Secure Cloud Architecture

Dr. Akhilesh Saini

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

Abstract:- A secure cloud architecture brings together the robustness, depth of security, and visibility of the modern data center with the agility and service-based model of the public cloud. Cloud computing is set of resources and services offered through the Internet. Cloud services are delivered from data centers located throughout the world. Cloud computing facilitates its consumers by providing virtual resources via internet. The biggest challenge in cloud computing is the security and privacy problems caused by its multi-tenancy nature and the outsourcing of infrastructure, sensitive data and critical applications. Enterprises are rapidly adopting cloud services for their businesses, measures need to be developed so that organizations can be assured of security in their businesses and can choose a suitable vendor for their computing needs. Cloud computing depends on the internet as a medium for users to access the required services at any time on pay-per-use pattern. However this technology is still in its initial stages of development, as it suffers from threats and vulnerabilities that prevent the users from trusting it. A cloud security architecture (also sometimes called a "cloud computing security architecture") is defined by the security layers, design, and structure of the platform, tools, software, infrastructure, and best practices that exist within a cloud security solution. A cloud security architecture provides the written and visual model to define how to configure and secure activities and operations within the cloud, including such things as identity and access management; methods and controls to protect applications and data; approaches to gain and maintain visibility into compliance, threat posture, and overall security; processes for instilling security principles into cloud services development and operations; policies and governance to meet compliance standards; and physical infrastructure security components.

I. INTRODUCTION

An organization's growing reliance on the cloud comes with added security concerns. While most data outside of the network resides in cloud services sanctioned by IT, countless other cloud services are used without a vetting process. This data movement to cloud service providers and various devices challenges an enterprise's visibility and control. Collaboration within the cloud bypasses any remaining network controls. Sensitive data accessed by unmanaged personal devices can disappear indefinitely.

Security and risk management professionals are left with a patchwork of controls at the device, network, and cloud with significant gaps in visibility to their data. Living with these gaps and the patchwork of security born out of the network is an open invitation to breach attempts and noncompliance.

Many cloud providers do not provide detailed control information about their internal environments, and quite a few common security controls used internally may not translate directly to the public cloud.

Infrastructure-as-a-Service (IaaS) – IaaS is a cloud computing model that provides virtualized computing resources including networking, storage, and machines accessible through the internet. In IaaS, the Cloud Service Provider (CSP) is responsible for the controls that protect their underlying servers and data including security of servers, storage and networking hardware, virtualization, and the hypervisor. The enterprise's security responsibilities include user access, data, applications, operating systems, and network traffic. According to Gartner, by 2021, 50% of enterprises will unknowingly and mistakenly have exposed some IaaS storage services, network segments, applications, or APIs directly to the public internet, up from 25% at YE18.

IaaS cloud security models also require these security features:

- Audit and monitor resources for misconfiguration
- Automate policy corrections
- Prevent data loss with DLP
- Capture custom app activity and enforce controls
- Detect malicious user activity and behavior
- Detect and remove malware

- Discover rouge IaaS services and accounts
- Identify provisioned user risk
- Enrich native cloud platform forensics
- Manage multiple IaaS providers

According to Gartner, through 2023, at least 99% of cloud security failures will be the customer's fault. Through 2024, workloads that leverage the programmability of cloud infrastructure to improve security protection will demonstrate improved compliance and at least 60% fewer security incidents than those in traditional data centers. As with on-premises data centers, the majority of successful cloud attacks are caused by mistakes, such as misconfiguration, missing patches, or mismanaged credentials. To achieve more secure cloud-based infrastructure and platform services, Gartner recommends a systematic and risk-based approach for IaaS/PaaS security using a set of layered capabilities.

