QCTaaS (Quality Cloud Teaching as a Service): An Immersive Framework for Teaching Cloud Computing for Cybersecurity Majors

Dr. Mahmoud K Quweider, The University of Texas Rio Grande Valley

M K Quweider is a Professor of Computer and Cybersecurity Sciences at the U. of Texas at UTRGV. He received his Ph.D. in Engineering Science (Multimedia and Imaging Specialty) and B.S. In Electrical Engineering, M.S. in Applied Mathematics, M.S. in Engineering Science, and M.S. in Biomedical Engineering all from the University of Toledo, Ohio. He also holds a Bachelor/Master of English and a Master of Business Administration from the University of Texas at Brownsville. He recently obtained a Master's in Digital Forensics from Champlain College after which he founded the B.Sc. in Cyber Security. After graduation, he was employed at several corporations including Pixera, a digital multimedia processing company in Cupertino, CA, 3COM, a networking and communication company in Schaumberg, IL, and Mercantec, an E-Commerce company in Naperville, IL. He has more than 50 publications in the field and has served as a reviewer and moderator for several scientific and educational journals and conferences. He joined UTB (UTRGV) in the Spring of 2000. His areas of interest include AI/Machine Learning, Networking and Cyber Security, and Digital Imaging.

Dr. Liyu Zhang

Liyu Zhang is an Associate Professor in the Department of Computer Science Department of Computer Science at the University of Texas Rio Grande Valley. He received his Ph. D. in Computer Science from the State University of New York at Buffalo in Septemb

Alexis Aaron De La Cruz

CTaaS (Cloud Teaching as a Service): An Immersive Framework for Teaching Cloud Computing for Cybersecurity Majors

Abstract

Cloud Computing and Cybersecurity are at the heart of our recently created new bachelor-level degree in cybersecurity that addresses the national need for cybersecurity specialists. Cloud Computing involves many service models, including IaaS, PaaS, and SaaS, and many deployment models, including Public, Private, and Hybrid clouds. Within the services and deployment models lie many concepts and practical implementations that a Cyber-analyst needs to master. We have adopted an immersive approach to teaching Cloud Computing services that introduces standard concepts based on clearly defined objectives from national certification authorities such as CompTIA Cloud+, covering all significant services offered by the big three players Amazon (AWS), Google (GCP), and Microsoft (Azure). These services include instances and managed instance groups, storage classes, compute engines, databases, and big data. Theoretical concepts are supplanted with hands-on labs taught by graduate students. In subsequent upper-level courses, students must use some of the services they learned in the upper-level courses to get a real feeling about the setup, operation, monitoring, management, and maintenance of a cloud-based business. This paper covers our academic, hands-on, immersive approach to our newly developed CTaaS framework. In particular, we will present:

- The list of ten teaching modules:
  - Description of each module.
  - The list of objectives and sub-objectives for each module.
  - Topics covered by Cloud+ certification.
- Collaboration with major cloud providers:
  - Acquisition of a small grant for free student credit.
  - Public cloud platforms used in class.
- The list of hands-on labs:
  - Delivery method of each lab
  - Design of lab by instructor/graduate students.
    - Delivery of lab by graduate students.
    - Feedback mechanism.
- Mechanisms for enforcing cloud computing concepts and services:
  - Through projects and assignments.
  - Through targeted upper-level courses.
  - Through individualized capstone projects.
- Resources made available to students:
  - Internal and external.
  - Free and for pay.
- Cloud+ Certification:
  - Institutional resources.
  - Externally funded resources.

By presenting our efforts, we hope that other institutions considering expanding their programs of study to include Cloud Computing, Cyber Security, and Cloud+ Certification can benefit from our experience by adopting best practices while avoiding pitfalls.

Keywords: Cloud Computing, Cyber Security, Pair Teaching, Cloud+, Integrative Lab, Project-based Learning.

Introduction and Motivation

We have recently created a new bachelor's degree in cyber security (BSCS) that is part of a newly created Informatics and Engineering Systems department. Details of the degree are presented in [1] and [2], where we cover the overall objective and learning outcomes, course details, and the degree plan. One new course we offer is Cloud Computing and Security, under the course number CYBI-3346 Cloud Security. The course is considered a junior-level course. The full course description with prerequisites is given in Table 1, while the overall architecture of the course is given in Fig. 1, taken from [1-2].

