Cloud Computing/ Cyber Security

About:

Significant innovations in virtualization and distributed computing, as well as improved access to high-speed internet, have accelerated interest in cloud computing. But what is cloud computing?

According to Microsoft,

Simply put, cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet (“the cloud”) to offer faster innovation, flexible resources, and economies of scale. You typically pay only for cloud services you use, helping lower your operating costs, run your infrastructure more efficiently and scale as your business needs change.

According to IBM,

Cloud computing is on-demand access, via the internet, to computing resources—applications, servers (physical servers & virtual servers), data storage, development tools, networking capabilities, and more—hosted at a remote data center managed by a cloud services provider (or CSP). IaaS (Infrastructure-as-a-Service), PaaS (Platform-as-a-Service), and SaaS (Software-as-a-Service) are the three most common models of cloud services

A cloud service has three distinct characteristics that differentiate it from traditional web hosting:

- Users can access large amounts of computing power on demand. It is typically sold by the minute or the hour.

- It is elastic -- a user can have as much or as little of a service as they want at any given time.

- The service is fully managed by the provider (the consumer needs nothing but a personal computer and internet access).

Organizations transmit sensitive data across networks and to other devices in the course of doing business, and a significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. With the internet access and virtualization growth, along with positive developments, there was a sharp rise in the data-theft threats too.

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. End-user protection or endpoint security is a crucial aspect of cyber security. After all, it is often an individual (the end-user) who accidentally uploads malware or another form of cyber threat to their desktop, laptop or mobile device.

This is the reason that these two topics – Cloud Computing and Cyber Security are bundled together under one domain.

Pre-Requisites:

Topics Involved:

- Virtualization
- Google Cloud
- Amazon AWS/Lambda
- Microsoft Azure
- VMWare
- Docker/ Kubernetes
- Linux
- Networking

Syllabus

Level 1:

- **Create AWS EC2 Virtual Machine**

Amazon Elastic Compute Cloud is the service you use to create and run virtual

machines (VM), also known as instances. Launch an Amazon EC2 Instance; Connect to Amazon EC2 Instance via SSH; Terminate Amazon EC2 Instance

- **AWS Cloudfront: Serve content from multiple S3 buckets**

  Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment. Whereas Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. Create multiple AWS S3 buckets & serve or distribute its content using AWS Cloudfront via AWS management console within the AWS Free Tier.

- **Hosting a Static Website (HTML/CSS/Javascript) in AWS S3**

  Amazon Web Services provides a Simple Storage Service S3 Free Tier that can be also used to host a static website with no servers and no complexity. Deploy static website in AWS S3; Understand AWS S3 Public permissions; AWS S3 versioning

- **Get started with Azure**

  Understand about the Azure's subscriptions and accounts along with the architecture; Explore database services that are available on Microsoft Azure; Take advantage of several virtualization services in Azure compute; Know about different storage options that are available in Azure Storage services; Check about Azure

Virtual Network; Use Azure VPN Gateway and Azure ExpressRoute to create secure communication tunnels between your 2 different locations. (https://www.coursera.org/learn/microsoft-azure-cloud-services)

- **Google Cloud - Build a Bookshelf app**

  Create a sample web app that shows how to use a variety of Google Cloud products, including: App Engine flexible environment; Cloud SQL; Datastore; Cloud Storage; Compute Engine. You can use the programming language of your choice (Python, NodeJS, Java)

  https://cloud.google.com/python/docs/getting-started

  https://cloud.google.com/nodejs/getting-started

  https://cloud.google.com/java/getting-started

- **Cyber Security Foundations**

Learn about the foundations of Computer Security such as Design of Secure Systems, Goals, key concepts of Cybersecurity, popular attacks, Buffer Overflow, Cryptography, Types of Cryptography, Designing a security system, case studies, etc.

https://www.greatlearning.in/academy/learn-for-free/courses/introduction-to-cyber-security

- Introduction to Cyber Security Course

Familiarize yourself with the current cyber security landscape and acquire the knowledge of relevant tools to assess and manage security protocols in information processing systems. You will also perform business impact analysis and disaster recovery testing through this program.

https://www.simplilearn.com/learn-cyber-security-basics-skillup

- Develop ethical hacking tools using Python

As a cybersecurity analyst or penetration tester, you can develop tools in Python that will give you an edge. Learn to code and use Python for hacking so you can create your own tools to automate your security assessment processes.

