Jaipur Engineering College & Research Centre, Jaipur

Notes

Cloud Computing

[6CS4-06]

Prepared By:

Suniti Chouhan
Abhishek Jain

VISION AND MISSION OF INSTITUTE

VISION

To become renowned centre of outcome based learning and work towards academic, professional, cultural and social enrichments of the lives of individual and communities”

MISSION

M1. Focus on evaluation of learning outcomes and motivate students to inculcate research aptitude by project based learning.

M2. Identify areas of focus and provide platform to gain knowledge and solutions based on informed perception of Indian, regional and global needs.

M3. Offer opportunities for interaction between academia and industry.

M4. Develop human potential to its fullest extent so that intellectually capable and imaginatively gifted leaders can emerge in a range of professions.

VISION AND MISSION OF DEPARTMENT

VISION

To become renowned Centre of excellence in computer science and engineering and make competent engineers & professionals with high ethical values prepared for lifelong learning.

MISSION

M1: To impart outcome based education for emerging technologies in the field of computer science and engineering.

M2: To provide opportunities for interaction between academia and industry.

M3: To provide platform for lifelong learning by accepting the change in technologies

M4: To develop aptitude of fulfilling social responsibilities.

COURSE OUTCOMES

CO1: Implement the cloud computing architecture i.e, the model, types of clouds, various service models and programming concepts.

CO2: Acquire knowledge about the recent trends in area of cloud computing like Hadoop, programming of Google app engine and virtualization technology and resource management.

CO3: Identify the various threats related to cloud and as well as disaster recovery related to same.

CO4: Analyze the cloud platforms in IT industry and various case studies on the industries providing cloud services.

Program Outcomes (PO)

1. **Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex Engineering problems.
2. **Problem analysis**: Identify, formulate, research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and Engineering sciences.
3. **Design/development of solutions**: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
4. **Conduct investigations of complex problems**: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
5. **Modern tool usage**: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
6. **The engineer and society**: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional Engineering practice.
7. **Environment and sustainability**: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
8. **Ethics**: Apply ethical principles and commit to professional ethics and responsibilities and norms of the Engineering practice.
9. **Individual and team work**: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
10. **Communication**: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
11. **Project management and finance**: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one’s own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
12. **Life-long learning**: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

Program Educational Objectives (PEO)

1. To provide students with the fundamentals of Engineering Sciences with more emphasis in Computer Science & Engineering by way of analyzing and exploiting Engineering challenge

2. To train students with good scientific and engineering knowledge so as to comprehend, analyze, design, and create novel products and solutions for the real life problems.

3. To inculcate professional and ethical attitude, effective communication skills, teamwork skills, multidisciplinary approach, entrepreneurial thinking and an ability to relate engineering issues with social issues.

4. To provide students with an academic environment aware of excellence, leadership, written ethical codes and guidelines, and the self-motivated life-long learning needed for a successful professional career.

5. To prepare students to excel in Industry and Higher education by Educating Students along with High moral values and Knowledge.

MAPPING CO-PO

Cos/POs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	3	3	3	3	2	2	2	1	2	2	3
CO2	3	3	3	3	3	2	2	2	1	2	2	3
CO3	3	3	3	3	2	2	2	2	2	2	2	3
CO4	3	3	3	3	2	2	2	2	2	2	2	3

PSO

PSO1: Ability to interpret and analyze network specific and cyber security issues, automation in real word environment.

PSO2: Ability to Design and Develop Mobile and Web-based applications under realistic constraints.

SYLLABUS

UNIT 1: Introduction: Objective, scope and outcome of the course.

UNIT 2: Introduction: Objective, scope and outcome of the course. Introduction Cloud Computing: Nutshell of cloud computing, Enabling Technology, Historical development, Vision, feature Characteristics and components of Cloud Computing. Challenges, Risks and Approaches of Migration into Cloud. Ethical Issue in Cloud Computing, Evaluating the Cloud's Business Impact and economics, Future of the cloud. Networking Support for Cloud Computing. Ubiquitous Cloud and the Internet of Things.

UNIT 3: Cloud Computing Architecture: Cloud Reference Model, Layer and Types of Clouds, Services models, Data centre Design and interconnection Network, Architectural design of Compute and Storage Clouds. Cloud Programming and Software: Fractures of cloud programming, Parallel and distributed programming paradigms-Map Reduce, Hadoop, High level Language for Cloud. Programming of Google App engine.