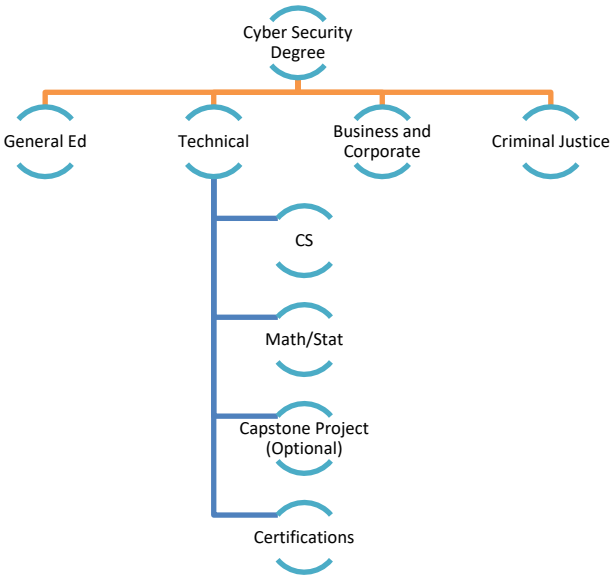


Figure 1. Cyber Security Degree Architecture

Table 1. Course Description	
CYBI-3346: Cloud Security	This course is a top-down, hands-on view of cloud computing, from applications and administration to programming and infrastructure. Topics include clouds, clusters, data centers, grids/P2P, and the Internet of Things (IoT). Specific topics include server clusters, supercomputers, P2P networks, virtual machines, data/computational grids, Internet clouds, IoT, social networks, and big data security. Students will study state-of-the-art solutions for cloud computing developed by current leading companies. Prerequisite: Pre- or co-requisite in CYBI 3335 (*Data Communications & Networking*).

The course was offered for the first time in 2021, and the authors were tasked with teaching the course and establishing a framework for future instructors to follow. As this is a non-engineering course and the degree under which the course falls is geared toward graduating cybersecurity analysts, we decided to create a customized course for our students and our degree. What follows are the course module's design details, the associated labs, and the resources dedicated to the course.

Course Design

Cloud Computing has emerged as the dominant computing model of the 21st century due to its utility. This metered model replaces the on-premises capital expenditure with the less expensive on-demand operational expenditure. The NIST (The National Institute of Standards and Technology) defines Cloud Computing [4], as a model for enabling ubiquitous, convenient, on-demand network access to shared pools of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud Computing has the following five characteristics that distinguish it from on-premises computing [5]. 1) On-Demand Self-Service; 2) Broad Network Access; 3) Resource Pooling; 4) Rapid Elasticity; 5) Measured Service. It is essential for students to know and appreciate these characteristics as they transition toward corporate culture by the time they graduate. So, an important objective of our course is to amply illustrate the qualities of Cloud Computing in the Cloud Computing course and other courses that can simulate the need for such characteristics, such as in E-commerce, Databases, Artificial Intelligence, and Machine Learning.

Cloud Computing is not monolithic, and it comes in many service models. However, the three service models that every student should know about are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). They constitute the foundation for the endless combinations we see budding in every field, such as media and communication (Communication as a Service), Storage (Storage as a Service), and ransomware (Ransomware as a Service), to mention a few. Fig. 3 shows the three models along with the legacy on-site model. The green color shows the layers the customer controls, while the red shows the ones under the provider's control.

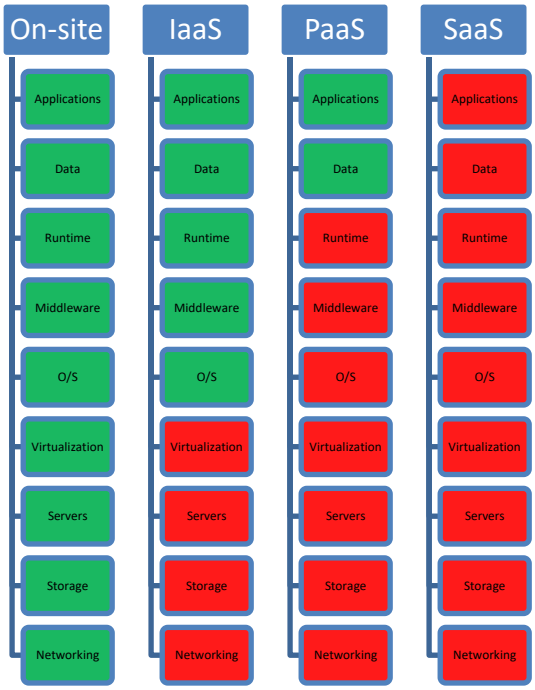


Figure 2. Cloud Service Models

CTaaS

Approaching the teaching of the course holistically, we created a CTaaS (Cloud Teaching as a Service) teaching framework. CTaaS is a comprehensive framework that addresses the academic goals and objectives of the course, allows the students to practice with hands-on modules, and prepares the students for the much sought-after national certifications. CTaaS stack is shown in Fig 3. It consists of the following layers/sublayers, which we will discuss in detail.