Learn how to combine multiple Python libraries that are related to cybersecurity so that they can build an automated process of information gathering. You will need to know how to code a keylogger, as well as how to write a ZIP password bruteforcer in Python.

https://www.cybrary.it/course/developing-ethical-hacking-tools-with-python/

- **Build keylogger**

Key logger is a computer program that records every keystroke made by a computer, especially in order to gain fraudulent access to passwords and other confidential information. You can develop a process to detect and delete keyloggers or to capture the system's keystrokes.

https://dzone.com/articles/how-to-make-a-windows-keylogger-by-yourself

https://www.instructables.com/Simple-Keylogger-Python/

https://searchsecurity.techtarget.com/definition/keylogger

- Kali Linux - Install and Basic understanding

Kali Linux is a Debian-based Linux distribution that contains several hundred tools aimed at numerous information security tasks including penetration testing, computer forensics, security research, and reverse engineering.

https://www.cybrary.it/course/kali-linux-fundamentals/

- Cross site Scripting

Learn about what XSS is, how these types of attacks happen and the impact they cause, and ways to mitigate this popular type of attack. Three different types of cross-site scripting: stored XSS, reflected XSS, and DOM based XSS - need to be browsed.

https://www.cybrary.it/course/cross-site-scripting/

- **Learn about TCPDump Tool**

TCPDump is one of the best light-weight utilities for performing network traffic capture. It's extremely simple to use, but performs network scanning effectively and efficiently without all of the overhead associated with tools like Wireshark, making it a key part of any Cybersecurity practitioner's toolbox.

https://opensource.com/article/18/10/introduction-tcpdump

- Use tcpdump to intercept network traffic

Learn how to use tcpdump to intercept network traffic. First, you will install and configure the FTP service. Next, you will test the security of FTP by intercepting network traffic to discover whether the authentication information is exposed. Finally, you will intercept SSH traffic to discover whether the authentication information is exposed.

https://www.cybrary.it/catalog/learn-on-demand/use-tcpdump-to-intercept-network-traffic/

- Learn about the harvester tool

Reviewing a reconnaissance and information-gathering tool known as “theharvester”. This program is used by hackers and cybersecurity professionals alike to gather crucial points of information on targets. This includes names of organizational members, email addresses, webhost, domain names, and even open ports.

https://www.cybrary.it/course/theharvester-tutorial/

- Create basic network scanner

A network scanner is a tool used for analysing hosts that are available on the network. Create a basic network scanner using a programming language to scan through a list of IP addresses and identify possible hosts on the network .

https://www.geeksforgeeks.org/network-scanner-in-python/
https://secdev.github.io/
https://www.thepythoncode.com/article/building-network-scanner-using-scapy

- Create Reverse shell

A reverse shell is a type of a shell in which the target machine communicates back to the attacking machine . The attacking machine has a listener port on which it receives the connection, which by using, code or command execution is achieved.

https://www.netsparker.com/blog/web-security/understanding-reverse-shells/

https://www.hackingtutorials.org/networking/hacking-netcat-part-2-bind-reverse-shells/

- Packet sniffing (Network Analyser)

Packet sniffing is the practice of gathering, collecting and logging network packets which pass through a network. A packet analyser is a computer program which can intercept and log network traffic as it passes through the network.
Collect , identify and analyse the different types of packets and details as they cross the network.In this project you can use the popular packet analysers such as wireshark , TCP dump or Wind-up to collect and evaluate packet details.

https://www.wireshark.org/

https://www.tcpdump.org/

https://www.winpcap.org/windump/

https://youtu.be/TkCSr30UojM

- Phishing attack

Learn the basics of phishing, how and why phishing continues to work, how to craft the perfect phishing email and what you can do to defend against these increasingly clever social engineering attempts. Social engineering attacks are still the number one method of entry into an organization's network and systems by both penetration testers (ethical hackers) and adversaries. Phishing attacks are just one way that a social engineering attack can be performed, and are designed to take advantage of the human element in cybersecurity.

