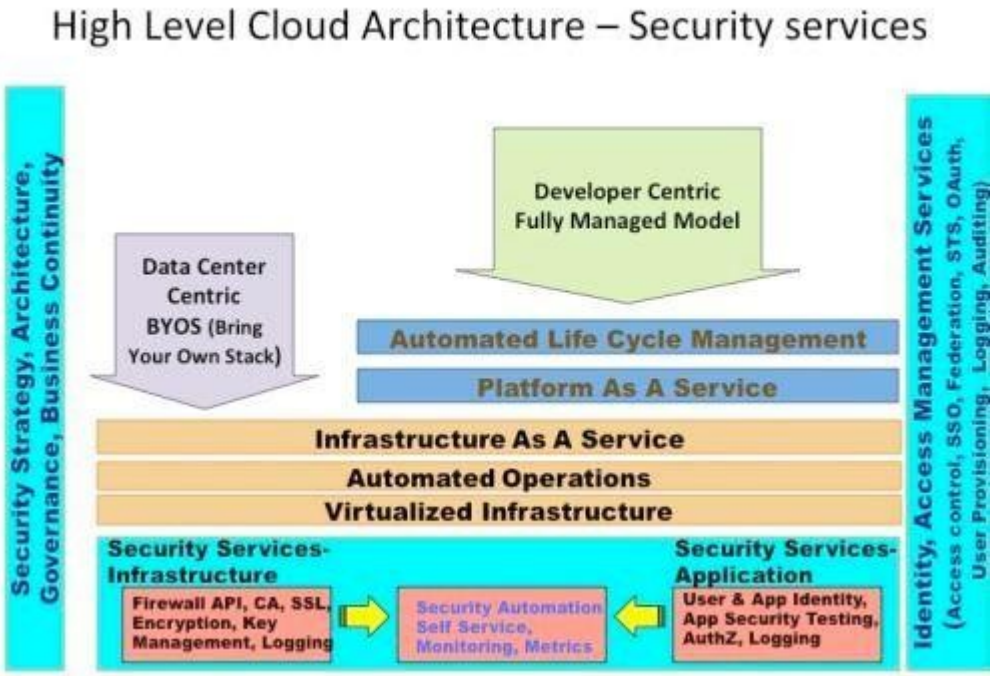
UNIT-5

Cloud Security

Cloud Security Architecture – Plan

As a first step, architects need to understand what security capabilities are offered by cloud platforms (PaaS, IaaS). The figure below illustrates the architecture for building security into cloud services.



Security offerings and capabilities continue to evolve and vary between cloud providers. Hence you will often discover that security mechanisms such as key management and data encryption will not be available. For example: the need for a AES 128 bit encryption service for encrypting security artifacts and keys escrowed to a key management service. For such critical services, one will continue to rely on internal security services. A "Hybrid cloud" deployment architecture pattern may be the only viable option for such applications that dependent on internal services. Another common use case is Single Sign-On (SSO). SSO implemented within an enterprise may not be extensible to the cloud application unless it is a federation architecture using SAML 1.1 or 2.0 supported by the cloud service provider.

The following are cloud security best practices to mitigate risks to cloud services:

Architect for security-as-a-service –

Application deployments in the cloud involve orchestration of multiple services including automation of DNS, load balancer, network QoS, etc. Security automation falls in the same category which includes automation of firewall policies between cloud security zones, provisioning of certificates (for SSL), virtual machine system configuration, privileged accounts and log configuration. Application deployment processes that depend on security processes such as firewall policy creation, certificate provisioning, key distribution and application pen testing should be migrated to a self-service model. This approach will eliminate human touch points and will enable a security as a service scenario. Ultimately this will mitigate threats due to human errors, improve operational efficiency and embed security controls into the cloud applications.

Implement sound identity, access management architecture and practice –

Scalable cloud bursting and elastic architecture will rely less on network based access controls and warrant strong user access management architecture. Cloud access control architecture should address all aspects of user and access management lifecycles for both end users and privileged users – user provisioning & deprovisioning, authentication, federation, authorization and auditing. A sound architecture will enable reusability of identity and access services for all use cases in public, private and hybrid cloud models. It is good practice to employ secure token services along with

proper user and entitlement provisioning with audit trails. Federation architecture is the first step to extending enterprise SSO to cloud services. Refer to cloud security alliance, Domain 12 for detailed guidance here.

Leverage APIs to automate safeguards –
Any new security services should be deployed with an API (REST/SOAP) to enable automation. APIs can help automate firewall policies, configuration hardening, and access control at the time of application deployment. This can be implemented using open source tools such as puppet in conjunction with the API supplied by cloud service provider.

Always encrypt or mask sensitive data –
Today's private cloud applications are candidates for tomorrow's public cloud deployment. Hence architect applications to encrypt all sensitive data irrespective of the future operational model.

Do not rely on an IP address for authentication services –
IP addresses in clouds are ephemeral in nature so you cannot solely rely on them for enforcing network access control. Employ certificates (self-signed or from a trusted CA) to enable SSL between services deployed on cloud.

Log, Log, Log –
Applications should centrally log all security events that will help create an end-to-end transaction view with non-repudiation characteristics. In the event of a security incident, logs and audit trails are the only reliable data leveraged by forensic engineers to investigate and understand how an application was exploited. Clouds are elastic and logs are ephemeral hence it is critical to periodically migrate log files to a different cloud or to the enterprise data center.

Continuously monitor cloud services –
Monitoring is an important function given that prevention controls may not meet all the enterprise standards. Security monitoring should leverage logs produced by cloud services, APIs and hosted cloud applications to perform security event correlation. Cloud audit (cloudaudit.org) from CSA can be leveraged towards this mission

Cloud Security Architecture Patterns

Architecting appropriate security controls that protect the CIA of information in the cloud can mitigate cloud security threats. Security controls can be delivered as a service (Security-as-a-Service) by the provider or by the enterprise or by a 3rd party provider. Security architectural patterns are typically expressed from the point of security controls (safeguards) – technology and processes. These security controls and the service location (enterprise, cloud provider, 3rd party) should be highlighted in the security patterns.

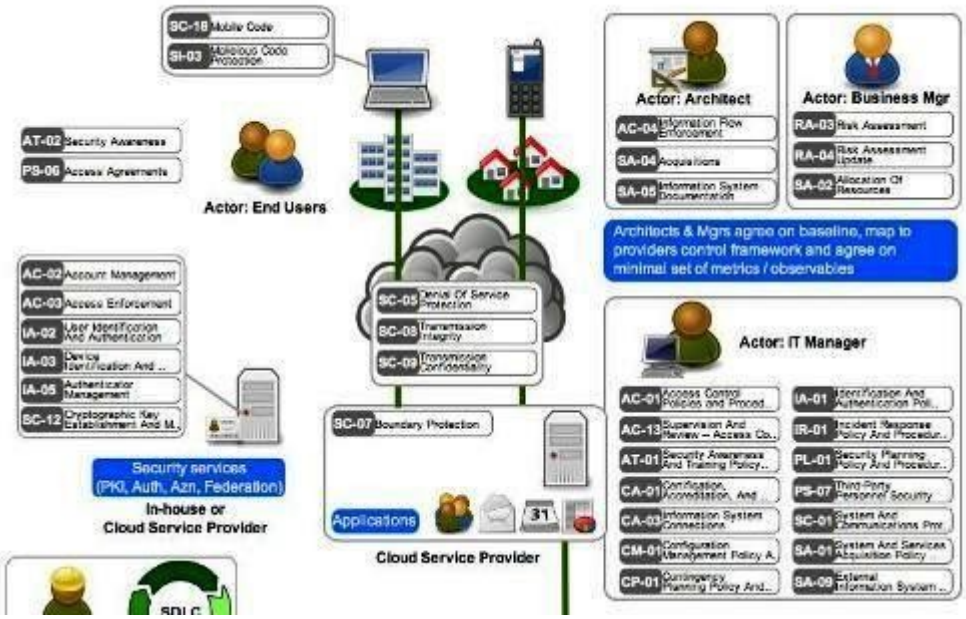
Security architecture patterns serve as the North Star and can accelerate application migration to clouds while managing the security risks. In addition, cloud security architecture patterns should highlight the trust boundary between various services and components deployed at cloud services. These patterns should also point out standard interfaces, security protocols (SSL, TLS, IPSEC, LDAPS, SFTP, SSH, SCP, SAML, OAuth, Tacacs, OCSP, etc.) and mechanisms available for authentication, token management, authorization, encryption methods (hash, symmetric, asymmetric), encryption algorithms (Triple DES, 128-bit AES, Blowfish, RSA, etc.), security event logging, source-of-truth for policies and user attributes and coupling models (tight or loose).Finally the patterns should be leveraged to create security checklists that need to be automated by configuration management tools like puppet.

In general, patterns should highlight the following attributes (but not limited to) for each of the security services consumed by the cloud application:

- Logical location – Native to cloud service, in-house, third party cloud. The location may have an implication on the performance, availability, firewall policy as well as governance of the service.
- Protocol – What protocol(s) are used to invoke the service? For example REST with X.509 certificates for service requests.
- Service function – What is the function of the service? For example encryption of the artifact, logging, authentication and machine finger printing.
- Input/Output – What are the inputs, including methods to the controls, and outputs from the security service? For example, Input = XML doc and Output =XML doc with encrypted attributes.
- Control description – What security control does the security service offer? For example, protection of information confidentiality at rest, authentication of user and authentication of application.

- Actor – Who are the users of this service? For example, End point, End user, Enterprise administrator, IT auditor and Architect.