Platform-as-a-Service (PaaS) – The CSP secures a majority of a PaaS cloud service model, however, the enterprise is responsible for the security of its applications. PaaS builds upon IaaS deploying applications without taking on the cost and resources required to buy and manage hardware, software, and hosting capabilities. These features can include:

- Cloud Access Security Brokers (CASB)
- Cloud workload protection platforms (CWPP)
- Cloud security posture management (CSPM)
- Business analytics/intelligence
- Logs
- IP restrictions
- API gateways
- Internet of Things (IoT)

Software-as-a-Service (SaaS) – Terms of security ownership within SaaS are negotiated with the CSP as part of their service contract. SaaS often hosts an enterprise's physical, infrastructure, hypervisor, network traffic, and operating system. SaaS apps and infrastructure controls can include:

- Enforce data loss prevention (DLP)
- Prevent unauthorized sharing of sensitive data to wrong people
- Block sync/download of corporate data to personal devices
- Detect compromised account, insider threats, and malware
- Gain visibility into unsanctioned applications
- Audit for misconfiguration

New architectural elements of enterprise security in the cloud

CASB-Anchored Multi-Cloud Safety Net

Central shared security for:

- Cloud Edge
- Cloud-related traffic monitoring and preventative controls
- Data, user behavior, and activity monitoring within and across authorized and unauthorized SaaS CSPs
- Malware protection across CSPs
- Shadow cloud use protection
- Cloud Infrastructure

- Configuration management for IaaS/PaaS
- Container security, data protection, and other shared aspects application security
- Traffic within/to/from IaaS/PaaS
- Threat management

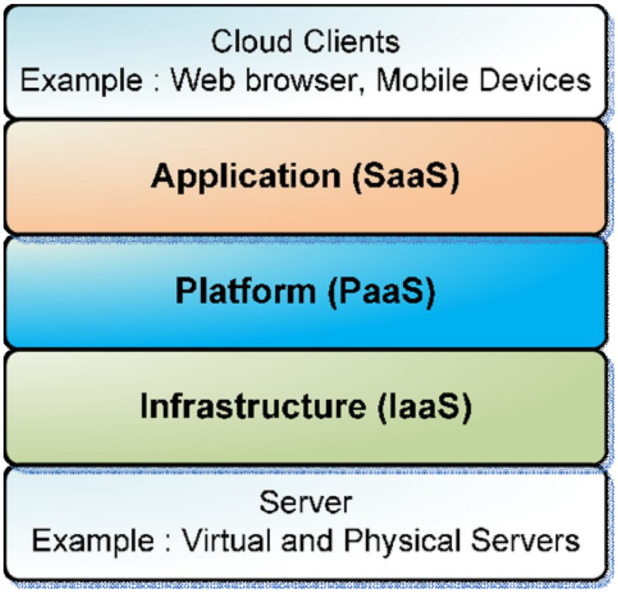
Cross-CSP Identity, Authorization and Authentication:-

- Must be implemented across all cloud providers in use and authorization/authentication security

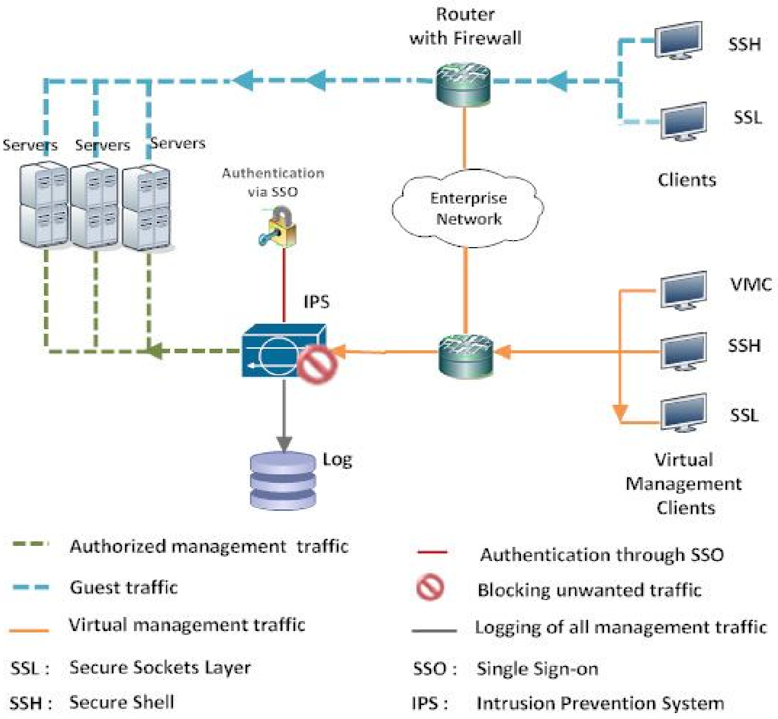
CSP and Application Project Security Basics:-

