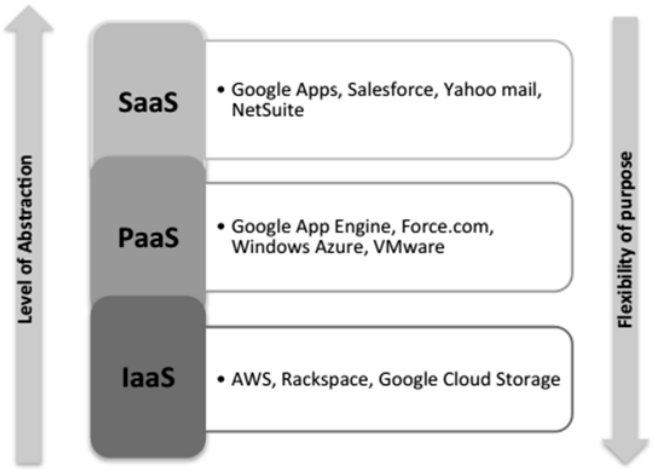


Figure 3.2: Cloud Delivery Models

Security Considerations for the Cloud

Wellbeing endeavours expected in the cloud must be made available to the customers to get their trust. In 2011, the Cloud Security Alliance (CSA) Cloud security bearing for fundamental domains to focus in Cloud Computing, keeping an eye on 14 spaces. These are Cloud Computing Architecture, Governance and Enterprise Risk Management, Compliance and Audit, Legal issues, Information Management and Data Security, Portability and Interoperability, Traditional Security, Business Continuity and Disaster Recovery, Data Centre Operations, Incident Response, Notification and Remediation, Application Security, Encryption and Key Management, Identity and Access Management, Security as a Service,Virtualization ***(CSA, 2011)***. In solicitation to have an ensured about Cloud computing course of action, all of these domains must be considered.

3.3 Security Architecture for Cloud Computing

The demonstration of applying a comprehensive and careful method for portraying current or future structure of enormous business information security systems is a normal practice for attempts to change security to targets. In any case, in the cloud, the occupation of huge business sketcher has moved and it is at present coursed among cloud master associations. The undertaking, cloud provider and also pariah are as of now drawn in with passing on reasonable security controls to direct cloud security threats. Figure 3.4 addresses the predictable depiction of Cloud Computing security designing, the cloud on-screen characters and the security building parts portrayed for each performer.

The NIST Cloud Computing reference designing describes five huge performers in the cloud: cloud client, cloud provider, cloud carrier, cloud commentator and cloud delegate. Each performer is a component (an individual or an affiliation) that participates in a trade or measure or possibly performs endeavours in Cloud Computing. A cloud provider is an individual, affiliation or component obligated for making an establishment, stage or programming open to cloud buyers as assistance. The individual or affiliation that keeps up a business relationship with, and uses at any rate one of these organizations from cloud providers, is a cloud purchaser. The cloud examiner is a social occasion that can lead free assessment of cloud organizations, execution and security of cloud use, the cloud shipper is a substance that manages the usage, execution and movement of cloud organizations while the cloud carrier is the centre individual that gives organization and transport of cloud organizations from cloud providers to cloud customers (NIST, 2011).