Here is a subset of the cloud security architecture pattern published by open security architecture group

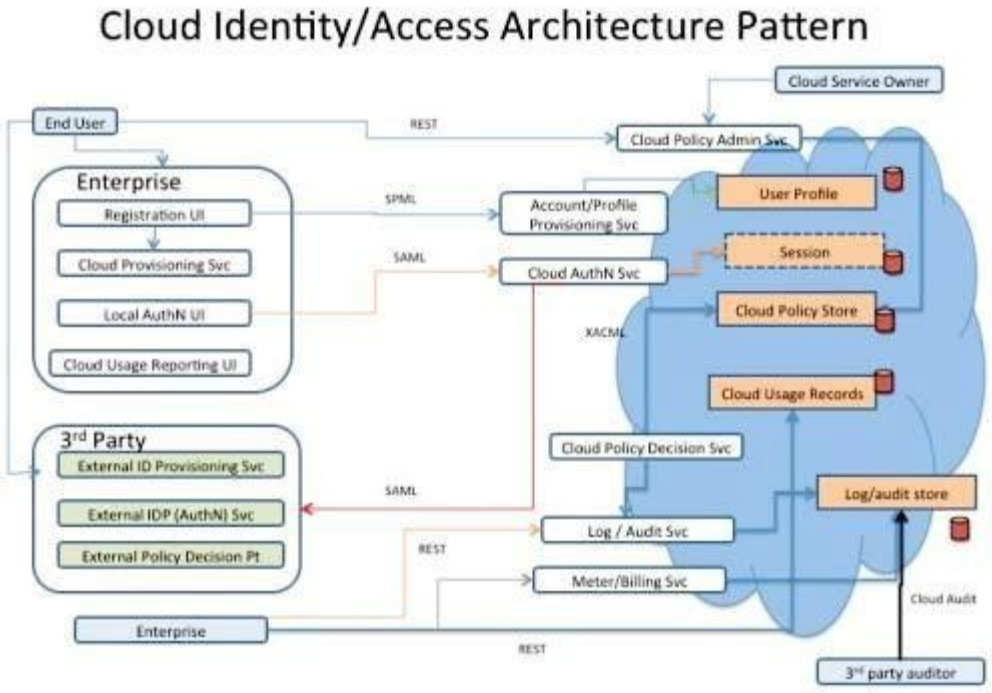


This pattern illustrates the actors (architect, end user, business manager, IT manager), interacting with systems (end point, cloud, applications hosted on the cloud, security services) and the controls employed to protect the actors and systems (access enforcement, DoS protection, boundary protection, cryptographic key & management, etc). Let's look at details communicated by the pattern.

Infrastructure Security services (controls) at cloud service providers
As per the pattern a cloud service provider is expected to provide security controls for DoS protection and protection of confidentiality and integrity for sessions originating from Mobile as well as PC. Typically these sessions initiated by browsers or client applications and are usually delivered using SSL/TLS terminated at the load balancers managed by the cloud service provider. Cloud service providers usually don't share the DoS protection mechanisms as hackers can easily abuse it.

Application Security Services (in-house or cloud service provider)
Security services such as user identification, authentication, access enforcement, device identification, cryptographic services and key management can be located either with the cloud service provider, within the enterprise data center or some combination of the two.

The second pattern illustrated below is the identity and access pattern derived from the CSA identity domain.



This pattern illustrates a collection of common cloud access control use cases such as user registration, authentication, account provisioning, policy enforcement, logging, auditing and metering. It highlights the actors (end user, enterprise business user, third party auditor, cloud service owner) interacting with services that are hosted in the cloud, in-house (enterprise) and in third party locations.

This pattern communicates the following:

Identity Security services (controls) at cloud service providers
The cloud hosts the following services:

- Authentication service that supports user authentication originating from an enterprise portal (Local AuthN UI) and typically delivered using SAML protocol. The authenticated session state is maintained in a cloud session store.
- Account and profile provisioning service supports the provisioning of new accounts and user profiles, typically invoked via SPML (Service Provisioning Markup Language) or a cloud service provider specific API. Profiles are stored in the user profile store.
- Cloud policy admin service is used for managing policies that dictate which resources in the cloud can be accessed by end users. Using this service, cloud service owners (enterprise) can perform administrative functions and end users can request for access to cloud resources. Cloud policies are stored in the cloud policy store.
- Logging and auditing service supports dual functions. The first function is event logging, including security events, in the cloud and the second is for audit purposes. Cloud Audit protocols and APIs can be employed to access this service.
- Metering service keeps track of cloud resource usage. Finance departments can use this service for charge-back as well as for billing reconciliation.

Identity Security services in the Enterprise
In this pattern, a subset of the applications is hosted in the enterprise:

Cloud registration UI provides the UI service for end users to register, manage and provision new cloud resources. Authentication and Authorization is enforced by the cloud services.
Cloud usage reporting UI is utilized by end users to generate usage reports.
Cloud provisioning service is used to provision cloud resources (compute, storage, network, application services). Access control (AuthN, AuthZ) and session management are enforced at the cloud service end.
Identity Security services at the third party location
In this pattern, cloud applications rely on identity services offered by a third party and hosted at their location. These services offer support for third party users who will need access to cloud resources to perform business functions on behalf of the enterprise. For example backup and application monitoring services. In this model, user provisioning, authentication and access enforcement functions are delegated to the third party service.

Principles of Cloud Security Architecture
A well-designed cloud security architecture should be based on the following key principles:

Identification—
Knowledge of the users, assets, business environment, policies, vulnerabilities and threats, and risk management strategies (business and supply chain) that exist within your cloud environment.
Security Controls—
Defines parameters and policies implemented across users, data, and infrastructure to help manage the overall security posture.
Security by Design—
Defines the control responsibilities, security configurations, and security baseline automations. Usually standardized and repeatable for deployment across common use cases, with security standards, and in audit requirements.
Compliance—
Integrates industry standards and regulatory components into the architecture and ensures standards and regulatory responsibilities are met.
Perimeter Security—
Protects and secures traffic in and out of organization's cloud-based resources, including connection points between corporate network and public internet.
Segmentation—
Partitions the architecture into isolated component sections to prevent lateral movement in the case of a breach. Often includes principles of 'least privilege'.
User Identity and Access Management—
Ensures understanding, visibility, and control into all users (people, devices, and systems) that access corporate assets. Enables enforcement of access, permissions, and protocols.
Data encryption—
Ensures data at rest and traveling between internal and external cloud connection points is encrypted to minimize breach impact.
Automation—
Facilitates rapid security and configuration provisioning and updates as well as quick threat detection.
Logging and Monitoring—
Captures activities and constant observation (often automated) of all activity on connected systems and cloud-based services to ensure compliance, visibility into operations, and awareness of threats.
Visibility—
Incorporates tools and processes to maintain visibility across an organization's multiple cloud deployments.
Flexible Design—Ensuring architecture design is sufficiently agile to develop and incorporate new components and solutions without sacrificing inherent security.

Some threats and issues may also be more specific to the type of cloud service:

IaaS Cloud Security Threats

Availability disruption through denial-of-service attacks

- Injection flaws
- Broken authentication
- Sensitive data exposure
- XML external entities
- Broken access control
- Security misconfigurations
- Cross-site scripting (XSS)
- Insecure deserialization
- Using components with known vulnerabilities
- Insufficient logging and monitoring
- Data leakage (through inadequate ACL)
- Privilege escalation through misconfiguration
- DoS attack via API
- Weak privileged key protection
- Virtual machine (VM) weaknesses
- Insider data theft

PaaS Cloud Security Threats

- Privilege escalation via API
- Authorization weaknesses in platform services
- Run-time engine vulnerabilities
- Availability disruption through denial-of-service attacks
- Injection flaws
- Broken authentication
- Sensitive data exposure
- XML external entities
- Broken access control
- Security misconfigurations
- Cross-site scripting (XSS)
- Insecure deserialization
- Using components with known vulnerabilities
- Insufficient logging and monitoring
- Data leakage (through inadequate ACL)
- Privilege escalation through misconfiguration
- DoS attack via API
- Privilege escalation via API
- Weak privileged key protection
- Virtual machine (VM) weaknesses
- Insider data theft

SaaS Cloud Security Threats

- Weak or immature identity and access management
- Weak cloud security standards
- Zero-day vulnerabilities
- Shadow IT/unsanctioned cloud applications/software
- Service disruption through denial-of-service attacks
- Phishing
- Credential stuffing attacks
- Weak compliance and auditing oversight
- Stolen or compromised credentials
- Weak vulnerability monitoring

Authentication and Authorization in Cloud Computing

Security is a vital component in any cloud computing solution. As these services provide a shared access model where everything runs on the same platform, they need to separate and protect customer systems and data. Cloud service providers use authentication and authorization to achieve these security goals. In fact, cloud computing platforms could not provide economies of scale via their shared resourcing model without authentication and authorization.

Authentication

- Authentication is used by a server when the server needs to know exactly who is accessing their information or site.
- Authentication is used by a client when the client needs to know that the server is system it claims to be.
- In authentication, the user or computer has to prove its identity to the server or client.
- Usually, authentication by a server entails the use of a user name and password. Other ways to authenticate can be through cards, retina scans, voice recognition, and fingerprints.
- Authentication by a client usually involves the server giving a certificate to the client in which a trusted third party such as Verisign or Thawte states that the server belongs to the entity (such as a bank) that the client expects it to.
- Authentication does not determine what tasks the individual can do or what files the individual can see. Authentication merely identifies and verifies who the person or system is.

Authorization

- Authorization is a process by which a server determines if the client has permission to use a resource or access a file.
- Authorization is usually coupled with authentication so that the server has some concept of who the client is that is requesting access.
- The type of authentication required for authorization may vary; passwords may be required in some cases but not in others.
- In some cases, there is no authorization; any user may be use a resource or access a file simply by asking for it. Most of the web pages on the Internet require no authentication or authorization.

Encryption

- Encryption involves the process of transforming data so that it is unreadable by anyone who does not have a decryption key.
- The Secure Shell (SSH) and Socket Layer (SSL) protocols are usually used in encryption processes. The SSL drives the secure part of "https://" sites used in e-commerce sites (like E-Bay and Amazon.com.)
- All data in SSL transactions is encrypted between the client (browser) and the server (web server) before the data is transferred between the two.
- All data in SSH sessions is encrypted between the client and the server when communicating at the shell.
- By encrypting the data exchanged between the client and server information like social security numbers, credit card numbers, and home addresses can be sent over the Internet with less risk of being intercepted during transit.

Using authentication, authorization, and encryption

Authentication, authorization, and encryption are used in every day life. One example in which authorization, authentication, and encryption are all used is booking and taking an airplane flight.

