UNIT-I

What is Cloud computing?

Cloud computing is the delivery of computing as a servicerather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility (like the electricity grid) over a network (typically the Internet).Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly.

Cloud computing is a practical approach to experience direct cost benefits and it has the potential to transform a data center from a capital-intensive set up to a variable priced environment.

The idea of cloud computing is based on a very fundamental principal of „reusability of IT capabilities'. The difference that cloud computing brings compared to traditional concepts of "grid computing", "distributed computing", "utility computing", or "autonomic computing" is to broaden horizons across organizational boundaries.

Forrester defines cloud computing as:

"A pool of abstracted, highly scalable, and managed compute infrastructure capable of hosting end-customer applications and billed by consumption."

NIST defines cloud computing as" Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Characteristics of Cloud computing?

Cloud computing exhibits the following key characteristics:

- Agility improves with users' ability to re-provision technological infrastructure resources.
- Application programming interface (API) accessibility to software that enables machines to interact with cloud software in the same way that a traditional user interface (e.g., a computer desktop) facilitates interaction between humans and computers. Cloud computing systems typically use Representational State Transfer (REST)-based APIs.
- Cost: cloud providers claim that computing costs reduce. A public-cloud delivery model converts capital expenditure to operational expenditure. This purportedly lowersbarriers to entry, as infrastructure is typically provided by a third party and does not need to be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained, with usage-based options and fewer IT skills are required for implementation (in-house). The e-FISCAL project's state-of-the-art repositorycontains several articles looking into cost aspects in more detail, most of them concluding that costs

savings depend on the type of activities supported and the type of infrastructure available in-house.

- Device and location independence enable users to access systems using a web browser regardless of their location or what device they use (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect from anywhere.
- Maintenanceof cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.
- Multitenancy enables sharing of resources and costs across a large pool of users thus allowing for:
  - centralization of infrastructure in locations with lower costs (such as real estate, electricity, etc.)
  - peak-load capacity increases (users need not engineer for highest possible load-levels)
  - utilisation and efficiency improvements for systems that are often only 10–20% utilised.
- Performance is monitored, and consistent and loosely coupled architectures are constructed using web services as the system interface.
- Productivity may be increased when multiple users can work on the same data simultaneously, rather than waiting for it to be saved and emailed. Time may be saved as information does not need to be re-entered when fields are matched, nor do users need to install application software upgrades to their computer.
- Reliability improves with the use of multiple redundant sites, which makes well-designed cloud computing suitable for business continuityand disaster recovery.
- Scalability and elasticity via dynamic ("on-demand") provisioning of resources on a fine-grained, self-service basis in near real-time (Note, the VM startup time varies by VM type, location, os and cloud providers[]), without users having to engineer for peak loads
- Securitycan improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels.Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford to tackle.However, the complexity of security is greatly increased when data is distributed over a wider area or over a greater number of devices, as well as in multi-tenant systems shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.

The National Institute of Standards and Technology's definition of cloud computing identifies "five essential characteristics":

- On demand self-services: computer services such as email, applications, network or server service can be provided without requiring human interaction with each service provider. Cloud service providers providing on demand self-services include Amazon Web Services (AWS), Microsoft, Google, IBM and Salesforce.com. New York Times and NASDAQ are examples of companies using AWS (NIST). Gartner describes this characteristic as service based

- Broad network access: Cloud Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms such as mobile phones, laptops and PDAs.

- Resource pooling: The provider's computing resources are pooled together to serve multiple consumers using multiple-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. The resources include among others storage, processing, memory, network bandwidth, virtual machines and email services. The pooling together of the resource builds economies of scale (Gartner).

- Rapid elasticity: Cloud services can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

- Measured service: Cloud computing resource usage can be measured, controlled, and reported providing transparency for both the provider and consumer of the utilised service. Cloud computing services use a metering capability which enables to control and optimise resource use. This implies that just like air time, electricity or municipality water IT services are charged per usage metrics – pay per use. The more you utilise the higher the bill. Just as utility companies sell power to subscribers, and telephone companies sell voice and data services, IT services such as network security management, data center hosting or even departmental billing can now be easily delivered as a contractual service.

Why use Clouds?

Clouds can provide users with a number of different benefits. Many businesses large and small use cloud computing today either directly (e.g. Google or Amazon) or indirectly (e.g. Twitter) instead of traditional on-site alternatives. There are a number of reasons why cloud computing is so widely used among businesses today.

- Reduction of costs – unlike on-site hosting the price of deploying applications in the cloud can be less due to lower hardware costs from more effective use of physical resources.

- Universal access - cloud computing can allow remotely located employees to access applications and work via the internet.

- Up to date software - a cloud provider will also be able to upgrade software keeping in mind feedback from previous software releases.

- Choice of applications. This allows flexibility for cloud users to experiment and choose the best option for their needs. Cloud computing also allows a business to use, access and pay only for what they use, with a fast implementation time

Potential to be greener and more economical - the average amount of energy needed for a computational action carried out in the cloud is far less than the average amount for an on-site deployment. This is because different organisations can share the same physical resources securely, leading to more efficient use of the shared resources.

- Flexibility – cloud computing allows users to switch applications easily and rapidly, using the one that suits their needs best. However, migrating data between applications can be an issue.

How clouds are changing?

"Cloud computing has the potential to generate a series of disruptions that will ripple out from the tech industry and ultimately transform many industries around the world," says John Hagel, co-chairman of the Deloitte Center for the Edge, Deloitte's Silicon Valley-based research center. Here are some of the ways the cloud's ability to access, analyze, store and share information could change our business and personal lives:

Everyone will become a gamer.

Gaming is called the "killer app" of cloud computing, and gamers have salivated over demos with complex 3-D graphics delivered to mobile devices through the cloud. While some technical wrinkles remain, players can now enjoy breathtaking gaming experiences anywhere because of the cloud's power to provide higher speed without interruption.

Fixing stuff will be easier.

Thanks to the cloud, you can expect to get earlier notice when things around your house or office are about to go on the fritz. For example, a cloud-based app alerts drivers of electric cars when their batteries will run out of juice, letting them get to a charging station without needing to call a tow truck. A major medical equipment company developed a cloud-based application that feeds information to field system engineers who need to maintain health equipment, helping them head off problems. And when stuff needs to be fixed, the cloud will make that easier, too.

Computers will become invisible.

When people use search engines, they usually don't realize they are accessing billion-dollar computer networks. As the power of the cloud spreads, one effect will be to make software and computing more invisible.

You'll actually find what you want in stores.

With the cloud, inventory records will be much more visible and reliable. Connected shoppers, who browse brick-and-mortar aisles with web browser in hand, are beginning to exercise their leverage, such as asking the store to match a price found on a competitor's website. Retailers' brand value will be dramatically affected by how they satisfy these mobile-savvy shoppers.

Everyone will want to give you advice.

In an age of information overload and unlimited choice, companies in all industries will want to become your trusted advisor—which is also a key way retailers will fight against commoditization. "Companies will be less interested in the immediate sale than in providing advice in order to develop a relationship," Hagel says. The need for guidance will spawn new companies that leverage the insights from the many footprints we leave online. Now, for example, shopping sites might offer suggestions of movies or videos based on previous purchases. "The next level will be companies that make those suggestions based on not just your activity on one specific site, but across a range of places—what you watch on web TV, on YouTube and other sites," Hagel says. "If a company can capture all my online activity, as it occurs in real time, it can have an integrated view of me as an individual and suggest things I didn't even know I wanted to look at."

You will be sold to differently.

Scott Crenshaw, vice president and general manager of the Cloud Business Unit of Red Hat, the open source technology solutions provider, says the cloud is fundamentally changing the way companies sell to businesses and consumers. "The old mantra used to be people buy from people," he says. "But customers are moving to more online transactions, which is fundamentally a cloud phenomenon. Even in industries where the transaction requires direct personal interaction, buyers will form their opinions of products and services based on input from online communities." The cloud will "give small, niche retailers the ability to tweak their offerings and develop a closer understanding of their customers," notes Crenshaw. In addition, he expects companies to lure customers with new kinds of "freemiums"—free online versions of their wares. The idea is that a portion of customers taking advantage of free versions will eventually shift to paid versions with more features.

You'll be able to make smarter decisions.

Having just-in-time training won't be the only way the cloud will help you make wiser choices. Burrus points out the cloud can turn any mobile device into a "supercomputer." This means you can access processing power as needed from the cloud to analyze virtually any type of information wherever you are. Imagine, for example, that you combined live stock market data, weather projections, scanned news stories, tweets and comments in blogs, gauging the sentiment or subtle changes in public opinions. Put those streams of information together, feed them into an advanced simulation on your mobile phone and you could gain unique insight that leads to profitable stock choices. Even if you don't play the market, processing power on demand will make it easier for you to do original research on any topic that comes to mind, such as combining sales projections with just-in-time raw material inventories to make sure your department meets customer demands.

Small businesses will go global…in days.

To satisfy the new markets being created by the cloud, small- and medium-size companies will leverage the cloud and get a bigger slice of the action. "Small- and medium-size businesses will go from being constrained to certain geographies due to budget limitations to having the ability to scale globally with significantly reduced overhead costs," says David Dobson, an executive vice president at CA Technologies, a maker of IT management software and solutions that enables the cloud for SMBs through its managed service provider customers. "Perhaps the most fascinating part is all of this can happen without building a physical data center at a new location. For example, instead of deploying on-site infrastructure to run their operations, companies can access infrastructure as a service, via managed service providers." And they'll be able to do it in days, rather than the months this often took in the past, giving them a huge advantage over slower competitors, and allowing them to keep pace with larger companies.

Road trips will be less stressful.

If you've ever caravanned with a group of cars, you know the pressure of constantly looking in your rear-view mirror to make sure everyone is keeping up. Leave it to a group of college students to figure out how cloud computing could improve the road trip. As part of a class project, some University of Michigan students developed a mobile app that uses cloud computing to allow a cluster of vehicles traveling together to track each other during the journey. The app lets travelers view vehicle telemetry about their speed and fuel usage; send alerts about stops along the way; notify fellow caravanners by texting road condition and hazards; and select the best route. The combination of location tracking, social media and cloud-based analytics could improve all types of transportation scenarios.

Laptop security breaches will decline.

One study found that some 10,278 laptops are reported lost every week at 36 of the largest U.S. airports, subjecting companies to embarrassment and financial risk if important information is exposed. “In the traditional model, people can carry a laptop with all their secrets, like customer and payroll information,” says Greg Bell, practice leader for information protection at KPMG, LLP, the U.S. audit, tax and advisory firm. “To protect that information, we encrypt it. But there is a fear that many countries restrict the importation of encrypted laptops, so we run the risk of breaking local country laws and having the laptop subjected to review which might disclose that information.” The cloud can eliminate those concerns by having all data securely stored on the Internet. The laptop no longer stores the data; rather, it becomes the instrument by which to access it.

“Bedside manner” will become app-infused.

Over the past year, the number of medical students who said they turned to the Internet for information dropped from 52 percent to 33 percent, while those who cited “mobile” as their preferred information source zoomed from 19 percent to 34 percent. The desire for info-on-the-go dovetails with the growth of mobile dashboard applications, which are becoming a red-hot niche with the many new touchscreen smartphones hitting the market. “Imagine a doctor or dentist who is able to pull up a patient’s radiograph and zoom into particular areas of the radiograph with the touch of a button,” says Dan Shey, practice director, Enterprise for ABI Research, a technology research company. This development would harness the cloud’s computational ability to render the image so it could be viewed on a mobile device with the touch, zoom and screen resolution of the device itself. This would allow medical practitioners to make medical decisions almost instantaneously, regardless of their location or whether they have access to a desktop computer. It is just one example of how the cloud can overcome the processing power and data storage limitations of mobile devices.

Public/private clouds will make homes healthier.

Honorio J. Padrón III, a principal and global practice leader at the Hackett Group, a global consulting firm, sees great opportunities in the convergence of the enterprise and consumer clouds. Consider the burgeoning area of home health monitoring. The cloud allows doctors to wirelessly monitor patients with sleep apnea, collect information and then tap into a network of experts to devise a treatment plan. At a recent trade show, experimental technology was showcased that uses an infrared camera mounted above the bathroom mirror to take a daily photo of a person’s face. Over time, the images can be stored and analyzed for changes, alerting doctors of pre-cancerous skin cells so treatment can begin earlier.

Developing countries will become new markets and new competitors.

Bell notes that China and other emerging countries have not developed robust IT infrastructures, which means they can embrace the cloud quicker — and exploit new opportunities faster—since they won't be as delayed by tasks like integrating legacy technology. At the same time, the cloud will provide new opportunities in these emerging countries. In India, for example, far more people use cell phones than landlines. As the cloud eliminates barriers to what mobile devices can do, the devices will become the conduit to open up huge new markets.

Companies will use more suppliers.

The desire for greater efficiency has dictated that companies should streamline the number of suppliers they use. The cloud could reverse that by allowing companies to coordinate a more diversified group of suppliers, giving these companies the flexibility to meet unanticipated needs. The secret is "community clouds"—an embryonic type of cloud computing that allows business partners to coordinate their activities over a secure platform (which protects their secrets even from each other). One community cloud, for example, supports employees with complicated travel itineraries, coordinating the changes to hotel bookings and restaurant reservations if, say, a flight is cancelled.

Everyone will bootstrap.

The cloud offers individuals exciting ways to collaborate, develop products and test ideas rapidly and cheaply, which could accelerate the rising rate of entrepreneurialism. "You see small startups using the cloud to do complex modeling of new product offers," Hagel says. "The speed at which you can identify what people are interested in, and what they will pay, really changes the nature of innovation."

Language barriers will fade.

"Today, cloud computing gives mobile-device users a level of speech recognition accuracy that is virtually on par with call center-based transcription services," says Marcello Typrin, vice president of product development for Yap, a company that makes a free iPhone application that converts voicemail messages into text. The cloud's massive computational power may make language barriers fade in other ways as well. Imagine you were at a client site and needed to confer with a colleague in another country who speaks only Italian. You contact him on your mobile device and both your words are instantly translated into each other's language using voice recognition and translation software. "The scenario is possible today with latency near real-time, assuming you have a network with capable bandwidth on each end," Typrin says.

Driving factors towards cloud?

A number of pressing factors are driving the growth of cloud computing. I'll cover some of the biggest drivers towards cloud computing adoption here.

Improved IT Agility:-As recently as a few years ago, it took far too long for many IT departments to respond to increasing demand for computing capacity. Too much paperwork, too many approvals, and a reliance on hard-to-deploy physical servers meant that IT was often slow to respond to variable organizational needs. Virtualization helped that situation immensely, and the arrival of cloud computing gives IT organizations even more of an ability to easily (and cost-effectively) expand and reduce computing resources to meet fluctuating demands.

Cost Savings and ROI:-Cloud computing isn't a panacea, but there are clear-cut cases where moving part of your IT infrastructure to the cloud makes solid operational and financial sense. Here at Penton Media we recently moved from a cumbersome legacy email newsletter tool—developed in house—that required an ongoing (and expensive) commitment in terms of user training and application maintenance to a new cloud-based email newsletter solution. If you have legacy software applications in your own organization, are they really worth the time, expense, and human capital needed to keep them running when superior cloud-based alternatives are available?

Private Cloud vs. Public Cloud:-The concept of the private cloud has gathered steam over the past 12 months. Public cloud computing services generally rely on having your data on someone else's infrastructure. That can be a non-starter for many IT administrators, especially if your organization operates under tricky auditing, compliance, or data location requirements. That's where the private cloud steps in: Leveraging virtualization and commodity hardware, the private cloud can provide some of the elastic benefits of public cloud computing without some of the inherent risks that public cloud computing still needs to address.

Cloud-Savvy IT Staff:-A new breed of IT professionals is stepping into leadership positions in many organizations. Some fear that cloud computing could mean the end of their careers, but savvy IT pros realize that someone in the organization has to take the lead in selecting what IT platforms and services are moved to the cloud while simultaneously educating management and the rest of the organization why other elements aren't good candidates for cloud computing treatment.

UNIT 2

Cloud integration is the process of configuring multiple application programs to share data in the cloud. In a network that incorporates cloud integration, diverse applications communicate either directly or through third-party software.

Cloud integration offers the following advantages over older, compartmentalized organizational methods.

- Each user can access personal data in real time from any device.
- Each user can access personal data from any location with Internet access.
- Each user can integrate personal data such as calendars and contact lists served by diverse application programs.
- Each user can employ the same logon information (username and password) for all personal applications.
- The system efficiently passes control messages among application programs.
- By avoiding the use of data silos, data integrity is maintained and data conflicts (which can arise from redundancy) are avoided.
- Cloud integration offers scalability to allow for future expansion in terms of the number of users, the number of applications, or both.

In recent years, cloud integration has gained favor among organizations, corporations, and government agencies that implement SaaS (Software as a Service), a software distribution model in which applications are hosted by a vendor or service provider and made available to users over the Internet.

Cloud Security

Primary concerns around cloud solutions have to do with security. In the most basic situation, the cloud provider is serving many organizations within the same network environment. An organization could be concerned that their data might be hacked (accessed without permission) by another organization operating in the same area of the cloud data center. Even in cases where the cloud service provider has created a separate private cloud environment for an organization, operating on a separate network, behind a separate firewall, there must be concern for whether the service provider is providing adequate security from intruders.

The physical security provisions of the cloud service provider may be a concern, although since the provider is supporting security for all their customers and security is a differentiator, they are probably providing physical security which exceeds the internal capabilities of most individual organizations.

Additionally, the data security laws of the country where the cloud provider is operating its physical data center will be of concern to some organizations. For example, a Canadian company may not want to use a cloud service provider operating in the United States because its data could be subpoenaed by an American court.

Certain types of organizations will not be able to utilize public cloud solutions for their most private and sensitive information, such as the customer data from financial institutions or classified data from government organizations, but most organizations may find that the capabilities offered by cloud service providers are both less expensive and more secure than those they could support internally and would have many uses. Even the most security-conscious organization may find it useful to be able to create development environments in the cloud quickly, thus speeding up development of custom applications and familiarity with new vendor packages, while their internal organizations are provisioning environments within their own firewalls and data centers.

What many chief security officers are discovering, to their horror, is that cloud services are so easy and inexpensive to acquire that parts of their organizations may already have data out in public cloud environments without having been concerned with the issues of adequate security. Cloud services are so easy to obtain that the inventory of organizational data assets may suddenly be uncertain. Like data on laptops and mobile devices, data in the cloud is outside the organization's physical control and adds greater complexity to the problems of managing data security.

Cloud Latency

There are three basic reasons that the speed of data integration with data housed in a cloud environment might be slower than data located in a local data center: the speed of the network infrastructure might be slower, extra time is needed to pass through the cloud security, and extra time is needed for the data to traverse to the physical location of the cloud data center.

The network infrastructure of an internal data center might or might not be constructed with faster connections than a cloud data center. Although an internal data center would probably be using expensive and fast components for their network, especially for production systems (i.e., fiber-optic network), it is likely that a cloud data center would also be investing in fast network infrastructure even though they would be using commodity (cheap) hardware. Delays may not be within the cloud data center but rather within the path data must take to get to and from the cloud data center.

Moving data to or from a cloud data center, or accessing data in a cloud data center, will involve passing through the extra security layers (firewall) around of the cloud data center, with the extra time that would be involved, even though that may be minimal.

What cloud service purveyors minimize in their advertising is that cloud data centers actually do exist in the real world in an actual physical location. Data passing to and from these physical data centers are limited by real-world constraints such as the speed constraints of how long it takes for digital information to pass to and from the physical site of the cloud data center. The physical distance of a cloud data center may have latency just as interaction between sites in different regions of the world will have latency. The physical distance from the cloud data center combined with the network infrastructure to and from the cloud data center may exacerbate any delay.

Although data integration solutions don't necessarily need to be different in including data from a public cloud as they would for local data integration, if very low latency is a requirement, it may be necessary to architect a data integration solution similar to the integration of geographically separated hubs of data located on different continents. Solutions such as database replication can be used to make up for latency of geographically distributed data, but the extra disk required may negate much of the savings benefits of the cloud solution.

Cloud Redundancy

The servers and disk being used in most cloud configurations are commodity devices: inexpensive, easy to acquire, install, and configure. Therefore, the management of these commodity servers includes an assumption that there will be more frequent errors than in traditional in-house server configurations. That is, the mean time to failure is higher on commodity hardware. In order to create a fault-tolerant environment using commodity hardware, most cloud-oriented architectures use some form of data redundancy to enable smooth continuity of processing.