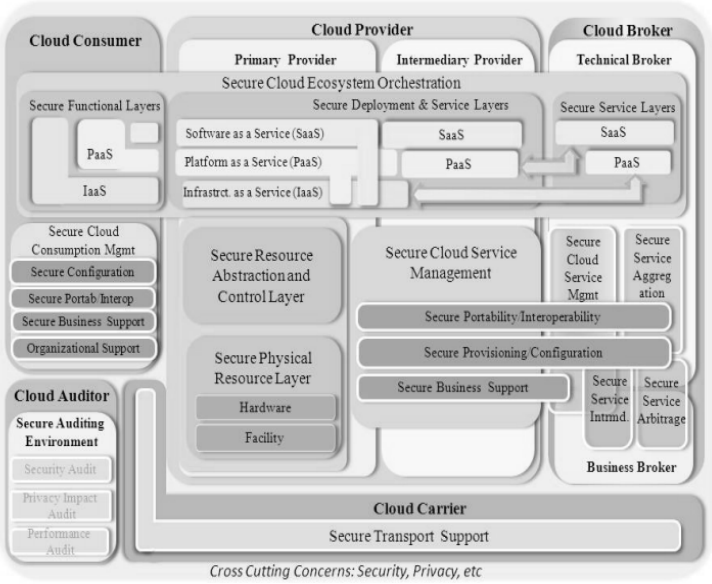


Figure 3.4: Computing Security Reference Architecture

Security Challenges of Cloud Computing

- As per various overviews, security issues are the highest in the cloud. Cloud Computing has numerous security problems that come under two general classes: security issues looked at by cloud providers (i.e., cloud-based SaaS, IaaS and PaaS associations) and security concerns looked at by cloud customers. Explicit security problems include programming involving virtualization. Perlin et al. (2010) observed that the majority of security problems arise from loss of control, lack of confidence and multi-tenure.
- **Loss of Control:** This is because the cloud provider and customers need to rely on specialist organizations for information security and protection, accessibility of assets and control or fixing of administrations or assets for information applications and assets.
- **Lack of Trust:** Trust means facing difficulties. Trust and danger are essentially the opposite sides of a similar coin, and some ability to verify or inspect will be necessary to create the degree of trust.
- **Multi-tenure:** Cloud inhabitants share a pool of resources and have minimal expectations that are capable of realizing irreconcilable circumstances. Additionally,

having the physical equivalent the paradigm brings new dangers to the state of Cloud Computing, which because of the distributed concept of the cloud model, makes it a very increasingly desirable target for gatecrashers. In addition, due to the popularized definition of the cloud condition, there may be different driving factors for contending inhabitants to initiate assaults against each other (***Zargar, Takabi, and Joshi, 2011; Perlin et al, 2010)***.

Cloud Computing Security Solutions

Security arrangements and guidelines for the cloud have been established by numerous conferences and associations. The Cloud Security Alliance (CSA) has created a security directory that recognises various territories for cloud computing security concerns. The CSA published its third form of 'Security Guidelines for Critical Focus Areas in Cloud Computing' before the end of 2011, in which one design room, five administration spaces and eight operational areas are recognised and reviewed, giving a lot of rules for cloud providers to follow ***(CSA, 2011)***.

In addition, cryptography is a frequently promoted cloud security solution based on its entirely homomorphism encryption (FHE), called by some as the "Sacred goal" of the field and late recognised as a fully utilitarian construct with cloud safety assurance. In any event, ***Dijk and Juels (2010)*** argued that the defence demanded by standard Cloud Computing administrations cannot be enforced by cryptography alone, even with such incredible assets as FHE, and that various types of security implementation are needed, such as carefully built equipment, distributed figuring, and complex biological confidence systems.

Kailash et al. (2012) referenced that data and calculation privacy and trustworthiness issues are a major obstacle to efforts to understand Cloud Computing and suggested a method to create a confident figuring condition for the Cloud Computing system by integrating the confided in the registration stage.

In addition, numerous studies ***(Juniper Networks, 2013; Fang Hao, 2010)*** concentrate on improving server farm systems, virtual machine (VM) independence in the field, adaptability, and private systems in server farms to ensure information is assured. The equivalent physical computer may be based on virtual machines of different clients, and their data packages may have a similar neighbourhood (LAN). For example, such lack of disengagement brings security risks to customers that it is feasible for a programmer to lead attacks on another flexible Amazon figuring (EC2) customer who imparts equipment assets to the cloud programmer. As scalable server farm organisation architecture, Secure Flexible Cloud Computing (SEC2) was proposed to support secure cloud computing for both enterprise and individual customers. SEC2 removes the adaptability limit created by VLANs that provide convincing disconnection between multiple customers while allowing physical asset sharing.