- Encryption is used when a person buys their ticket online at one of the many sites that advertises cheap ticket. Upon finding the perfect flight at an ideal price, a person goes to buy the ticket. Encryption is used to protect a person's credit card and personal information when it is sent over the Internet to the airline. The company encrypts the customer's data so that it will be safer from interception in transit.
- Authentication is used when a traveler shows his or her ticket and driver's license at the airport so he or she can check his or her bags and receive a boarding pass. Airports need to authenticate that the person is who he or she says she is and has purchased a ticket, before giving him or her a boarding pass.
- Authorization is used when a person shows his or her boarding pass to the flight attendant so he or she can board the specific plane he or she is supposed to be flying on. A flight attendant must authorize a person so that person can then see the inside of the plane and use the resources the plane has to fly from one place to the next.

Here are a few examples of where encryption, authentication, and authorization are used by computers:

- Encryption should be used whenever people are giving out personal information to register for something or buy a product. Doing so ensures the person's privacy during the communication. Encryption is also often used when the data returned by the server to the client should be protected, such as a financial statement or test results.
- Authentication should be used whenever you want to know exactly who is using or viewing your site. Weblogin is Boston University's primary method of authentication. Other commercial websites such as Amazon.com require people to login before buying products so they know exactly who their purchasers are.
- Authorization should be used whenever you want to control viewer access of certain pages. For example, Boston University students are not authorized to view certain web pages dedicated to professors and administration. The authorization requirements for a site are typically defined in a website's .htaccess file.
- Authentication and Authorization are often used together. For example, students at Boston University are required to authenticate before accessing the Student Link. The authentication they provide determines what data they are authorized to see. The authorization step prevents students from seeing data of other students

IAM:

While IT professionals might think IAM is for larger organizations with bigger budgets, in reality, the technology is accessible for companies of all sizes

Basic components of IAM

An IAM framework enables IT to control user access to critical information within their organizations. IAM products offer role-based access control, which lets system administrators regulate access to systems or networks based on the roles of individual users within the enterprise.

In this context, access is the ability of an individual user to perform a specific task, such as view, create or modify a file. Roles are defined according to job, authority and responsibility within the enterprise.

IAM systems should do the following: capture and record user login information, manage the enterprise database of user identities, and orchestrate the assignment and removal of access privileges.

That means systems used for IAM should provide a centralized directory service with oversight and visibility into all aspects of the company user base.

Digital identities are not just for humans; IAM can manage the digital identities of devices and applications to help establish trust.

In the cloud, IAM can be handled by authentication as a service or identity as a service (IDaaS). In both cases, a third-party service provider takes on the burden of authenticating and registering users, as well as managing their information. Read more about these cloud-based IAM options.

Benefits of IAM

IAM technologies can be used to initiate, capture, record and manage user identities and their related access permissions in an automated manner. An organization gains the following IAM benefits:

Access privileges are granted according to policy, and all individuals and services are properly authenticated, authorized and audited.

Companies that properly manage identities have greater control of user access, which reduces the risk of internal and external data breaches.

Automating IAM systems allows businesses to operate more efficiently by decreasing the effort, time and money that would be required to manually manage access to their networks.

In terms of security, the use of an IAM framework can make it easier to enforce policies around user authentication, validation and privileges, and address issues regarding privilege creep.

IAM systems help companies better comply with government regulations by allowing them to show corporate information is not being misused. Companies can also demonstrate that any data needed for auditing can be made available on demand.

Companies can gain competitive advantages by implementing IAM tools and following related best practices. For example, IAM technologies allow the business to give users outside the organization -- like customers, partners, contractors and suppliers -- access to its network across mobile applications, on-premises applications and SaaS without compromising security. This enables better collaboration, enhanced productivity, increased efficiency and reduced operating costs.

Types of digital authentication

With IAM, enterprises can implement a range of digital authentication methods to prove digital identity and authorize access to corporate resources.

Unique passwords. The most common type of digital authentication is the unique password. To make passwords more secure, some organizations require longer or complex passwords that require a combination of letters, symbols and numbers. Unless users can automatically gather their collection of passwords behind a single sign-on entry point, they typically find remembering unique passwords onerous.

Pre-shared key (PSK). PSK is another type of digital authentication where the password is shared among users authorized to access the same resources -- think of a branch office Wi-Fi password. This type of authentication is less secure than individual passwords.

A concern with shared passwords like PSK is that frequently changing them can be cumbersome.

Behavioral authentication. When dealing with highly sensitive information and systems, organizations can use behavioral authentication to get far more granular and analyze keystroke dynamics or mouse-use characteristics. By

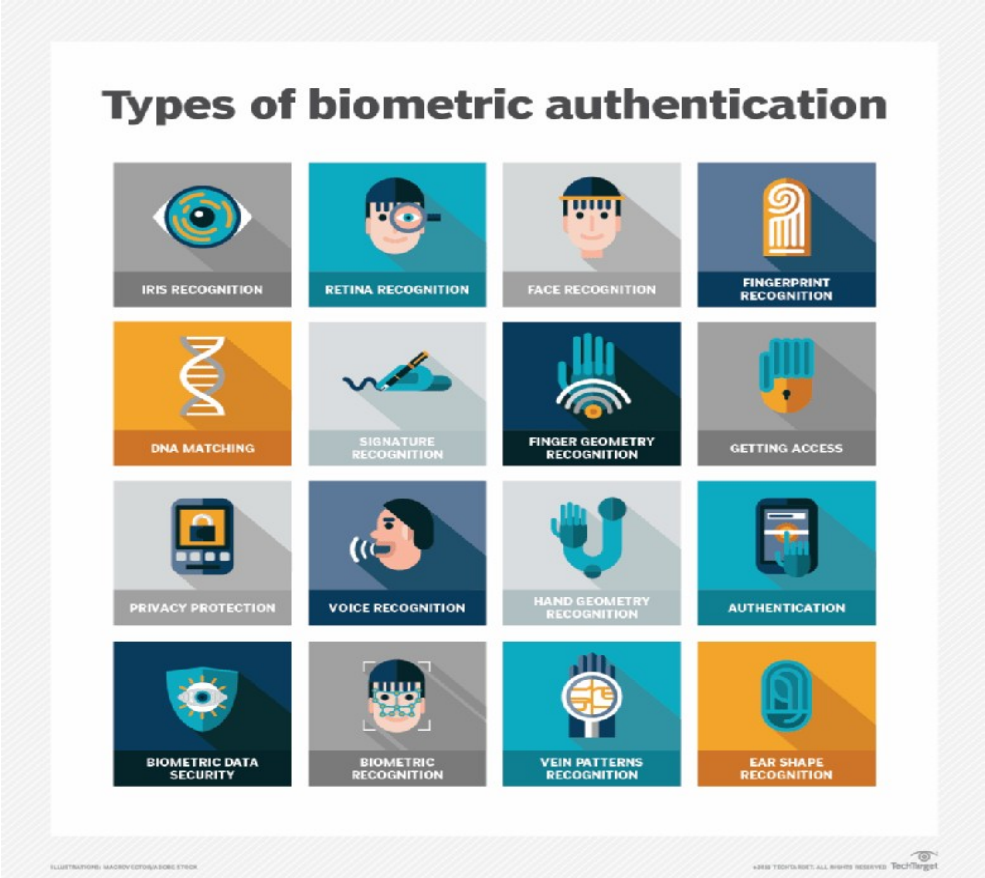
applying artificial intelligence, a trend in IAM systems, organizations can quickly recognize if user or machine behavior falls outside of the norm and can automatically lock down systems.

Biometrics. Modern IAM systems use biometrics for more precise authentication. For instance, they collect a range of biometric characteristics, including fingerprints, irises, faces, palms, gaits, voices and, in some cases, DNA. Biometrics and behavior-based analytics have been found to be more effective than passwords.

When collecting and using biometric characteristics, companies must consider the ethics in the following areas:

- data security (accessing, using and storing biometric data);
- transparency (implementing easy-to-understand disclosures);
- optionality (providing customers a choice to opt in or out); and
- biometric data privacy (understanding what constitutes private data and having rules around sharing with partners.

One danger in relying heavily on biometrics is if a company's biometric data is hacked, then recovery is difficult, as users can't swap out facial recognition or fingerprints like they can passwords or other non-biometric information. Another critical technical challenge of biometrics is that it can be expensive to implement at scale, with software, hardware and training costs to consider.
Before getting attached to passwordless IAM, make sure you understand the pros and cons of biometric authentication.



Data security in cloud computing;

Cloud data security is the combination of technology solutions, policies, and procedures that the enterprise implements to protect cloud-based applications and systems, along with the associated data and user access.
The core principles of information security and data governance—data confidentiality, integrity, and availability (known as the CIA triad)—also apply to the cloud:

- Confidentiality: protecting the data from unauthorized access and disclosure
- Integrity: safeguard the data from unauthorized modification so it can be trusted
- Availability: ensuring the data is fully available and accessible when it’s needed

Some of the common cloud-related risks that organizations face include:

- Regulatory noncompliance—whether it's the General Protection Data Regulation (GDPR) or the Healthcare Insurance Portability and Accountability Act (HIPAA), cloud computing adds complexity to satisfying compliance requirements.
- Data loss and data leaks—data loss and data leaks can result from poor security practices such as misconfigurations of cloud systems or threats such as insiders.
- Loss of customer trust and brand reputation—customers trust organizations to safeguard their personally identifiable information (PII) and when a security incident leads to data compromise, companies lose customer goodwill.
- Business interruption—risk professionals around the globe identified business disruption caused by failure of cloud technology / platforms or supply chains as one of their top five cyber exposure concerns.[2]
- Financial losses—the costs of incident mitigation, data breaches, business disruption, and other consequences of cloud security incidents can add up to hundreds of millions of dollars.