1. **Pedagogy Components:**
    a. Cloud Computing
        i. Theory & Concepts
        ii. Lab Modules
        iii. Assessment
        iv. Q/A Sessions
2. **Platform Support:**
    a. Primary: GCP (Google Gloud Platform)
    b. Secondary: AWS, Azure
3. **Degree Support Courses:**
    a. Electives: AI/ML
    b. Required: Capstone Project
4. **Job Support Certifications:**
    a. Primary: Cloud+ and GCP/AWS/Azure
    b. Secondary: Linux+

We designed the CTaaS framework as a seamlessly integrated system where components complement each other without requiring any extra effort beyond what is required by the cybersecurity degree. In the following, we go over CTaaS's details.

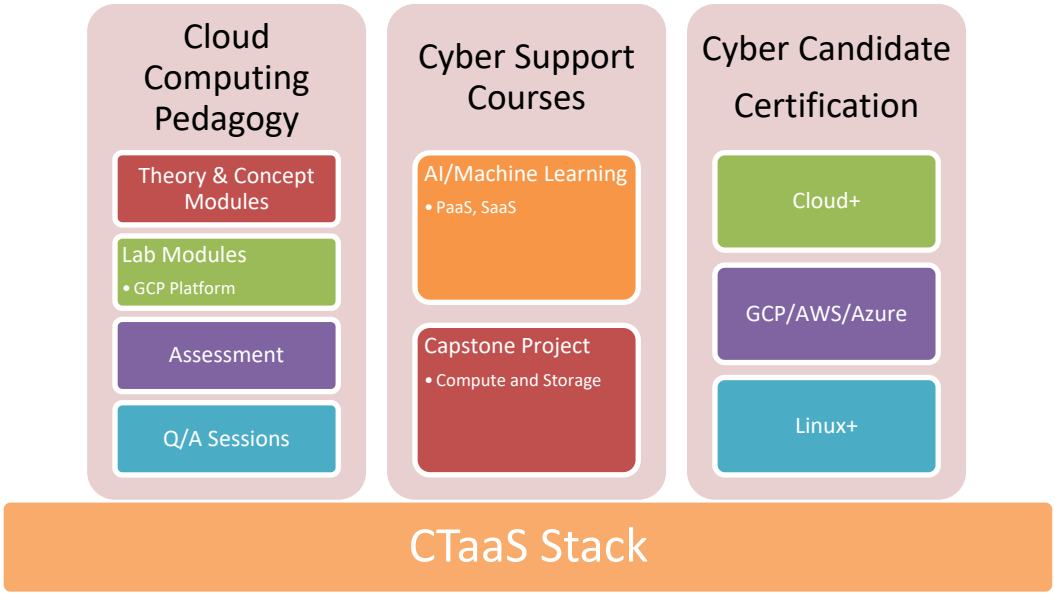


Figure 3. CTaaS Architecture

CTaaS Pedagogy Components

CTaaS Pedagogy Components cover theory/concepts, lab modules, assessments, and Q&A sessions.

Theory/Concepts Modules

We created the theory/concepts teaching modules specifically for the course. They cover various topics that interest the job market and enterprises deploying or migrating their business to the cloud. The following is a summary of each module. Appendix A gives a summary of all teaching modules.

1. **Cloud Computing Fundamentals**
   Module 1 introduces the topic of cloud computing and the evolution of computing in general.
2. **Cloud Computing Service Models**
   Module 2 introduces the CC Stack and the IaaS, PaaS, and SaaS service models. It also introduces public, private, and hybrid computing with examples.
3. **Cloud Computing Storage**
   Module 3 discusses the IaaS Storage infrastructure. It introduces the main types of storage in the cloud: Block storage, Object/file storage, and Filesystem storage.
4. **Cloud Computing Networking**
   Module 4 discusses IaaS Network Virtualization. It introduces L2 and L3 NV methods. It also introduces Inlay and Overlay Tunnels, VXLANs, VPNs, and Firewalls. CLOS topology is also introduced in detail.
5. **Cloud Computing Virtualization**
   Module 5 discusses Virtualization techniques. It introduces Type 1 (hardware or bare metal) and Type 2 (hosted) virtualizations. It also introduces Full virtualization with binary translation, OS-assisted Paravirtualization, and Hardware-assisted virtualization.
6. **Cloud Computing Data Centers**
   Module 6 discusses Data Centers. It introduces types of data centers. It also introduces all components in the data center and the ANSI/TIA-942: Infrastructure Standard for Data Centers virtualization.
7. **Cloud Computing Identity & Account Management**
   Modules 7 discusses IAM. It introduces policies and roles.
8. **Cloud Computing Identity & Account Management**
   Modules 8 discusses IAM. It introduces security, monitoring, and accounting.