Clients should define and interact with their individual security and QoS strategy settings in the same way as they deal with ordinary on-site systems. This engineering will also allow customers to flawlessly consolidate cloud-based assets via VPN with their current system foundation.

Google also suggested a "administration cloud" at the opposite end of the spectrum, making completely separate facilities, programming, and managers (with suitable personal investigations) for specific customers. Although such cloud management can be extremely reliable, it is also extravagant, almost like structuring a separate server farm for each customer ***(Fang Hao, 2010)***. In addition, components such as RBAC and ABAC are used to monitor the cloud to ensure that approved customers access the information and system ***(Khan, 2012)***.

3.7 Access Control for Cloud Computing Security

In order to guarantee Cloud Computing security, these field audits are regulated as a response. Companies use components to monitor the risks of unauthorised access to their data, properties, and frameworks. A few frameworks can be used to compare access control systems and access control models, using different innovations and basic framework segments with shifting degrees of multi-faceted design. In any event, with Cloud Computing, the existing methods of access control are not sufficient to resolve the problems of the state of Cloud Computing as they were designed to support the condition of the endeavour. Due to the complicated and varied nature of the cloud phase, it is important to have a solid access control set up to ensure data or data protection in the cloud.

3.7.1 Access Control Basics

Access control is worried about deciding the permitted exercises of authentic clients, intervening each endeavour by a client to get to an asset in the framework by actualizing security arrangements. A commonplace

design of an entrance control framework is as portrayed in the engineering of a SBA framework in Section 2.4.1. Reflections to be viewed as when wanting to actualize an entrance control framework are as depicted.

- **Plans:** High-level prerequisites that specify how access is monitored and under what circumstances who can access data.
- **Mechanisms:** For example, get to control records (ACL) these decipher customers' entry asks for and execute get to control approaches at an elevated level.
- **Model:** This is a proper implementation of the system-approved security strategy and is useful for illustrating hypothetical framework constraints. Models for access control transcend any obstacle between policy and method in deliberation. Usually security models are composed to reflect the security characteristics of an entrance control system, such as optional access control (DAC). From one point of view, a paradigm may be inflexible in executing a solitary arrangement while enabling a wide variety of techniques to be applied and expressed on the other.

From Figure 3.5, the formalisation stage between the description of the technique and its use as a part makes the meaning of a traditional model that speaks to the method and its application, allowing it conceivable to define and demonstrate safety properties that would be appreciated by frameworks implementing the model. "On these lines, showing that the model is "safe" and that the model is implemented correctly by the instrument means that the system is "secure" ***(Samarati and Vimercati)***. The distinction between approaches and resources recognises autonomy between protection prerequisites that are retained on the one hand and structures that authorise them on the other, making it conceivable to:

Discussing security conditions independently of their application, Compare distinctive approaches to access control as well as different tools implementing a similar strategy and
Designing frameworks that are able to approve various strategies.

The downside of binding a part to a specific strategy is avoided by instruments ready to approve various strategies, in view of the fact that a change to the method will entail changing the whole system. After selecting which access control model (e.g. DAC, MAC, RBAC) to upgrade, it is possible to improve different imaginable access control systems that are accessible to operate within these models at that stage. To upgrade protection approaches, the entry control system, which determines whether or not the entry demand is accepted, collects demand between an approved customer and assured assets.

Access Control Policies :-

There are a few notable methods for access management, which can be sorted as either optional or non-optional.