Cloud computing threats to data security

While cybersecurity threats that apply to on-premises infrastructure also extend to cloud computing, the cloud brings additional data security threats. Here are some of the common ones:

- Unsecure application programming interfaces (APIs)—many cloud services and applications rely on APIs for functionalities such as authentication and access, but these interfaces often have security weaknesses such as misconfigurations, opening the door to compromises.
- Account hijacking or takeover—many people use weak passwords or reuse compromised passwords, which gives cyberattackers easy access to cloud accounts.
- Insider threats—while these are not unique to the cloud, the lack of visibility into the cloud ecosystem increases the risk of insider threats, whether the insiders are gaining unauthorized access to data with malicious intent or are inadvertently sharing or storing sensitive data via the cloud.

Key Management in Cloud Services

Key management is the management of cryptographic keys in a cryptosystem. A reliable key management system (KMS) helps meet a business's compliance and data control requirements and benefits the overall security of the organization.

Key Takeaways:

- The conceptual architecture of a KMS, including 4 examples of cloud KMS patterns
- Encryption key management and control, including example controls for the different phases of the key management lifecycle
- Recommendations for utilizing the 2 most commonly used API architectures in the industry: REST (REpresentational State TRansfer) and SOAP (Simple Object Access Protocol)
- Practical considerations for API management
- Features of 5 major cloud service providers' KMS offerings

Cloud Security Audit:

A cloud audit is a test of a cloud environment, typically conducted by an independent third-party. During an audit, the auditor gathers evidence via physical inspection, inquiry, observation, re-performance, or analytics.

Cloud security audits commonly focus on an organization's security controls – these are the operational, procedural, or technical protections an organization uses to safeguard the integrity and confidentiality of its information systems. In the cloud, an auditor may evaluate which security controls exist, whether they are implemented correctly, whether they are working as expected, and how effective they are at mitigating threats.

Benefits of Cloud Security Audits

Here are a few ways in which security audits can improve the security of your cloud environment:

- Overseeing access control – employees join and leave the organization and personnel move to new roles and departments. A security audit can ensure that access control is managed responsibly, for example ensuring that access is revoked when employees leave, and that new employees are granted minimal privileges.

- Secure access to the cloud – a cloud security audit can help verify that employees and other users access cloud systems in a secure manner – for example, using a VPN over an encrypted channel.
- Security of APIs and third-party tools – most cloud environments use a large variety of APIs and third-party technologies. Every API or third-party tool is a potential security risk. Audits can identify security weaknesses in APIs and tools and help the organization remediate them.
- Verifying backup strategies – the cloud makes it easy to perform backups. However, this is only effective if an organization's cloud platform is configured to carry out the backups regularly. An audit can ensure that the organization is performing backups for all critical systems, and adopting security measures to safeguard those backups.

6 Steps to Conducting a Cloud Security Audit

1. Evaluate the Cloud Provider's Security Posture

The first step of a cloud security audit is evaluating the cloud provider's security posture, and establishing a relationship with cloud provider staff to receive the necessary information. As part of your audit, evaluate security procedures and policies, and work to determine the risk inherent in cloud systems, based on reliable data from cloud systems.

2. Determine The Attack Surface

Cloud environments are complex and have low visibility. Use modern cloud monitoring and observability technology to identify the attack surface, prioritize assets at higher risk, and focus remediation efforts.

Understand what applications are running within cloud instances and containers, and whether they are approved by the organization, or represent shadow IT. All workloads must be standardized and must have the appropriate security measures to ensure compliance.

This type of monitoring can address the difficulties of the shared responsibility model, by providing visibility into the security profile of the cloud assets you manage on an ongoing basis.

Related content: Read our guide to cloud security monitoring (coming soon)

3. Set Strong Access Controls

Access management breaches are one of the most prevalent cloud security risks. There are many ways in which credentials to critical cloud resources can fall into the wrong hands. Here are some steps you can take to minimize risk from your side:

Create strong password standards and policies
Make multi-factor authentication (MFA) a must
Limit administrative privileges
Practice the least privilege principle for all cloud assets

4. Develop External Sharing Standards

You must implement standards for data sharing via shared drives, calendars, files, and folders. The best approach is to begin with the strictest standards and loosen security restrictions if there is a special need.

Folders and files featuring the most sensitive data, including personally identifiable information (PII), financial, and protected medical information (PHI), should not be permitted for external access and sharing, except in special circumstances.

5. Automate Patching

You should regularly patch to ensure your cloud environment is secure. However, mastering patch management can be challenging for security and IT teams. Multiple studies found that it takes organizations over a month on average to patch a security weakness.

The key to effective patching is to prioritize the most important patches, and ensure that critical assets are patched automatically on a regular basis. Complement automation with regular manual reviews to ensure that patching mechanisms are functioning properly.

6. Use SIEM to Standardize Cloud Logs

Security information and event management (SIEM) systems can help organizations comply with many industry standards and regulations. Log management, a function of SIEM, is an industry-standard approach for auditing activity on an IT network. SIEM systems can collect cloud logs in a standardized format, and allow editors to explore log data, and automatically generate reports needed for various compliance standards.

Cloud for Industry, Healthcare &Education:

Basics for clouds in healthcare
A cloud is a virtual storage facility accessed by different computers over the Internet, regardless of location. In the cloud, companies store their data or use the environment as a server for software and apps. When companies do not manage the cloud themselves, they save resources. In these cases, the entire IT infrastructure is located with a service provider who provides the technology. Doctors or hospitals connect to the cloud environment via networks and use it from then on.

Cloud computing in the healthcare industry is based on the private cloud model. A company's IT department sets up this platform, which they then make available to employees throughout the company. In addition, so-called public clouds also exist, but they are out of the question for all medical institutions for reasons of data protection and data security. Dropbox, OneDrive from Microsoft or Amazon are examples of such cloud types.

To remain flexible, many organizations combine cloud types and use a hybrid cloud. Sensitive data with a high risk remains in the private cloud environment or is transferred via end-to-end encrypted cloud services. This ensures secure access and data security.

Cloud solutions in the medical sector
Healthcare produces an enormous amount of data every day. Patient information from a doctor's office or the results of an examination from a clinic are essential for further treatments. However, the ways of exchanging data between doctors are sometimes outdated and take longer accordingly. Results are still sent to the specialist by fax. X-ray images are usually still stored as a recording on a DVD, which patients hand over to the doctor in charge or send by mail.

The problem is that with these methods, the applicable requirements for security, confidentiality and usability suffer. Information provided by fax for the next doctor is therefore not encrypted during transmission and may therefore fall into the wrong hands. In addition, the values must first be re-entered into the computer by the staff at the other practice in order for them to be permanently available and accessible.

Clouds in healthcare: Data security with TeamDrive
Since January 2021, politicians in Germany have been relying on the electronic patient record. In this system, this patient data is stored securely in a cloud environment. Access is only permitted to specialists, hospitals or health insurance companies. TeamDrive has also established itself as an encrypted cloud service in the healthcare sector. TeamDrive users have the option of creating individual user rights and managing secure access themselves.

Sensitive data can then only be viewed by those who have the rights to do so. All other users and TeamDrive itself never have access to confidential content, so that the requirements of medical confidentiality are met. Therefore, an inexpensive, flexible and very secure cloud service such as TeamDrive is precisely designed to meet the needs that arise for the secure exchange of data between laboratory and doctor as well as hospital, doctor and health insurance company.

Patients themselves have access to their own data via an app or their home computer. Findings from the doctor or the laboratory are sent to them digitally. However, the cost of their own cloud technology is often a challenge for medical practices. TeamDrive offers individual solutions here and provides cloud services tailored to requirements. IT security also plays a central role in cloud computing because personal data is processed and stored. The IT environment of a cloud provider must therefore comply with very high standards.

TeamDrive offers data protection and secure encryption
TeamDrive meets the following requirements for a healthcare cloud:

- independent and secure
- compliance with all requirements of the GDPR
- separate contract for professional secrecy holders according to § 203 StGB (German penal code)
- compatibility and encryption
- Access at any time and from any location
- End-to-end encrypted sending of e-mail attachments, even to recipients without TeamDrive
- Automatic synchronization of lab reports

BENEFITS OF CLOUD COMPUTING IN HEALTHCARE

- Accelerates clinical analyses and care processes.
- Automates data processing and scalability.
- Increases patient data accessibility.
- Reduces network equipment and staff costs.

- Reduces risk of data loss

cloud computing for energy system:

The energy sector is in the midst of a major transformation. As countries seek to reduce their carbon footprint and move towards renewable options, the need for storing, managing, and analyzing data has become increasingly important. Cloud technology has been instrumental in helping energy companies manage their data and use it effectively. This blog post looks at how cloud technology will continue to be an essential tool for energy companies over the next few years, with a focus on 2023. We'll explore the business needs & challenges that organizations face when it comes to digital transformation and how cloud solutions can help them meet those challenges head-on.

The current state of the energy sector

The energy sector is in a state of flux. A move away from traditional means of generation, such as coal and nuclear, towards renewable sources, such as solar and wind, is underway. This shift is being driven by a number of factors, including the need to reduce greenhouse gas emissions and the falling cost of renewables. The rise of new technologies, such as storage and smart grids, is also playing a role.

All of these changes have an impact on the way the energy sector operates. For example, the growth of renewables has led to a more distributed generation mix, with electricity being generated closer to where it is needed. This has implications for transmission and distribution networks. New technologies are also changing how consumers interact with the energy system, with some able to generate and store their own electricity.

The energy sector is undergoing a period of transformation that is likely to continue in the years ahead. The growing need for cloud computing is one consequence of this change. Cloud services can provide the flexibility and scalability needed to support a more dynamic and decentralized energy system. They can also help utilities manage data associated with new technologies like storage and smart meters.

The trend of digitalization in the energy sector

The trend of digitalization in the energy sector is driven by a number of factors. One is the increasing adoption of smart grid technologies. Smart grids are equipped with sensors and other devices that allow for two-way communication between utilities and consumers. This allows for more efficient management of energy resources and can help to reduce costs. Another factor is the rise of renewable energy sources, such as solar and wind power, which is becoming increasingly cost-competitive with traditional fossil fuels, making them a more attractive option for both utilities and consumers.