- Implementation, configuration, and audit of security design and configurations necessarily within each SaaS or IaaS/PaaS CSP, like CSP-end IAM configuration or network configuration. Often implemented initially through individual projects, then centrally for application projects within a specific CSP.

Cloud security, in general, refers to the protection of information, applications, data, platforms, and infrastructure that operate or exist within the cloud. Cloud security is applicable to all types of cloud computing infrastructures, including public clouds, private clouds, and hybrid clouds. Cloud security is a type of cyber security.


Cloud Clients
Example : Web browser, Mobile Devices
Application (SaaS)
Platform (PaaS)
Infrastructure (IaaS)
Server
Example : Virtual and Physical Servers

Cloud Computing represented as a stack of service


Router
with Firewall
SSH
SSL
Clients
Servers
Servers
Servers
Authentication
via SSO
Enterprise
Network
IPS
VMC
SSH
SSL
Log
Virtual
Management
Clients
Authorized management traffic
Guest traffic
Virtual management traffic
SSL : Secure Sockets Layer
SSH : Secure Shell
Authentication through SSO
Blocking unwanted traffic
Logging of all management traffic
SSO : Single Sign-on
IPS : Intrusion Prevention System

Secure Cloud Architecture.

THREAT MODEL FOR CLOUD:- An abstract view of threat model for Cloud computing is shown in Figure.
Cloud clients are facing two types of security threats viz; external and internal attacks.
Threat model for Cloud computing. Advanced Computing: Malicious user outside the Cloud often performs DoS or DDoS attacks to affect the availability of Cloud services and resources. Port scanning, IP spoofing, DNS poisoning, phishing are also executed to gain access of Cloud resources. A malicious user can capture and analyze the data in the packets sent over this network by packet sniffing. IP spoofing occurs when a malicious user impersonates a legitimate users IP address where they could access information that they would not have been able to access otherwise. Availability is very important. Not having access to services when needed can be a disaster for anyone especially in the case of being denied service. This can occur when exhaustion of the host servers causes requests from legitimate consumers to be denied. This can cost a company large amounts of money and time if the services they depend on to operate are not available. Internal attacker (authorized user) can easily get access to other user's resources without being detected. An insider has higher privileges and knowledge (related to network, security mechanism and resources to attack) than the external attacker. Therefore, it is easy for an insider to penetrate an attack than external attackers.