• Discretionary Access Control Policies (DAC): Discretionary access control awards rely on the character of applicants and provide adaptability to the asset owner's appointment of access rights. It is also known as Identity-Based Access Control (IBAC) or Authorization-based control of access. An important framework for DAC representation is given by the entrance control network. Authorization Table, Access Control List (ACL) and Capability list are included in the running of the mill tools for implementing DAC approaches. The entrance lattice is deciphered and modified alternately by each of them. In general, the DAC strategy would be genuinely adaptable and commonly used in business and government divisions. Be that as it may, it has the following drawbacks:

- Knowledge can be duplicated from one object to the next, which makes it difficult to keep up.
- Protection arrangements and affirm that when opening the system up to Trojan pony defenselessness, health techniques are not traded off.
- No restrictions apply to the use of data as it is accessed by a customer.
- The owner of the article prefers the rights to get to objects instead of a broad system structure that mirrors the protection needs of the association.
- As the number of clients and assets grows, DAC brings in adaptability and executive challenges. Moreover, clients do not really understand their delegated rights and duties, and the root or chairman's abuse of capabilities can truly subvert system security.
- Non-Discretionary Access Control Policies: The Non-Discretionary Access Control (NDAC) category groups all access control policies other than DAC. Policies in this group have rules which are not laid down at the user's discretion. Controls are only generated by administrative acts and cannot be altered by users. Compulsory access control (MAC), role-based access control (RBAC) and temporal constraints are common non-discretionary access control policies.

Access Control Mechanisms :-

The Access Management Tool (ACM) is a component for managing the access to assets (documents and registries) of a system (tasks like perusing, composing, and erasing). The aspect of access control defines the low level of work (programming and equipment) that carries out the controls imposed by the strategy and officially articulated in the model. In order to assess the willingness of a customer to conduct an operation, the entry control system looks at the safety characteristics of the customers for example, identifiers, occupations, meetings) of the assets (for example, forms, get to control documents, affectability names) in view of the measurement of trait alignment or pre-decided arrangement of rules. It is possible to either focus or decentralise ACMs.

- **Centralized:** Data from access control is put away on the device. Concentrated ACMs are highly adaptable and fast to implement. In any event, because of the rise in the amount of data needed to be tracked as the amount of customer increments, they are not as adaptable and easy to keep up as decentralised ACM.

- **Decentralized:** Here, a small segment of the data on getting to control is placed on the device, which makes it easier to keep up with this instrument as data needed by a customer is placed on the side of the part at that access control point, making it more flexible than concentrated ACM ***(Arakawa and Sasada, 2011)***.

Access control tool instances include access control records (ACL) and functionality records, components of job-based access control (RBAC), rule-based access control (RuBAC) and XML-based systems.

- **Access Control Lists (ACLs) and Capability records:** ACLs are an old security component that provides a direct way for a predefined client or gathering of clients to allow or refuse access. Inside an entrance control lattice, the ACL is a section indicating different subjects that can enter an object, while the capability list is the column containing the genuine permissions granted to a subject. See Illustration 3.6. The ACL has execution hits, wasteful elements are stored, fine granularity is required and support for the least gain is needed. In circumstances where client turnover is important, ACLs have real problems and are subordinate to the point. With a show of ability or access, it is difficult to survey the subjects that can get to a particular object.

Capability →

Subject	File 1	File 2	File 3	File 4
Larry	Read	Read, Write	Read	Read, Write
Curly	Full Control	No Access	Full Control	Read
Mo	Read, Write	No Access	Read	Full Control
Bob	Full Control	Full Control	No Access	No Access

ACL

Figure 3.6: Capability List bound to Subjects and ACL bound to Objects

• **Role-based Access Control (RBAC) Mechanism:** RBAC is increasingly viewed by and wide as an aspect of efficient access control that facilitates security organizations by dumping customers into jobs and thus requires a layer of customer and consent deliberation. As an elective way to deal with traditional access control tools, RBAC has been suggested both to rearrange the distribution of access control organisations and to easily help work-based access control (Kumar and Kumar, 2013).