As the trend of digitalization in the energy sector continues to grow, so too will the need for cloud computing. Cloud computing provides a number of advantages over traditional on-premises IT infrastructure, which makes it well-suited for handling the increasing complexity of energy data. With cloud computing, energy companies can benefit from increased flexibility, scalability, and efficiency – all of which are critical as the sector continues to evolve.

Nine advantages of Cloud in the energy sector

1. Data Management and Analysis: Cloud computing allows for the efficient storage, processing, and analysis of large amounts of data generated by the energy sector, which can help to improve operational efficiency by providing real-time insights into the performance of energy systems.
2. Smart Grid Management: Cloud computing allows for the efficient management and analysis of data from smart grids, which can help to improve the reliability and efficiency of the electrical grid.
3. Predictive Maintenance: By using machine learning algorithms on data from sensor networks, cloud computing can help to predict when equipment may fail, allowing for proactive maintenance to be scheduled.
4. Renewable Energy Integration: Cloud can be used to predict the output of renewable energy sources, such as solar and wind power, which can help to improve the integration of these sources into the grid.
5. Energy Trading: Cloud-based platforms are being used to facilitate energy trading between consumers and producers, allowing for a more efficient and transparent market.
6. Energy Management: Cloud-based energy management systems allow businesses and households to monitor and control their energy consumption in real time, which can help to reduce costs and improve energy efficiency.
7. Carbon Trading: Cloud-based platforms can be used to facilitate carbon trading between businesses and organizations, which can help to reduce carbon emissions by creating financial incentives for companies to reduce their carbon footprint.
8. Automation: Cloud-based automation systems can help to reduce manual processes and improve the efficiency of energy operations by automating tasks such as meter reading, billing, and data analysis.

9. Remote Monitoring: Cloud computing enables remote monitoring of energy systems and infrastructure, allowing for real-time monitoring and control of operations, which can help to improve efficiency by reducing the need for on-site visits.

cloud computing for transportation system

The cloud powered solutions find their application in many industries catering to a diverse range of customers. The flexibility and scalability inherent in any cloud computing service make it nearly a one size fits all solution.
The transportation industry is a very capital intensive. Companies that want to do well need to cover a large geographical area and offer frequent trips back and forth from main destinations. This demands a large fleet of vehicles and meticulous planning.

Procuring and maintaining a large fleet of vehicles is a daunting challenge in itself, as it is a major burden on a transport company's financial and administrative resources. This leaves little or no resources for the back end operations of transportation.

In the present era of severe competitiveness, operational efficiency is instrumental in achieving break even and maybe profitability. This is where the cloud comes into play.

Real-time Vehicle Tracking
Before proliferation of the cloud, the services of specialized vehicle tracking companies had to be engaged to track and monitor the location of vehicles in real time. In most cases, these companies would mandate the purchase of costly hardware.
Some of this hardware would be installed over the vehicles themselves, while its major chunk was deployed at the premise of transport company. Then, this hardware would also entail recurring maintenance and up gradation costs.

Fast forward to the era of cloud computing and this matter stands resolved in a very easy manner. Cloud Service Providers (CSP) are more than happy to provide real time tracking service for the fleet of vehicles under the Software as a Service (SaaS) model.

What this means for the transport company is zero hardware on premise. So, not only are hardware procurement costs eliminated, but with no hardware to maintain, operational expenses are also curtailed.

E-Ticketing Management
Before the cloud, the very facility of e-ticketing was either not available or offered by a handful of companies. Most of the e-ticketing was limited to the extent of airlines industry. This made the task of buying tickets cumbersome and time consuming.

To offer the online reservation and purchase of tickets, transportation companies would have to install costly servers and other support hardware that was capable of handling the peak passenger loads such as the holidays season.

Here's the biggest catch of deploying I.T hardware on premise, you always have to plan for the worst case scenario, which in this case is peak demand. The outcome is that a transport company ends up investing in hardware which will never be utilized optimally.

Now, if the same e-ticketing mechanism is sourced from the cloud, scalability of the service is in-built. The implication would be that in times of heightened passenger demand, the CSP would allocate more computing resources to the transport company.

Without procuring any hardware whatsoever, the transport company would handle the times of abnormal demand seamlessly, just by paying the CSP an additional usage fee for the additional resources consumed.

The passengers, who in fact are the company's customers, would be able to plan and book their transport from the comfort of their homes. This is a win-win situation for the transport company, passengers as well as the CSP.

Logistical Space Planning
Transportation companies tend to add logistical movement in a bid to diversify their portfolio and remain competitive. Planning logistics is way more complicated than passengers, which count as somewhat a standard payload.

When it comes to moving items, a transportation company has to plan the weight, mass and physical placement of each item very intricately. For this, a company would typically need some sort of modeling software.

If this type of solution is deployed on premise, it would again need dedicated hardware, entailing both procurement and maintenance costs. CSPs offer highly intelligent and capable virtual modeling software that can be used by transport companies.

Firstly, this sort of modeling software is delivered from the hardware resources of the CSP, so no hardware needs to be deployed on premise. Secondly, as such solutions are costly; the transport company will pay only for what it uses.
Passenger Entertainment
As part of a pleasurable ride, a transport company needs to provide in ride entertainment. The company can save a lot of effort and money by using a cloud based streaming service such as Netflix. This will enhance passenger experience and increase brand loyalty.

Real Time Updates
The transport industry is susceptible to unforeseen delays such as road closures, diversions or severe traffic jams at busy intersections. Using a cloud based tracking and messaging solution, passengers can be updated in real time about changes in ride schedule.

Although this would not alleviate the wastage of additional time spent in the travel, it would definitely keep the passengers engaged. This service would also help those clients who are planning to visit the transport company to collect or deliver their parcel.

Vehicle Health Monitoring
Most vehicles in the transport industry are highly strained to meet tight schedules. This raises concerns about vehicle health as minimal time is spared for maintenance related activities. However, this can be detrimental to passenger safety and company repute.

To solve this issue, a transport company can install sensors at critical components of their vehicles that constantly feed data to a cloud powered analytical tool. As soon as the value of a sensor breaches the defined threshold, the vehicle can be scheduled for repairs.

cloud computing for manufacturing industry

Cloud computing uses internet connections to store software and information used in businesses. This technology has an increasing use in manufacturing business operations and production processes. In 2017, 25% of finished product inputs were made using some type of digital technology, such as cloud computing.

Compared to traditional technology that uses individual computers to have updated software for information processing, cloud computing offers several advantages. The benefits of cloud computing for manufacturers include the following:

- Reliability: Cloud-based technology has fewer technical problems than software used on individual computers.
- Cost savings: Cloud solutions do not require in-house servers.
- Scalability: Cloud computing grows with the business or can easily scale back during slower times.
- Less time wasted in updating computers: Technology based in the cloud stays updated without IT departments wasting time making sure everyone has the latest version of the software.
- Marketplace advantage over companies not using cloud technology: Better productivity and communications give companies that use cloud manufacturing solutions a competitive edge.
- Centralized management: Access programs can happen from any computer in the organization, improving management capabilities.

Smart manufacturing is a future-forward method of allowing computers and devices to communicate with each other to optimize productivity and efficiency. Smaller businesses that don't have the IT infrastructure to implement smart manufacturing can leverage the applications of cloud technology. Cloud computing can make smart manufacturing possible for any size company.

Applications of Cloud Computing in Manufacturing
In manufacturing, cloud computing offers numerous solutions for every part of the process, from marketing to productivity. Integrating cloud technology into multiple operational areas increases the benefits gained from using it. A few common applications of cloud computing in the manufacturing sector include the following.

Cloud-Based Marketing

The comprehensive nature of cloud technology makes it a natural match for the intricacies of marketing campaigns. Manufacturers use cloud-based applications to aid in planning, executing and managing marketing campaigns. By using data on production and sales, manufacturers can also track the effectiveness of marketing campaigns.

Product Development
Product planning and development tie heavily into production. By merging product planning and development information into supply chain data and communications, manufacturers can prepare their operations for full production. With comprehensive integration, products can move from idea to engineering to prototype to small production and finally to full-scale manufacturing and shipping much faster.

Production and Stock Tracking
Once production starts, cloud technology can benefit the process of producing and stocking products. With enterprise resource planning (ERP) software, companies can match their production levels to available stock and sales. The software can manage price quotes, order intake and customer requests. Fewer mistakes happen when using a standard product to track these, thus lowering order cycle times.

Productivity Management
Rarely do manufacturers maintain the same level of production for all products throughout the year. To meet the market's changing needs, manufacturers can use cloud-based applications to monitor when to change production. Plus, by allowing communications throughout the supply chain, these software solutions ensure producers have the required amount of raw materials on hand and can readily change their orders to match their future productivity levels.

SaaS Solutions in Cloud Technology in Manufacturing
Cloud technology has three main forms — software as a service (SasS), platform as a service (Paas) and infrastructure as a service (IaaS). IaaS lets manufacturers of all sizes use an enterprise-level infrastructure to help with operation scaling, data storage and information processing. Companies use PaaS to develop their own applications in rented production or development solutions. Lastly, SaaS offers internet-based software programs for use by anyone in a company. Among these, SaaS ranks as one of the simplest solutions to quickly integrate into a business.

Limited Misinformation or Disconnected Data
With a single software location, everyone refers to the same information and documents. When using cloud-based ERP, only one main source for company information exists. The prevalence of misinformation reduces because everyone uses the same source for company data.

Ease of Making Changes for the Future
Cloud technology's scalability and constant updates make planning for the future simpler. Using a SaaS network avoids issues of outdated software or operating systems on an individual computer. By eliminating these concerns, SaaS makes integrating smart manufacturing technology and other future-forward solutions easier.

Improved Collaboration
By connecting to the same files in the same software, everyone in the SaaS network participates in data collaboration. Because they reference a shared document, they all have the most updated information for decision-making and planning. Even those located remotely can contribute to operations and collaborate on projects with cloud-based manufacturing software.

cloud computing for education industry:

CLOUD COMPUTING: HOW DOES IT BRING INNOVATION IN EDUCATION

Cloud computing refers to a setup of computing resources that can be shared anywhere, irrespective of the location of the users. By implementing cloud computing, it becomes possible to bring teachers and learners together on a single, unified platform. Educational organizations such as schools, colleges, and universities need not buy, own, and maintain their own servers and data centers. Rather, they can leverage cloud computing to avail compute power, databases, storage, and other services when they need them. Additionally, they can always be sure about their resources being secure on the cloud. Let us elaborate on the extensive benefits of cloud computing in the field of education.