UNIT 4: Virtualization Technology: Definition, Understanding and Benefits of Virtualization. Implementation Level of Virtualization, Virtualization Structure/Tools and Mechanisms, Hypervisor VMware, KVM, Xen. Virtualization: of CPU, Memory, I/O Devices, Virtual Cluster and Resources Management, Virtualization of Server, Desktop, Network, and Virtualization of data-centre.

UNIT 5: Securing the Cloud: Cloud Information security fundamentals, Cloud security services, Design principles, Policy Implementation, Cloud Computing Security Challenges, Cloud Computing Security Architecture . Legal issues in cloud Computing. Data Security in Cloud: Business Continuity and Disaster Recovery , Risk Mitigation , Understanding and Identification of Threats in Cloud, SLA-Service Level Agreements, Trust Management

UNIT 6: Cloud Platforms in Industry: Amazon web services , Google AppEngine, Microsoft Azure Design, Aneka: Cloud Application Platform -Integration of Private and Public Clouds Cloud applications: Protein structure prediction, Data Analysis, Satellite Image Processing, CRM

Unit 4: Securing the Cloud

Fundamentals of cloud security

Organizational pressure to reduce costs and optimize operations has led many enterprises to investigate cloud computing as a viable alternative to create dynamic, rapidly provisioned resources powering application and storage platforms. Despite potential savings in infrastructure costs and improved business flexibility, security is still the greatest barrier to implementing cloud initiatives for many companies. Information security professionals need to review a staggering array of security considerations when evaluating the risks of cloud computing.

With such a broad scope, how can an organization adequately assess all relevant risks to ensure that their cloud operations are secure? While traditional security challenges such as loss of data, physical damage to infrastructure, and compliance risk are well known, the manifestation of such threats in a cloud environment can be remarkably different. The blurring of boundaries between software-defined and hardware infrastructure in the datacenter demand a different perspective.

One of the first steps towards securing enterprise cloud is to review and update existing IT polices to clearly define guidelines to which all cloud-based operations must adhere. Such policies implement formal controls and processes with the specific aim of protecting data and systems in addition to fulfilling regulatory compliance obligations. Government bodies such as NIST, the US Department of Commerce, and the Australian Government Department of Finance and Deregulation (PDF) have produced cloud computing security documents that outline comprehensive policies for their departments, which can be a useful starting point for implementing a corporate policy.

Cloud security policies should be applied to both internal and third-party managed cloud environments. Whether building private or utilizing public cloud infrastructure within the enterprise, the responsibility for cloud security is shared between your organization and any cloud service providers you engage with. When conducting due diligence on cloud service providers, carefully review their published security policies and ensure that that it aligns with your own corporate policies.

A fundamental security concept employed in many cloud installations is known as the defense- in-depth strategy. This involves using layers of security technologies and business practices to protect data and infrastructure against threats in multiple ways. In the event of a security failure at one level, this approach provides a certain level of redundancy and containment to create a durable security net or grid. Security is more effective when layered at each level of the cloud stack.

When implementing a cloud defense-in-depth strategy, there are several security layers that may be considered. The first and most widely known protection mechanism is data encryption. With appropriate encryption mechanisms, data stored in the cloud can be protected even if access is gained by malicious or unauthorized personnel. A second layer of defense is context-based access control, a type of security policy that filters access to cloud data or resources based on a combination of identity, location, and time. Yet another popular security layer in cloud-based systems is application auditing. This process logs all user activity within an enterprise application and helps information security personnel detect unusual patterns of activity that might indicate a security breach. Finally, it is critical to ensure that all appropriate security policies are enforced where data is transferred between applications or across systems within a cloud environment.

When it comes to cloud security, no universal solutions are available to neutralize all threats against IT infrastructure. Corporate firewalls no longer demarcate a secure perimeter, which can often be extended well beyond the datacenter and into the cloud. It is similarly unwise to assume the security policies of third-party public and hybrid cloud service providers meet the standards and levels of compliance mandated by your internal policies. It is imperative that security requirements expected of third-parties are clearly defined and agreed upon.