• **Rule-based Access Control Mechanism (RuBAC):** RuBAC enables clients to rely on pre-ordained and arranged concepts to access frameworks and data. RuBAC has an extensive application set and could be combined with various models, such as RBAC and DAC, for example. RuBAC blocks each request for entry and compares the customer's values and rights to decide on making choices.

• **XML-approach Access Control Mechanism:** XML-approach and various access control dialects have the opportunity to shape agreements without any planning, enabling customers to indicate a plan, along with language programming approvals. Be that as it may, the impediment is for example, the declarations of chronicled-based criteria and area restrictions in the expressive strength of higher-request justification, like the RuBAC. The development of XML-approach frameworks for unique access control was promoted by Endeavours. XACML by OASIS and XACL.

IBM are unique strategic frameworks equipped to ensure that XML records can also be applied to various properties. Right now these dialects do not provide MAC and DAC assistance, but RBAC is still being increased by XACML fuses.

Access Control Models

Access control models are often concerned with interceding with a subject's activities e.g. client, framework) to get to an article (e.g. index, log, computer, monitor, memory, stockpiling, printer), and how this entry will occur. Models of access control are generally seen as frameworks to implement and maintain the honesty of security strategies that control how data can be accessed and exchanged on a framework ***(Garg and Mishra, 2012)***.

Three models of access control are exemplary: MAC, DAC and RBAC. These models make the partition between confirmation and acceptance a known one. Certification-based access control has been suggested in open and complex environments, where consumers and servers can not be known to each other in advance. It is

no longer possible to apply traditional partitioning between verification and acceptance and trust the executives as a response was suggested. These are focused on choices that rely on certificate-containing strategies that adequately incorporate validation and approval ***(Zhao H., 2012)***.

As of late, models based on market processes can be managed and their relative feasibility controlled ***(Garg and Mishra, 2012)***. Next, MAC/DAC, RBAC, ABAC ***(Burmester, 2012)*** and TBAC are examples of several well-known models of access control.

ORIENTATION FRAMEWORKS

This section discusses the standard structures (RBAC, ABAC, TBAC) and conventions (SAML and confidence model) used in this theory for the trading of verification, approval and quality details. It also introduces the arrangement language (XACML) and the form of the theoretical order for cloud recognition to manage needs. As a consequence of its expressiveness and adaptability in signalling access control structures, XACML is used for specific approaches.

XACML

The eXtensible Access Control Mark-up Language (XACML), a fine-grained technique language based on XML, is a settled standard for arrangements to be characterised and implemented. With the strategy structure set somewhere around IETF and DMTF, and commonly used, it is predictable ***(Garden of the Desert, 2013)***.

Sections as shown for the standard IETF and access control architecture are remembered in the basic parts of XACML engineering: Plan Enforcement Point (PEP), Plan Decision Point (PDP), Plan Information Point (PIP), Plan Administration Point (PAP), and administration of commitments. By approving option requests, advising the PDP for approval choice, and executing the choices, the PEP performs get to power. The PDP, along with commitments and exhortations, reviews suitable approaches and yields acceptance options, assuming any.

The PIP is a wellspring of characteristic attributes, such as properties of the subject, asset, operation and condition. The PAP handles and makes them available to the PDP for plans and strategy sets. The administration of commitments manages commitments submitted by the PEP. Be that as it may, XACML does not indicate how the administration of PIP, PAP and commitments should proceed and how they should be updated. Figure 4.1 below explains XACML's substantial level of improvement in recalling various interfaces and entertainers for approval decisions ***(OASIS, 2013).***

- Three types of XML reports are determined by XACML: solicitations, responses, and approaches. In the creation of access control agreements, Standard XACML uses three basic components: law, strategy and strategy set and allows for different levels of settlement. See Illustration 4.2.
- The most basic arrangement feature is the XACML law. It has three main segments: a target, a condition and an effect.
- A number of topics (S), properties (R), and activities (A) to which a standard, strategy or strategy set applies are defined by the target.
- The impact (E) is the prediction of the arrival of the assessment, which can be either allowable, refused, unacceptable or ambiguous. On the off chance of a request starting from a subject to perform an operation within a domain on an asset. In the solicitation, the property figures are contrasted and those remembered for the objective and on the off chance that all the qualities coordinate, the solicitation is applicable at that stage.