Cloud operating systems and data management systems, such as Hadoop, keep an odd number (as in not even) of copies of data. Additionally, data is usually distributed across multiple servers or nodes. When a server fails, processing falls back to one of the data copies. Having an odd number of copies allows for the nodes to compare versions of the data to verify that none of the copies have been corrupted or lost. The more critical the data, the greater the number of copies that are specified in the configuration, and, of course, the greater the rental cost.

The disk usually used in internal production environments is a "smart" disk with redundancy and fault tolerance built in, costing as much as 10 times that of commodity disk. Having three or five copies of data on commodity disk in a cloud environment should still be less expensive than internal disk, especially when including support costs.

More than with data kept internally, data kept in the cloud should include an inventory and auditing that no data has been lost or misplaced. With thousands and millions of commodity servers being constantly provisioned and deactivated, cloud services users should ensure that

they have access to and are processing all the data they think they are. Also, when deactivating servers in the cloud, some concern should be taken to ensure that all data is entirely deleted prior to surrendering the servers.

Cloud computing is picking up traction with businesses, but before you jump into the cloud, you should know the unique security risks it entails

Cloud computing is fraught with security risks, according to analyst firm Gartner. Smart customers will ask tough questions and consider getting a security assessment from a neutral third party before committing to a cloud vendor, Gartner says in a June report titled "Assessing the Security Risks of Cloud Computing."

Cloud computing has "unique attributes that require risk assessment in areas such as data integrity, recovery, and privacy, and an evaluation of legal issues in areas such as e-discovery, regulatory compliance, and auditing," Gartner says. (Compare security products.)

Amazon's EC2 service and Google's Google App Engine are examples of cloud computing, which Gartner defines as a type of computing in which "massively scalable IT-enabled capabilities are delivered 'as a service' to external customers using Internet technologies."

[Learn more about what cloud computing really means and the new breed of utility computing and platform-as-a-service offerings.]

Customers must demand transparency, avoiding vendors that refuse to provide detailed information on security programs. Ask questions related to the qualifications of policy makers, architects, coders and operators; risk-control processes and technical mechanisms; and the level

of testing that's been done to verify that service and control processes are functioning as intended, and that vendors can identify unanticipated vulnerabilities.

Here are seven of the specific security issues Gartner says customers should raise with vendors before selecting a cloud vendor.

1. Privileged user access. Sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the "physical, logical and personnel controls" IT shops exert over in-house programs. Get as much information as you can about the people who manage your data. "Ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access," Gartner says.

2. Regulatory compliance. Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications. Cloud computing providers who refuse to undergo this scrutiny are "signaling that customers can only use them for the most trivial functions," according to Gartner.

3. Data location. When you use the cloud, you probably won't know exactly where your data is hosted. In fact, you might not even know what country it will be stored in. Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers, Gartner advises.

4. Data segregation. Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure-all. "Find out what is done to segregate data at rest," Gartner advises. The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists. "Encryption accidents can make data totally unusable, and even normal encryption can complicate availability," Gartner says.

5. Recovery. Even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster. "Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure," Gartner says. Ask your provider if it has "the ability to do a complete restoration, and how long it will take."

6. Investigative support. Investigating inappropriate or illegal activity may be impossible in cloud computing, Gartner warns. "Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If you cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already

successfully supported such activities, then your only safe assumption is that investigation and discovery requests will be impossible."

7. Long-term viability. Ideally, your cloud computing provider will never go broke or get acquired and swallowed up by a larger company. But you must be sure your data will remain available even after such an event. "Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application," Gartner says.

From security holes to support issues, below are eight risks all users take when migrating to and storing their data in the cloud.

1. Someone else is looking after your data

Unlike a data center, which is run by an in-house IT department, the cloud is an off-premise system in which users outsource their data needs to a third party provider. The provider does everything from performing all updates and maintenance to managing security. The bigger picture, however, is that users are trusting their data for someone else to look after, said Steve Santorelli, a former Scotland Yard detective, now manager of outreach at the Internet security research group Team Cymru.

"The downside is that you are abrogating responsibility for your data. Someone else has access to it and someone else is responsible for keeping it safe," Santorelli said.

Although cloud providers may ensure your data is safe, Santorelli said some are not always looking after your best interests.

"No business is ever going to be as rabid about looking after your data as you would or should be. They are in the business of making money from you, after all. Securing your data sometimes becomes a marketing mantra more than a way of life," he said.

2. Cyberattacks

Any time you store data on the Internet, you are at risk for a cyberattack. This is particularly problematic on the cloud, where volumes of data are stored by all types of users on the same cloud system.

"The scary thing is the vulnerability to Distributed Denial of Service (DDoS) attacks and the concentration of so much data," Santorelli said. "The single point of failure is the cloud. If something goes bad it impacts a very wide group of people. It's easier to steal and disrupt in bulk."

Although most cloud providers have stringent security measures, as technology becomes more sophisticated, so do cyberattacks.

"When cloud companies get the security right — and many actually do a pretty reasonable job — then miscreants have to get creative to get to the data," Santorelli said. For instance, instead of hacking the cloud, hackers will attempt to hack your account instead.

"Passwords and secret answers become the soft underbelly of your security. Just like when banks made online account hacking harder, the miscreants turned to phishing to get around the restrictions and steal your passwords," he said.

3. Insider threats

Just as cyberattacks are on the rise, so are security breaches from the inside.

"Vodafone's breach of 2 million customer records and the Edward Snowden breach at the NSA are wake-up calls that the most serious breaches are due to insider threats and privileged user access," said Eric Chiu, president and co-founder of HyTrust, a cloud infrastructure control company

Once an employee gains or gives others access to your cloud, everything from customer data to confidential information and intellectual property are up for grabs.

"The cloud makes this problem 10 times worse since administrative access to the cloud management platform, either by an employee or an attacker posing as an employee, enables access to copy and steal any virtual machine, undetected,
as well as potentially destroy the entire cloud environment in a matter of
minutes," Chiu said.

4. Government intrusion

With the recent NSA leaks and the ensuing reports on government surveillance programs, competitors aren't the only ones who may want to take a peek at your data.

"Something that has been in the news recently is that government entities and technology companies in the U.S. and elsewhere may be inspecting your data as it is transmitted or where it resides in the Internet, including within clouds," said Scott Hazdra, principal security consultant for Neohapsis, a security and risk management consulting company specializing in mobile and cloud security.

Granted, privacy has always been a concern with the cloud. But instead of just worrying about competitors, disgruntled customers or employees breaching cloud security, businesses now have to worry about government intrusion as well.

"Loss of confidentiality to data is not a new risk; however, the threat sources might not have been one companies were previously worried about," Hazdra said. "For instance, a company may have a concern that competitors will try to steal their data so they encrypt transmission and storage of it. Now that someone other than a competitor may be interested in that data doesn't fundamentally change the risk."

5. Legal liability

Risks associated with the cloud are not limited to security breaches. They also include its aftermath, such as lawsuits filed by or against you.

"The latest risks to using cloud for business are compliance, legal liability and business continuity," said Robert J. Scott, managing partner of Scott & Scott LLP, an intellectual property and technology law firm. "Data breach incidences are on the rise, and so are lawsuits."

Scott, who is also a cloud law speaker and author, said that while the cloud is all about ease of access, collaboration and rapidity, its benefits have to be weighed against the extent of security measures.

"Information security has always been finding a balance between ease of access and the sharing of information verses completely locked down security," he said. "The more you have of one, the less you have of the other."

6. Lack of standardization

What makes a cloud "safe"? A provider could have the latest security features, but due to the general lack of cloud standardization, there are no clear-cut guidelines unifying cloud providers. Further, given the plethora of cloud services in different sectors, this is especially problematic for users when determining exactly how "safe" their cloud really is.

"The question of how safe the cloud is has many facets, and the answer depends on the cloud services provider, the type of industry a company is in, and the accompanying regulations concerning the data it is considering storing in the cloud," Scott said.

Since not all cloud providers are built the same, one provider's definition of "safe" may not be the same as another's, Scott said.

7. Lack of support

Imagine being unable to access your cloud before a big meeting or, worse, being in the middle of a cyberattack that has taken down your entire bread and butter —your website. Now imagine trying to contact your provider, only to find that their customer service is nonexistent. While some cloud providers have excellent customer support, others could leave you in the cold.

"The most frustrating thing when something goes wrong is not being able to speak directly with an engineer," said April Sage, director of Healthcare Vertical at Online Tech, a cloud provider specializing on compliant cloud hosting.

"If your systems are not mission-critical, you don't need to worry so much about security and availability," Sage said. "However, if you support mission-critical systems, or your online presence is critical for your business to operate smoothly, you have to be prepared to invest in a cloud and cloud provider that is capable of providing a level of protection commensurate with your needs."

8. There's always a risk

The biggest risk when it comes to cloud computing is that you never know what is up ahead. Hackers have been around from the start and they are not going anywhere any time soon. And as technology advances, so do the risks that come with adopting them.

From security holes to support issues, below are eight risks all users take when migrating to and storing their data in the cloud.

1. Someone else is looking after your data

Unlike a data center, which is run by an in-house IT department, the cloud is an off-premise system in which users outsource their data needs to a third party provider. The provider does everything from performing all updates and maintenance to managing security. The bigger picture, however, is that users are trusting their data for someone else to look after, said Steve Santorelli, a former Scotland Yard detective, now manager of outreach at the Internet security research group Team Cymru.

"The downside is that you are abrogating responsibility for your data. Someone else has access to it and someone else is responsible for keeping it safe," Santorelli said.

Although cloud providers may ensure your data is safe, Santorelli said some are not always looking after your best interests.

"No business is ever going to be as rabid about looking after your data as you would or should be. They are in the business of making money from you, after all. Securing your data sometimes becomes a marketing mantra more than a way of life," he said.

2. Cyberattacks

Any time you store data on the Internet, you are at risk for a cyberattack. This is particularly problematic on the cloud, where volumes of data are stored by all types of users on the same cloud system.

"The scary thing is the vulnerability to Distributed Denial of Service (DDoS) attacks and the concentration of so much data," Santorelli said. "The single point of failure is the cloud. If something goes bad it impacts a very wide group of people. It's easier to steal and disrupt in bulk."

Although most cloud providers have stringent security measures, as technology becomes more sophisticated, so do cyberattacks.

"When cloud companies get the security right — and many actually do a pretty reasonable job — then miscreants have to get creative to get to the data," Santorelli said. For instance, instead of hacking the cloud, hackers will attempt to hack your account instead.

"Passwords and secret answers become the soft underbelly of your security. Just like when banks made online account hacking harder, the miscreants turned to phishing to get around the restrictions and steal your passwords," he said.

3. Insider threats

Just as cyberattacks are on the rise, so are security breaches from the inside.

"Vodafone's breach of 2 million customer records and the Edward Snowden breach at the NSA are wake-up calls that the most serious breaches are due to insider threats and privileged user access," said Eric Chiu, president and co-founder of HyTrust, a cloud infrastructure control company

Once an employee gains or gives others access to your cloud, everything from customer data to confidential information and intellectual property are up for grabs.

"The cloud makes this problem 10 times worse since administrative access to the cloud management platform, either by an employee or an attacker posing as an employee, enables access to copy and steal any virtual machine, undetected,
as well as potentially destroy the entire cloud environment in a matter of
minutes," Chiu said.

4. Government intrusion

With the recent NSA leaks and the ensuing reports on government surveillance programs, competitors aren't the only ones who may want to take a peek at your data.

"Something that has been in the news recently is that government entities and technology companies in the U.S. and elsewhere may be inspecting your data as it is transmitted or where it resides in the Internet, including within clouds," said Scott Hazdra, principal security consultant for Neohapsis, a security and risk management consulting company specializing in mobile and cloud security.

Granted, privacy has always been a concern with the cloud. But instead of just worrying about competitors, disgruntled customers or employees breaching cloud security, businesses now have to worry about government intrusion as well.

"Loss of confidentiality to data is not a new risk; however, the threat sources might not have been one companies were previously worried about," Hazdra said. "For instance, a company may have a concern that competitors will try to steal their data so they encrypt transmission and storage of it. Now that someone other than a competitor may be interested in that data doesn't fundamentally change the risk."

5. Legal liability

Risks associated with the cloud are not limited to security breaches. They also include its aftermath, such as lawsuits filed by or against you.

"The latest risks to using cloud for business are compliance, legal liability and business continuity," said Robert J. Scott, managing partner of Scott & Scott LLP, an intellectual property and technology law firm. "Data breach incidences are on the rise, and so are lawsuits."

Scott, who is also a cloud law speaker and author, said that while the cloud is all about ease of access, collaboration and rapidity, its benefits have to be weighed against the extent of security measures.

"Information security has always been finding a balance between ease of access and the sharing of information verses completely locked down security," he said. "The more you have of one, the less you have of the other."

6. Lack of standardization

What makes a cloud "safe"? A provider could have the latest security features, but due to the general lack of cloud standardization, there are no clear-cut guidelines unifying cloud providers. Further, given the plethora of cloud services in different sectors, this is especially problematic for users when determining exactly how "safe" their cloud really is.

"The question of how safe the cloud is has many facets, and the answer depends on the cloud services provider, the type of industry a company is in, and the accompanying regulations concerning the data it is considering storing in the cloud," Scott said.

Since not all cloud providers are built the same, one provider's definition of "safe" may not be the same as another's, Scott said.

7. Lack of support

Imagine being unable to access your cloud before a big meeting or, worse, being in the middle of a cyberattack that has taken down your entire bread and butter —your website. Now imagine trying to contact your provider, only to find that their customer service is nonexistent. While some cloud providers have excellent customer support, others could leave you in the cold.

"The most frustrating thing when something goes wrong is not being able to speak directly with an engineer," said April Sage, director of Healthcare Vertical at Online Tech, a cloud provider specializing on compliant cloud hosting.

"If your systems are not mission-critical, you don't need to worry so much about security and availability," Sage said. "However, if you support mission-critical systems, or your online presence is critical for your business to operate smoothly, you have to be prepared to invest in a cloud and cloud provider that is capable of providing a level of protection commensurate with your needs."

8. There's always a risk

The biggest risk when it comes to cloud computing is that you never know what is up ahead. Hackers have been around from the start and they are not going anywhere any time soon. And as technology advances, so do the risks that come with adopting them.

From security holes to support issues, below are eight risks all users take when migrating to and storing their data in the cloud.

1. Someone else is looking after your data

Unlike a data center, which is run by an in-house IT department, the cloud is an off-premise system in which users outsource their data needs to a third party provider. The provider does everything from performing all updates and maintenance to managing security. The bigger picture, however, is that users are trusting their data for someone else to look after, said Steve Santorelli, a former Scotland Yard detective, now manager of outreach at the Internet security research group Team Cymru.

"The downside is that you are abrogating responsibility for your data. Someone else has access to it and someone else is responsible for keeping it safe," Santorelli said.

Although cloud providers may ensure your data is safe, Santorelli said some are not always looking after your best interests.

"No business is ever going to be as rabid about looking after your data as you would or should be. They are in the business of making money from you, after all. Securing your data sometimes becomes a marketing mantra more than a way of life," he said.

2. Cyberattacks

Any time you store data on the Internet, you are at risk for a cyberattack. This is particularly problematic on the cloud, where volumes of data are stored by all types of users on the same cloud system.

"The scary thing is the vulnerability to Distributed Denial of Service (DDoS) attacks and the concentration of so much data," Santorelli said. "The single point of failure is the cloud. If something goes bad it impacts a very wide group of people. It's easier to steal and disrupt in bulk."

Although most cloud providers have stringent security measures, as technology becomes more sophisticated, so do cyberattacks.

"When cloud companies get the security right — and many actually do a pretty reasonable job — then miscreants have to get creative to get to the data," Santorelli said. For instance, instead of hacking the cloud, hackers will attempt to hack your account instead.

"Passwords and secret answers become the soft underbelly of your security. Just like when banks made online account hacking harder, the miscreants turned to phishing to get around the restrictions and steal your passwords," he said.

3. Insider threats

Just as cyberattacks are on the rise, so are security breaches from the inside.

"Vodafone's breach of 2 million customer records and the Edward Snowden breach at the NSA are wake-up calls that the most serious breaches are due to insider threats and privileged user access," said Eric Chiu, president and co-founder of HyTrust, a cloud infrastructure control company

Once an employee gains or gives others access to your cloud, everything from customer data to confidential information and intellectual property are up for grabs.

"The cloud makes this problem 10 times worse since administrative access to the cloud management platform, either by an employee or an attacker posing as an employee, enables access to copy and steal any virtual machine, undetected, as well as potentially destroy the entire cloud environment in a matter of minutes," Chiu said.

4. Government intrusion

With the recent NSA leaks and the ensuing reports on government surveillance programs, competitors aren't the only ones who may want to take a peek at your data.

"Something that has been in the news recently is that government entities and technology companies in the U.S. and elsewhere may be inspecting your data as it is transmitted or where it resides in the Internet, including within clouds," said Scott Hazdra, principal security consultant for Neohapsis, a security and risk management consulting company specializing in mobile and cloud security.

Granted, privacy has always been a concern with the cloud. But instead of just worrying about competitors, disgruntled customers or employees breaching cloud security, businesses now have to worry about government intrusion as well.

"Loss of confidentiality to data is not a new risk; however, the threat sources might not have been one companies were previously worried about," Hazdra said. "For instance, a company may have a concern that competitors will try to steal their data so they encrypt transmission and storage of it. Now that someone other than a competitor may be interested in that data doesn't fundamentally change the risk."

5. Legal liability

Risks associated with the cloud are not limited to security breaches. They also include its aftermath, such as lawsuits filed by or against you.

"The latest risks to using cloud for business are compliance, legal liability and business continuity," said Robert J. Scott, managing partner of Scott & Scott LLP, an intellectual property and technology law firm. "Data breach incidences are on the rise, and so are lawsuits."

Scott, who is also a cloud law speaker and author, said that while the cloud is all about ease of access, collaboration and rapidity, its benefits have to be weighed against the extent of security measures.

"Information security has always been finding a balance between ease of access and the sharing of information verses completely locked down security," he said. "The more you have of one, the less you have of the other."

6. Lack of standardization

What makes a cloud "safe"? A provider could have the latest security features, but due to the general lack of cloud standardization, there are no clear-cut guidelines unifying cloud providers. Further, given the plethora of cloud services in different sectors, this is especially problematic for users when determining exactly how "safe" their cloud really is.

"The question of how safe the cloud is has many facets, and the answer depends on the cloud services provider, the type of industry a company is in, and the accompanying regulations concerning the data it is considering storing in the cloud," Scott said.

Since not all cloud providers are built the same, one provider's definition of "safe" may not be the same as another's, Scott said.

7. Lack of support

Imagine being unable to access your cloud before a big meeting or, worse, being in the middle of a cyberattack that has taken down your entire bread and butter —your website. Now imagine trying to contact your provider, only to find that their customer service is nonexistent. While some cloud providers have excellent customer support, others could leave you in the cold.

"The most frustrating thing when something goes wrong is not being able to speak directly with an engineer," said April Sage, director of Healthcare Vertical at Online Tech, a cloud provider specializing on compliant cloud hosting.

"If your systems are not mission-critical, you don't need to worry so much about security and availability," Sage said. "However, if you support mission-critical systems, or your online presence is critical for your business to operate smoothly, you have to be prepared to invest in a cloud and cloud provider that is capable of providing a level of protection commensurate with your needs."

8. There's always a risk

The biggest risk when it comes to cloud computing is that you never know what is up ahead. Hackers have been around from the start and they are not going anywhere any time soon. And as technology advaFrom security holes to support issues, below are eight risks all users take when migrating to and storing their data in the cloud.

1. Someone else is looking after your data

Unlike a data center, which is run by an in-house IT department, the cloud is an off-premise system in which users outsource their data needs to a third party provider. The provider does everything from performing all updates and maintenance to managing security. The bigger picture, however, is that users are trusting their data for someone else to look after, said Steve Santorelli, a former Scotland Yard detective, now manager of outreach at the Internet security research group Team Cymru.

"The downside is that you are abrogating responsibility for your data. Someone else has access to it and someone else is responsible for keeping it safe," Santorelli said.