Cloud security can be a daunting issue with wide-reaching implications for business. Threats and potential vulnerabilities are magnified and the scope of responsibility expanded dramatically: from protecting data and infrastructure from theft, intrusion or attack through to maintaining regulatory compliance. In following articles, I will outline major trends impacting cloud security , some of the challenges faced when securing a cloud environment , and provide you with suggestions and recommendations for strengthening data, access, and platform protection in your cloud environment.

Cloud Security Services

Security poses a major challenge to the widespread adoption of **cloud computing**, yet an association of cloud users and vendors sees the cloud as a provider of information security services.

The 10 security-as-a-service categories are:

1. **Identity and Access Management** should provide controls for assured identities and

access management. **Identity and access management** includes people, processes and systems that are used to manage access to enterprise resources by assuring the identity of an entity is verified and is granted the correct level of access based on this assured identity. Audit logs of activity such as successful and failed authentication and access attempts should be kept by the application/solution.

2. **Data Loss Prevention** is the monitoring, protecting and verifying the security of data at rest, in motion and in use in the cloud and on-premises. **Data loss prevention** services offer protection of data usually by running as some sort of client on desktops/servers and running rules around what can be done. Within the cloud, data loss prevention services could be offered as something that is provided as part of the build, such that all servers built for that client get the data loss prevention software installed with an agreed set of rules deployed.
3. **Web Security** is real-time protection offered either on-premise through software/appliance installation or via the cloud by proxying or redirecting web traffic to the cloud provider. This provides an added layer of protection on top of things like AV to prevent malware from entering the enterprise via activities such as web browsing. Policy rules around the types of web access and the times this is acceptable also can be enforced via these **web security** technologies.
4. **E-mail Security** should provide control over inbound and outbound e-mail, thereby protecting the organization from phishing and malicious attachments, enforcing corporate policies such as acceptable use and spam and providing business continuity options. The solution should allow for policy-based encryption of e-mails as well as integrating with various e-mail server offerings. Digital signatures enabling identification and non-repudiation are features of many cloud e-mail security solutions.
5. **Security Assessments** are third-party audits of cloud services or **assessments** of on-premises systems based on industry standards. Traditional security assessments for infrastructure and applications and compliance audits are well defined and supported by multiple standards such as NIST, ISO and CIS. A relatively mature toolset exists, and a number of tools have been implemented using the SaaS delivery model. In the SaaS delivery model, subscribers get the typical benefits of this cloud computing variant elasticity, negligible setup time, low administration overhead and pay-per-use with low initial investments.

6. **Intrusion Management** is the process of using pattern recognition to detect and react to statistically unusual events. This may include reconfiguring system components in real time to stop/prevent an intrusion. The methods of intrusion detection, prevention and response in physical environments are mature; however, the growth of virtualization and massive multi-tenancy is creating new targets for intrusion and raises many questions about the implementation of the same protection in cloud environments.

7. **Security Information and Event Management** systems accept log and event information. This information is then correlated and analyzed to provide real-time reporting and alerting on incidents/events that may require intervention. The logs are likely to be kept in a manner that prevents tampering to enable their use as evidence in any investigations.

8. **Encryption** systems typically consist of algorithms that are computationally difficult or infeasible to break, along with the processes and procedures to manage **encryption** and

9. Decryption, hashing, digital signatures, certificate generation and renewal and key exchange.

10. **Business Continuity and Disaster Recovery** are the measures designed and implemented to ensure operational resiliency in the event of any service interruptions. **Business continuity and disaster recovery** provides flexible and reliable failover for required services in the event of any service interruptions, including those caused by natural or man-made disasters or disruptions. Cloud-centric business continuity and disaster recovery makes use of the cloud's flexibility to minimize cost and maximize benefits.

11. **Network Security** consists of security services that allocate access, distribute, monitor and protect the underlying resource services. Architecturally, **network security** provides services that address security controls at the network in aggregate or specifically addressed at the individual network of each underlying resource. In a cloud/virtual environment, network security is likely to be provided by virtual devices alongside traditional physical devices.

Implementing the Cloud Security Principles:

1. Data in transit protection

User data transiting networks should be adequately protected against tampering and eavesdropping.

2. Asset protection and resilience

User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.

3. Separation between users

A malicious or compromised user of the service should not be able to affect the service or data of another.