VULNERABILITIES TO CLOUD COMPUTING In Cloud, existing vulnerabilities, threats, and associated attacks raise several security concerns. Vulnerabilities in Cloud can be defined as the loopholes in the security architecture of Cloud, which can be exploited by an adversary via sophisticated techniques to gain access to the network and other infrastructure resources. In this section, we discuss major Cloud specific vulnerabilities, which pose serious threats to Cloud computing. Session Riding and Hijacking Session hijacking refers to use of a valid session key to gain unauthorized access for the information or services residing on a computer system, it also refers to theft of a cookie used to authenticate a user to a remote server and it is relevant to web application technologies weaknesses in the web application structure at their disposal that gives the chance to hackers in order to accomplish a wide variety of malicious activities. While session riding refers to the hackers sending commands to a web application on behalf of the targeted user by just sending that user an email or tricking the user into visiting a specially crafted website. Session riding deletes user data, executes online transactions like bids or orders, sends spam to an intranet system via internet and changes system as well as network configurations or even opens the firewall. However, the web technologies evolution and refinement also brings new techniques that compromise sensitive data, provide access to theoretically secure networks and pose threats to the daily operation of online businesses.
Reliability and Availability of Service In terms of reliability and availability, cloud computing is not a perfect technology. For example in February 2008, Amazon's Web Service (Amazons-S3) cloud storage infrastructure went down for several hours, causing data loss and access issues with multiple Web 2.0 services. With more services being built on top of cloud computing infrastructures, an outage or failure can create a domino effect by taking down large amounts of Internet based services and applications which raise several questions such as in cases of failure, what forms of settlement exist for stakeholders? What is the responsibility of cloud providers? What will be appropriate procedures to overcome these issues?. Insecure Cryptography Attackers' can decode any cryptographic mechanism or algorithm as main methods to hack them are discovered. It's common to find crucial flaws in cryptographic algorithm Advanced Computing: For example in cloud virtualization providers uses virtualization software to partition servers into images that are provided to the users as on-demand services . Although utilization of those VMs into cloud providers' data centres provides more flexible and efficient setup than traditional servers but they don't have enough access to generate random numbers needed to properly encrypt data. This is one of the fundamental problems of cryptography. How do computers produce truly random numbers that can't be guessed or replicated? In PCs, OS typically monitors users' mouse movements and key strokes to gather random bits of data that are collected in a so-called Entropy Pool (a set of unpredictable numbers that encryption software automatically pulls to generate random encryption passkeys). In servers,

one that don't have access to a keyboard or mouse, random numbers are also pulled from the unpredictable movements of the computer's hard drive. VMs that act as physical machines but are simulated with software have fewer sources of entropy. For example Linux-based VMs, gather random numbers only from the exact millisecond time on their internal clocks and that is not enough to generate strong keys for encryption Data Protection and Portability:- Although the cloud services are offered based on a contract among client and a provider but what will happen when the contract is terminated and client doesn't wants to continue anymore. The question is, will the sensitive data of client be deleted or misused by the provider. Secondly if the provider went out of business due to any reason, what will happen to the services and data of the client? Will the provider handout the data of client to some other provider, if yes, will client trust the new provider? Considering these questions we can say that data protection and portability remains as one of main weaknesses of cloud computing.

THREATS TO CLOUD COMPUTING:- In this section, we discuss threats relevant to the security architecture of Cloud services. We discuss here some potential threats relevant to Cloud and their remedies based on our experience of implementing the cloud.

Changes to business model Cloud computing changes the way in which IT services are delivered. As servers, storage and applications are provided by off-site external service providers, organizations need to evaluate the risks associated with the loss of control over the infrastructure. This is one of the major threats which hinder the usage of Cloud computing services. Mitigation: A reliable end-to-end encryption and appropriate trust management scheme can simplify such a threat to some extent. Abusive use of Cloud computing Cloud computing provides several utilities including bandwidth and storage capacities. Some vendors also give a predefined trial period to use their services. However, they do not have sufficient control over the attackers, malicious users or spammers that can take advantages of the trials. These can often allow an intruder to plant a malicious attack and prove to be a platform for serious attacks. Areas of concern include password and key cracking, etc. Such threats affect the IaaS and PaaS service models. Mitigation: To remediate this, initial registration should be through proper validation/verification and through stronger authentication. In addition to this, the user’s network traffic should be monitored comprehensively. Advanced Computing: APIs to allow their customers to design an interface for interacting with Cloud services. These interfaces often add a layer on top of the framework, which in turn would increase the complexity of Cloud. Such inter- faces allow vulnerabilities (in the existing API) to move to the Cloud environment. Improper use of such interfaces would often pose threats such as clear-text authentication, transmission of content, improper authorizations, etc. Such type of threat may affect the IaaS, PaaS, and SaaS service models. Mitigation: This can be avoided by using a proper security model for Cloud provider’s interface and ensuring strong authentication and access control mechanism with encrypted transmission. Malicious insiders Most of the organizations hide their policies regarding the level of access to employees and their recruitment procedure for employees. However, using a higher level of access, an employee can gain access to confidential data and services. Due to lack of transparency in Cloud provider’s process and procedure, insiders often have the privilege. Insider activities are often bypassed by a firewall or Intrusion Detection system (IDS) assuming it to be a legal activity. However, a trusted insider may turn into an adversary. In such a situation, insiders can cause a considerable effect on Cloud service offerings, for example, malicious insiders can access confidential data and gain control over the Cloud services with no risk of detection. This type of threat may be relevant to SaaS, PaaS, and IaaS. Mitigation: To avoid this risk, more transparency is required in security and management process including compliance reporting and breach notification.

