

# The Relevance of Cloud Computing for Cybersecurity Education

*Miguel A. Rodriguez Delgado*  
Polytechnic University of Puerto Rico  
[mianrodel27@gmail.com](mailto:mianrodel27@gmail.com)

*Xaymarie N. Garcia Collazo*  
Polytechnic University of Puerto Rico  
[xaymariegar@gmail.com](mailto:xaymariegar@gmail.com)

## Abstract

Cloud computing has revolutionized data management, access, and storage. Cloud computing has grown over the past ten years because it provides scalable and affordable solutions, especially advantageous for small and medium-sized businesses (SMEs). The shift to cloud environments brings cybersecurity flaws, which calls for discovering and blocking fresh attack avenues. In response to these issues, this paper suggests creating two specialist courses centered on cloud architecture and security based on the Cloud Security Alliance Crucial Domains. These courses aim to provide graduates with the knowledge and abilities to comprehend and tackle cybersecurity threats unique to cloud systems. Through the provision of focused instruction in this crucial domain, educational establishments can enhance the readiness of their graduates to make valuable contributions towards a more secure and protected digital environment.

**Key Terms:** Cloud Computing, Distributed Computing, Cloud Vulnerabilities, CSA Cloud Security Domains, Cloud Computing Course, Cloud Risk Management, Cloud Environment Assessments.

## Introduction

Cloud computing is a paradigm that facilitates universal, user-friendly, and instant access to a communal reservoir of adaptable computing assets (such as networks, servers, storage, applications, and services) via the Internet. These resources can be swiftly allocated and relinquished with little administrative overhead or necessary for direct service providers' engagement (Mell & Grance, 2011). It has drastically changed how we store, access, and manage data. The field of cloud computing has experienced significant growth over the last decade (Alhebaishi et al., 2017), and it is easy to see why. These solutions offer elasticity (Mousavi et al., 2017) to businesses by allowing them to scale up or down depending on the demand. By only paying for the resources consumed, small to medium-sized enterprises are not left to maintain systems that are not currently active. Due to these benefits, SMEs have rapidly embraced its adoption (Islam et al., 2013).

Cybersecurity vulnerabilities are always present and eliminating them is a virtual impossibility. The migration to cloud computing environments brings nuance to these issues. Based on a literature review from (Guanco, Lehnert & Lumpe, 2023), these attack vectors include:

- **Exploitable Workloads:** Exploitable workloads refer to any virtual machine or container accessible to an internal or external attacker due to misconfiguration of the cloud networks.
- **Unsecured Encryption:** This attack vector shows cleartext or unprotected credentials on a cloud workload, service, or code repository.
- **Exploitable IAM:** This attack vector details an entity's improper management and authentication, such as user, workload, function, role, group, etc.




- **Third-Party Cross-Environment/Account Access:** This attack vector details the trust of a third-party entity or resource to access the customer’s cloud environment.

Table 1 shows an important consideration when implementing a cloud environment: understanding the shared responsibility model related to each implementation (National Cyber Security Centre, 2022). The National Institute of Standards and Technology (NIST) recognized three main cloud models in the NIST SP 800-145 (Mell & Grance, 2011): Software as a Service, Platform as a Service, and Infrastructure as a Service. According to NIST, the user does not manage infrastructure or underlying application capabilities in SaaS. In a PaaS, the user does not control the underlying infrastructure but does control the applications and some configuration settings. In an IaaS model, the user does not control the underlying infrastructure but does have control over operating systems, applications, and settings.

**TABLE 1:** Cloud Environment Responsibility Testing

	on premise	IaaS	PaaS	SaaS
Application configuration	Customer is predominantly responsible for security	Customer is predominantly responsible for security	Customer is predominantly responsible for security	Customer is predominantly responsible for security
Identity & access controls	Customer is predominantly responsible for security	Customer is predominantly responsible for security	Both customer and cloud service have security responsibilities	Both customer and cloud service have security responsibilities
Application data storage	Customer is predominantly responsible for security	Customer is predominantly responsible for security	Both customer and cloud service have security responsibilities	Cloud service is fully responsible for security
Application	Customer is predominantly responsible for security	Customer is predominantly responsible for security	Customer is predominantly responsible for security	Cloud service is fully responsible for security
Operating system	Customer is predominantly responsible for security	Customer is predominantly responsible for security	Cloud service is fully responsible for security	Cloud service is fully responsible for security
Network flow controls	Customer is predominantly responsible for security	Both customer and cloud service have security responsibilities	Cloud service is fully responsible for security	Cloud service is fully responsible for security
Host infrastructure	Customer is predominantly responsible for security	Cloud service is fully responsible for security	Cloud service is fully responsible for security	Cloud service is fully responsible for security
Physical security	Customer is predominantly responsible for security	Cloud service is fully responsible for security	Cloud service is fully responsible for security	Cloud service is fully responsible for security