4. Governance framework

The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined.

5. Operational security

The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes.

6. Personnel security

Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel.

7. Secure development

Services should be designed and developed to identify and mitigate threats to their security. Those which aren’t may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity.

8. Supply chain security

The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement.

9. Secure user management

Your provider should make the tools available for you to securely manage your use of their service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorized access and alteration of your resources, applications and data.

10. Identity and authentication

All access to service interfaces should be constrained to authenticated and authorized individuals.

11. External interface protection

All external or less trusted interfaces of the service should be identified and appropriately defended.

12. Secure service administration

Systems used for administration of a cloud service will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data.

13. Audit information for users

You should be provided with the audit records needed to monitor access to your service and the data held within it. The type of audit information available to you will have a direct impact on your ability to detect and respond to inappropriate or malicious activity within reasonable timescales.

14. Secure use of the service

The security of cloud services and the data held within them can be undermined if you use the service poorly. Consequently, you will have certain responsibilities when using the service in order for your data to be adequately protected.

SECURITY ISSUES IN CLOUD COMPUTING

1. Organizational Security Risks

Organizational risks are categorized are categorized as the risks that may impact the structure of the organization or the business as an entity . If a CSP goes out of business or gets acquired by another entity, this may negatively affect their CSPs since any Service Level Agreements (SLA)they had may have changed and they would then have to migrate to another CSP that more closely aligns with their needs. In addition to this, there could be the threat of malicious insiders in the organization who could do harm using the data provided by their CSCs.

2. Physical Security Risks

The physical location of the cloud data center must be secured by the CSP in order to prevent unauthorized on-site access of CSC data. Even firewalls and encryption cannot protect against the physical theft of data. Since the CSP is in charge of the physical infrastructure, they should implement and operate appropriate infrastructure controls including staff training, physical location security, network firewalls. It is also important to note that the CSP is not only responsible for storing and process data in specific jurisdictions but is also responsible for obeying the privacy regulations of those jurisdictions.

3. Technological Security Risks

These risks are the failures associated with the hardware, technologies and services provided by the CSP. In the public cloud, with its multi tenancy features, these include resource sharing isolation problems, and risks related to changing CSPs, i.e. portability. Regular maintenance and audit of infrastructure by CSP is recommended.

4. Compliance and Audit Risks

These are risks related to the law. That is, risks related to lack of jurisdiction information, changes in jurisdiction, illegal clauses in the contract and ongoing legal disputes. For example, depending on location, some CSPs may be mandated by law to turn over sensitive information if demanded by government.

5. Data Security Risks

There are a variety of data security risks that we need to take into account. The three main properties that we need to ensure are data integrity, confidentiality and availability. We will go more into depth on this in the next subsection since this is the area most at risk of being compromised and hence where the bulk of cloud security efforts are focused.

Cloud Computing Security Challenges

1: DDoS attacks

As more and more businesses and operations move to the cloud, cloud providers are becoming a bigger target for malicious attacks. Distributed denial of service (DDoS) attacks are more common than ever before. Verisign reported IT services, cloud and SaaS was the most frequently targeted industry during the first quarter of 2015.

A DDoS attack is designed to overwhelm website servers so it can no longer respond to legitimate user requests. If a DDoS attack is successful, it renders a website useless for hours, or even days. This can result in a loss of revenue, customer trust and brand authority.

Complementing cloud services with DDoS protection is no longer just good idea for the enterprise; it’s a necessity. Websites and web-based applications are core components of 21st century business and require state-of-the-art security.

2: Data breaches

Known data breaches in the U.S. hit a record-high of 738 in 2014, according to the Identity Theft Research Center, and hacking was (by far) the number one cause. That’s an incredible statistic and only emphasizes the growing challenge to secure sensitive data.

Traditionally, IT professionals have had great control over the network infrastructure and physical hardware (firewalls, etc.) securing proprietary data. In the cloud (in private, public and hybrid scenarios), some of those controls are relinquished to a trusted partner. Choosing the right vendor, with a strong record of security, is vital to overcoming this challenge.

3: Data loss

When business critical information is moved into the cloud, it’s understandable to be concerned with its security. Losing data from the cloud, either though accidental deletion, malicious tampering (i.e. DDoS) or an act of nature brings down a cloud service provider, could be disastrous for an enterprise business. Often a DDoS attack is only a diversion for a greater threat, such as an attempt to steal or delete data.