Hands-on Lab Modules Description

There is almost one-to-one correspondence between each teaching module and the accompanied lab module. specifically for the course. The labs were created by the instructor of record but were delivered by the graduate teaching assistant. The graduate students who teach the labs are usually students who have taken a graduate version of the Cloud Computing course in the master's program. Following in Table 2. is a summary of each lab module.

Table 2. Hands-on Lab Modules Summary

Lab Module	Description

Hands-on Lab 01: Introduction and VM Instances	In this lab, you will learn how to create a VM instance with a set of configurations related to CPUs/GPUs, Memory, Storage, Type of OS, and default Networking.
Hands-on Lab 02: VM Templates and MIGs	In this lab, you will learn how to create a VM template and create a VM based on such templates. You will also understand Managed instant groups and how to create them.
Hands-on Lab 03: VM Desktop Creation	In this lab, you will learn how to create an Ubuntu VM graphic interface for your virtual desktop on the GCP cloud
Hands-on Lab 04: Bucket Storage in the GCP	In this lab, you will learn how to create Cloud Storage buckets and be able to manage and configure them. This includes uploading, listing, moving, and deleting buckets in a project.
Hands-on Lab 05: Key Management Systems	In this lab, you will learn how to create Key rings and Keys to use for encrypting and decrypting different types of storage.
Hands-on Lab 06: VM Creation and Sharing File Systems with File Store	In this lab, you will create and set up an NFS File System using the File Store service for sharing your files with others in the Google Cloud Platform.
Hands-on Lab 07: GCloud CLI Commands	In this lab, you will practice using the GCloud CLI to create VMs, Templates, MIGs, Buckets, and NFS sharing.
Hands-on Lab 08: Networking with VPC and Peering	In this lab, you will create a VPC network next to the default network in your account. You will also create two peering VPC network connections.
Hands-on Lab 09: Networking with VPNs	In this lab, you will create a Cloud VPN that securely connects your peer network to your Virtual Private Cloud (VPC) network through an IPsec VPN connection.
Hands-on Lab 10: IAM, Identity & Access Management	In this lab, you will get familiar with Cloud IAM to define who has what access to which resource on the Google Cloud. You will also experiment with fine-grained access control and visibility for

Platform Support

GCP and other providers

The major public cloud platforms are Amazon Web Services (AWS), Google Cloud Platform, and Microsoft Azure. They all offer some free trial services that students can benefit from. For teaching and academic purposes, we got small grants in the form of free vouchers ranging from $50-$100 for graduate and undergraduate students. The credits are usually valid for more than 90 days, and it saves the students from entering their credit cards, which might be a concern for some students. We have also complemented GCP vouchers with the university's contracted OneDrive, so students can always move large amounts of data between the two platforms. Part of CTaaS's goals is to make the cloud a normal development environment for students before they graduate. So as the modules and labs were taught to the students, students were encouraged to

apply the service models in their other courses. A more systematic way to apply the concepts and services is described later on.

Degree Support Courses

The virtual nature of Cloud Computing allows students access to numerous resources and services, too many to master in one class. Therefore, part of the CTaaS objective is to continue Cloud Computing education beyond the main course and into other courses and projects in the degree.
We have identified two initial courses where students can benefit immensely from the Cloud Computing environments. One class is a resource-intensive course in Machine Learning, and the other is a Capstone project required for graduation. Both courses are geared toward exploring the nature of data as it relates to cyber security The two courses are usually done in groups and require a considerable amount of computing and storage, which are perfect for the metered utility nature of the Cloud.

Job Support Certifications

Our Cyber Security degree requires two vendor-neutral certifications, and although we focus on Network+ and Security+, the degree allows for any other certification the student is interested in. As explained in [3], we focus on vendor-neutral or vendor-agnostic certifications because they emphasize the main concepts and general approaches used in a given field or technology. They highlight best practices and mastery of different technologies without being tied to a specific one. They provide a perfect fit for our graduating students in the CS program, presenting them as highly employable and more adaptable across a wide range of companies.