Although cloud providers may ensure your data is safe, Santorelli said some are not always looking after your best interests.

"No business is ever going to be as rabid about looking after your data as you would or should be. They are in the business of making money from you, after all. Securing your data sometimes becomes a marketing mantra more than a way of life," he said.

2. Cyberattacks

Any time you store data on the Internet, you are at risk for a cyberattack. This is particularly problematic on the cloud, where volumes of data are stored by all types of users on the same cloud system.

"The scary thing is the vulnerability to Distributed Denial of Service (DDoS) attacks and the concentration of so much data," Santorelli said. "The single point of failure is the cloud. If something goes bad it impacts a very wide group of people. It's easier to steal and disrupt in bulk."

Although most cloud providers have stringent security measures, as technology becomes more sophisticated, so do cyberattacks.

"When cloud companies get the security right — and many actually do a pretty reasonable job — then miscreants have to get creative to get to the data," Santorelli said. For instance, instead of hacking the cloud, hackers will attempt to hack your account instead.

"Passwords and secret answers become the soft underbelly of your security. Just like when banks made online account hacking harder, the miscreants turned to phishing to get around the restrictions and steal your passwords," he said.

3. Insider threats

Just as cyberattacks are on the rise, so are security breaches from the inside.

"Vodafone's breach of 2 million customer records and the Edward Snowden breach at the NSA are wake-up calls that the most serious breaches are due to insider threats and privileged user access," said Eric Chiu, president and co-founder of HyTrust, a cloud infrastructure control company

Once an employee gains or gives others access to your cloud, everything from customer data to confidential information and intellectual property are up for grabs.

"The cloud makes this problem 10 times worse since administrative access to the cloud management platform, either by an employee or an attacker posing as an employee, enables access to copy and steal any virtual machine, undetected,
as well as potentially destroy the entire cloud environment in a matter of
minutes," Chiu said.

4. Government intrusion

With the recent NSA leaks and the ensuing reports on government surveillance programs, competitors aren't the only ones who may want to take a peek at your data.

"Something that has been in the news recently is that government entities and technology companies in the U.S. and elsewhere may be inspecting your data as it is transmitted or where it resides in the Internet, including within clouds," said Scott Hazdra, principal security consultant for Neohapsis, a security and risk management consulting company specializing in mobile and cloud security.

Granted, privacy has always been a concern with the cloud. But instead of just worrying about competitors, disgruntled customers or employees breaching cloud security, businesses now have to worry about government intrusion as well.

"Loss of confidentiality to data is not a new risk; however, the threat sources might not have been one companies were previously worried about," Hazdra said. "For instance, a company may have a concern that competitors will try to steal their data so they encrypt transmission and storage of it. Now that someone other than a competitor may be interested in that data doesn't fundamentally change the risk."

5. Legal liability

Risks associated with the cloud are not limited to security breaches. They also include its aftermath, such as lawsuits filed by or against you.

"The latest risks to using cloud for business are compliance, legal liability and business continuity," said Robert J. Scott, managing partner of Scott & Scott LLP, an intellectual property and technology law firm. "Data breach incidences are on the rise, and so are lawsuits."

Scott, who is also a cloud law speaker and author, said that while the cloud is all about ease of access, collaboration and rapidity, its benefits have to be weighed against the extent of security measures.

"Information security has always been finding a balance between ease of access and the sharing of information verses completely locked down security," he said. "The more you have of one, the less you have of the other."

6. Lack of standardization

What makes a cloud "safe"? A provider could have the latest security features, but due to the general lack of cloud standardization, there are no clear-cut guidelines unifying cloud providers. Further, given the plethora of cloud services in different sectors, this is especially problematic for users when determining exactly how "safe" their cloud really is.

"The question of how safe the cloud is has many facets, and the answer depends on the cloud services provider, the type of industry a company is in, and the accompanying regulations concerning the data it is considering storing in the cloud," Scott said.

Since not all cloud providers are built the same, one provider's definition of "safe" may not be the same as another's, Scott said.

7. Lack of support

Imagine being unable to access your cloud before a big meeting or, worse, being in the middle of a cyberattack that has taken down your entire bread and butter —your website. Now imagine trying to contact your provider, only to find that their customer service is nonexistent. While some cloud providers have excellent customer support, others could leave you in the cold.

"The most frustrating thing when something goes wrong is not being able to speak directly with an engineer," said April Sage, director of Healthcare Vertical at Online Tech, a cloud provider specializing on compliant cloud hosting.

"If your systems are not mission-critical, you don't need to worry so much about security and availability," Sage said. "However, if you support mission-critical systems, or your online presence is critical for your business to operate smoothly, you have to be prepared to invest in a cloud and cloud provider that is capable of providing a level of protection commensurate with your needs."

8. There's always a risk

The biggest risk when it comes to cloud computing is that you never know what is up ahead. Hackers have been around from the start and they are not going anywhere any time soon. And as technology advances, so do the risks that come with adopting them.

How internal data breaches happen

There are numerous outlets for data on the modern PC, including USB and Firewire ports, CD and DVD recorders and even built-in storage media slots. Combined with the fact that storage space on portable devices has rapidly increased, business professionals can now use personal storage devices, such as USB memory sticks, iPods, digital cameras and smart phones, to remove or copy sensitive information either for malicious intent or personal gain.

This type of method is also known as "podslurping", whereby an employee downloads a large amount of important data to their iPod or MP3 device. The USB port can extract data at high speed in a variety of ways, including removable hard drives and media players. This makes the USB port one of the most vulnerable points of attack for stealing sensitive and confidential data such as customer records, bank account numbers, patient medical records and internal account information.

Another growing threat is "bluesnarfing", which involves the theft of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs.

How internal data breaches can be prevented

So how can organisations reduce the risk of employees walking away with data?

Organisations need to take a proactive approach and prevent potential breaches while dealing with the challenge that USB storage devices are heavily relied on by businesses to conveniently transport and transfer data.

Developing a rigid "no-use" policy could hamper normal business operation for many employees, such as remote workers. The solution is a compromise developing strict policies for USB port use on a user-specific basis, rather than prohibiting the use of all portable devices.

Through third-party software, IT administrators have the power to be more granular when setting policies. For example, policies can be set to allow "read-only" access on available devices for a specific set of users, while completely allowing (or denying) access for others. Further, these policies can be applied to both local and remote users. Businesses should look for software solutions that can lock all possible avenues of data leakage, and put permissions and policies in place to control who has access to which files, where and when.

In addition, it is important IT administrators can report and track data breaches. Central collection of an audit trail enables administrators to see all attempts at restricted activities including: the person involved the type of activity and when and where the breach was attempted.

The implementation of a strong and flexible security policy is essential to creating a healthy balance between organisations and employees. In the end, a high-quality third party security software solution can provide rules and permissions that are understandable to both the employee and those implementing them so that data is prevented from leaving the office.

How to Reduce Security Breaches in Cloud Computing Networks

Cloud security has to be a part of your company's overall security strategy. Reducing security breaches in cloud computing networks requires planning and strategy to be successful. Companies need to devote just as much energy toward securing their cloud as they do securing their data center, buildings, people, and information.

Security risks, threats, and breaches can come in so many forms and from so many places that many companies take a comprehensive approach to security management. Many companies will focus on the broad range of potential vulnerabilities to its data center as well as ways to safeguard sensitive corporate, customer, and partner information, including using built-in applications and data level protections. Even with all that, it's not always enough.

In general, follow these steps to reduce the risk of suffering security breaches:

1. Authenticate all people accessing the network.
2. Frame all access permissions so users have access only to the applications and data that they've been granted specific permission to access.
3. Authenticate all software running on any computer — and all changes to such software.

   This includes software or services running in the cloud.

   Your cloud provider needs to automate and authenticate software patches and configuration changes, as well as manage security patches in a proactive way. After all, many service outages come from configuration mistakes.

4. Formalize the process of requesting permission to access data or applications.

   This applies to your own internal systems and the services that require you to put your data into the cloud.

5. Monitor all network activity and log all unusual activity.

   Deploy intruder-detection technology. Even if your cloud services provider enables you to monitor activities on its environment, you should have an independent view.

   Even when cloud operators have good security (physical, network, OS, application infrastructure), it is *your* company's responsibility to protect and secure your applications and information.

6. Log all user activity and program activity and analyze it for unexpected behavior.

   Nearly 70 percent of security breaches are caused by insiders (or by people getting help from insiders). Insiders rarely get caught.

7. Encrypt, up to the point of use, all valuable data that needs extra protection.
8. Regularly check the network for vulnerabilities in all software exposed to the Internet or any external users.

   Given the importance of security in the cloud environment, you might assume that a major cloud services provider would have a set of comprehensive service level agreements for its customers. In fact, many of the standard agreements are intended to protect the service provider — not the customer.

What happens when cloud data is lost?

The basic idea - that data and software are hosted remotely - has many benefits, but its reputation has just taken a serious knock.

Users of T-Mobile's Sidekick service got a taste of the downside of cloud computing this month when they went to their cloud-stored applications to find the data cupboards bare. All their photos, calendar entries, notes and contacts had vanished.

Though at first it seemed that their data was lost forever, Microsoft - whose technology is behind the system - says now that most, if not all customer data has been recovered.

This was no doubt painful and distressing for people whose only copies of beloved photos or vital information seemed lost, but consumer services are often run with a higher tolerance for error.

But what if the servers had held your corporate data? More and more companies are entrusting their data and processing needs to cloud-based providers.

The upsides of the cloud often include affordable monthly fees, rather than huge capital outlays, and access to bursts of massive processing power or storage as and when it is needed.

The Sidekick debacle offers some lessons for corporate customers. They should realise, just as Sidekick users have, that no operator is perfect. Just as your own IT department can lose data forever, so can an outsourced service. Major bugs or glitches you can't predict or prevent; what you can do is minimise the damage.

That is all to do with the contract you are offered when you sign up to a hosted service. The standard terms and conditions that accompany most cloud services are drafted heavily in favour of the service provider. That should come as no surprise. These agreements typically exclude all liability for the corruption or irretrievable loss of data, and they come with almost no guarantees. If the service fails, tough luck: you'll get service credits - ie, a few extra days of service for nothing - and that's your lot.

As many cloud services are provided free, or at a low price, small businesses are rarely in a position to negotiate better terms. They must take the standard offer or leave it. But if you are paying big bucks for the service, and especially if you are entrusting mission critical data to a cloud provider, there are risks that absolutely must be catered for in the agreement or managed externally using additional systems.

You are unlikely to persuade a supplier to guarantee compensation for a data disaster - but you can take steps to minimise the likelihood of a disaster and its impact on your business.

Find out how the service provider will protect your data from corruption. Microsoft made backups of the Sidekick data, but the failure wrecked the copies as well as the live database. A similar issue hit Magnolia, a website bookmark storage provider, earlier this year when its live database became corrupted. Magnolia's backup process dutifully kicked in and overwrote the only good copy of the data there was.

So be prepared to demand information on how backups are taken and how that data is checked for integrity. If you're not satisfied with the responses, negotiate alternative arrangements or walk away.

Also find out how you can retrieve your data from the service provider. You might want to move to a new supplier in the future, or your service provider might go out of business. Will your data be in a format that can be migrated easily to a replacement service? Answering these basic questions before selecting a provider can save great pain and expense further down the line.

What are the considerations and risks of using persistent block storage?

- Data loss is expected: Say what? Yes, that's right: it's not if, but when, these volumes will fail, just like physical hard drives. Cloud providers are trying to be forthright about this reality. For example, Amazon EBS publicly gives an expected annual failure rate (AFR) of around 0.5% for an EBS volume. The developer docs for Google Compute Engine warn, "To protect against data loss, always back up your data and have data recovery policies in place." To put this into another perspective, if you have 100 customers running in the cloud, each with 2 EBS volumes (one OS and one data), then you can expect about 1 EBS volume to fail each year.
- Silent data corruption is possible: Unless systems are engineered from the ground up to address silent data corruption from end-to-end, previously stored data and new data is at risk of being corrupted. Public clouds are no different. Amazon engineers have stated in forums that silent data corruption with EBS volumes is possible. eFolder is only one of a small handful of storage cloud providers that openly discusses and guards against silent data corruption. Certainly none of the big players are addressing this. (If you know of examples where they are, please send me details!)
- Write caching issues: Another problem is caused by how a cloud provider caches writes and flushes writes to stable storage. In a serious outage event (e.g., as in the recent June 29th AWS outage), data writes that were temporarily in flight may not be properly flushed to disk. Cloud providers are not fully disclosing how they are handling commit, cache flush, or "fsync" operations. For example, Amazon's comments here and here indicate that volume corruption was possible because of the recent outage, and were placing any EBS volumes that had in-flight writes at the time of the failure in an "impaired" state until users manually checked (e.g., chkdsk'd) their volumes and manually resumed I/O. Even if the filesystem was OK, this could have potentially catastrophic consequences for critical applications (e.g., databases) that depend on storage properly honoring cache flushes and write ordering guarantees. It's the same problem as if you were running a database server on a RAID controller with write caching turned on but without a battery-backed (or capacitor-backed) write cache and the power goes out. You'd have to run some application-specific integrity checks to be sure your data was good still.Guaranteeing proper write ordering and flush semantics is difficult and must be dealt with at every layer in the cloud — inside the instance OS and paravirtualized device drivers, in the hypervisor, in the hypervisor "host" OS (if relevant), in the network, in the storage processing nodes, in the storage HBAs, in the enclosure storage controllers, and in the hard drives themselves. Rather than engineer cloud services to fully guarantee data integrity, public cloud services have been engineered for performance and scale, and instead give the expectation that data loss and corruption are possible and expected to happen.

Account or Service Hijacking:

Account or service hijacking is not new. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks.

Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.

Examples

No public examples are available at this time.

Remediation

- Prohibit the sharing of account credentials between users and services.
- Leverage strong two-factor authentication techniques where possible.
- Employ proactive monitoring to detect unauthorized activity.
- Understand cloud provider security policies and SLAs.

Definition - What does Account Hijacking mean?

Account hijacking is a process through which an individual's email account, computer account or any other account associated with a computing device or service is stolen or hijacked by a hacker.

It is a type of identity theft in which the hacker uses the stolen account information to carry out malicious or unauthorized activity.

How Safe is Your Cloud Data from Service Traffic Hijacking?

In a recent survey, 69 percent of North American IT professionals expressed a belief that the risks of using a cloud based service currently outweighed the benefits. The main reason cited was a concern over data security. This concern has made many business leaders hesitant to switch over to the cloud, but the reality is the cloud is growing and is not going away, especially with the possibility of big data cloud computing.

In fact, Forrester Research predicts that the cloud business will grow from its current worth at $40 billion to $160 billion by 2020. Rather than ignoring the cloud, business leaders should learn about the vulnerabilities, what their implications are and the steps they can take to protect their

data. This article will specifically address the vulnerability to service traffic hijacking and how it can be addressed.

Service Traffic Hijacking Vulnerabilities

In its 2013 report the Cloud Security Alliance identified service traffic hijacking as the third-greatest cloud computing security risk. In this type of security breach, hackers seek to hijack your account by stealing your security credentials and then eavesdropping on your activities and transactions. These hackers can also manipulate your data, insert false information and redirect your clients to illegitimate sites.

This type of vulnerability is particularly scary because hackers are able to use your reputation and the trust you have built up to manipulate your clients. In 2010, Amazon faced an attack that allowed hackers to steal the session IDs that grant users access to their accounts after entering their passwords. This left the client's credentials exposed to the hackers. The bug was removed 12 hours after it was discovered, but many Amazon users unknowingly fell for the attack during that time.

Implications for Businesses

It's not hard to imagine the negative implications a data breach like Amazon's would have on a company. Depending on what the hacker chose to do with the information, you could be left with your integrity and reputation destroyed or with confidential data leaked or falsified. For companies in highly regulated industries, such as health care, this could even have potential legal implications if client's confidential data was exposed.

Tips to Ensure Safety

Some businesses looking to stem this threat may decide to take the wait and see approach. Industry standards for cloud platforms are still being developed, and many businesses are waiting until more standards are in place to ensure the safety of their data and compliance with the law. While this option does eliminate some security risks, these company's are also risking not taking advantage of this platform while their competitors are.

Instead, there are some proactive steps companies can take to protect themselves. For example, companies can do this by:

1. Setting up protocol that prohibits sharing account credentials between employees or services.
2. Using a strong two-factor authentication technique and track employee use of the platform for unauthorized activity.
3. Utilizing a secure encryption management system, such as that offered by Venafi, should also be prioritized and developed specifically for use with a cloud platform.

As businesses select a cloud service provider they should go through potential contracts carefully and make comparisons of the clouds' security and data-integrity systems. Try to take a data-driven approach when evaluating potential cloud service providers rather than relying on inaccurate or out-of-date anecdotal evidence. Factors to look at include the number of data loss or interference incidents a cloud service experienced compared to members of your organization. How often does the cloud experience downtime and how does it monitor and manage vulnerabilities? Does the contract grant you access to this data, and will you be able to audit the cloud's performance in these areas?

Ultimately, an organization's data faces the risk of exposure no matter where it is housed, so companies should stay up to date on the threats and take the proper precautions to increase security. As the cloud continues to develop new insights and regulations will come into place that will hopefully make the transition easier and less risky for business leaders.

ways to reduce risk and security breaches

• Encrypt: as a baseline, unbreakable code – like military grade 256-bit AES – can scramble sensitive information into undecipherable gibberish to protect it from unauthorised viewers. Installing a cloud information protection platform at the network's edge ensures any data moving to the cloud is fully protected before it leaves the organisation.
• Retain keys: keep the keys that encrypt and decipher information under the control of the user organisation. This ensures that all information requests must involve the owner, even if information is stored on a third-party cloud.
• Cloud data loss prevention: customise policies on this to scan, detect and take action to protect information according to its level of sensitivity. This provides an additional level of security and control.
• Cloud malware detection: screen information exchanges, including external and internal user uploaded attachments, in cloud applications in real-time for virus, malware and other embedded threats.

1. Know who's accessing what
People within your organisation who are privileged users, – such as database administrators and employees with access to highly valuable intellectual property – should receive a higher level of scrutiny, receive training on securely handling data, and stronger access control.

2. Limit data access based on user context
Change the level of access to data in the cloud depending on where the user is and what device they are using. For example, a doctor at the hospital during regular working hours may have full access to patient records. When she's using her mobile phone from the neighborhood coffee shop, she has to go through additional sign-on steps and has more limited access to the data.

3. Take a risk-based approach to securing assets used in the cloud
Identify databases with highly sensitive or valuable data and provide extra protection, encryption and monitoring around them.

4. Extend security to the device
Ensure that corporate data is isolated from personal data on the mobile device. Install a patch management agent on the device so that it is always running the latest level of software. Scan mobile applications to check for vulnerabilities.

5. Add intelligence to network protection
The network still needs to be protected – never more so than in the cloud. Network protection devices need to have the ability to provide extra control with analytics and insight into which users are accessing what content and applications.

6. Build in the ability to see through the cloud

Security devices, such as those validating user IDs and passwords, capture security data to create the audit trail needed for regulatory compliance and forensic investigation. The trick is to find meaningful signals about a potential attack or security risk in the sea of data points.

Aspects of Identity Management in Cloud Computing

Identity management is a broad topic that applies to most areas of the data center. However, it's particularly important in protecting the cloud computing environment. Because the cloud is about sharing and virtualizing physical resources across many internal (and often external) users, you must know who has access to what services.

1. Corralling the data with identity management in cloud computing

Identity data generally is scattered around systems. Establish a common database or directory as a first step in gaining control of this information. This step involves inputting data to and gathering data from various user directories.

2. Integrating a cloud computing identity management system

An identity management system must integrate effectively with other applications. In particular, the system must have a direct interface to the following:

- Human resources system, where new joiners and leavers are first recorded
- Supply-chain systems, if partners and suppliers use corporate systems
- Customer databases (if customers require access to some systems), although customer identity management normally is handled by a separate component of an identity management system

3. Beefing up authentication for access to the cloud computing system

When you require authentication stronger than passwords, the identity management system must work with products that provide that authentication, such as biometric systems (fingerprints, handprints, iris verification, and the like) and identity token systems.

4. Provisioning for cloud computing

When you link all systems that use identity information, you can automate provisioning. If this process is automated, a single status change (of an employee or anyone else with access rights) can be defined in the identity management system and sent across all affected systems from that point.