Shared technology issues/multi-tenancy nature In multi-tenant architecture, virtualization is used to offer shared on-demand services. The same application is shared among different users having access to the virtual machine. However, as highlighted earlier, vulnerabilities in a hypervisor allow a malicious user to gain access and control of the legitimate users’ virtual machine. IaaS services are delivered using shared resources, which may not be designed to provide strong isolation for multi-tenant architectures. This may affect the overall

architecture of Cloud by allowing one tenant to interfere in the other, and hence affecting its normal operation. This type of threat affects IaaS. Mitigation: Implementation of SLA for patching, strong authentication, and access control to administrative tasks are some of the solutions to address this issue.

Data loss and leakage: Data may be compromised in many ways. This may include data compromise, deletion, or modification. Due to the dynamic and shared nature of the Cloud, such threat could prove to be a major issue leading to data theft. Examples of such threats are lack of authentication, authorization and audit control, weak encryption algorithms, weak keys, risk of association, unreliable data center, and lack of disaster recovery. This threat can applicable to SaaS, PaaS, and IaaS. Mitigation: Solutions include security of API, data integrity, secure storage for used keys, data backup, and retention policies.

Service hijacking Service hijacking may redirect the client to an illegitimate website. User accounts and service instances could in turn make a new base for attackers. Phishing attack, fraud, exploitation of software vulnerabilities, reused credentials, and passwords may pose service or account hijacking. This threat can affect IaaS, PaaS, and SaaS. Advanced Computing:

Risk profiling Cloud offerings make organizations less involved with ownership and maintenance of hardware and software. This offers significant advantages. However, these makes them unaware of internal security procedures, security compliance, hardening, patching, auditing, and logging process and expose the organization to greater risk. Mitigation: To avoid this Cloud provider should disclose partial infrastructure details, logs, and data. In addition to this, there should also be a monitoring and alerting system.

Identity theft Identity theft is a form of fraud in which someone pretends to be someone else, to access resources or obtain credit and other benefits. The victim (of identity theft) can suffer adverse consequences and losses and held accountable for the perpetrator’s actions. Relevant security risks include weak password recovery workflows, phishing attacks, key loggers, etc. This affects SaaS, PaaS, and IaaS. Mitigation: The solution is to use strong authentication mechanisms.

ATTACKS ON CLOUD COMPUTING:- By exploiting vulnerabilities in Cloud, an adversary can launch the following attacks.

Zombie attack Through the Internet, an attacker tries to flood the victim by sending requests from innocent hosts in the network. These types of hosts are called zombies. In the Cloud, the requests for Virtual Machines (VMs) are accessible by each user through the Internet. An attacker can flood the large number of requests via zombies. Such an attack interrupts the expected behavior of Cloud affecting availability of Cloud services. The Cloud may be overloaded to serve a number of requests, and hence exhausted, which can cause DoS (Denial of Service) or DDoS (distributed denial of service) to the servers. Cloud in the presence of attacker’s flooded requests cannot serve valid user’s requests. Mitigation: However, better authentication and authorization and IDS/IPS can provide protection against such an attack.

Service injection attack Cloud system is responsible for determining and eventually instantiating a free-to- use instance of the requested service. The address for accessing that new instance is to be communicated back to the requesting user.
An adversary tries to inject a malicious service or new virtual machine into the Cloud system and can provide malicious service to users. Cloud malware affects the Cloud services by changing (or blocking) Cloud functionalities. Consider a case wherein an adversary creates his/her malicious services like SaaS, PaaS, or IaaS and adds it to the Cloud system. If an adversary succeeds to do this, then valid requests are redirected to the malicious services automatically. Mitigation: To defend against this type of attack, service integrity checking module should be implemented. Strong isolation between VMs may disable the attacker from injecting malicious code in the neighbor’s VM.