Due to the nature of Cloud Computing and its heavy use of command line interface and scripting, many of the teaching modules, as well as the lab modules, were designed with Cloud+ and Linux+, both of which are considered Infrastructure certifications.
The details of the Cloud+ and Linux+ are taken from [6-8].

Table 3. Cloud Computing Support Certifications

Certificate Name	• CompTIA Cloud+ • CompTIA Linux+

Cloud+:
CompTIA Cloud+ is a global certification that validates the skills needed to deploy and automate secure cloud environments that support the high availability of business systems and data.

Skill Set

- Attacks, Threats, and Vulnerabilities: Focusing on more threats, attacks, and vulnerabilities on the Internet from newer custom devices that must be mitigated, such as IoT and embedded devices, newer DDoS attacks, and social engineering attacks based on current events.
- Cloud Architecture & Design: Analyze the different cloud models to design the best solution to support business requirements.
- Cloud Security: Manage and maintain servers, including OS configurations, access control, and virtualization.

- Cloud Deployment: Analyze system requirements to successfully execute workload migrations to the cloud.
- Operations & Support: Maintain and optimize cloud environments, including proper automation and orchestration procedures, backup and restore operations, and disaster recovery tasks.
- Troubleshooting: Troubleshoot capacity, automation, connectivity, and security issues related to cloud implementations.

Linux+:

CompTIA Linux+ validates the skills administrators need to secure the enterprise, power the cloud and keep systems running.

Skill Set

- System Management: Configure and manage software, storage and process and services.
- Security: Understand best practices for permissions and authentication, firewalls, and file management.
- Scripting, Containers & Automation: Create simple shell scripts and execute basic BASH scripts, version control using Git, and orchestration processes.
- Troubleshooting: Analyze system properties and processes and troubleshoot user, application, and hardware issues

Discussion

Teaching Cloud Computing for Cyber Security majors proves to be challenging but rewarding. The framework we present provides a holistic approach that goes beyond the classroom and ensures that skills acquired in the course are applied in other courses and stay relevant to industry standards and certifications. The reinforcement of concepts and applications of services in senior-level courses allowed the students to build prototypes of what a service such as IaaS or PaaS would entail in the real world. The students acquire technical skills and master the much-needed soft skills such as team formation, project monitoring and evaluation, and project and account management, among many others.

By allowing graduate TAs to deliver the hands-on modules, our students were very responsive and interactive with the instructor. The discussion sessions conducted using Zoom allowed students to catch up on any issues that arose during the labs. Sometimes, the TA created extra hands-on when students were not clear on some of the concepts the professor covered in class. Feedback from course evaluation was positive overall, and many liked the course split between theory and practice, between professor of instruction and lab TAs. We are currently collecting data from the course evaluations, and we hope to analyze the data and present the results in future work.

Conclusions and Future Work

This paper presented a comprehensive framework for teaching cloud computing in higher education. The framework forces the student to use the Cloud throughout his academic career in such a way that prepares him for certification as well as entry to mid-level jobs in the industry. The hands-on lab modules are delivered to students by students, which encourages students to be interactive and responsive. Outside the class, Q&A sessions allowed students to research any issues and catch up with the rest of the class. Students who are motivated to be certified beyond the minimum requirements of the degree have the chance to do so. By incorporating the Cloud+

goals and objectives in the course, students are ready to take the certification. While the hands-on labs were built specifically for GCP, future improvements for the course include adding modules for the three major providers and allowing the student to select his/her platform of choice.

Acknowledgment
Special thanks to the Department of Informatics and Engineering Systems (IES) for supporting Alexis De La Cruz, who conducted the Cloud Computing and Security Labs for the class.

References

1. Quweider, MK, et al., (2022, August), *Crafting a Degree, Empowering Students, Securing a Nation: The Creation of a Modern Cyber Security Degree for the 21st Century*. Paper presented at 2022 ASEE Annual Conference & Exposition, Minneapolis, Minnesota. https://peer.asee.org/41292
2. Quweider, MK, et al., (2023, July), *Early Integrating of Industry Certification Domains and Objectives into a Modern Cybersecurity Degree Curriculum.* Paper presented at 2023 ASEE Annual Conference & Exposition, Baltimore, Maryland. https://nemo.asee.org/public/conferences/327/papers/37056/view
3. Baharuddin, Ampera, D., Fibriasari, H., Sembiring, M. A. R., & Hamid, A. (2021). Implementation of cloud computing system in learning system development in engineering education study program. International Journal of Education in Mathematics, Science, and Technology (IJEMST), 9(4), 728-740. https://doi.org/10.46328/ijemst.2114
4. Mell, P., & Grance. P. (2011). The NIST Definition of Cloud Computing. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930. http://csrc.nist.gov/publications/nistpubs/800-145/ Special Publication 800-145
5. https://www.synopsys.com/cloud/insights/essential-cloud-computing-characteristics.html#:~:text=The%20National%20Institute%20of%20Standards,rapid%20elasticity%2C%20and%20measured%20service.
6. https://www.comptia.org/about-us
7. https://www.utrgv.edu/cyberspace/academics/index.htm.
8. Ahmad, A. (2016, June), *Articulation of Certification for Manufacturing* Paper presented at 2016 ASEE Annual Conference & Exposition, New Orleans, Louisiana. 10.18260/p.26278