1. STRONG VIRTUAL CLASSROOM ENVIRONMENTS

With cloud-based software, it becomes possible for educational organizations to have virtual classrooms for the students. The concept reduces the infrastructural costs to a considerable extent. They can even reduce the expenses of onboarding regular teachers in their faculty. Rather, they can collaborate with skilled trainers who work remotely and serve as cost-

effective resources. At the same time, teachers can create and deliver online courses to students anywhere. Students can even appear for virtual exams, saving their time and expenses effectively.

2. Ease of accessibility

The potential of the cloud is unmatched when it comes to accessibility. Users can easily access the course content, applications, and data anytime and anywhere. They can enroll in courses and participate in group activities as well. The barriers of place and time no longer exist the cloud ensures seamless delivery of content at all times. What's more, it even sends across content on mobile devices so that students can easily learn even while on the go.

3. Extensive cost-savings

Another benefit of cloud computing that you cannot ignore is extensive cost savings. Both learners and providers can experience big benefits in this context. Students need not invest in expensive books and applications as these learning resources are available on the cloud. Providers too can lower the management costs by simplifying processes such as enrollment and assignment tracking. And of course, the infrastructural costs reduce too, as explained before. The best part about cloud computing is that you pay as you go, which makes it cost-effective.

4. Secure data storage

Besides accessibility and cost savings, cloud computing also serves the benefit of secure data storage. Organizations that deliver learning through the cloud can adopt a VPN for ensuring data security. VPN protocols such as IKEv2 are responsible for the automatic encryption of outgoing data and traffic. This means that the learning content can be easily transferred to the users without compromising its integrity. At the same time, learners can protect their privacy by using VPN for cloud-based learning applications.

5. Scalability

Scalability refers to the ability of the applications to match the growing numbers of users. Cloud computing covers the schools, colleges, and universities on this front as well. It enables them to scale up the learning applications and experiences quickly and easily. As a result, they can handle an increasing number of students. Additionally, scalability also helps them to manage the usage peaks and traffic spikes caused due to events like training registrations and assignment submissions. Similarly, they can scale down instantly during the low activity period to prevent wastage of resources.

6. Agility and innovation

Another way learning providers can benefit from cloud computing is through agility and innovation. It gives them the ability to experiment faster and more frequently. Consequently, they can innovate to create better learning experiences for the students. This becomes possible because new tools and features can be developed, tested, and deployed in the applications to make them better than before.

7. Greater reach for the students

Cloud computing in the education industry brings the opportunity for the students to expand their horizons. Those who are not happy with the traditional learning systems can now explore the new concept of online education. This works wonders for students who want to opt for remote learning or even pursue courses overseas. Working professionals who are unable to attend conventional classes but want to upgrade their skills can also take virtual classes.

8. Minimal hardware requirements

With cloud-based applications, the requirements of hardware resources are minimal. These applications can operate seamlessly on internet browsers, both on desktops and mobile devices. Students can manage to learn with the mobile phone that they own. There is no need to invest in an expensive computer for taking the course. Additionally, they do not require external storage devices because they get access to free cloud-based storage. Learning could not get simpler than this!

The benefits of cloud computing for the education sector are immense. It does not come as a surprise that major providers in the industry are fast embracing cloud tech so that they can enhance the services they deliver. Simultaneously, the cloud is emerging as the best option for the students as well. Nothing matches the convenience of accessing learning at the fingertips and cloud tech makes it possible. Whether it is a large university, a small school or a student, everyone in the industry is experiencing the positive impact of the cloud and things are going to get bigger and better in the future.

Migration into a Cloud

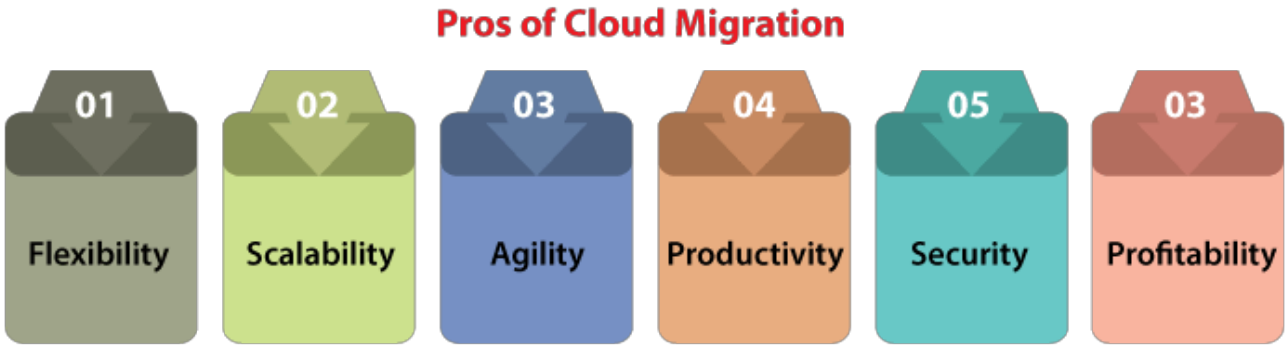
Cloud migration is the procedure of transferring applications, data, and other types of business components to any cloud computing platform. There are several parts of cloud migration an organization can perform. The most used model is the applications and data transfer through an on-premises and local data center to any public cloud.

But, a cloud migration can also entail transferring applications and data from a single cloud environment or facilitate them to another- a model called cloud-to-cloud migration. The other type of cloud migration is reverse cloud migration, cloud exit, and cloud repatriation where applications or data are transferred and back to the local data center.

Pros of Cloud Migration

Organizations migrate to a cloud for various reasons, but, normally when faced with many challenges of developing IT infrastructure within the most secure and cost-effective way possible.

Some of the advantages of migrating to a cloud are as follows:



- Flexibility: No organization facilitating experiences a similar demand level by a similar number of users every time. If our apps face fluctuations in traffic, then cloud infrastructure permits us to scale down and up to meet the demand. Hence, we can apply only those resources we require.
- Scalability: The analytics grow as the organization grows with databases, and other escalates workloads. The cloud facilitates the ability to enhance existing infrastructure. Therefore, applications have space to raise without impacting work.
- Agility: The part of the development is remaining elastic enough for responding to rapid modifications within the technology resources. Cloud adoption offers this by decreasing the time drastically it takes for procuring new storage and inventory.
- Productivity: Our cloud provider could handle the complexities of our infrastructure so we can concentrate on productivity. Furthermore, the remote accessibility and simplicity of most of the cloud solutions define that our team can concentrate on what matters such as growing our business.
- Security: The cloud facilitates security than various others data centers by centrally storing data. Also, most of the cloud providers give some built-in aspects including cross-enterprise visibility, periodic updates, and security analytics.
- Profitability: The cloud pursues a pay-per-use technique. There is no requirement to pay for extra charges or to invest continually in training on, maintaining, making, and updating space for various physical servers.

Cloud Migration Strategies Types

Migrating to a cloud can be a good investment for our business. We might be admiring where to start like several companies.

Gartner specified some options that are widely called "the six Rs of migration", defined as follows:

1. Rehosting (lift-and-shift)
The most general path is rehosting (or lift-and-shift), which implements as it sounds. It holds our application and then drops it into our new hosting platform without changing the architecture and code of the app. Also, it is a general way for enterprises unfamiliar with cloud computing, who profit from the deployment speed without having to waste money or time on planning for enlargement.

Besides, by migrating our existing infrastructure, we are applying a cloud just like other data centers. It pays for making good use of various cloud services present for a few enterprises. For example, adding scalable functions to our application to develop the experience for an improving segment of many users.

2. Re-platforming
Re-platforming is called "lift-tinker-and-shift". It includes making some cloud optimizations without modifying our app's core architecture. It is the better strategy for enterprises that are not ready for configuration and expansion, or those enterprises that wish to improve trust inside the cloud.

3. Re-factoring
It means to rebuild our applications from leverage to scratch cloud-native abilities. We could not perform serverless computing or auto-scaling. A potential disadvantage is vendor lock-in as we are re-creating on the cloud infrastructure. It is the most expensive and time-consuming route as we may expect. But, it is also future-proof for enterprises that wish to take benefit from more standard cloud features.
It covers the most common three approaches for migrating our existing infrastructure.

4. Re-purchasing
It means replacing our existing applications along with a new SaaS-based and cloud-native platform (such as a homegrown CRM using Salesforce). The complexity is losing the existing training and code's familiarity with our team over a new platform. However, the profit is ignoring the cost of the development.
Re-purchasing is the most cost-effective process if moving through a highly personalized legacy landscape and minimizing the apps and service number we have to handle. Once we have accessed the nature and size of our application portfolio, we may detect cloud migration is not correct for us.

5. Retiring
When we don't find an application useful and then simply turn off these applications. The consequencing savings may boost our business situation for application migration if we are accessible for making the move.

6. Re-visiting
Re-visiting may be all or some of our applications must reside in the house. For example, applications that have unique sensitivity or handle internal processes to an enterprise. Don't be scared for revisiting cloud computing at any later date. We must migrate only what makes effects to the business.

Process of Cloud Migration
The way we consider the strategies of cloud migration as mentioned above depends on migration goals, the complexity, size of our current environment, and our business model. At this time, we will want to trust our IT team's expertise to understand the various outs and in of our environment.
Whether we transfer all services and apps at once or take the hybrid path of keeping a few applications on-premise, most of the migrations pursue a similar basic procedure as listed below:

1. Plan our migration
Cloud migration needs a solid planning strategy to be successful. Get clear over our reasons for the transfer and which of the migration strategy best helps them before getting begun. Here is where we might apply cloud migration resources and tools for supporting our migration plan by:

Giving complete visibility into our on-premise platform including each system dependency.
Assessing security, server, and performance requirements. Also, examine what type of training our team will require.
2. Select our cloud environment
We are ready to select any cloud provider that matches our requirements after evaluating our latest application resource needs.
The most popular environments include Google Cloud Platform, Microsoft Azure, and AWS (Amazon Web Services). All of these environments provide a lot of distinct cloud models for adopting, whether it is multi-cloud, private cloud, hybrid cloud, or public cloud. Price out, test, and build out a virtual workspace for seeing how things appear in distribution.