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

B. 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.

C. 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

D. a number of public/private (in-house IT infrastructure)/community clouds. Intuitively, on demand computing makes sense only for CPU intensive jobs.

E. 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

F. 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.

G. 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 met specifications. 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.

H.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.

I. 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

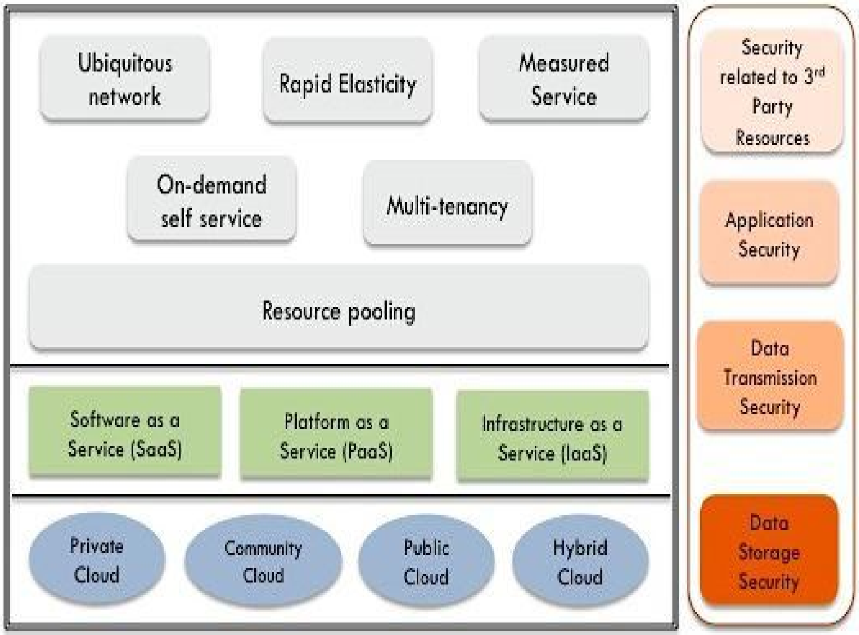
Cloud computing security is an emerging sub-area of PC security, security management, and much more comprehensively, data security. This refers to a comprehensive collection of techniques, developments, and controls conveyed to secure information, applications, and the associated Cloud

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.

(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

What is Cloud Security Architecture?

A cloud security architecture (also sometimes called a "cloud computing security architecture") is defined by the security layers, design, and structure of the platform, tools, software, infrastructure, and best practices that exist within a cloud security solution. A cloud security architecture provides the written and visual model to define how to configure and secure activities and operations within the cloud, including such things as identity and access management; methods and controls to protect applications and data; approaches to gain and maintain visibility into compliance, threat posture, and overall security; processes for instilling security principles into cloud services development and operations; policies and governance to meet compliance standards; and physical infrastructure security components.

Cloud security, in general, refers to the protection of information, applications, data, platforms, and infrastructure that operate or exist within the cloud. Cloud security is applicable to all types of cloud computing infrastructures, including public clouds, private clouds, and hybrid clouds. Cloud security is a type of cybersecurity.

Key Elements of a Cloud Security Architecture

When developing a cloud security architecture several critical elements should be included:

- Security at Each Layer
- Centralized Management of Components
- Redundant & Resilient Design
- Elasticity & Scalability
- Appropriate Storage for Deployments
- Alerts & Notifications
- Centralization, Standardization, & Automation

Shared Responsibility within Cloud Security Architectures

The types of service models in use by a business define the types of cloud security architectures that are most applicable. The service models are: Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS).