Appendix A: CTaaS Teaching Modules Description

Module 01 (Summary & Resources)

Cloud Computing & Security	CYBI- 3346 Fall 2023
Module 1 Summary	
Summary:	*What is Cloud Computing* Module 1 introduces the topic of cloud computing and the evolution of computing in general.
Readings/ Watching:	Module 01 Slides. Video Lecture.
Resources:	• Module 01 Notes [Power Point Slides] • Video Lecture.
Deliverables/ Assignments:	1. Description: Lab Module 01. Getting your GCP Account Activated. 2. Participate in the discussion Q/A session with your TA

Module 02 (Summary & Resources)

Cloud Computing & Security	CYBI- 3346 Fall 2023
Module 2 Summary	
Summary:	*CC Service Models* Module 2 introduces the CC Stack and the IaaS, PaaS, and SaaS service models. It also introduces public, private, and hybrid computing with examples.
Readings/ Watching:	Module 02 Slides. Video Lecture.
Resources:	• Module 02 Notes [Power Point Slides] • Video Lecture.
Deliverables/ Assignments:	1. Description: Lab Module 02. GCP overview and Compute Engine. 2. Participate in the discussion Q/A session with your TA

Module 03 (Summary & Resources)

Cloud Computing & Security	CYBI- 3346 Fall 2023

Module 3 Summary

Summary:	*CC IaaS: Storage* Module 3 discusses the IaaS Storage infrastructure. It introduces the main types of storage in the cloud: Block storage, Object/file storage, and Filesystem storage.
Readings/ Watching:	Module 03 Slides. Video Lecture.
Resources:	• Module 03 Notes [Power Point Slides] • Video Lecture.
Deliverables/ Assignments:	1. Description: Lab Module 03. GCP Compute Engine VMs. 2. Participate in the discussion Q/A session with your TA

Module 04 (Summary & Resources)

Cloud Computing & Security	CYBI- 3346 Fall 2023

Module 4 Summary

Summary:	*CC IaaS: Networking* Module 4 discusses IaaS Network Virtualization. It introduces L2 and L3 NV methods. It also introduces Inlay and Overlay Tunnels, VXLANs, VPNs, and Firewalls. CLOS topology is also introduced in detail.
Readings/ Watching:	Module 04 Slides. Video Lecture.
Resources:	• Module 04 Notes [Power Point Slides] • Video Lecture.
Deliverables/ Assignments:	1. Description: Lab Module 04. GCP VM Templates and MIGs. 2. Participate in the discussion Q/A session with your TA

Module 05 (Summary & Resources)

Cloud Computing & Security	CYBI- 3346 Fall 2023

Module 5 Summary

Summary:	*CC IaaS: Virtualization Techniques* Module 5 discusses Virtualization techniques. It introduces Type 1 (hardware or bare metal) and Type 2 (hosted) virtualizations. It also introduces Full virtualization with binary translation, OS-assisted Paravirtualization, and Hardware-assisted virtualization.
Readings/ Watching:	Module 05 Slides. Video Lecture.
Resources:	• Module 05 Notes [Power Point Slides] • Video Lecture.
Deliverables/ Assignments:	1. Description: Lab Module 05. GCP Storage with Buckets. 2. Description: Lab Module 06. GCP Storage File Store and NFS. **3.** Participate in the discussion Q/A session with your TA

Module 06 (Summary & Resources)

Cloud Computing & Security	CYBI- 3346 Fall 2023

Module 6 Summary

Summary:	*CC IaaS: Data Centers* Module 6 discusses Data Centers. It introduces types of data centers. It also introduces all components in the data center as well as the **ANSI/TIA-942**: Infrastructure Standard for Data Centers virtualization.
Readings/ Watching:	Module 06 Slides. Video Lecture.
Resources:	• Module 06 Notes [Power Point Slides] • Video Lecture.
Deliverables/ Assignments:	1. Description: Lab Module 07. GCP GCloud CLI Commands. 2. Description: Lab Module 08. GCP VPC and peering. **3.** Participate in the discussion Q/A session with your TA.