https://www.cybrary.it/course/phishing/

https://www.vadesecure.com/en/blog/5-common-phishing-techniques

- **Know about Man in the middle attack (MITM)**

A man-in-the-middle attack is a type of eavesdropping attack, where attackers interrupt an existing conversation or data transfer. After inserting themselves in the "middle" of the transfer, the attackers pretend to be both legitimate participants.This type of attack is similar to the game of telephone, where one person's words are carried along from participant to participant until it has changed by the time it reaches the final person. In a man-in-the-middle attack, the middle participant manipulates the conversation unknown to either of the two legitimate participants, acting to retrieve confidential information and otherwise cause damage.

https://whatismyipaddress.com/mac-address

https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/

- ARP Spoofing

ARP poisoning is a type of mitm attack that allows hackers to spy on communications between two parties over a LAN. Here in this project learn how to do ARP spoofing and run the spoofing attack

https://tutorialedge.net/security/arp-spoofing-for-mitm-attack-tutorial/

https://null-byte.wonderhowto.com/how-to/use-ettercap-intercept-passwords-with-arp-spoofing-0191191/

- Caesar Cipher – Encryption/Decryption

This simple mini project on Cybersecurity offers you the opportunity to work on and understand encryption and decryption using Caesar Cipher. You need to follow the simple logic of a numeric cipher value that is used to shift the place values of respective alphabets of a certain text and create the Cipher using a Program across any programming language that can work on the encryption and decryption of the given text.

https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/caesar-cipher

https://searchsecurity.techtarget.com/definition/cipher

https://inventwithpython.com/hacking/chapter7.html

https://medium.com/swlh/breaking-the-code-analysis-of-brute-force-attack-with-code-in-python-6070389449d4

Level 2:

- **Google IT automation with Python**

  Manipulate files and processes on your computer's operating system. Apply automation to manage fleets of computers - How to automate the process for deploying new computers, keeping those machines updated, managing large-scale changes, etc

  https://www.coursera.org/professional-certificates/google-it-automation

Level 3:

You now have the skills required to work on a project of your own. Feel free to use any/all of the skills you have learnt until now.

Assessment:

Level 1:

After completing this level, upload a photograph/video of the functioning circuit or model and show it to your domain co-ordinator.

You are required to provide a detailed report consisting of:

1. Project specifications
2. Challenges faced
3. Documentation Material used
4. What you have learnt

After successfully completing the report, you'll be allowed to move on to level 2

Level 2:

After completing each project, upload a photograph/video of the functioning circuit or model and show it to your coordinator.

When you finish level 2, you are required to provide a detailed report consisting of:

1. Project specifications
2. Challenges faced
3. Documentation (circuits,photographs etc.)
4. Materials used
5. What you have learnt

A date will be fixed on which you give a brief seminar on your report. After successfully completing both the report and seminar, you'll be allowed to move to level 3.

Level 3:

Level 3 assessment will be on a case-by-case basis. Contact your coordinator for more details.

References:

Useful Links:

- https://www.securitymadesimple.org/cybersecurity-blog/can-i-teach-myself-cybersecurity
- https://www.globalknowledge.com/us-en/topics/cybersecurity/glossary-of-terms/#gref
- https://dst.gov.in/interdisciplinary-cyber-physical-systems-icps-division
- https://www.globalknowledge.com/us-en/

Courses:

- https://www.coursera.org/learn/cloud-computing-basics
- https://www.coursera.org/professional-certificates/ibm-full-stack-cloud-developer
- https://www.coursera.org/specializations/microsoft-azure-fundamentals-az-900
- https://www.coursera.org/learn/microsoft-azure-cloud-services
- https://www.cybrary.it/catalog/cybersecurity/security-fundamentals/
- https://www.cybrary.it/catalog/cybersecurity/ethical-hacking/
- https://www.edx.org/course/cyber-security-basics-a-hands-on-approach
- https://www.edx.org/course/building-a-cybersecurity-toolkit
-

Notes:

https://repo.zenk-security.com/Magazine%20E-book/Hacking-%20The%20Art%20of%20Exploitation%20(2nd%20ed.%202008)%20-%20Erickson.pdf

https://www.knowbe4.com/hubfs/Art%20of%20Invisibility_Slides.pdf