3. Migrate our data and apps
We have three options for moving a local data center to a public cloud such as online transfer with either private network or public internet, or an offline transfer (offline). Here, we upload data on an appliance for shipping to any cloud provider. One of the best approaches relies on the type and amount of data we are speed and moving on which to implement it.
4. Certify post-move success
Our work is not complete until we can show any return over investment in our migration.

Cloud Migration Tools
Third-party vendors and cloud providers facilitate a lot of automated, cloud-based, and open-source services and tools designed to:

- Certify post-migration success
- Manage and monitor its progress
- Help develop for cloud migration

7 STEP MODEL OF MIGRATION INTO THE CLOUD

1. ASSESSMENT
Migration starts with an assessment of the issues relating to migration, at the application, code, design, and architecture levels. Moreover, assessments are also required for tools being used, functionality, test cases, and configuration of the application. The proof of concepts for migration and the corresponding pricing details will help to assess these issues properly.

2. ISOLATE
The second step is the isolation of all the environmental and systemic dependencies of the enterprise application within the captive data center. These include library, application, and architectural dependencies. This step results in a better understanding of the complexity of the migration.

3. MAP
A mapping construct is generated to separate the components that should reside in the captive data center from the ones that will go into the cloud.

4. RE-ARCHITECT
It is likely that a substantial part of the application has to be re-architected and implemented in the cloud. This can affect the functionalities of the application and some of these might be lost. It is possible to approximate lost functionality using cloud runtime support API.

5. AUGMENT
The features of cloud computing service are used to augment the application.

6. TEST
Once the augmentation is done, the application needs to be validated and tested. This is to be done using a test suite for the applications on the cloud. New test cases due to augmentation and proof-of-concepts are also tested at this stage.

7. OPTIMISE
The test results from the last step can be mixed and so require iteration and optimization. It may take several optimizing iterations for the migration to be successful. It is best to iterate through this seven step model as this will ensure the migration to be robust and comprehensive.

Organizational readiness and Change Management in The Cloud Age

Introduction

- The studies for Organization for Economic Co-operation and Development (OECD) economics demonstrated that there is a strong correlation between changes in organization and workplace practices and investment in IT.
- In order to effectively enable and support enterprise business goals and strategies, IT must adapt new technologies and continually change.
- Organization should have a transition to a desirable level of CMM (Change ManagementMaturity) by having following key knowledge:
- Domain 1: Managing the Environment, understanding the organization (people,process and culture)
- Domain 2: Recognizing and Analyzing the Trends (Business and Technology), observerthe key driver for changes.
- Domain 3:Leading for Results, Assess organizational readiness and architect solution that delivers definite business values

Basic Concept of organizational readiness

- People in the organization face the change as challenging. They have fear or uncertainties. This is called FUD syndrome: Fear, Uncertainty and Doubt.
- Employees are used to their roles and responsibility and are familiar with their environment and management's expectations.
- But when corporate changes are made, it is common that people tend to become uncomfortable and excited regardless the level and intensity of change.
- Surveys are made and studies say that project fails to meet the objectives, money are wasted, opportunities are lost due to lack of focus and interest in the change.

Drivers for changes: A framework to comprehend the competitive environment

The five driving factors for change given by the framework are:

- Economic (global and local, external and internal)
  Economic factors are usually dealing with the state of economy,both local and global in scale. Managers and groups are expected to deal with the unpleasant facts of shrinking market share, declining profit margins, unsatisfactory earnings, new and increasing competition. Managers are often asked to do more with less, and this is done during downturn.
- Legal, political, and regulatory compliance
  This deals with issues of transparency, compliance and conformity. The objective is to be a good corporate citizen and industry leader and to avoid the potential cost of legal threats from external factors.
- Environmental (industry structure and trends)
  Environmental factors usually deal with the quality of natural environments, human health, and safety.
- Technology developments and innovation
  New technologies and innovations in every has played very important part and has changed the lives of so many fields.
- Socio cultural (markets and customers)
  It sees the societal expectations and trends and how cloud computing change the world of markets and customers.

Creating a winning environment

At the cultural level of an organization, change too often requires a lot of planning and resource. The management and executives communicate employees to make sure that every employee understands

- The new direction of the firm
- The urgency of the change needed
- What the risks are to – maintain status quote and making the change.
- What the new role of the employee will be
- What the potential rewards are.

Build the business savvy organization

Common change management models

There are many different change management approaches and models.

1) Lewin's Change Management Model

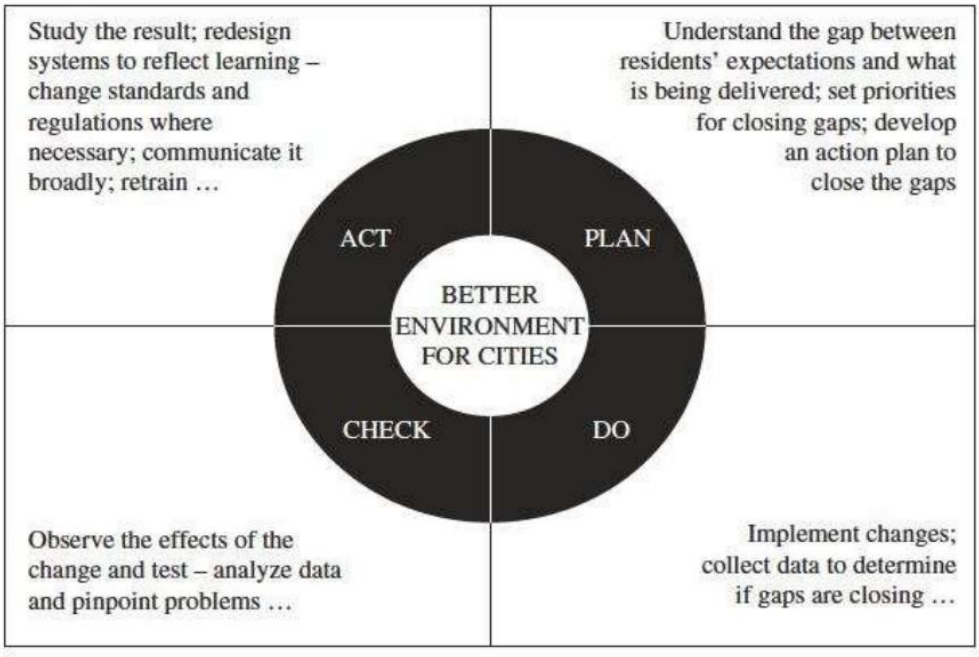
- Kurt Lewin, a psychologist by training, observed that there are three stages of changes, which are Unfreeze, Transition and Refreeze.
- It is recognized that people tend to become comfortable in this freeze or unchanging environment and they wish to remain in this safe/comfort zone. Any disturbance to them will make them uncomfortable.

- To encourage change, its necessary to unfreeze the environment by motivating people to accept the change. Motivation for change must be generated before change can occur. This is the unfreezing stage from which change begins.
- The transition phase is when the change plan is executed and actual change is being implemented.
- The last phase is Refreeze, this is the stage when the organization once becomes unchanging/fozen until the next time a change is initiated.

2) Deming Cycle(Plan, Do, Study, Act)

- The Deming cycle is also known as the PDCA cycle.
- It is a continuous improvement model with four sequential sub processes: Plan, Do, Check and Act.
- The PDCA cycle is usually implemented as an evergreen process, which means that the end of one complete cycle or pass flows into the beginning of the next pass and thus supports the concept of continuous quality improvement.
- PLAN : Recognize an opportunity and plan a change.
- DO : Execute the plan in a small scale to prove the concept.
- CHECK :Evaluate the performance of the change and report the results to sponsor.
- ACT : Decide on accepting the change and standardizing it as a part of the process.

Incorporate what has been learned from the previous steps to plan new improvements and begin a new cycle.



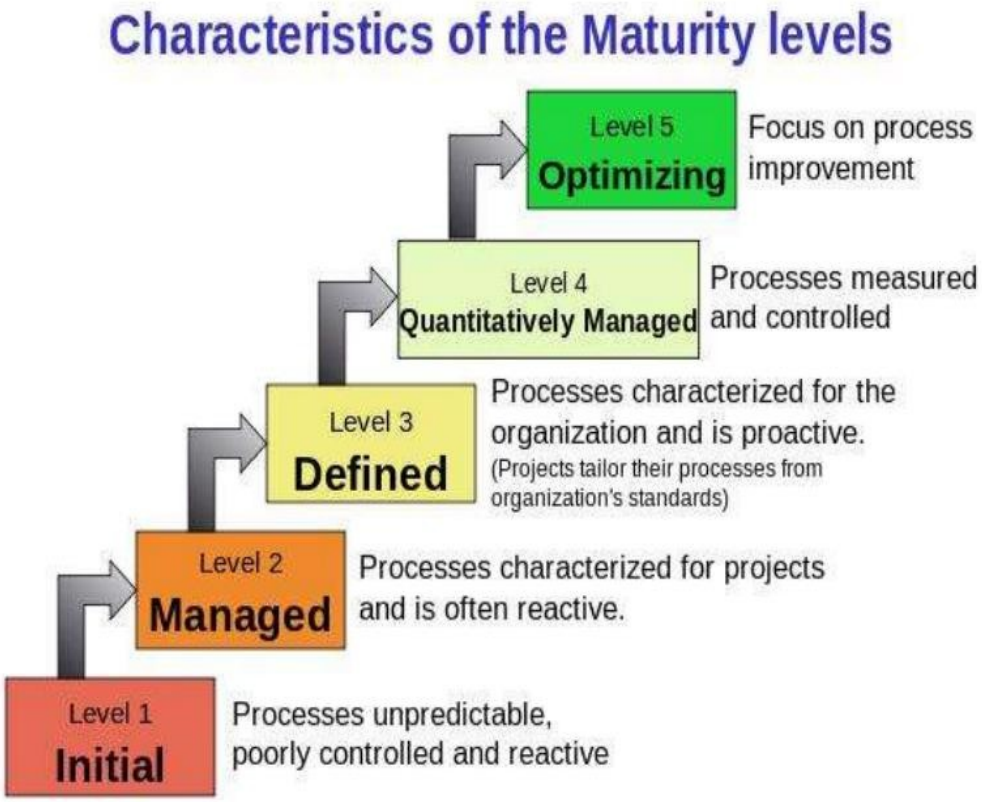
Change Management Maturity model (CMMM)