Module 07 (Summary & Resources)

Cloud Computing & Security	CYBI- 3346 Fall 2023
Module 7 Summary	
Summary:	*CC IaaS: Identity and Access Management (IAM)* Module 7 discusses IAM. It introduces policies, security, and roles.
Readings/ Watching:	Module 07 Slides. Video Lecture.
Resources:	• Module 07 Notes [Power Point Slides] • Video Lecture.
Deliverables/ Assignments:	1. Description: Lab Module 09. GCP VPN. 2. Participate in the discussion Q/A session with your TA

Module 08 (Summary & Resources)

Cloud Computing & Security	CYBI- 3346 Fall 2023
Module 8 Summary	
Summary:	*CC IaaS: Identity and Access Management (IAM)--continued* Module 8 continues IAM, including policies, security, and roles.
Readings/ Watching:	Module 08 Slides. Video Lecture.
Resources:	• Module 08 Notes [Power Point Slides] • Video Lecture.
Deliverables/ Assignments:	1. Description: Lab Module 10. IAM Policy and Roles. 2. Participate in the discussion Q/A session with your TA

Appendix B: Sample Hand-on Lab Lecture *(Prepared for TA Presentation)*
CYBI-3346 Cloud Security
1st 8 slides of 43

1

Google Cloud Platform

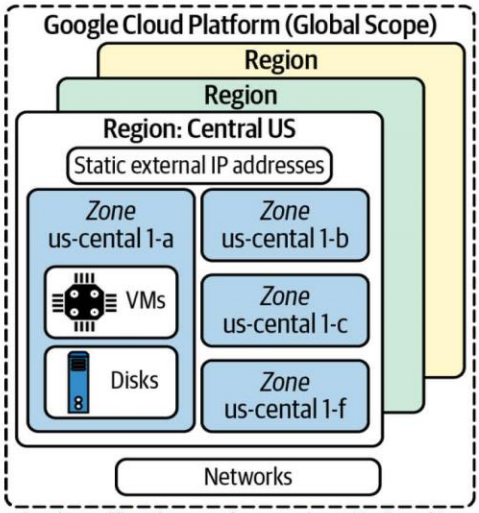
HANDS-ON MODULES:
INTRO TO GCP / VM INSTANCES

2

Google Cloud Overview

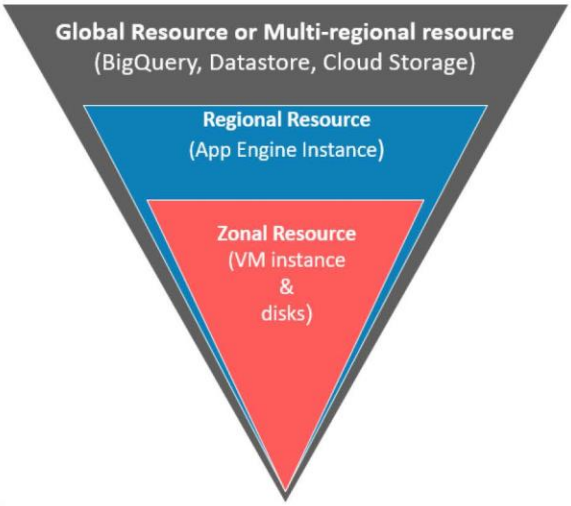
Google Cloud is a collection of physical resources such as servers and storage as well as higher-level services like BigQuery or AppEngine built on top of them, all running in Google data centers.

- The platform is organized into zones, regions, multi-regions (continents), and then the entire globe
  - **Zone**: A large cluster of compute in one or several data center buildings. Should be considered a single failure domain
  - **Region**: A cluster of data center buildings (campus). Made of multiple zones. Each zone is generally on a different power and network infrastructure and on a different upgrade schedule. Regional services will be served out of multiple zones or automatically fail over in the case of a zonal outage.
  - **Multi-region**: A group of regions generally on the same continent. Multiregional services will be served out of multiple regions and handle a regional failure.
  - **Globe**: A service deployed across Google Cloud regions around the globe.