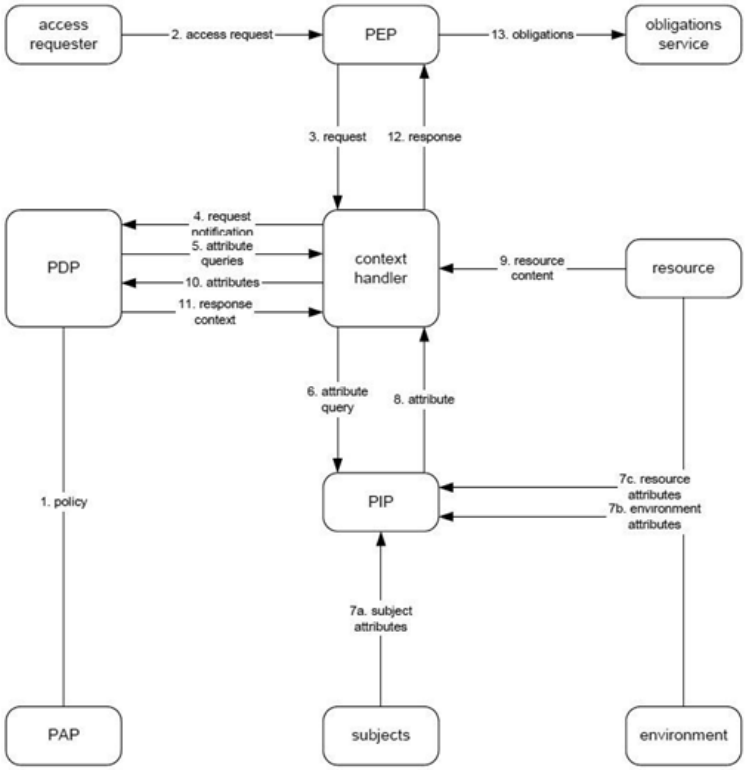


Figure XACML Authorization (OASIS, 2013)

- On the off chance that the invitation and the objective characteristics do not co-ordinate, the invitation is not important at that level, and on the off chance that the evaluation brings about an error, the invitation is ambiguous at that point. In the off chance that an application fulfils the purpose of a strategy, the application is further tested at that point according to the normal structure of the approach; the arrangement is skipped without any further evaluation in any case.
- The condition recognizes limits on the values in the target and refines the standard's importance. The normal perusing of a XACML decision is that in the event that the state of the norm assesses that it is correct, the impact property is provided at that point the option of entry control to perform operation by a subject on an asset.
- A strategy may consist of a number of rules.
- A strategy collection includes methods and other collections of arrangements.

In order to recursively define the option of a negotiated guideline/strategy, the XACML strategy evaluation calculation utilizes strategy consolidating calculations (PCA). Four normal joining calculations are distinguished by the OASIS determination:

Deny-abrogates: If any of the laws or arrangements are rejected, the entire response is denied.
Permit-supersedes: If any of the agreements or laws allow, grants are implied by the entire reaction.
First-material: Based on the first rule or technique from the overview of acceptable criteria, the outcome is evaluated.
Just-one-material the outcome ensures that only a single approach to the approaching request is appropriate.