- A Change Management Maturity Model (CMMM) helps organization to analyze, understand, and visualize the strength and weakness of the firm's change management process and identify opportunities for improvement and building competitiveness.
- The model should be simple enough to use and flexible to adapt to different situations
- The business value of CMMM can be expressed in terms of improvements in business efficiency and effectiveness. All organizational investments are business investments, including IT investments. The resulting benefits should be measured in terms of business returns.
- Therefore CMMM value can be articulated as the ratio of business performance to CMMM investment;
- ROIT (CMMM) = Estimated Total business performance improvement
- Total CMM investment (TCO)

Where,

- ROIT : Obeserved business value or total return on investment from IT initiative (CMMM)
- Business performance improvement – Reduce error rate
- Increase cutomer/user satisfaction – customer and employee retension
- Increase market share and revenue
- Increase sales from existing customer
- Improve productivity
- CMMM investment – initial capital investment and total cost of ownership over the life of investment

CMM levels



Organizational Readiness self-assessment:(Who, When, Where and How)

- An organizational assessment is a process intending to seek a better understanding of as-is (current) state of the organization.
- It also defines the roadmap required to fill the gap and to get the organization moving toward where it wants to go.
- The process implies that the organization needs to complete the strategy analysis process first and to formulate the future goals.
- The assessment can be conducted by either an internal or external professional. During the effective organization readiness assessment, it is desirable to achieve following:

  - Articulate and reinforce the reason for change.
  - Determine the as-is state
  - Identify gap between future and current state
  - Assess barriers to change
  - Establish action plan to remove barriers.

- It is also important to select the right people for the assessment across the organization.
- Asking right questions is also essential. The assessment should provide insight into your challenges and help determine some of the key questions that need to be asked.

Legal Issues in Cloud Computing

Cloud computing is here to stay, all thanks to its several benefits. When connected to the right cloud infrastructure, you can save costs and enjoy broad network access and rapid elasticity.

While it is easy to be clouded by the benefits of cloud computing, you must also consider some legal issues. Doing so would ensure that you make an informed decision, especially in your choice of Cloud Service Provider (CSP). Plus, you can adequately protect yourself from the adverse effects of these legal issues in cloud computing. Today, I'll be discussing some of the issues you need to look out for.

Data Protection
Data protection is one of the most critical legal issues you must consider when using the cloud for your operations. It is especially important if your business includes handling the personal data of individuals in any form. There are data protection regulations with strict provisions on how you handle the personal data of individuals.

Under most of these regulations, including the General Data Protection Regulation, which deals with handling data of EU citizens, you can't just export citizens' personal data to the cloud without obtaining the necessary consent. You must also comply with the data protection standards as stipulated by these regulations. Failure to do so would attract strict sanctions.

You need to understand what the law says about data protection in your jurisdictions.

Data Privacy and Security
Another essential legal issue in cloud computing that you should pay attention to is data privacy and security. If a third party receives unauthorized access to private information about your clients, it can damageyour company's reputation. Your business risks losing sensitive and corporate confidential information in the case of a security breach. You may also have to compensate your customer for violating their data privacy, which would cost your business a lot.

Make sure you engage a CSP that would offer you the highest privacy and security standard possible. You should also ensure that there are necessary firewalls to prevent a security breach.

Data Ownership (Intellectual Property Rights)
It is safe to assume that you own all the rights to data sent to the cloud by your company. However, it is advisable that your Service Level Agreement (SLA) with the CSP expressly indicates that your company has full rights to the data stored in the cloud and can retrieve it whenever you want. It is also essential to have these provisions in place, especially concerning data generated inside the cloud. The CSP may want to claim newly generated data because it was generated in the cloud through a data analytics solution.

Let the SLA provide that data generated in and out of the cloud by your company belongs to your company.

Cloud Contracting model Issues
License agreements and service agreements have quite distinct core concepts. Cloud is served by the service agreement rather than licensing agreement. Due to rapid growth of cloud computing the click warp agreement is frequently being employed nowadays. It gives the user or consumer no room for discussion. With the growth of cloud computing, conventional, negotiated cloud contracts will eventually become the norm. Though, on a personal level, this is still a distant goal. In absence of negotiation the legal provisions and clauses about the liability and risk responsibility are added during the construction of the contract.

Jurisdictional issues raised by virtualization and data location
The issue of differences in laws applicable across different jurisdictions is one of the legal issues in cloud computing. For instance, the government can require CSPs to disclose client data in some jurisdictions. However, in some other jurisdictions, there is express protection for data stored in the cloud, and in those jurisdictions, governments cannot access it without following due process.

You may want your SLA to contain express provisions that the CSP can only hold your data in specific jurisdictions. The ability of a court to adjudicate actions carried out inside a specific geographic area is known as "jurisdiction". Because of cloud features like "Virtualization" and "Multi-tenancy," it is more challenging and important to determine jurisdiction in cases of legal disputes involving cloud services. The technology enables the users to determine what data is stored on machines at any particular time.

Multi-tenancy is the ability of a cloud provider to provide services to many persons or organizations from single shared software. Since the data of different users are only virtually isolated and not physically, there is a risk that the data of one user could be viewed by another user without their permission. Additionally, it makes data backup and restoration challenges too.

The flexibility that the cloud provides for data location guarantees that it is used and accessible with the greatest possible efficiency. But it also raises a host of legal problems.

Now, there is a chance that if the multiple sites are subject to various jurisdictions and legal systems then there may be contradictory legal provisions governing data in the different locations. So it is a big legal issue that various countries have with different laws governing data privacy and government access.

commercial andbusiness considerations

The present and future of cloud computing have also been greatly influenced by other economic and business factors, such as the need to reduce risk, ensure data integrity, make data accessible and available, and adhere to Service Level Agreements. Additionally, it brings about a variety of predictable and unforeseen problems that call for specific legislation to solve them.

Moreover, laws are always formed to provide the legal structure to technological advancements. This helps in reducing the complexity of cloud innovations and software services like (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). So the lawful framework is determined and set to create an effective legal system that offers legal remedies to prevent and rectify the harms that result. Thus it is important to fix tensions between legal and technical as it can enable the business owners to balance the business.

Special Topics

These are special major issues in Cloud Computing:

1. Privacy: The user data can be accessed by the host company with or without permission. The service provider may access the data that is on the cloud at any point in time. They could accidentally or deliberately alter or even delete information.

2. Compliance: There are many regulations in places related to data and hosting. To comply with regulations (Federal Information Security Management Act, Health Insurance Portability and Accountability Act, etc.) the user may have to adopt deployment modes that are expensive.

3. Security: Cloud-based services involve third-party for storage and security. Can one assume that a cloud-based company will protect and secure one's data if one is using their services at a very low or for free? They may share users' information with others. Security presents a real threat to the cloud.

4. Sustainability: This issue refers to minimizing the effect of cloud computing on the environment. Citing the server's effects on the environmental effects of cloud computing, in areas where climate favors natural cooling and renewable electricity is readily available, the countries with favorable conditions, such as Finland, Sweden, and Switzerland are trying to attract cloud computing data centers. But other than nature's favors, would these countries have enough technical infrastructure to sustain the high-end clouds?

5. Abuse: While providing cloud services, it should be ascertained that the client is not purchasing the services of cloud computing for a nefarious purpose. In 2009, a banking Trojan illegally used the popular Amazon service as a command and control channel that issued software updates and malicious instructions to PCs that were infected by the malware So the hosting companies and the servers should have proper measures to address these issues.

6, Higher Cost: If you want to use cloud services uninterruptedly then you need to have a powerful network with higher bandwidth than ordinary internet networks, and also if your organization is broad and large so ordinary cloud service subscription won't suit your organization. Otherwise, you might face hassle in utilizing an ordinary cloud service while working on complex projects and applications. This is a major problem before small organizations, that restricts them from diving into cloud technology for their business.

7. Recovery of lost data in contingency: Before subscribing any cloud service provider goes through all norms and documentations and check whether their services match your requirements and sufficient well-maintained resource infrastructure with proper upkeeping. Once you subscribed to the service you almost hand over your data into the hands of a third party. If you are able to choose proper cloud service then in the future you don't need to worry about the recovery of lost data in any contingency.

8. Upkeeping(management) of Cloud: Maintaining a cloud is a herculin task because a cloud architecture contains a large resources infrastructure and other challenges and risks as well, user satisfaction, etc. As users usually pay for how much they have consumed the resources. So, sometimes it becomes hard to decide how much should be charged in case the user wants scalability and extend the services.

9. Lack of resources/skilled expertise: One of the major issues that companies and enterprises are going through today is the lack of resources and skilled employees. Every second organization is seeming interested or has already been moved to cloud services. That's why the workload in the cloud is increasing so the cloud service hosting companies need continuous rapid advancement. Due to these factors, organizations are having a tough time keeping up to date with the tools. As new tools and technologies are emerging every day so more skilled/trained employees need to grow. These challenges can only be minimized through additional training of IT and development staff.

10. Pay-per-use service charges: Cloud computing services are on-demand services a user can extend or compress the volume of the resource as per needs. so you paid for how much you have consumed the resources. It is difficult to define a certain pre-defined cost for a particular quantity of services. Such types of ups and downs and price variations make the implementation of cloud computing very difficult and intricate. It is not easy for a firm's owner to study consistent demand and fluctuations with the seasons and various events. So it is hard to build a budget for a service that could consume several months of the budget in a few days of heavy use.