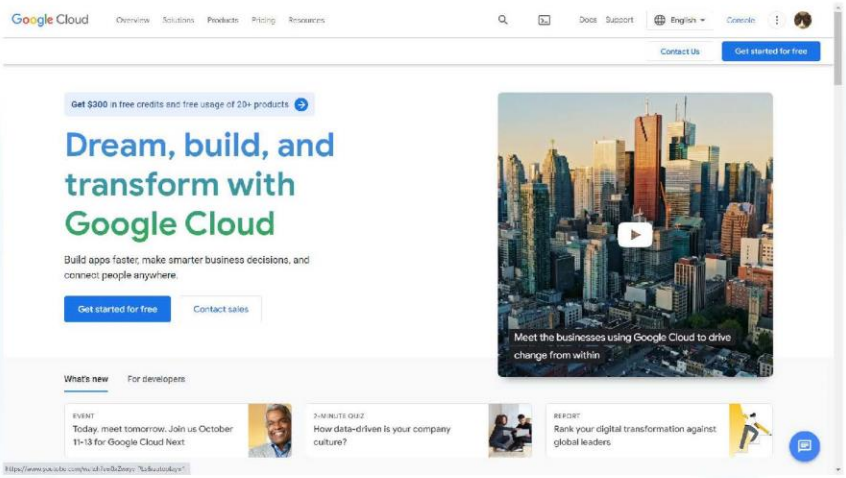
Different services have different scopes; for example, a virtual machine (VM) lives in a zone, whereas an L7 network load balancer exists globally

Google Cloud Overview



Creating an Account

- Go to https://cloud.google.com/



Creating an Account (UTRGV)

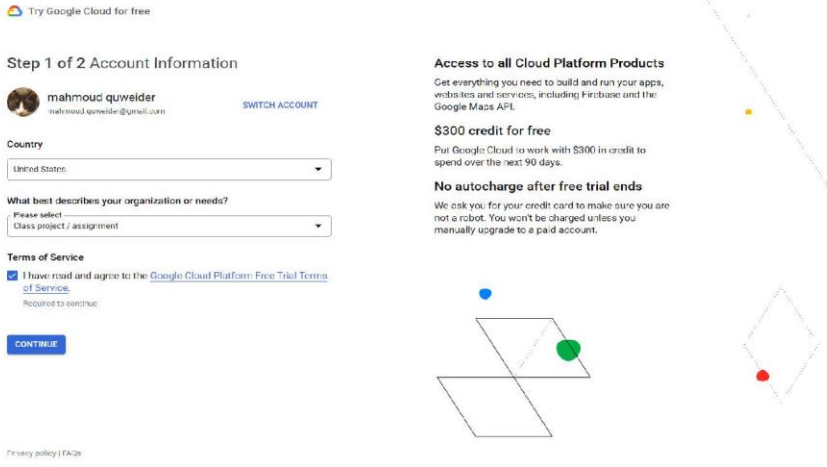
- Class notes have instructions on how to claim the 50$ credit Dr. Q. applied for for the students.
  - Verify your email & get your voucher
  - Make sure your billing is linked to the Educational Account
- The TA can help you if you have any issues.

Creating an Account (Personal)

- Go to https://cloud.google.com/
- Have your own personal ***Gmail Account***
  - Here, we'll set up an empty Google Cloud project and get $300 in free credits

Creating an Account

- Click Get Started for Free. Fill the form



Appendix C: Sample Hand-on Lab (edited for formatting)

CYBI-3346 Cloud Security: Lab-001

Individual Work

Take a screenshot after each step you perform and add it to this document as your report.

I. You are asked to create a ***single VM machine*** with the following specifications:

a. Machine name (instance name): utrgv-cybersecurity-lab-01-yourlastname

b. CPU family: E2; number of CPU: 2vCPU ; RAM:4 GB

c. Use default region and zone:

d. Add the following labels for metadata and indexing/searching.
lead: yourlastname-firstname
project: cccloud2022

e. OS: Debian GNU/Linux 11 (bullseye)with 20 GB storage (increase the default value by another 10 GB)

f. Startup bash script as follows:

```
#! /bin/bash
sudo su
apt update
apt -y install apache2
sudo service apache2 start
sudo update-rc.d apache2 enable
echo "Hello World" > /var/www/html/index.html
echo "Hello From your-firstname world from $(hostname) $(hostname -I)" >
/var/www/html/index.html
```

g. Allow HTTP traffic.

h. Note the IP addresses and write them down:

- Internal IP address:_____
- External IP address:_____

i. Test that the external IP address shows a static web page installed during the start of the machine.
Take screenshot.

j. Show that you can SSH into the VM

k. Install the following software on the VM machine. Use sudo if you need to.

- SW1: Tree and display the top level (/) of your machine.

l. After you are done and have all the screenshots, show the instructor the machine before cleaning up.

- Stop your machine and delete it before moving to the next task.