When provisioning is automated, users rarely (or never) get more access than necessary. Providing broad levels of access happens frequently in manual provisioning because it's easier to specify broad access. Additionally, an automated process never fails to revoke former employees' access to the network.

5. Single sign-on function for cloud computing

Single sign-on means providing all users an interface that validates identity as soon as a user signs on anywhere; this interface requires the user to enter a single password. Thereafter, all systems should know the user and her permissions.

Some single sign-on products don't provide the full gamut of identity management capabilities, but all identity management products deliver single sign-on capability.

6. Security administration and cloud computing

Identity management reduces security administration costs because security administrators don't have to manually authorize; the identity management system handles that workflow automatically.

The automatic ID management handling is particularly useful for organizations that have distributed security administration over several locations because it enables security administration to be centralized.

7. Analyzing data in the cloud

After you centralize all user data, you can generate useful reports on resource and application use or carry out security audits. For example:

- If you're having problems with internal hacking you can check a log that lists every user's activity.
- If you have logging software for databases and files, you can monitor who did what to any item of data and when, including who looked at specific items of data. This audit capability is important for implementing data privacy and data protection compliance.

Considerations for Identity Management in Cloud Computing

How do organizations achieve effective identity management in cloud computing without losing control over internally provisioned applications and resources? Context is king. Who is doing what, what is their role and what are they trying to access? This requires the use of threat-aware identity and access management capabilities in order to secure their extended enterprise.

Tying user identities to back-end directories is a must, even for external identities. For this, systems should be used to provide cloud-based bridges to directories. Special attention should be paid to privileged users, which cost US businesses $348 billion per year in corporate losses, according to SC Magazine. Single sign-on capabilities are also a must since having too many passwords tends to lead to insecure password management practices.

Recent research reported by Dark Reading shows that 61 percent of people use the same password for multiple accounts and applications. Deprovisioning of access when it is no longer required is another absolute necessity since orphan accounts caused by poor deprovisioning leaves organizations open to fraud and other security incidents. According to recent research by GroupID, 19 percent of employees change job responsibilities each year, and on average, 5 percent of users in Active Directory are no longer employed by the organization.

But how do you prove that everything is working correctly? For compliance and corporate oversight purposes, all activities related to application access and authorization should be monitored, with comprehensive audit and reporting capabilities provided at a granular level so that all activities can be attributed to specific individuals. The security measures provided are another important consideration to reduce risks associated with fraud, theft or loss of customer data or sensitive, valuable information such as intellectual property.

How to Benefit From Identity Management in Cloud Computing

Identity management's primary goal in cloud computing is managing personal identity information so that access to computer resources, applications, data, and services is controlled properly. Identity management is the one area of IT security that offers genuine benefits beyond reducing the risk of security breaches.

Identity management helps prevent security breaches and plays a significant role in helping your company meet IT security compliance regulations. The benefits of keeping your customer or company financial data safe from unauthorized access can be huge.

In addition, you reap many benefits from identity management that occurs every day, not just during a major threat.

- Improved user productivity: Productivity improvement comes from simplifying the sign-on interface and the ability to quickly change access rights. Productivity is likely to improve further where you provide user self-service.
- Improved customer and partner service: Customers and partners also benefit from a more streamlined, secure process when accessing applications and data.
- Reduced help desk costs: IT help desks typically experience fewer calls about forgotten passwords when an identity management process is implemented.

- Reduced IT costs: Identity management enables automatic *provisioning*, providing or revoking users' access rights to systems and applications. Provisioning happens whether you automate it or not.

  In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it.[1] Encryption does not of itself prevent interception, but denies the message content to the interceptor.[2]:374 In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, generating ciphertext that can only be read if decrypted.[2] For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skill are required. An authorised recipient can easily decrypt the message with the key, provided by the originator to recipients but not to unauthorised interceptors.

  Types of encryption:

  1. *Symmetric*

Symmetric cryptography, also called private-key cryptography, is one of the oldest and most secure encryption methods. The term "private key" comes from the fact that the key used to encrypt and decrypt data must remain secure because anyone with access to it can read the coded messages. A sender encodes a message into ciphertext using a key, and the receiver uses the same key to decode it.

People can use this encryption method as either a "stream" cipher or a "block" cipher, depending on the amount of data being encrypted or decrypted at a time. A stream cipher encrypts data one character at a time as it is sent or received, while a block cipher processes fixed chunks of data. Common symmetric encryption algorithms include Data Encryption Standard (DES), Advanced Encryption Standard (AES), and International Data Encryption Algorithm (IDEA).

2. Asymmetric, or public key, cryptography is, potentially, more secure than symmetric methods of encryption. This type of cryptography uses two keys, a "private" key and a "public key," to perform encryption and decryption. The use of two keys overcomes a major weakness in symmetric key cryptography, since a single key does not need to be securely managed among multiple users. In asymmetric cryptography, a public key is freely available to everyone and used to encrypt messages before sending them. A different, private key remains with the receiver of ciphertext messages, who uses it to decrypt them. Algorithms that use public key encryption methods include RSA and Diffie-Hellman.

- SSL (Secure Sockets Layer) is a standard security technology for establishing an encrypted link between a server and a client—typically a web server (website) and a browser; or a mail server and a mail client (e.g., Outlook).
- SSL allows sensitive information such as credit card numbers, social security numbers, and login credentials to be transmitted securely. Normally, data sent between browsers and web servers is sent in plain text—leaving you vulnerable to eavesdropping. If an attacker is able to intercept all data being sent between a browser and a web server they can see and use that information.
- More specifically, SSL is a security protocol. Protocols describe how algorithms should be used; in this case, the SSL protocol determines variables of the encryption for both the link and the data being transmitted.

What is an SSL Certificate and How Does it Work?

SSL Certificates have a key pair: a public and a private key. These keys work together to establish an encrypted connection. The certificate also contains what is called the "subject," which is the identity of the certificate/website owner.

To get a certificate, you must create a Certificate Signing Request (CSR) on your server. This process creates a private key and public key on your server. The CSR data file that you send to the SSL Certificate issuer (called a Certificate Authority or CA) contains the public key. The CA uses the CSR data file to create a data structure to match your private key without compromising the key itself. The CA never sees the private key.

Once you receive the SSL Certificate, you install it on your server. You also install a pair of intermediate certificates that establish the credibility of your SSL Certificate by tying it to your CA's root certificate. The instructions for installing and testing your certificate will be different depending on your server.

UNIT 3

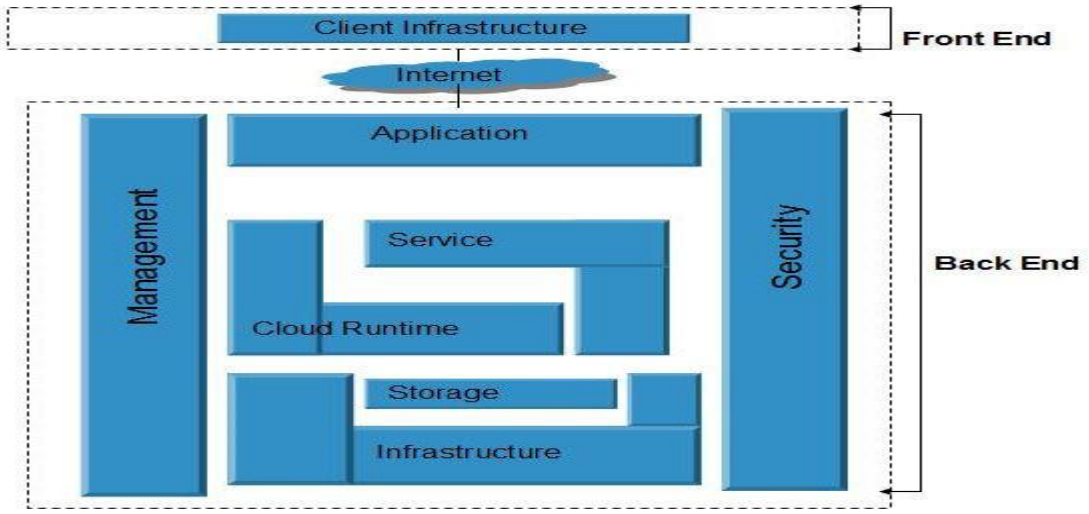
A cloud service is any resource that is provided over the Internet.

Cloud services means services made available to users on demand via the Internet from a cloud computing provider's servers as opposed to being provided from a company's own on-premises servers. Cloud services are designed to provide easy, scalable access to applications, resources and services, and are fully managed by a cloud services provider.
A cloud service can dynamically scale to meet the needs of its users, and because the service provider supplies the hardware and software necessary for the service, there's no need for a company to provision or deploy its own resources or allocate IT staff to manage the service. Examples of cloud services include online data storage and backup solutions, Web-based e-mail services, hosted office suites and document collaboration services, database processing, managed technical support services and more.

The Cloud Computing architecture comprises of many cloud components, each of them are loosely coupled. We can broadly divide the cloud architecture into two parts:

- Front End
- Back End

Each of the ends are connected through a network, usually via Internet. The following diagram shows the graphical view of cloud computing architecture:



FRONT END

Front End refers to the client part of cloud computing system. It consists of interfaces and applications that are

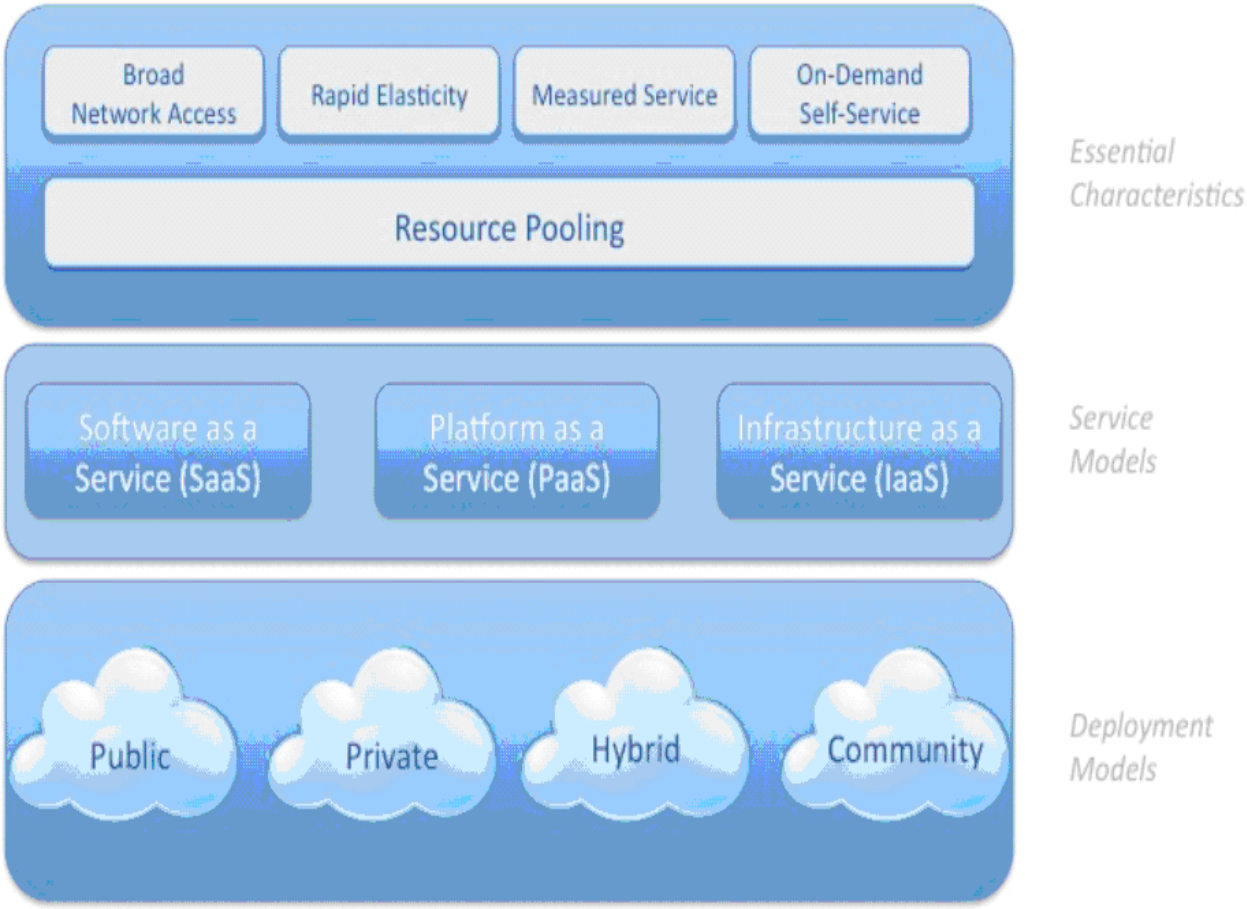
required to access the cloud computing platforms, e.g., Web Browser.

BACK END

Back End refers to the cloud itself. It consists of all the resources required to provide cloud computing services. It comprises of huge data storage, virtual machines, security mechanism, services, deployment models, servers, etc.

Important Points

- It is the responsibility of the back end to provide built-in security mechanism, traffic control and protocols.
- The server employs certain protocols, known as middleware, helps the connected devices to communicate with each other.



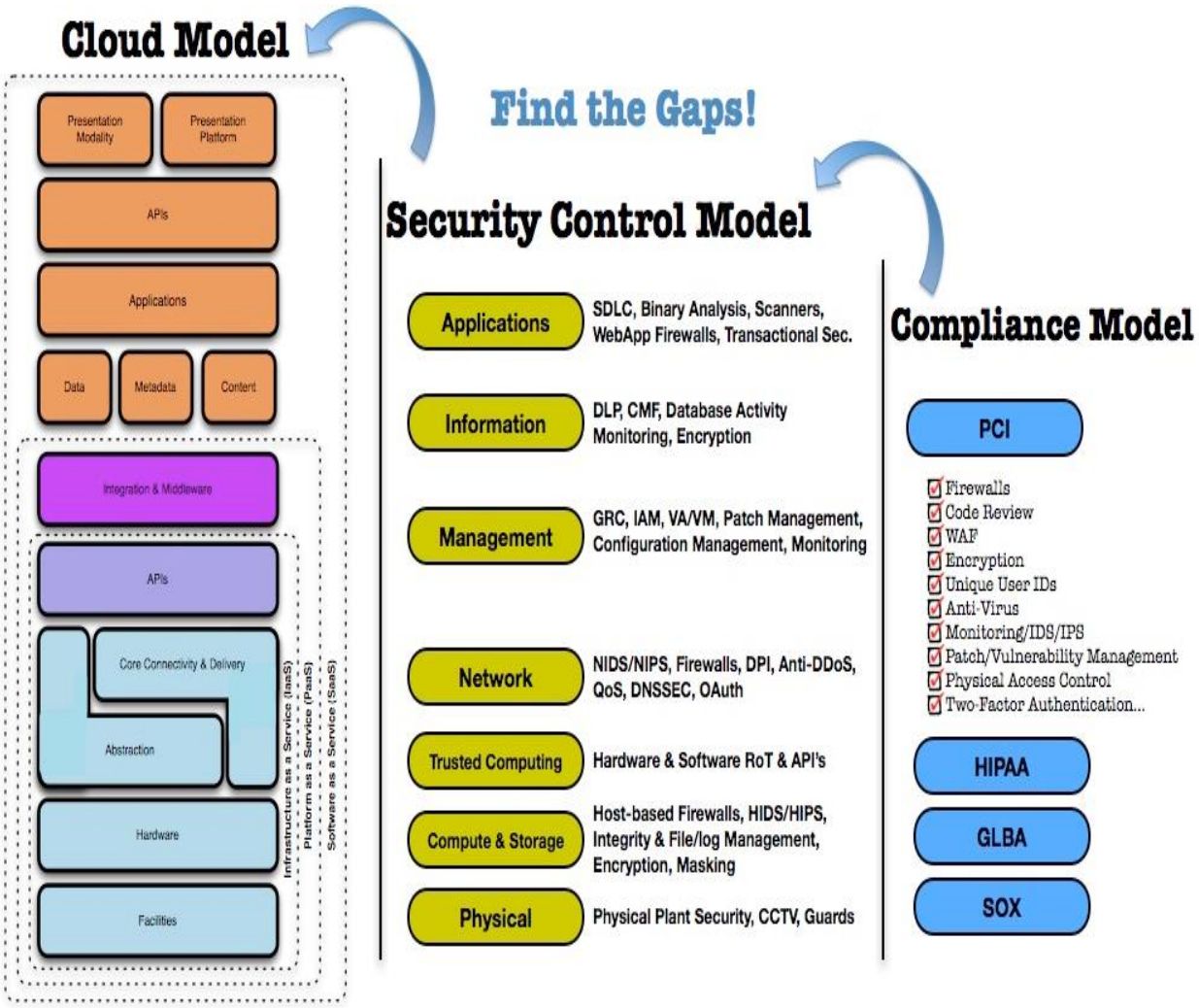


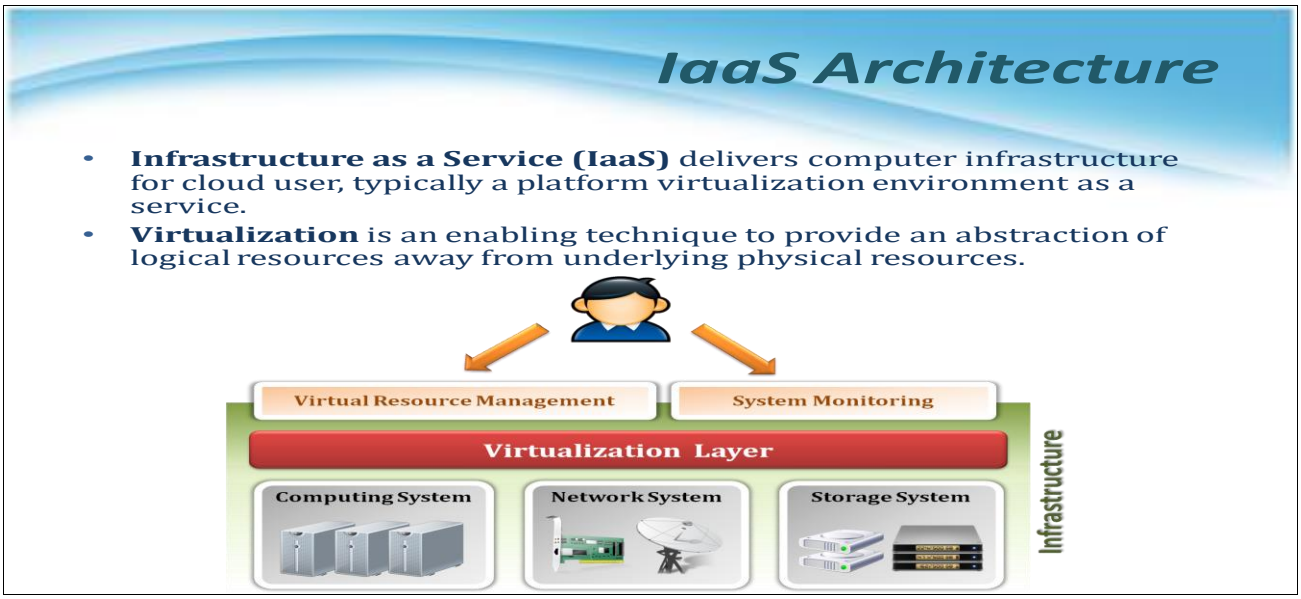
Figure shows reference model of cloud computing

Service Models:

- *Cloud Software as a Service (SaaS).* The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- *Cloud Platform as a Service (PaaS).* The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers,

operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

- *Cloud Infrastructure as a Service (IaaS)*. The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).