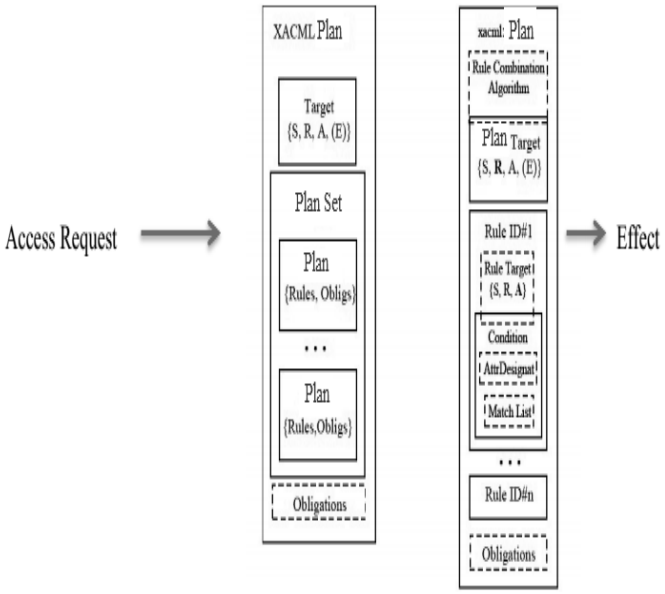


Figure: XACML Plan Model

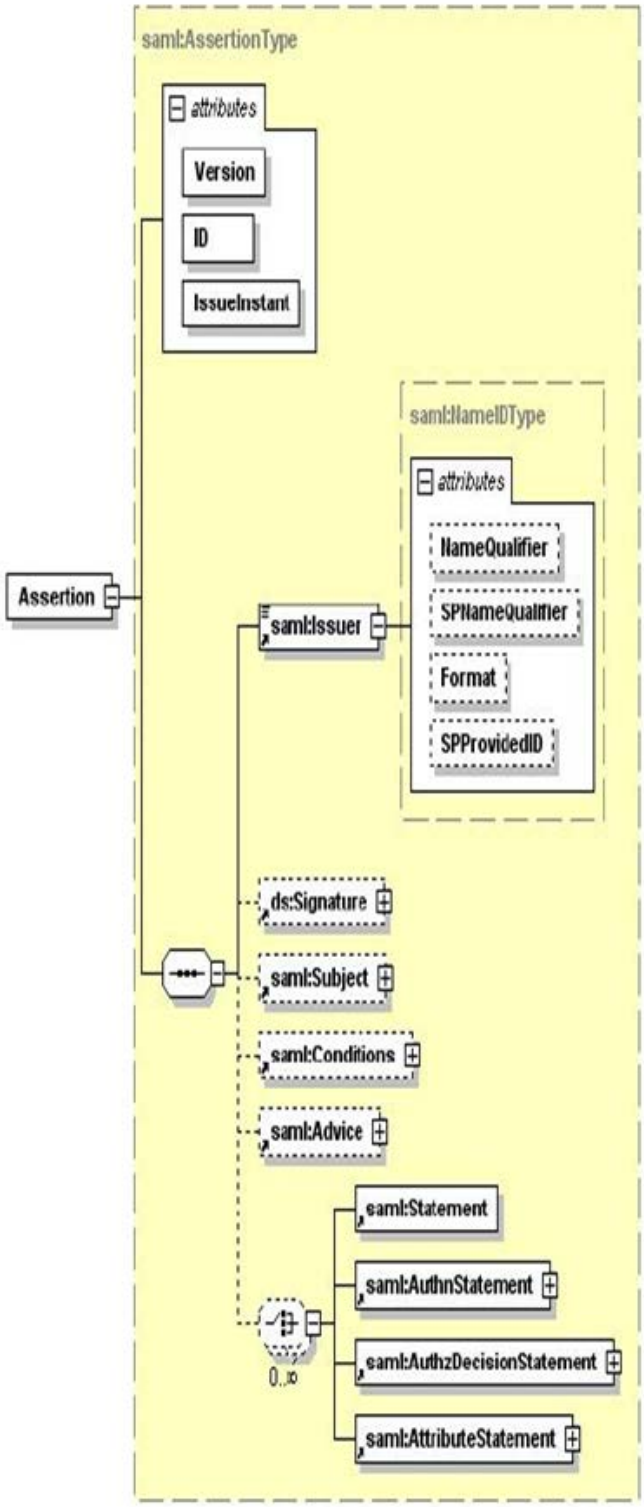
The RBAC (OASIS) XACML profile specifies a profile for the use of XACML in order to satisfy the specifications of RBAC. Roles are expressed as XACML subject attributes in this specification, except in position assignments where roles are resource attributes. The use of different functions also helps the hierarchical RBAC to be facilitated. The assigning to users of different role attributes and the activation of those attributes within a session is beyond the XACML PDP scope. However, role assignment organisations may use XACML role assignment policies to decide which users are permitted to enable different role attributes and under what circumstances. These role assignment policies are a distinct collection of instances used to evaluate the access permissions associated with each role from the authorization plan. Only when the XACML Request comes from a role assignment agency are the role assignment policies used. A role assignment or enabling entity is a device entity or entity responsible for assigning user role attributes and allowing those attributes to be used within a given session, and one role and one permission plan package (OASIS) are defined for each role. Although XACML provides the means to express and execute a Plan, it does not specify how the appropriate attributes are requested and retrieved, i.e. how to specify a communication protocol between the PEP and PDP. For this protocol, SAML is a highly suitable candidate.