Organizations that offer cloud services typically adhere to a shared responsibility model—that is, the cloud service provider is responsible for the security of the components necessary to operate the cloud service (software, computing, storage, database, networking, hardware, infrastructure, etc.). The customer is responsible for protecting the data and information that is stored in the cloud, as well as how they may access that data (identity and access management). Responsibilities vary slightly depending on the type of service (IaaS, SaaS, or PaaS).

Infrastructure as a Service (IaaS) Shared Responsibility

With an IaaS, a business purchases the infrastructure from a cloud provider and the business typically installs their own operating systems, applications, and middleware. An example of an IaaS is Azure (Microsoft). In an IaaS, the customer is usually responsible for the security associated with anything they own or install on the infrastructure.

Software as a Service (SaaS) Shared Responsibility

With a SaaS, an organization purchases the use of a cloud-based application from a provider. Examples of SaaS include Office 365 or Salesforce. In a SaaS, the customer is typically only responsible for the security components associated with accessing the software, such identity management, customer network security, etc. The software provider manages the security backend.

Platform as a Service (PaaS) Shared Responsibility

With a PaaS, a business purchases a platform from a cloud provider to develop, run, and manage applications without developing or managing the underlying platform infrastructure required for the applications. An example of a PaaS would be Amazon Web Services (AWS). In a PaaS, the customer is responsible for the security associated with application implementation, configurations, and permissions.

Cloud Security Architectures by Service Model

IaaS Cloud Security Architecture Components

Security architecture components in an IaaS cloud environment may include endpoint protection (EPP), a cloud access security broker (CASB), a vulnerability management solution, access management, and data and network encryption.

SaaS Cloud Security Architecture Components

SaaS security architecture components should include application security, identity and access management as well as a cloud access security broker (CASB) to facilitate visibility, access controls and data protection using APIs, proxies, or gateways.

PaaS Cloud Security Architecture Components

A PaaS security architecturemay require both standard cloud security architecture solutions, as well as less common solutions, such as a Cloud Workload Protection Platform (CWPP).

Types of Cloud Security Architectures

A cloud security architecture typically includes components and best practices relevant to the types of cloud security services the business wishes to secure. Examples include an AWS cloud security architecture, Google infrastructure security, or an Azure security architecture. Additional key components of a cloud security architecture include the cloud “shared responsibility model” and the principles of “zero trust architecture.”

Principles of Cloud Security Architecture

A well-designed cloud security architecture should be based on the following key principles:

Identification—Knowledge of the users, assets, business environment, policies, vulnerabilities and threats, and risk management strategies (business and supply chain) that exist within your cloud environment.

Security Controls—Defines parameters and policies implemented across users, data, and infrastructure to help manage the overall security posture.

Security by Design—Defines the control responsibilities, security configurations, and security baseline automations. Usually standardized and repeatable for deployment across common use cases, with security standards, and in audit requirements.

Compliance—Integrates industry standards and regulatory components into the architecture and ensures standards and regulatory responsibilities are met.

Perimeter Security—Protects and secures traffic in and out of organization’s cloud-based resources, including connection points between corporate network and public internet.

Segmentation—Partitions the architecture into isolated component sections to prevent lateral movement in the case of a breach. Often includes principles of ‘least privilege’.

User Identity and Access Management—Ensures understanding, visibility, and control into all users (people, devices, and systems) that access corporate assets. Enables enforcement of access, permissions, and protocols.

Data encryption—Ensures data at rest and traveling between internal and external cloud connection points is encrypted to minimize breach impact.

Automation—Facilitates rapid security and configuration provisioning and updates as well as quick threat detection.

Logging and Monitoring—Captures activities and constant observation (often automated) of all activity on connected systems and cloud-based services to ensure compliance, visibility into operations, and awareness of threats.

Visibility—Incorporates tools and processes to maintain visibility across an organization’s multiple cloud deployments.

Flexible Design—Ensuring architecture design is sufficiently agile to develop and incorporate new components and solutions without sacrificing inherent security.

CONCLUSION:-

Although Cloud computing can be seen as a new phenomenon which is set to revolutionizes 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.