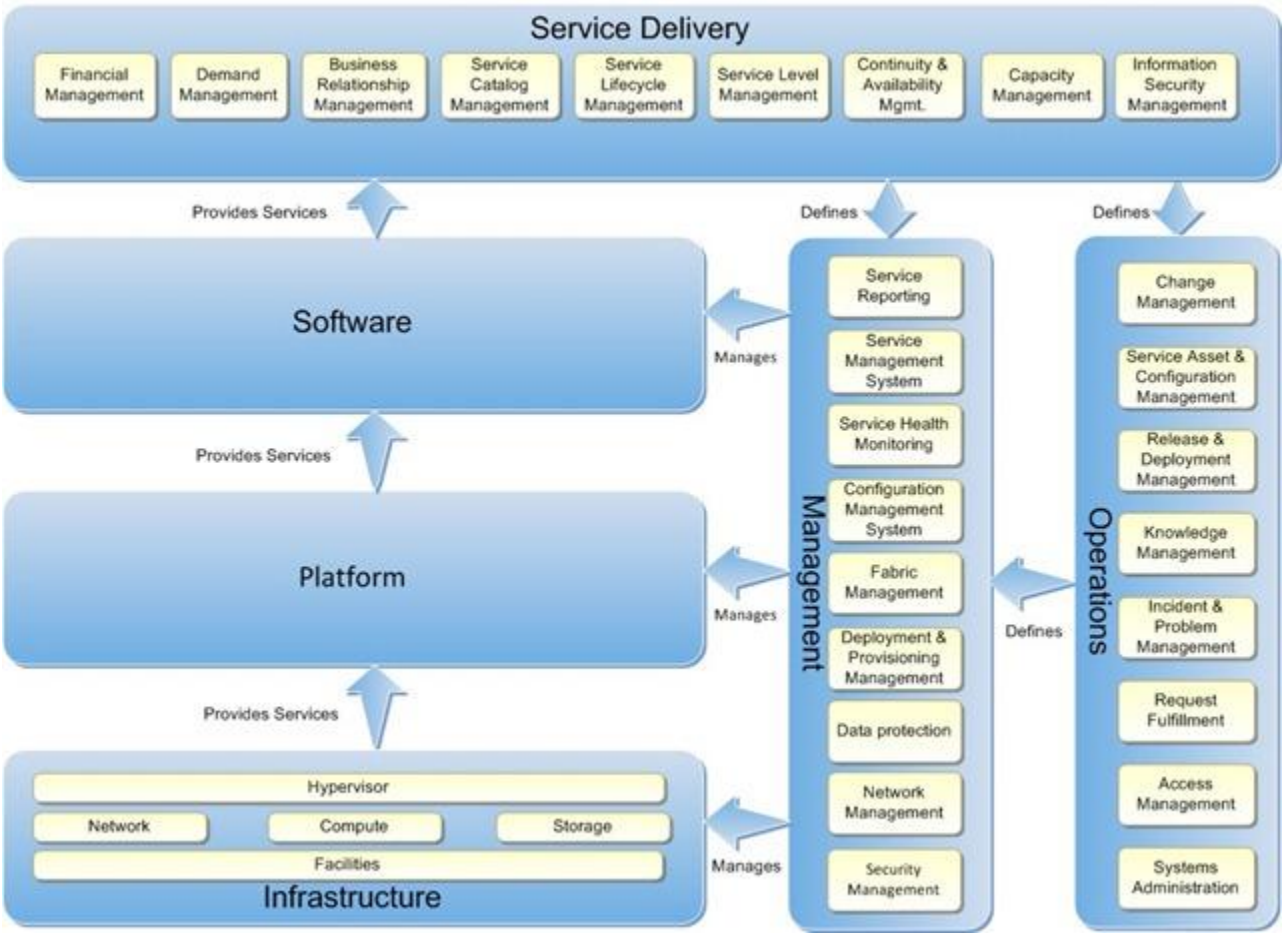
Comparison of Cloud Service Models

Type	Consumer	Service Provided By Cloud	Service Level Coverage	Customization
SaaS	End user	• Finished application	• Application uptime • Application Performance	• Minimal to no customization • Capabilities dictated by market or provider
PaaS	Application owner	• Runtime environment for application code • Cloud storage • Other Cloud services such as integration	• Environment availability • Environment performance • No application coverage	• High degree of application level customization available within constraints of the service offered • Many applications will need to be rewritten
IaaS	Application owner or IT provides OS, middleware and application support	• Virtual server • Cloud storage	• Virtual server availability • Time to provision • No platform or application coverage	• Minimal constraints on applications installed on standardized virtual OS builds

Expanding the Reference Model

In the content above we describe several characteristics, service models and deployment models that are aligned to the NIST definition of cloud computing. Now we couple this with Infrastructure layer components that are briefly described in the Blueprint for Private Cloud Infrastructure as a Service and expand the Infrastructure Layer in the Private Cloud Reference Model.

This expanded reference model illustrated in the figure below shall be the basis of the Private Cloud Infrastructure as a Service architecture design contained in this series.



Throughout the Infrastructure as a Service series the focus will be upon the Infrastructure Layer of the Reference Model however as illustrated the Infrastructure Layer has a light coupling with the Management Layer and the Platform Layer. Further the Infrastructure and Management Layers are influenced by the Operations Layer. Certain key areas of the Management Layer such as Fabric Management are covered in detail in this Infrastructure as a Service series while remaining areas of the Management, Operations Layer and Service Delivery Layers are covered in later or future content in the Private Cloud Reference Architecture.

We can now define that Private Cloud Infrastructure as IaaS is an advanced state of IT maturity that has a high degree of automation, integrated-service management, and efficient use of resources. Virtualization can be a key enabler of IaaS but in most models, including the NIST cloud definition, virtualization as common, not and essential, attribute. An infrastructure that is 100 percent virtualized may have no process automation; it might not provide management and monitoring of applications that are running inside virtual machines (VMs) or IT services that are

provided by a collection of VMs. In addition to virtualization, several other infrastructure-architecture layers are required to achieve the essential cloud attributes.

A rich automation capability is required. Automation must be enabled across all hardware components—including server, storage, and networking devices—as well as all software layers, such as operating systems, services, and applications. The Windows Management Framework—which comprises Windows Management Instrumentation (WMI), Web Services-Management (WS-Management), and Windows PowerShell—is an example of a rich automation capability that was initially scoped to Microsoft products, but that is now being leveraged by a wide variety of hardware and software partners.

A management layer that leverages automation and functions across physical, virtual, and application resources is another required layer for higher IT maturity. The management system must be able to deploy capacity, monitor health state, and automatically respond to issues or faults at any layer of the architecture.

Orchestration that manages all of the automation and management components must be implemented as the interface between the IT organization and the infrastructure. Orchestration provides the bridge between IT business logic, such as "deploy a new web-server VM when capacity reaches 85 percent," and the dozens of steps in an automated workflow that are required to actually implement such a change.

The IaaS solution’s primary purpose is to host other higher layers such as the PaaS and SaaS.

The final layer is the Service Delivery layer providing interfaces for both service providers and service consumers.

The integration of virtualization, automation, management, and orchestration layers provides the foundation for achieving the highest levels of IT maturity.

High Level Design Concerns

Several key concerns must be established that are cross cutting in the overall design of a Private Cloud Infrastructure as a Service design. These concerns are grounded in the Private Cloud Reference Architecture and expanded here in the context of providing Infrastructure as a Service.

Datacenter and Location

The physical datacenter is the enterprise facility where the organizations cloud capability is deployed. When providing cloud services we generally think of services that just exist and not where they exist. However the physical datacenter we must consider location. For some organizations their datacenter may exist in one or more corporate locations. For large

organization there may be dedicated facilities just for location of their datacenter(s). Increasingly these considerations include locations that offer climates that enable the use of nature air to provide environmental climate control within the datacenter and reducing energy consumption. Location may also provide access to low cost costs for energy consumed by the datacenter. Location of a datacenter plays an active role in the design of Private Cloud Fault Domains and options available to the IT consumer when selecting capabilities to purchase and deploy through Private Cloud Self Service.

Scale Units

The Private Cloud Reference Architecture defines the private cloud pattern of a Scale Unit. However there is no specific predefined set or selection of values that comprise a scale unit. The determination is part of the private cloud design and planning process. A Scale Unit is a pool of compute, storage, and network resources that can be deployed as a single unit or in bundles that allow both extensibility and reuse or reallocation without physical reconfiguration. Examples of these resources are:

- Compute – Blade servers, deployed by one or more racks at a time.
- Storage – Enterprise SAN, with disk capacity to match compute capability.
- Network – New access and distribution designs to meet compute and storage requirements.

When selecting elements of a scale unit the architect should consider future availability as changes in hardware architectures will influence Management Fabric implementations over time. A scale unit should be sized to accommodate future growth over a period that meaningful to the business. Some businesses will plan on a quarterly basis while others may forecast by fiscal year or more.

Resource Pools

A resource pool is comprised of server, network, and storage scale units that share a common hardware and configuration baseline but does not share a single point of failure with any other resource pool other than the facility itself. Note that a resource pool could be subdivided further into Fault Domains. See Private Cloud Reference Architecture Principles, Patterns, and Concepts.

Fault Domains

The Physical Fault Domains pattern is defined in the Private Cloud Reference Architecture. In an Infrastructure as a Service design a fault domain is a set of physical infrastructure with a common configuration within a resource pool that does not share a single point of failure with any other fault domain.

Upgrade Domains

An upgrade domain is infrastructure within a resource pool that can be maintained, take offline, or upgraded without downtime to the workloads running in the resource pool.

Putting It All Together

Private Cloud Infrastructure as a Service is an evolution in the industry and IT. It forms the foundation of cloud computing for all cloud enabled workloads. Designing for Infrastructure as a Service raises the IT Capability and Maturity level to realize cloud capabilities in the allowing the business to focus on objectives, respond with agility and realize economies of scale.

nfrastructure as a Service (IaaS) Advantages

- You or your organization are responsible for the versioning/upgrades of software developed (this is also a disadvantage).
- The maintenance and upgrades of tools, database systems, etc. and the underlying infrastucture is your responsibility or the responsibility of your organization (this is also a disadvantage).
- Various pricing models may allow paying only for what you use. This, for example, can allow an individual or a small organization to use sophisticated development software that they could not afford if it was installed on an internal, dedicated server.
- Some IaaS Providers provide development options for multiple platforms: mobile, browser, and so on. If you or your organization want to develop software that can be accessed from multiple platforms, this might be an easy way to make that happen.
- If you have events such as high seasonal sales activity, then the elasticity of the Cloud with IaaS might provide an opportunity.
- The IaaS Cloud Provider may provide better security than your existing software (security—or inadequate security—can also be a disadvantage). Better security may come in part because it is critical for the IaaS Cloud Provider and is part of their main business. In-house security, on the other hand, is not usually an individual's or a organization's main business and, therefore, may not be as good as that offered by the IaaS Cloud Provider.
- No need to manage the introduction of new releases of the development or underlying software. This is handled by the IaaS Cloud Provider.
- No need to manage the underlying data center. This is handled by the IaaS Cloud Provider.
- Usually, there is no need to manage backups. This is handled by the IaaS Cloud Provider.
- If the IaaS Cloud Provider supports failover should the software (for example, the database management software) or the data center become unavailable, that failover is a concern of the IaaS Cloud Provider and you do not need to plan for it.

Infrastructure as a Service (IaaS) Disadvantages

- You or your organization are responsible for the versioning/upgrades of software developed (this is also an advantage).
- The maintenance and upgrades of tools, database systems, etc. and the underlying infrastucture is your responsibility or the responsibility of your organization (this is also an advantage).
- When it is mandatory that the underlying hardware be of a specific type or the underlying software be modified to support the deployed application.
- There may be legal reasons that preclude the use of off-premise or out-of-counry data storage.
- Security features of the IaaS Cloud Provider may not adequate for your needs.
- If you have a need for high-speed interaction between your internal software or software in another Cloud and the IaaS Cloud Provider, relying on an Internet connection may not provide the speed that you need.

A trade-off (or tradeoff) is a situation that involves losing one quality or aspect of something in return for gaining another quality or aspect. More colloquially, if one thing increases, some other thing must decrease. Tradeoffs can occur for many reasons, including simple physics (into a given amount of space, you can fit many small objects or fewer large objects).

Trade-offs? Yup, there are trade-offs involved in working with a public cloud. Let's talk about that for a moment.

On The Upside

The public cloud has a much lower cost of entry than an on-premise installation of enterprise software. The hardware cost is amortized over multiple customers, licensing costs can be eliminated through buying SaaS (Software as a Service) , and most of the maintenance is handled by the vendor hosting your instance. All this combines to lower the price-point of entry and provide overall lower short-terms costs…very good news. This is especially good news for small and medium-sized organizations, who now find high-quality enterprise software well within their reach.

On The Downside

As usual in life, there is some bad news to accompany the good news. The public cloud is no different. Three particular points come to mind:

- As Google has recently implied, those who put their data on the public Internet (and, yes, a public cloud is a part of the Internet) have waived any expectation of privacy . Google is right. We read about it in the news every day. Like it or not, security in the public cloud is currently a big issue.

- Integrating data between on-premise and cloud, or between different cloud instances, is a real stinker due to performance. Cloud-based integration is typical done via either SOAP - based Web Services or REST services . Neither were meant to move big chunks of data or heavy volumes of small chunks of data. When you attempt to do so, performance suffers…and I mean, really suffers. So things like real-time reporting tends to become a huge issue.

- Support turnaround times can drop like a stone. Copying an instance or fixing an issue can take a week or more. Vendors are still working to streamline and speed up their processes in this area. It will get better as the market matures, but for now turnaround can be very slow.

The Real Tradeoff

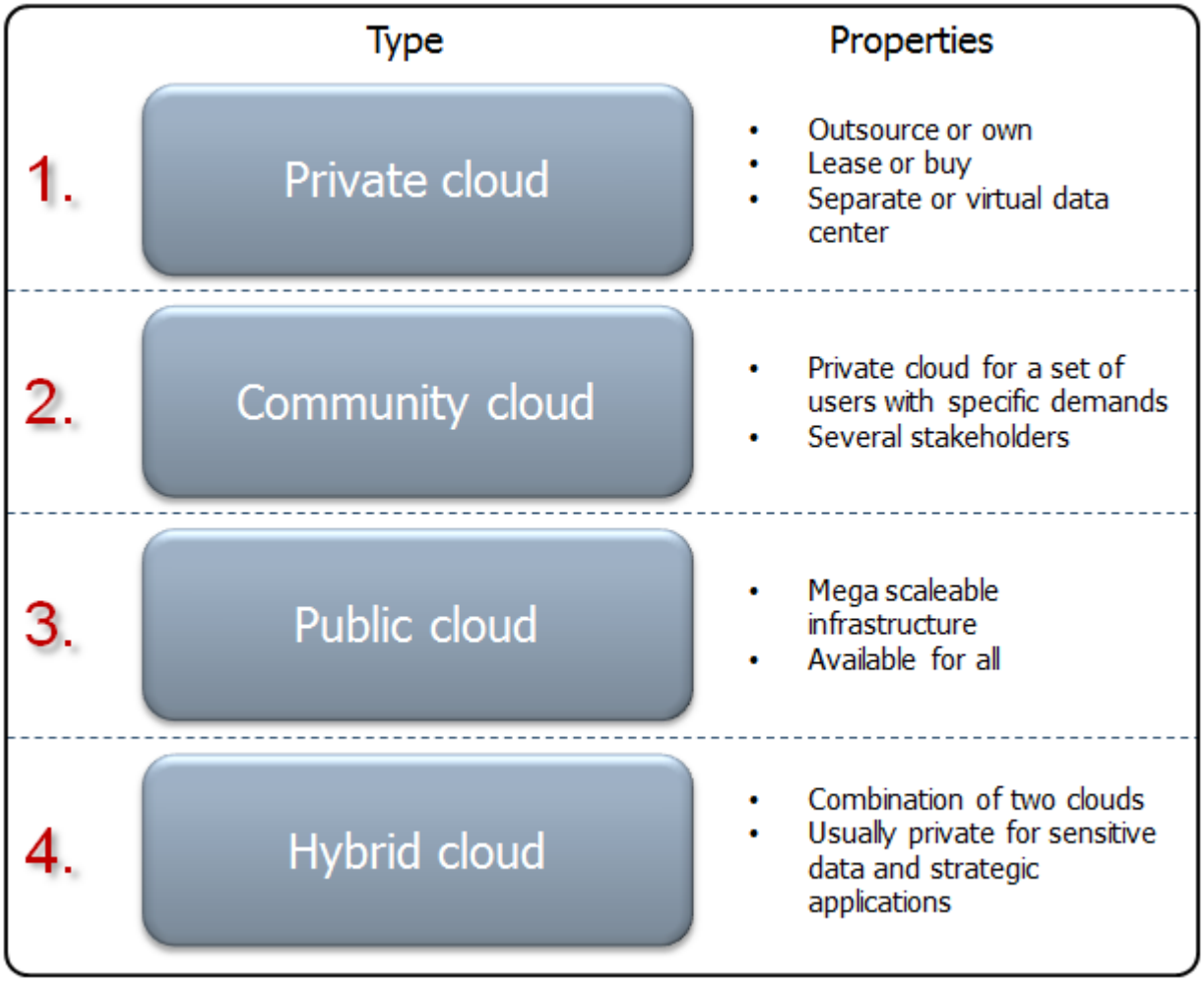
The real trade-off with the public cloud comes down to cost versus security and speed. Lower cost of entry and lower short-term cost of use versus lower levels of security (compared to data stored behind a corporate firewall) and longer turnaround times (for both information and service).

Yes, I'd like to hear Oracle address these trade-offs during OOW 13. There are some really bright people behind the public cloud strategy and I'd like to hear their viewpoints on this…no dig intended here, I'm just hoping to get more info to analyze the trade-offs.

Still, in the end, it's up to each of us to evaluate the technology and make the best determination for each of our unique situations. I'm just hoping we'll get the info needed to make well-informed evaluations.

UNIT 4

Cloud deployment scenarios



Cloud computing is a type of computing that mainly depends on resource sharing instead of handling applications by local servers or individual devices. Using the internet enabled devices, cloud computing permit the function of application software. Cloud computing, also known as

the cloud, can be used as a synonym for the Internet. Cloud computing can serve a diverse range of functions over the Internet like storage and virtual servers; applications and authorization for desktop applications. By taking advantage of resource sharing, cloud computing is able to achieve consistency and economies of scale. The types of cloud computing are classified based on two models. Cloud computing service models and cloud computing deployment models.

Cloud computing deployment models

Cloud hosting deployment models represent the exact category of cloud environment and are mainly distinguished by the proprietorship, size and access. It tells about the purpose and the nature of the cloud. Most of the organizations are willing to implement cloud as it reduces the capital expenditure and controls operating cost. In order to know which deployment model matches your website requirements it is necessary to know the four deployment models.

Public Cloud: is a type of cloud hosting in which the cloud services are delivered over a network which is open for public usage. This model is a true representation of cloud hosting; in this the service provider renders services and infrastructure to various clients. The customers do not have any distinguish ability and control over the location of the infrastructure. From the technical viewpoint, there may be slight or no difference between private and public clouds' structural design except in the level of security offered for various services given to the public cloud subscribers by the cloud hosting providers.

Public cloud is better suited for business requirements which require managing the load; host application that is SaaS-based and manage applications that many users consume. Due to the decreased capital overheads and operational cost this model is economical. The dealer may provide the service free or in the form of the license policy like pay per user. The cost is shared by all the users, so public cloud profits the customers more by achieving economies of scale. Public cloud facilities may be availed free an e.g. of a public cloud is Google.

Private Cloud: is also known as internal cloud; the platform for cloud computing is implemented on a cloud-based secure environment that is safeguarded by a firewall which is under the governance of the IT department that belongs to the particular corporate. Private cloud as it permits only the authorized users, gives the organisation greater and direct control over their data. What exactly constitutes a private cloud? It is difficult to define because when it's classified according to the services there are significant variations. Whether the physical

computers are hosted internally or externally they provide the resources from a distinct pool to the private cloud services. Businesses that have dynamic or unforeseen needs, assignments which are mission critical, security alarms, management demands and uptime requirements are better suited to adopt private cloud. Obstacles with regards to security can be evaded in a private cloud, but in case of natural disaster and internal data theft the private cloud may be prone to vulnerabilities.

Hybrid Cloud: is a type of cloud computing, which is integrated. It can be an arrangement of two or more cloud servers, i.e. private, public or community cloud that is bound together but remain individual entities. Benefits of the multiple deployment models are available in a hybrid cloud hosting. A hybrid cloud can cross isolation and overcome boundaries by the provider; hence, it cannot be simply categorized into public, private or community cloud. It permits the user to increase the capacity or the capability by aggregation, assimilation or customization with another cloud package / service. In a hybrid cloud, the resources are managed and provided either in-house or by external providers. It is an adaptation among two platforms in which the workload exchanges between the private cloud and the public cloud as per the need and demand.