SAML

Security Assertion Mark-up Language (SAML) is an XML-based standard for trading information between security areas that have formed trust relationships for verification, approval and trait trading. SAML includes elements of the statement and convention that could be used to recover traits for use in a XACML Request Context.

Figure 4.3 shows a SAML Attribute Statement that includes the quality guarantor's name, an advanced discretionary mark to validate the characteristic, a discretionary subject personality to which the characteristic is attached, and discretionary requirements for the use of the assertion that may include a validity period during which the credit is to be deemed valid. Such certification is appropriate for the removal of characteristics from the Attribute Repository, for the transfer of characteristics between the Attribute Authority and the Attribute Repository, and for the transfer of properties between the Attribute Repository and the PEP or XACML Context

Handler. SAML characterises the Attribute Query and Attribute Response components for asking an online Attribute Authority for characteristics, and for retaining a response to that query. SAML's relevant application zones include SSO, feature-based approval and protection for site administration. SAML relations describe the methods by which lower-level communication or telling conventions (e.g. HTTP or SOAP) are used to transfer SAML statements or convention messages.



CONCLUSION:- Today, cloud computing is being defined and talked about across the ICT industry under different contexts and with different definitions attached to it. The core point is that cloud computing means having a server firm that can host the services for users connected to it by the network. Technology has moved in this direction because of the advancement in computing, communication and networking technologies. Fast and reliable connectivity is a must for the existence of cloud computing. Cloud computing is clearly one of the most enticing technology areas of the current times due, at least in part to its cost-efficiency and flexibility. However, despite the surge in activity and interest, there are significant, persistent concerns about cloud computing that are impeding the momentum and will eventually compromise the vision of cloud computing as a new IT procurement model. Despite the trumpeted business and technical advantages of cloud computing, many potential cloud users have yet to join the cloud, and those major corporations that are cloud users are for the most part putting only their less sensitive data in the cloud. Lack of control is transparency in the cloud implementation – somewhat contrary to the original promise of cloud computing in which cloud implementation is not relevant. Transparency is needed for regulatory reasons and to ease concern over the potential for data breaches. Because of today's perceived lack of control, larger companies are testing the waters with smaller projects and less sensitive data. In short, the potential of the cloud is not yet being realized. Cloud computing is a new model of computing that promises to provide more flexibility, less expense, and more efficiency in IT services to end users. It offers potential opportunities for improving EHR adoption, health care services, and research. However, as discussed above, there are still many challenges to fostering the new model in health care. Perhaps the strongest resistance to the adoption of cloud computing in health IT centers concerns data security and legal issues.

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. *Microsoft 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.