To face this challenge, it’s imperative to ensure there is a disaster recovery process in place, as well as an integrated system to mitigate malicious attacks. In addition, protecting every network layer, including the application layer (layer 7), should be built-in to a cloud security solution.

4: Insecure access points

One of the great benefits of the cloud is it can be accessed from anywhere and from any device. But, what if the interfaces and APIs users interact with aren’t secure? Hackers can find these types of vulnerabilities and exploit them.

A behavioral web application firewall examines HTTP requests to a website to ensure it is legitimate traffic. This always-on device helps protect web applications from security breaches.

5: Notifications and alerts

Awareness and proper communication of security threats is a cornerstone of network security and the same goes for cloud security. Alerting the appropriate website or application managers as soon as a threat is identified should be part of a thorough security plan. Speedy mitigation of a threat relies on clear and prompt communication so steps can be taken by the proper entities and impact of the threat minimized.

Final Thoughts

Cloud security challenges are not insurmountable. With the right partners, technology and forethought, enterprises can leverage the benefits of cloud technology.

CD Networks’ cloud security solution integrates web performance with the latest in cloud security technology. With 160 points of presence, websites and web applications are accelerated on a global scale and, with our cloud security, our clients’ cloud-based assets are protected with 24/7 end to end security, including DDoS mitigation at the network and application levels.

Cloud Computing Security Architecture:

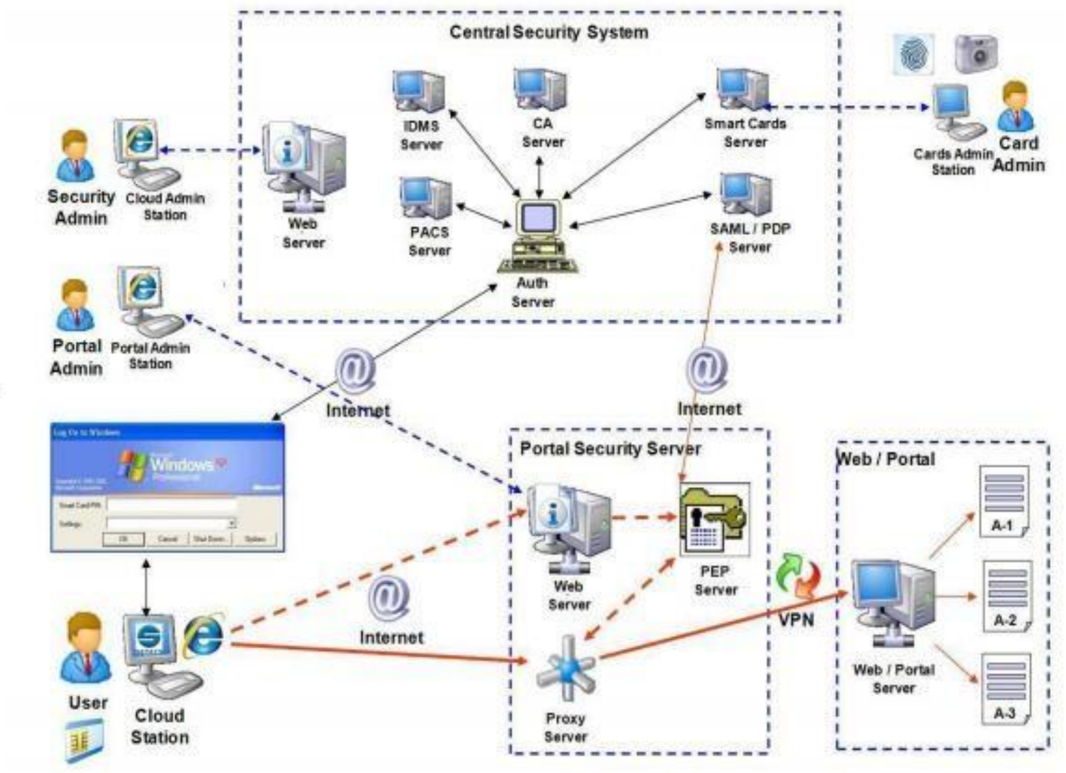

Fig: Cloud Computing Security Architecture