Resources that are non-critical like development and test workloads can be housed in the public cloud that belongs to a third-party provider. While the workloads that are critical or sensitive must be housed internally. Consider an e-commerce website, which is hosted on a private cloud that gives security and scalability, since security is not a prime concern for their brochure site it is hosted on a public cloud which is more economical as compared to a private cloud. Businesses that have more focus on security and demand for their unique presence can implement hybrid cloud as an effective business strategy. When facing demand spikes the additional resources that are required by a particular application can be accessed from the public cloud. This is termed as cloud bursting and is available with the hybrid cloud.

Organisations can use the hybrid cloud model for processing big data. On a private cloud, it can retain sales, business and various data and can initiate analytical queries over the public cloud as the public cloud is effective to meet the demand spikes. Hybrid cloud hosting is enabled with features like scalability, flexibility and security. If one is ready to overlook a few challenges like application program interface incompatibility, network connectivity issues and capital expenditures, then the hybrid cloud would be an appropriate option.

Community Cloud: is a type of cloud hosting in which the setup is mutually shared between many organisations that belong to a particular community, i.e. banks and trading firms. It is a multi-tenant setup that is shared among several organisations that belong to a specific group which has similar computing apprehensions. The community members generally share similar privacy, performance and security concerns. The main intention of these communities is to achieve their business related objectives. A community cloud may be internally managed or it can be managed by a third party provider. It can be hosted externally or internally. The cost is

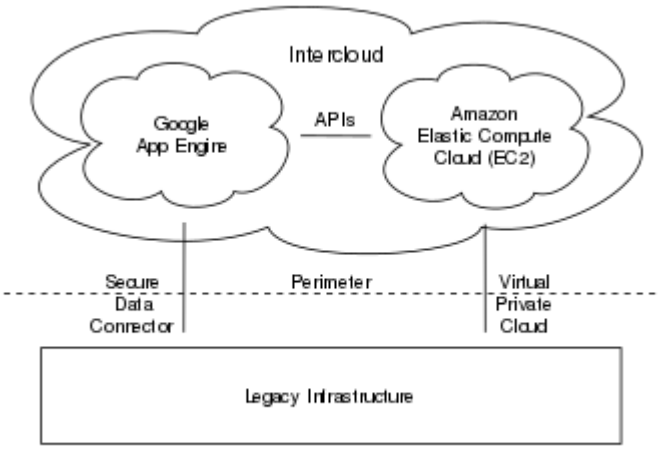
shared by the specific organisations within the community, hence, community cloud has cost saving capacity. A community cloud is appropriate for organisations and businesses that work on joint ventures, tenders or research that needs a centralised cloud computing ability for managing, building and implementing similar projects.

Organisations have understood that cloud hosting has a lot of potential. To be the best among the rest, selection of the right type of cloud hosting is needed. Thus, you need to know your business and analyze the demands. Once the appropriate type of cloud hosting is selected, you can achieve your business related goals more easily, you can channelize all your efforts to take those strategic steps that will help your business to succeed. Ex: Doctors, Scientist and some common communities use a cloud for common reason.

Virtual Private clouds

A virtual private cloud (VPC) is an on-demand configurable pool of shared computing resources allocated within a public cloud environment, providing a certain level of isolation between the different organizations (denoted as *users* hereafter) using the resources. The isolation between one VPC user and all other users of the same cloud (other VPC users as well as other public cloud users) is achieved normally through allocation of a private IP subnet and a virtual communication construct (such as a VLAN or a set of encrypted communication channels) per user. In a VPC, the previously described mechanism, providing isolation within the cloud, is accompanied with a VPN function (again, allocated per VPC user) that secures, by means of authentication and encryption, the remote access of the organization to its VPC cloud resources. With the introduction of the described isolation levels, an organization using this service is in effect working on a 'virtually private' cloud (that is, as if the cloud infrastructure is not shared with other users), and hence the name VPC.

VPC is most commonly used in the context of cloud infrastructure as a service. In this context, the infrastructure provider, providing the underlying public cloud infrastructure, and the provider realizing the VPC service over this infrastructure, may be different vendors.



Virtual Private Cloud (VPC)

Amazon Web Services launched Amazon Virtual Private Cloud on 26 August 2009, which allows the Amazon Elastic Compute Cloud service to be connected to legacy infrastructure over an IPsec virtual private network connection.

In AWS, VPC is free to use, however users will be charged for any virtual private networks (VPN) they use. EC2 and RDS instances running in a VPC can also be purchased using Reserved Instances, however will have a limitation on resources being guaranteed.

Google Cloud Platform resources can be provisioned, connected, and isolated in a virtual private cloud (VPC) across all GCP regions. Identity management policies and security rules allow for private access to Google's storage, big data, and analytics managed services. VPCs on Google Cloud Platform leverage the security of Google's data centers.

Microsoft Azure offers the possibility of setting up a VPC using Virtual Networks.

Migration Path for cloud

Cloud migration is the process of moving data, applications or other business elements from an organization's onsite computers to the cloud, or moving them from one cloud environment to another. Cloud migration sometimes involves moving data or other business elements between cloud environments, which is known as cloud-to-cloud migration. The process of transitioning to a different cloud provider is known as cloud service migration. In any case, successful migration to a service provider’s environment may require the use of middleware, such as a cloud integration tool, to bridge any gaps between the vendor’s and the customer’s (or other vendor’s) technologies.

Transitioning to the cloud or between cloud environments presents the usual IT issues, but the problems are compounded by having data stored and managed remotely, by external

organizations and often in multiple locations. Among these issues are special considerations for privacy, interoperability, data and application portability, data integrity, business continuity, and security.

Selection criteria for cloud deployment

Flexibility in terms of cost: The costing in cloud models is a variable. Cloud implementations

Allows business companies to 'pay for the resource as and when needed.' This offers the benefit of reduced capital expenditure in upgrading and running an in-house IT infrastructure.

Business scalability: Cloud provides flexibility. Resources in the cloud can scale up or down to support business growth and in times when business is lean. This is another benefit.

Adaptability in the market: All cloud models enable faster time to market, and provides scope for business innovations and explore new opportunities.

Context-driven variability: Increases the relevance of products and services and enables user defined experiences.

Connectivity with the existing ecosystem: Cloud models offer capabilities to fully integrate into existing infrastructure.

Polytech – Can the Platform Support Multiple Languages, Databases and Middleware?

You may need to use multiple languages or databases as you create your applications. Each application will have different needs as it is developed, and those needs also may change over time. By finding a cloud provider that can support multiple languages and databases, you'll avoid having to select a different cloud for each type of application. It's important not just to look at the service a cloud provider is offering, but whether that platform provides the depth and breadth you need.

For example, a SaaS company that helps developers build visual prototypes in the cloud leverages several PHP frameworks, as well as a variety of databases and queueing technologies to meet its clients' varying needs. And a sport merchandise company uses multiple languages and related frameworks and middleware to power its site to ensure customers can shop anytime.

Polycloud – Can the Provider Run on Multiple Infrastructures and Support Hybrid Options?

As demand increases for your applications, you'll need a provider that can grow with you. The key to ensuring compatibility with these changing requirements is not getting locked in.

Therefore you should look for a PaaS solution that supports multiple infrastructures and offers the combination of both private and public resources in hybrid cloud configurations.

For example, by deploying high availability and disaster recovery (HA/DR) across public clouds, one e-commerce company ensures its independent artists and designers can showcase their work without interruption. A gamification company separates its data and application infrastructures by deploying them on different public clouds with a low latency secure gateway for inter-cloud connectivity.

Complete Application Lifecycle Support – Can the Platform Deliver a Balance of Automation and Granular Control?

Your company's current IT processes and the size of your DevOps team will likely guide the level of automation or extent of control you want. As you're considering your cloud platform, you will want to make sure that it can provide, both, a high level of automation and granular control, so you are not locked in to your initial choice.

For example, a start-up may have a great idea for an app, but few employees in DevOps. In this scenario, automation is necessary to enable the small staff to write the code and easily deploy the app. But over time, as the company grows and scales, their applications may become more complex and require greater control. On the flipside, there are large enterprises that have historically managed in-house infrastructure, but now want the benefits of moving to the cloud. They often want a platform that provides the same level of control they are accustomed to, with more automation.

Proven – Does the Cloud Provider Have a Strong Track Record?

Because the cloud market is relatively new with strong growth potential, there are a myriad of young platform providers that are trying to get in on the opportunity. When considering cloud platform providers, it's critical to choose a stable company that can provide the service level you need, whether you're a small start-up, a development agency supporting many customers or running large enterprise applications. You should look for case studies and references that prove the provider's capabilities, and strongly consider selecting a provider with a history of delivering a commercial-grade platform that is reliable, secure and flexible.

Questions you should ask include: how long has the company been in business, how many apps they have in production, what's the expertise of both the management and development team, and are they comfortable with both legacy and new apps. With these answers, you won't risk your business-critical applications to an inexperienced provider that has service interruptions, poor support, and could unexpectedly go out of business.

Customer Support - How Involved Does Your Provider Get?

Many cloud platform providers offer basic help through a knowledge base or other online resources. That is often where the support ends, but it doesn't have to. Some providers are investing heavily in enhanced customer support. They employ experts who can help you speed your time to market and focus on developing and troubleshooting apps without having to hire more Ops staff. They provide advice on deployment, high availability strategies, scaling, code and security audits, application analysis and best practices. They will stay with you even after your app launches, not just reacting to problems, but providing proactive monitoring and support that keeps your apps running smoothly 24x7.

UNIT 5

Cloud security reference model

A Reference Architecture (RA) "should" provide a blueprint or template architecture that can be reused by others wishing to adopt a similar solution. A Reference Model (RM) should explain the concepts and relationships that underlie the RA. At Everware-CBDI we then use the term Reference Framework (RF) as a container for both. Reference architectures, models and frameworks help to make sense of Cloud Computing.

Unfortunately, such formality is absent from the various reference architectures, models and frameworks that have been published for Cloud Computing; these frequently mix elements of architecture and model, and then apply one of the terms seemingly at random.

In developing the CBDI-Service Architecture and Engineering Reference Framework (SAE) in support of SOA (Service Oriented Architecture) Everware-CBDI separated out various parts as shown in figure 1. We developed a detailed RA for SOA and a RM for SOA, with particular emphasis on a rich and detailed Meta Model for SOA and a Maturity Model for SOA. We also developed a detailed process and task decomposition for SOA activities.

But the RF is easily generalized, as shown in figure 1, where the various elements could be applied to any domain, and explicit references for example to "SOA Meta Model" or "SOA Standards" etc., can be removed.

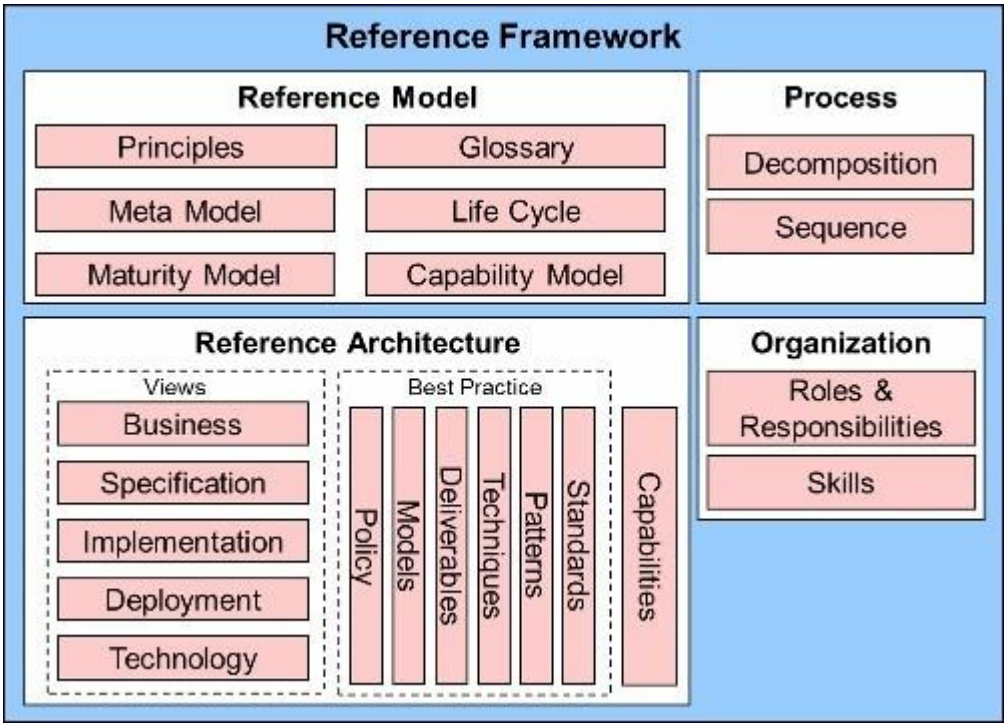


Figure 1 – Generalized Reference Framework

- Role-Based. Where activities or capabilities are mapped to roles such as cloud provider or consumer. For example,

1. DMTF Cloud Service Reference Architecture
2. IBM Cloud Computing Reference Architecture (which has been submitted to the Open Group)
3. NIST Cloud Computing Reference Architecture

- Layer-based. Where activities or capabilities are mapped to layers in an architecture such as application or resource layers or to the service management architecture or security architecture
- Cloud Security Alliance Reference Model is one of many layered models showing the cloud 'stack'
- CISCO Cloud Reference Architecture Framework is an architecture of architecture, placing Cloud on top of layers of Service, Security and Technology architectures
- IEFT Cloud Reference Framework goes into more depth, showing the capabilities for each layer.

Cloud security

Primary concerns around cloud solutions have to do with security. In the most basic situation, the cloud provider is serving many organizations within the same network environment. An organization could be concerned that their data might be hacked (accessed without permission)

by another organization operating in the same area of the cloud data center. Even in cases where the cloud service provider has created a separate private cloud environment for an organization, operating on a separate network, behind a separate firewall, there must be concern for whether the service provider is providing adequate security from intruders.

The physical security provisions of the cloud service provider may be a concern, although since the provider is supporting security for all their customers and security is a differentiator, they are probably providing physical security which exceeds the internal capabilities of most individual organizations.

Additionally, the data security laws of the country where the cloud provider is operating its physical data center will be of concern to some organizations. For example, a Canadian company may not want to use a cloud service provider operating in the United States because its data could be subpoenaed by an American court.

Certain types of organizations will not be able to utilize public cloud solutions for their most private and sensitive information, such as the customer data from financial institutions or classified data from government organizations, but most organizations may find that the capabilities offered by cloud service providers are both less expensive and more secure than those they could support internally and would have many uses. Even the most security-conscious organization may find it useful to be able to create development environments in the cloud quickly, thus speeding up development of custom applications and familiarity with new vendor packages, while their internal organizations are provisioning environments within their own firewalls and data centers.

What many chief security officers are discovering, to their horror, is that cloud services are so easy and inexpensive to acquire that parts of their organizations may already have data out in public cloud environments without having been concerned with the issues of adequate security. Cloud services are so easy to obtain that the inventory of organizational data assets may suddenly be uncertain. Like data on laptops and mobile devices, data in the cloud is outside the organization’s physical control and adds greater complexity to the problems of managing data security.

Understanding security risks

Although cloud computing can offer small businesses significant cost-saving benefits—namely, pay-as-you-go access to sophisticated software and powerful hardware—the service does come with certain security risks. When evaluating potential providers of cloud-based services, you should keep these top five security concerns in mind.

1. Secure data transfer. All of the traffic travelling between your network and whatever service you're accessing in the cloud must traverse the Internet. Make sure your data is always travelling on a secure channel; only connect your browser to the provider via a URL that begins with "https." Also, your data should always be encrypted and authenticated using industry standard protocols, such as IPsec (Internet Protocol Security), that have been developed specifically for protecting Internet traffic.

2. Secure software interfaces. The Cloud Security Alliance (CSA) recommends that you be aware of the software interfaces, or APIs, that are used to interact with cloud services. "Reliance on a weak set of interfaces and APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability, and accountability," says the group in its Top Threats to Cloud Computing document. CSA recommends learning how any cloud provider you're considering integrates security throughout its service, from authentication and access control techniques to activity monitoring policies.

3. Secure stored data. Your data should be securely encrypted when it's on the provider's servers and while it's in use by the cloud service. In Q&A: Demystifying Cloud Security, Forrester warns that few cloud providers assure protection for data being used within the application or for disposing of your data. Ask potential cloud providers how they secure your data not only when it's in transit but also when it's on their servers and accessed by the cloud-based applications. Find out, too, if the providers securely dispose of your data, for example, by deleting the encryption key.

4. User access control. Data stored on a cloud provider's server can potentially be accessed by an employee of that company, and you have none of the usual personnel controls over those people. First, consider carefully the sensitivity of the data you're allowing out into the cloud. Second, follow research firm Gartner's suggestion to ask providers for specifics about the people who manage your data and the level of access they have to it.

5. Data separation. Every cloud-based service shares resources, namely space on the provider's servers and other parts of the provider's infrastructure. Hypervisor software is used to create virtual containers on the provider's hardware for each of its customers. But CSA notes that "attacks have surfaced in recent years that target the shared technology inside Cloud Computing environments." So, investigate the compartmentalization techniques, such as data encryption, the provider uses to prevent access into your virtual container by other customers.

Principal security dangers to cloud computing

1. Someone else is looking after your data

Unlike a data center, which is run by an in-house IT department, the cloud is an off-premise system in which users outsource their data needs to a third party provider. The provider does everything from performing all updates and maintenance to managing security. The bigger picture, however, is that users are trusting their data for someone else to look after, said Steve Santorelli, a former Scotland Yard detective, now manager of outreach at the Internet security research group Team Cymru. The downside is that you are abrogating responsibility for your data. Someone else has access to it and someone else is responsible for keeping it safe," Santorelli said.Although cloud providers may ensure your data is safe, Santorelli said some are not always looking after your best interests. "No business is ever going to be as rabid about looking after your data as you would or should be. They are in the business of making money from you, after all. Securing your data sometimes becomes a marketing mantra more than a way of life," he said.

2. Cyberattacks

Any time you store data on the Internet, you are at risk for a cyberattack. This is particularly problematic on the cloud, where volumes of data are stored by all types of users on the same cloud system.

"The scary thing is the vulnerability to Distributed Denial of Service (DDoS)attacks and the concentration of so much data," Santorelli said. "The single point of failure is the cloud. If something goes bad it impacts a very wide group of people. It's easier to steal and disrupt in bulk."

Although most cloud providers have stringent security measures, as technology becomes more sophisticated, so do cyberattacks.

"When cloud companies get the security right — and many actually do a pretty reasonable job — then miscreants have to get creative to get to the data," Santorelli said. For instance, instead of hacking the cloud, hackers will attempt to hack your account instead.

"Passwords and secret answers become the soft underbelly of your security. Just like when banks made online account hacking harder, the miscreants turned to phishing to get around the restrictions and steal your passwords," he said.

3. Insider threats

Just as cyberattacks are on the rise, so are security breaches from the inside.
"Vodafone's breach of 2 million customer records and the Edward Snowden breach at the NSA are wake-up calls that the most serious breaches are due to insider threats and privileged user access," said Eric Chiu, president and co-founder of HyTrust, a cloud infrastructure control

company Once an employee gains or gives others access to your cloud, everything from customer data to confidential information and intellectual property are up for grabs.

4. Government intrusion

With the recent NSA leaks and the ensuing reports on government surveillance programs, competitors aren't the only ones who may want to take a peek at your data.

"Something that has been in the news recently is that government entities and technology companies in the U.S. and elsewhere may be inspecting your data as it is transmitted or where it resides in the Internet, including within clouds," said Scott Hazdra, principal security consultant for Neohapsis, a security and risk management consulting company specializing in mobile and cloud security.

Granted, privacy has always been a concern with the cloud. But instead of just worrying about competitors, disgruntled customers or employees breaching cloud security, businesses now have to worry about government intrusion as well.

"Loss of confidentiality to data is not a new risk; however, the threat sources might not have been one companies were previously worried about," Hazdra said. "For instance, a company may have a concern that competitors will try to steal their data so they encrypt transmission and storage of it. Now that someone other than a competitor may be interested in that data doesn't fundamentally change the risk."

5. Legal liability

Risks associated with the cloud are not limited to security breaches. They also include its aftermath, such as lawsuits filed by or against you.

"The latest risks to using cloud for business are compliance, legal liability and business continuity," said Robert J. Scott, managing partner of Scott & Scott LLP, an intellectual property and technology law firm. "Data breach incidences are on the rise, and so are lawsuits."

Scott, who is also a cloud law speaker and author, said that while the cloud is all about ease of access, collaboration and rapidity, its benefits have to be weighed against the extent of security measures.

"Information security has always been finding a balance between ease of access and the sharing of information verses completely locked down security," he said. "The more you have of one, the less you have of the other."

6. Lack of standardization

What makes a cloud "safe"? A provider could have the latest security features, but due to the general lack of cloud standardization, there are no clear-cut guidelines unifying cloud providers. Further, given the plethora of cloud services in different sectors, this is especially problematic for users when determining exactly how "safe" their cloud really is.

"The question of how safe the cloud is has many facets, and the answer depends on the cloud services provider, the type of industry a company is in, and the accompanying regulations concerning the data it is considering storing in the cloud," Scott said.

Since not all cloud providers are built the same, one provider's definition of "safe" may not be the same as another's, Scott said.

7. Lack of support

Imagine being unable to access your cloud before a big meeting or, worse, being in the middle of a cyber attack that has taken down your entire bread and butter —your website. Now imagine trying to contact your provider, only to find that their customer service is nonexistent. While some cloud providers have excellent customer support, others could leave you in the cold. "The most frustrating thing when something goes wrong is not being able to speak directly with an engineer," said April Sage, director of Healthcare Vertical at Online Tech, a cloud provider specializing on compliant cloud hosting.

"If your systems are not mission-critical, you don't need to worry so much about security and availability," Sage said. "However, if you support mission-critical systems, or your online presence is critical for your business to operate smoothly, you have to be prepared to invest in a cloud and cloud provider that is capable of providing a level of protection commensurate with your needs."

8. There's always a risk

The biggest risk when it comes to cloud computing is that you never know what is up ahead. Hackers have been around from the start and they are not going anywhere any time soon. And as technology advances, so do the risks that come with adopting them.

Given these current and future dangers, do the benefits of cloud computing outweigh its risks? Neil Rerup, author of "Cyber Peril" (Sutton Hart, 2013) and founder of Enterprise Cybersecurity Architects (ECSA), said it depends on the business.

"The cloud is not for everyone," Rerup said. "Like with all solutions, you have to weigh what level of risk you are comfortable dealing with."

Internal security breaches

1. Malicious cyberattacks
Research conducted by Cert has found the most likely perpetrators of cyberattacks are system administrators or other IT staff with privileged system access.

Technically proficient employees can use their system access to open back doors into computer systems, or leave programs on the network to steal information or wreak havoc. In 2006, IT programmer Roger Duronio was found guilty of planting a type of malware known as Unix logic bombs in the network of investment bank UBS. The company claimed the resulting damage cost more than $3m (£1.5m).

Prosecutors argued that Duronio had launched the attack when he received a bonus he felt was unreasonably low. He complained and eventually resigned from his job, but not without leaving behind a memorable parting gift.

The best protection against this sort of attack is to monitor employees closely and be alert for disgruntled employees who might abuse their positions. In addition, experts advise immediately cancelling network access and passwords when employees leave the company, to avoid them using passwords to remotely access the network in future.

2. Social engineering
Perhaps one of the most common ways for attackers to gain access to a network is by exploiting the trusting nature of your employees. After all, why go to the trouble of creating a program to steal passwords from the network, if people will simply give out this information on the telephone?

"You can have the best technical systems in place, but they're not effective if people aren't educated about the risks," says Mike Maddison, head of security and privacy services at Deloitte UK. A recent survey conducted by Deloitte found three-quarters of companies have not trained staff in the risks of information leakage and social engineering.

"It's vital that people understand, for example, that they shouldn't provide their password over the telephone, or that they recognise a phishing email," says Toralv Dirro, a security strategist with McAfee. "These sorts of messages are becoming increasingly sophisticated, and we're now seeing very personalised, targeted phishing emails that may even refer to projects that people work on, or members of their team."

3. Downloading malicious internet content

Some reports suggest the average employee in a small business spends up to an hour a day surfing the web for personal use — perhaps looking at video or file-sharing websites, playing games or using social media websites such as Facebook.

It's not just time that this activity could cost you. Analyst reports show that the number of malware and virus threats is increasing by more than 50 percent each year, and many of these destructive payloads can be inadvertently introduced to the network by employees.

"It's very easy for a rootkit to be hidden in a game or a video clip, and a novice user may not notice anything out of the ordinary," warns Graham Titterington, a principal analyst with Ovum.

The best advice is to constantly update and patch your IT systems to ensure you are protected...

...against new threats as they emerge, advises Paul Vlissidis, a technical director with NCC Group. "Don't rely on monthly or quarterly security downloads," he says. "The time between vulnerabilities being discovered and then exploited is shrinking all the time, so it's important to update patches and antivirus software regularly, and ideally layer several antivirus products rather than using just one."

In addition, consider whether your antivirus software can filter, monitor and block video content: few products can do this today, but a video of someone falling over can provide a cover for downloading all sorts of content onto the network, says Bob Tarzey, a service director with analyst firm Quocirca.

4. Information leakage

There are now a staggering number of ways that information can be taken from your computer networks and released outside the organisation. Whether it's an MP3 player, a CD-ROM, a digital camera or USB data stick, today's employees could easily take a significant chunk of your customer database out of the door in their back pocket.

"These types of devices are effectively very portable, very high-capacity hard drives," says Andy Kellett, a senior research analyst with Butler Group. "Someone can walk away with up to 60GB of data on a USB stick, so it's not a trivial matter."

Research conducted by Websense found that a quarter of UK workers who use PCs at work admit copying data onto mobile devices at least once a week. In addition, 40 percent say they use USB sticks to move data around, and a fifth have revealed their passwords to third parties.

Kellett advises companies to use software to specify policies on what devices can be connected to the corporate network, and what data can be downloaded. This should be enforced by the company — but workers should also be educated about why the policies are in place — or they will simply find a way to work around them. "It's not difficult to specify that the USB ports on desktop computers are disabled, or that CD-ROM drives are removed from computers where they aren't needed," Kellet says. "But you have to work with your employees to balance security and usability."

In addition, Kellett recommends considering whether to block access to web-based email and data-storage services, such as Gmail. "If someone can store confidential documents to an online storage site, that information is completely beyond your control," he says.

Finally, consider locking down networks to prevent wireless access using Bluetooth or Wi-Fi — except for authorised users with authorised devices. "Information loss over Bluetooth on an unsecured network is very difficult to detect indeed," says Kellett.

5. Illegal activities

It's important to remember that, as an employer, you are responsible for pretty much anything your employees do using your computer network — unless you can show you have taken reasonable steps to prevent this. Famously, the US-based Citibank was sued for $2m (£1m) when employees downloaded pornography from the internet, and UK companies have dismissed workers for a range of misdeeds, from selling drugs using company email to distributing racially and sexually offensive material over corporate intranets.

To protect yourself, experts advice a two-pronged approach. First, use monitoring software to check email and internet traffic for certain keywords or file types. You might also choose to block certain websites and applications completely.

Second, devise an Acceptable Use Policy spelling out employees' responsibility for network security, ensure it's signed by everyone and that workers fully understand the risks and their responsibilities. According to software company Websense, one in five UK workers say they don't really understand their company's security policy.

User account and service hijacking

Cloud account hijacking occurs when an individual or organization’s cloud account is stolen or hijacked by an attacker. Cloud account hijacking is a common tactic in identity theft schemes. The attacker uses the stolen account information to conduct malicious or unauthorized activity.

When cloud account hijacking occurs, an attacker typically uses a compromised email account or other credentials to impersonate the account owner.

In a report from the Cloud Security Alliance service traffic hijacking was identified as the third-greatest cloud computing security risk. These types of security breach occur when attackers hijack cloud accounts by stealing security credentials and eavesdropping on activities and transactions. Attackers manipulate data, insert false information, and redirect clients to illegitimate sites.

Cloud account hijacking at the enterprise level can be particularly devastating, depending on what the attackers do with the information. Company integrity and reputations can be destroyed, and confidential data can be leaked or falsified causing significant cost to businesses or their customers. Legal implications are also possible for companies and organisations in highly regulated industries, such as healthcare, if clients' or patients' confidential data is exposed during cloud account hijacking incidents.

Businesses also should take proactive steps when choosing cloud service providers. Carefully review potential contracts and compare the cloud security and data-integrity systems of cloud service providers. Companies should also take a data-driven approach when evaluating providers, including the number of data loss or interference incidents they have experienced. You should know how often they've had downtime and how vulnerabilities are managed and monitored. Companies should choose cloud service providers that allow clients to audit the provider's performance in all of these areas.

Steps to reduce cloud security breaches

1. Protect Information: Sensitive information must be protected wherever it is stored sent or used. Do not reveal personal information inadvertently.

2. Reduce transfer of data: The organisation should ban shifting data from one device to another external device. Losing removable media will put the data on the disk under risk.

3. Restrict download: Any media that may serve as an allegiance to the hackers should be restricted to download. This could reduce the risk of transferring the downloadable media to an external source.

4. Shred files: The organisation should shred all the files and folder before disposing a storage equipment. There are application which can retrieve information after formatting.

5. Ban unencrypted device: The institution should have a ban on the device that are unencrypted. Laptops and other portable devices that are unencrypted are prone to attack.

6. Secure transfer: The use of secure courier services and tamper proof packaging while transporting bulk data will help in preventing a breach.

7. A good password: The password for any access must be unpredictable and hard to crack. Change of password from time to time

8. Automate security: Automating systems that regularly check the password settings, server and firewall configuration might bring about reduction of risk in the sensitive information.

9. Identify threats: The security team should be able to identify suspicious network activity and should be prepared if there is an attack from the network.

10. Monitor data leakage: Periodically checking security controls will allow the security team to have a control on the network. Regular check on internet contents to locate if any private data is available for public viewing is also a good measure to monitor data.

11. Track data: Tracking the motion of data within the organisational network will prevent any unintentional use of sensitive information.

12. Define accessibility: Defining accessibility to those who are working on company's sensitive data will bring down the risk of malicious users.

13. Security training: Providing privacy and security training to all employees, clients and others related to data related activities will bring about awareness on data breach.

14. Stop incursion: Shutting down the avenues to the company's warehouse will prevent incursions by the hacker. Management, production and security solutions must be combined to prevent the targeted attacks.

15. Breach response: Having a breach response plan will help in triggering quick response to data breaches and help in the reduction of harm. The plan could contain steps involving notification of the concerned staff or the agency who could contain the breach.

Reducing cloud security

- Authenticate all people accessing the network.
- Frame all access permissions so users have access only to the applications and data that they've been granted specific permission to access.
- Authenticate all software running on any computer — and all changes to such software.
- This includes software or services running in the cloud.
- Your cloud provider needs to automate and authenticate software patches and configuration changes, as well as manage security patches in a proactive way. After all, many service outages come from configuration mistakes.
- Formalize the process of requesting permission to access data or applications.
- This applies to your own internal systems and the services that require you to put your data into the cloud.
- Monitor all network activity and log all unusual activity.
- Deploy intruder-detection technology. Even if your cloud services provider enables you to monitor activities on its environment, you should have an independent view.
- Even when cloud operators have good security (physical, network, OS, application infrastructure), it is *your* company's responsibility to protect and secure your applications and information.
- Log all user activity and program activity and analyze it for unexpected behavior.
- Nearly 70 percent of security breaches are caused by insiders (or by people getting help from insiders). Insiders rarely get caught.
- Encrypt, up to the point of use, all valuable data that needs extra protection.

Identity management: Detection and forensics

- Cloud computing service providers each have their own way of managing security. There are three specific groups of IT security products — activity logs, host-based intrusion protection systems and network-based intrusion protection systems, and data audit.

- ACTIVITY LOGS AS CLOUD COMPUTING SECURITY
- Many logging capabilities are included in operating systems, applications, databases, and devices such as hardware firewalls and network monitors. It costs to invoke logging

capabilities: Turning on logging requires the system to write log records constantly, and it also involves managing and archiving such data until it's no longer needed.

- Log files often provide some evidence of how fraud was perpetrated, however. Perpetrators of digital fraud often escape justice simply because the victim doesn't have sufficient evidence to prove what they did.

- HIPS AND NIPS AS CLOUD COMPUTING SECURITY
- Companies that would like to see a cloud service provider take over their internal platform and infrastructure services need to take a careful look at infrastructure protection.

HIPS and NIPS can include the following elements:

- System and log-file monitors: This software looks for traces of hackers in log files. The monitors can watch login accounts, for example, and issue alerts when account permissions change — often an indication that something untoward is going on.
- Network intrusion-detection systems (NIDS): These security programs monitor data packets that travel through a network, looking for any telltale signs of hacker activity. The effectiveness of a NIDS depends on whether it can sort real dangers from harmless threats and from legitimate activity. An ineffective NIDS raises too many false alarms and, thus, wastes time.
- Digital deception software: This software deliberately misleads anyone who's attempting to attack the IT network. It can range from the simple spoofing of various service names to setting up traps known as *honeypots* or *honeynets.*
- White-listing software: This software inventories valid executable programs running on a computer and prevents any other executables from running. White-listing severely hampers hackers, because even if they access a computer, they can't upload their own software to run on it. White-listing software reports on any attempt to run unauthenticated software. It also stops virus software stone dead.
- Unified threat management: This central function takes information from all the preceding components and identifies threats by analyzing the combined information.

Benefits of identity

1. Better Network Capabilities

The cloud supported Identity and Access management (IAM) makes it easier to share network capabilities to the entire grid of users connected to the network. For instance, if a new application or integrated software is added to the network, it is made available to the network users without any delays. The ability to use the network for distribution of integrations, features, and other 3rd party capabilities is something that is exclusive to software as a service.

2. Seamless Collaboration through Cloud-Based Solutions

SaaS is progressively being adapted and used as a hub to connect to virtual networks of numerous distributors, suppliers, and trading partners. Due to the fact that SaaS is cloud-based, it is ideal for easily adding new connections, which is necessary when it comes to identity and access.

3. Cloud-Native Architecture

As compared to legacy software, SaaS services have been developed to be cloud-ready. This does not require the use of agents, web server plugins, federation toolkits, and other APIs. This 'no software' SaaS architecture provides an approach which makes it integration easy.

4. Enhanced Business Agility

By implementing cloud-based services, businesses can enjoy enhanced agility and free themselves from the restrictions imposed by inflexible IT infrastructures, which are resistant to change and offer limited options.

5. Reduced Risk

Service based architecture greatly reduces the business risk associated with the software-business model. Contrary to the licensed software, any software as a service subscription can be cancelled if the solution fails to deliver as per the requirements of an organization.

6. Diminished Vendor Lock-In

When SaaS applications are considered, vendors have reduced amount of control mainly because lesser investment is needed. There is no expensive integration required for multiple systems – which enhances the scalability for an organization and also proves to be more cost-effective.

7. Better On-Demand Support

Cloud based solutions protects companies from problems that result from churn. There is 24/7 monitoring and support available, with on-demand technical support available from experts.

8. Service Mindset

SaaS vendors possess a service-oriented mindset because they understand the fact that they will lose a customer if their expectations are not met. This is precisely why cloud technologies have better support programs.

9. No More Complicated Upgrade Cycle

Cloud reduces the disruptions caused by upgrades while totally eliminating complex, expensive application upgrades, as was the case with legacy software.

10. Great Flexibility

Cloud based services offer greater flexibility and can meet the growing demands of companies without getting rid of any software or hardware at all.

11. Improved Productivity

The cloud based services are configured and hosted at service providers. Thus, these service-oriented solutions pose little or no hassle for end-users and clients. The hassle-free identity services make it easier to focus on business development and net results, improving overall productivity of the organization.

12. Centralized Management

Using cloud services, businesses can manage all their services and applications at one place i.e. single interface, single dashboard, single infrastructure (that too based on cloud) and one-click management for all.

Encryption techniques

Cloud encryption is the transformation of a cloud service customer's data into cipher text. Cloud encryption is almost identical to in-house encryption with one important difference - the cloud customer must take time to learn about the provider's policies and procedures for encryption and encryption key management. The cloud encryption capabilities of the service provider need to match the level of sensitivity of the data being hosted.

Because encryption consumes more processor overhead, many cloud providers will only offer basic encryption on a few database fields, such as passwords and account numbers. At this point in time, having the provider encrypt a customer's entire database can become so expensive that it may make more sense to store the data in-house or encrypt the data before sending it to the cloud. To keep costs low, some cloud providers have been offering alternatives to encryption that don’t require as much processing power. These techniques include redacting or obfuscating data

that needs to remain confidential or the use of proprietary encryption algorithms created by the vendor.

In the past, many businesses felt comfortable allowing the cloud provider to manage encryption keys, believing that security risks could be managed through contracts, controls and audits. Over time it has become apparent, however, that cloud providers cannot honor such commitments when responding to government requests for information.

Digital Signatures

Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message.

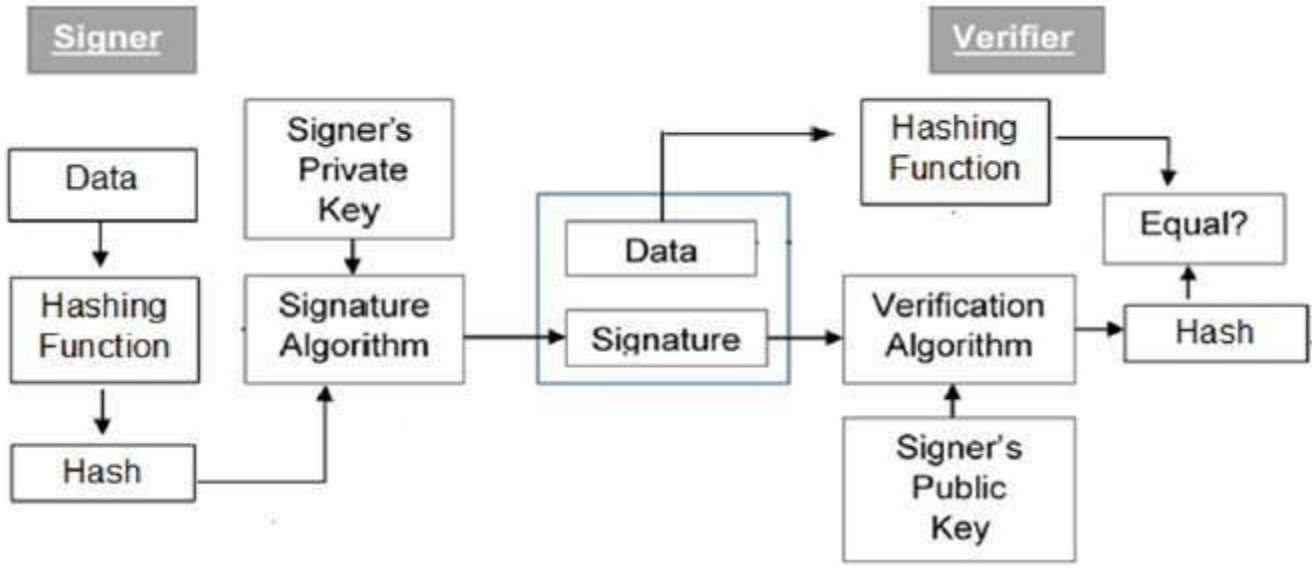
Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party.

Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message. This requirement is very crucial in business applications, since likelihood of a dispute over exchanged data is very high.

Model of Digital Signature

As mentioned earlier, the digital signature scheme is based on public key cryptography. The model of digital signature scheme is depicted in the following illustration −



The following points explain the entire process in detail −

- Each person adopting this scheme has a public-private key pair.
- Generally, the key pairs used for encryption/decryption and signing/verifying are different. The private key used for signing is referred to as the signature key and the public key as the verification key.
- Signer feeds data to the hash function and generates hash of data.
- Hash value and signature key are then fed to the signature algorithm which produces the digital signature on given hash. Signature is appended to the data and then both are sent to the verifier.
- Verifier feeds the digital signature and the verification key into the verification algorithm. The verification algorithm gives some value as output.
- Verifier also runs same hash function on received data to generate hash value.
- For verification, this hash value and output of verification algorithm are compared. Based on the comparison result, verifier decides whether the digital signature is valid.
- Since digital signature is created by 'private' key of signer and no one else can have this key; the signer cannot repudiate signing the data in future.

It should be noticed that instead of signing data directly by signing algorithm, usually a hash of data is created. Since the hash of data is a unique representation of data, it is sufficient to sign the hash in place of data. The most important reason of using hash instead of data directly for signing is efficiency of the scheme.

Let us assume RSA is used as the signing algorithm. As discussed in public key encryption chapter, the encryption/signing process using RSA involves modular exponentiation.

Signing large data through modular exponentiation is computationally expensive and time consuming. The hash of the data is a relatively small digest of the data, hence signing a hash is more efficient than signing the entire data.

Importance of Digital Signature

Out of all cryptographic primitives, the digital signature using public key cryptography is considered as very important and useful tool to achieve information security.

Apart from ability to provide non-repudiation of message, the digital signature also provides message authentication and data integrity. Let us briefly see how this is achieved by the digital signature −

- Message authentication − When the verifier validates the digital signature using public key of a sender, he is assured that signature has been created only by sender who possess the corresponding secret private key and no one else.

- Data Integrity − In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached.

- Non-repudiation − Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data. Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.

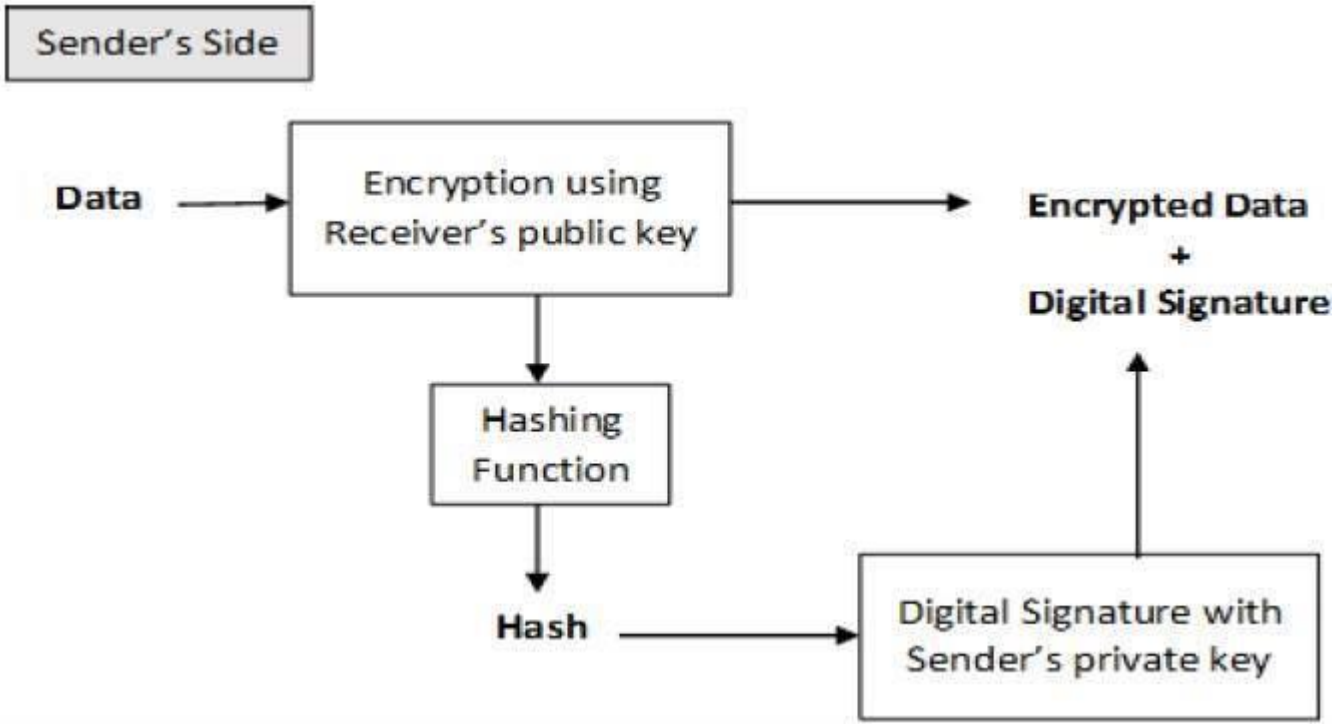
By adding public-key encryption to digital signature scheme, we can create a cryptosystem that can provide the four essential elements of security namely − Privacy, Authentication, Integrity, and Non-repudiation.

Encryption with Digital Signature

In many digital communications, it is desirable to exchange an encrypted messages than plaintext to achieve confidentiality. In public key encryption scheme, a public (encryption) key of sender is available in open domain, and hence anyone can spoof his identity and send any encrypted message to the receiver.

This makes it essential for users employing PKC for encryption to seek digital signatures along with encrypted data to be assured of message authentication and non-repudiation.

This can archived by combining digital signatures with encryption scheme. Let us briefly discuss how to achieve this requirement. There are two possibilities, sign-then-encrypt and encrypt-then-sign. However, the crypto system based on sign-then-encrypt can be exploited by receiver to spoof identity of sender and sent that data to third party. Hence, this method is not preferred. The process of encrypt-then-sign is more reliable and widely adopted. This is depicted in the following illustration −



The receiver after receiving the encrypted data and signature on it, first verifies the signature using sender's public key. After ensuring the validity of the signature, he then retrieves the data through decryption using his private key.

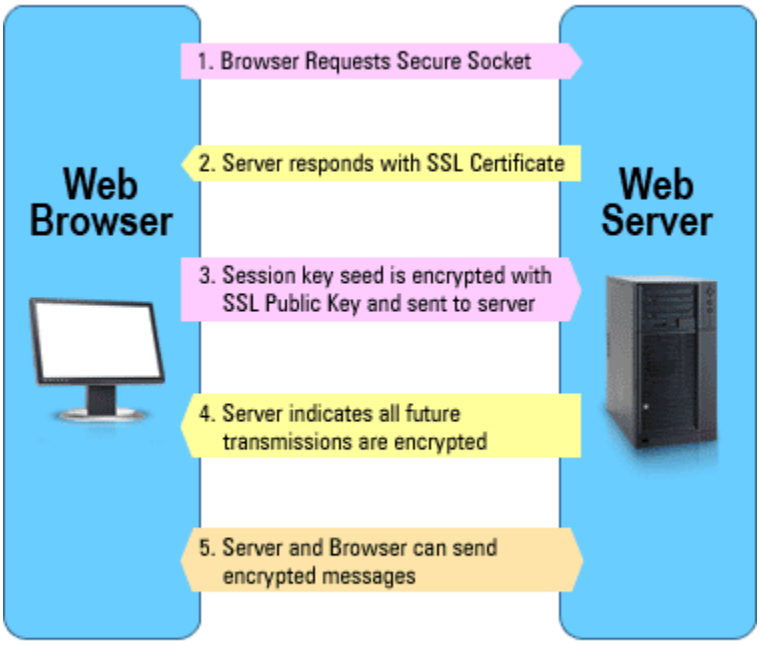
SSL (pronounced as separate letters) is short for Secure Sockets Layer.
Secure Sockets Layer (SSL) is a protocol developed by Netscapefor transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data − a public key known to everyone and a private or secret key known only to the recipient of the message.

SSL URLs
Most Web browsers support SSL, and many websites use the protocol to obtain confidential user information, including credit card numbers. By convention, URLs that require an SSL connection start with https: instead of http:.

How SSL Works
When a Web browser tries to connect to a website using SSL, the browser will first request the web server identify itself. This prompts the web server to send the browser a copy of the SSL Certificate. The browser checks to see if the SSL Certificate is trusted -- if the SSL Certificate is trusted, then the browser sends a message to the Web server. The server then responds to the browser with a digitally signed acknowledgement to start an SSL encrypted session. This allows encrypted data to be shared between the browser and the server. You may notice that your browsing session now starts with https (and not http).

Secure HTTP (S-HTTP)

Another protocol for transmitting data securely over the World Wide Web is Secure HTTP (S-HTTP). Whereas SSL creates a secure connection between a client and a server, over which any amount of data can be sent securely, S-HTTP is designed to transmit individual messages securely. SSL and S-HTTP, therefore, can be seen as complementary rather than competing technologies. Both protocols were approved by the Internet Engineering Task Force (IETF) as a standard.



IBM Smart Cloud

IBM SmartCloud is a line of enterprise-class cloud computing technologies and services for building and using private, public and hybrid clouds. SmartCloud offerings can be purchased as self-service or managed services.

IBM SmartCloud Enterprise+

IBM's largest cloud service offering is the SmartCloud Enterprise and Enterprise+, with Enterprise+ being available in the United States early 2012 (a global deployment is planned for by the end of 2012). IBM SmartCloud Enterprise+ offers a cost-effective scalable cloud infrastructure; in other words, the Enterprise+ and SmartCloud Enterprise are both a cloud model known as an infrastructure as a service (or IaaS).

In an IaaS model, the client is paying for a cloud service offering that is housed, ran and maintained by a separate owner; in this case, IBM. This cloud offering allows a company to have a method of creating, updating, maintaining and even scaling an enterprise-wide system without the cost-prohibitive task of purchasing the hardware to make this possible.

So what exactly does that mean in terms of IBM's SmartCloud? With Enterprise and Enterprise+, IBM is offering companies of all sizes a way to host enterprise-class, security-rich and cost-saving private clouds that aide in business growth. To put it another way, Enterprise and Enterprise+ are the base of a pyramid, the foundation of a structure that must be sound and sturdy before anymore building (i.e. business growth) can happen. And if the infrastructure is the base, then the next phase of construction is the platform.

IBM SmartCloud Application Services

Sitting nicely between IaaS and SaaS is the type of cloud offering known as platform as a service (PaaS). And IBM recently made a big move with the recent launch of their PaaS offerings. This new service allows enterprises to take advantages of a set of cloud-delivered services while still being able to have control over development, deployment, management and integration.

In our pyramid analogy, IBM's Application Services sit right on top of the foundation. It provides a set of automated services and tools that can be customizable to your business' unique needs. The service offerings include enterprise-grade security, Java and cross-platform support with no vendor lock-in. Run on the SmartCloud Enterprise and Enterprise+ (the IaaS foundation), they are designed for enterprise workloads. Other application services include application lifecycle, resources, environments, management and integration services.

Smaller software offerings

For businesses to take true advantage of IBM's SmartCloud Enterprise, they need to find both standard and custom solutions that work with their specific needs. So to complete the pyramid (i.e. tailor the technology system to a company's unique plan), the "builders" must top off their work with the right software for completion. And IBM's solution in this instance is the third and final cloud offering, the software as a service model (SaaS).

In the SaaS model, businesses can plug in a ready-made application to get them up-and-running in a certain area. In what is called a "vertical solution", IBM's service offerings include customer relationship management software (CRM), human resources (HR) applications, and financial

applications. Instead of overhauling your current system with an IaaS model or doing major tweaks with a PaaS option, integrating software for a specific need is a quick fix to a persistent issue.

With the options available and the many advantages to each, I'm sure there is one question that comes to mind when considering a cloud:

Which cloud model is right for your business?

And that depends on the kind of solution you're looking for. If you're happy with your current system and just want to beef up a few departmental needs, a SaaS solution will to the trick. If you're ready go from a paper-based system (complete with file cabinets and copy machines) to something that's entirely housed on the web, investing in an IaaS cloud service model can save you countless amounts in both hardware and physical space. If you're somewhere in between – a solid infrastructure in place but nothing more – then using a PaaS cloud offering to customize what's on top of your sturdy foundation is a good option.

With IBM's wide array of cloud service offerings, most companies will find the hardware, platform and/or software they need to grow their business. In addition to their excellent customer support, IBM offers a trusted unmatched speed and a trusted infrastructure that can help you take your business to the next level.

AWS

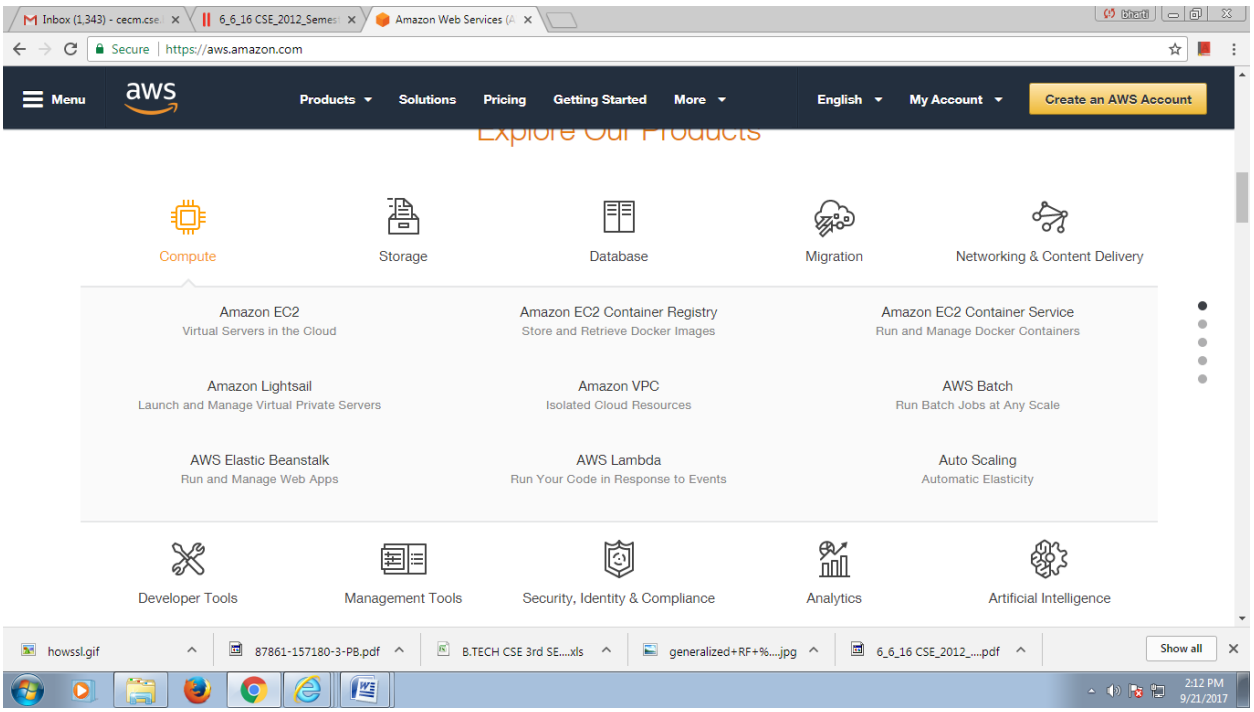
Amazon Web Services (AWS) is a comprehensive, evolving cloud computing platform provided by Amazon.com. Web services are sometimes called cloud services or remote computing services. The first AWS offerings were launched in 2006 to provide online services for websites and client-side applications.

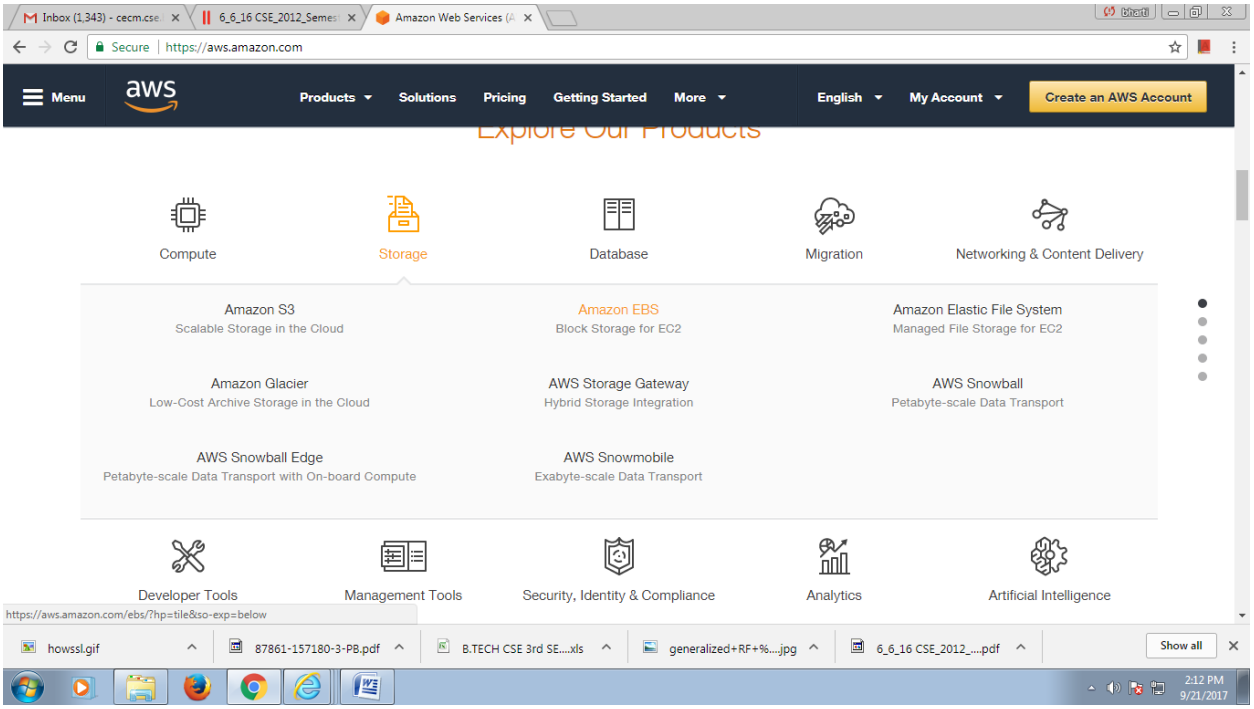
To minimize the impact of outages and ensure robustness of the system, AWS is geographically diversified into regions. These regions have central hubs in the Eastern USA, Western USA (two locations), Brazil, Ireland, Singapore, Japan, and Australia. Each region comprises multiple smaller geographic areas called availability zones.

The growing AWS collection offers over three dozen diverse services including:

- CloudDrive, which allows users to upload and access music, videos, documents, and photos from Web-connected devices. The service also enables users to stream music to their devices.
- CloudSearch, a scalable search service typically used to integrate customized search capabilities into other applications.

- Dynamo Database (also known as DynamoDB or DDB), a fully-managed NoSQLdatabase service known for low latencies and scalability.
- Elastic Compute Cloud, which allows business subscribers to run application programs and can serve as a practically unlimited set of virtual machines (VMs).
- ElastiCache, a fully managed caching service that is protocol-compliant with Memcached, an open source, high-performance, distributed memory object caching system for speeding up dynamic Web applications by alleviating database load.
- Mechanical Turk, an application program interface (API) that allows developers to integrate human intelligence into Remote Procedure Calls (RPCs) using a network of humans to perform tasks that computers are ill-suited for.
- RedShift, a petabyte-scale data warehouse service designed for analytic workloads, connecting to standard SQL-based clients and business intelligence tools.
- Simple Storage Service (S3), a scalable, high-speed, low-cost service designed for online backup and archiving of data and application programs.




Inbox (1,343) - cecm.cse
6_6_16 CSE_2012_Semes
Amazon Web Services (A
Secure | https://aws.amazon.com
Menu
aws
Products
Solutions
Pricing
Getting Started
More
English
My Account
Create an AWS Account
Explore Our Products
Compute
Storage
Database
Migration
Networking & Content Delivery
Amazon S3
Scalable Storage in the Cloud
Amazon EBS
Block Storage for EC2
Amazon Elastic File System
Managed File Storage for EC2
Amazon Glacier
Low-Cost Archive Storage in the Cloud
AWS Storage Gateway
Hybrid Storage Integration
AWS Snowball
Petabyte-scale Data Transport
AWS Snowball Edge
Petabyte-scale Data Transport with On-board Compute
AWS Snowmobile
Exabyte-scale Data Transport
Developer Tools
Management Tools
Security, Identity & Compliance
Analytics
Artificial Intelligence
https://aws.amazon.com/ebs/?hp=tile&so-exp=below
howssl.gif
87861-157180-3-PB.pdf
B.TECH CSE 3rd SE....xls
generalized+RF+%....jpg
6_6_16 CSE_2012_....pdf
Show all
2:12 PM
9/21/2017