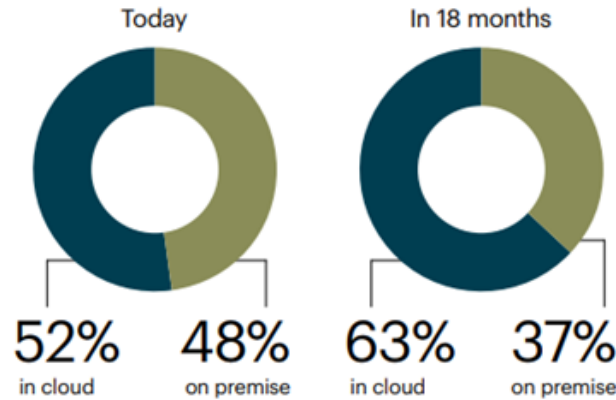
	Customer is predominantly responsible for security
	Both customer and cloud service have security responsibilities
	Cloud service is fully responsible for security

### Cloud Expansion and its Consequences

More and more public and private organizations have decided to migrate their services to the cloud due to operational cost reasons, scalability, and availability benefits. Foundry's 2023 Cloud Computing Survey polled 893 IT decision-makers involved in the cloud service adoption process and found that most of them either have or plan to have at least one application or part of their infrastructure in the cloud. Fifty-seven percent (57%) of the respondents have increased their cloud migration in the last 12 months (Foundry, 2023).

Figure 1 shows the distribution of in-cloud IT environment resources is fifty-two percent (52%), compared to forty-eight percent (48%) on-premises, and will continue skewing towards cloud environments by an additional eleven percent (11%) within 18 months (Foundry, 2023).

**Majority of IT environments in the cloud**



**Figure 1:** Majority of IT environments in the cloud.

Unfortunately, with the increased adoption of cloud services, various challenges have emerged, requiring more skilled workers to mitigate the threats to business performance. According to a survey conducted by 451's Macro Economic Outlook, 51% of respondents stated that it has been challenging to hire new employees or rehire suspended employees in the last 12 months (Forrest & Posey, 2023).

Figure 2 shows the results of a survey conducted by Voice of the Enterprise, Cloud Skills 2022, where 44% of respondents identify "difficulty finding qualified candidates to bring in as new hires" as the main challenge in addressing cloud skills gaps (Forrest & Posey, 2023).



**Figure 2:** Cloud Skill Gaps

The risks and security threats increase as organizations move their services to the cloud. It becomes even more challenging when IT personnel lack expertise in the cloud to design a robust security strategy. According to a study conducted by the Thales Global Security Study 2023, where they surveyed 3,000 IT and security professionals across 18 countries, one-third (38%) of organizations experienced a data breach in the cloud environment in 2023, which is an increase compared to the 35% reported for 2022. Human error is the primary cause of cloud data breaches, listed by more than half of the respondents (55%) (Thales

Group, 2023). Human errors lead to misconfigurations, and this becomes an issue when, every year, cloud providers add more services, each with different configurations and implementations (Puzas, 2024).

The Cloud Security Alliance provides a frame of reference for several domains that can be used as a guideline to educate cloud cybersecurity professionals. According to the CSA, several critical domains exist for properly implementing and maintaining cloud environments. These include Cloud Computing Concepts and Architectures, Governance and Enterprise Risk Management, Legal Issues, Contracts and Electronic Discovery, Compliance and Audit Management, Information Governance, Management Plane and Business Continuity, Infrastructure Security, Virtualization and Containers, Incident Response, Application Security, Data Security and Encryption, Identity, Entitlement and Access Management, Security as a Service, and Related Cloud Technologies (Mogul et al., 2017). With so many domains available within cloud security, it's natural to wonder how recent graduates are expected to interact with this complex environment. To nurture a more robust cybersecurity workforce, we propose an outline for two courses centered around cloud computing domains, with the expectation that well-prepared graduates can create a safer online environment.

## Objective Outline

These courses aim to give students a thorough grasp of cloud computing security in all areas suggested by the Cloud Security Alliance (CSA). Students will gain the knowledge and skills to ensure cloud-based systems and services' security, compliance, and resilience.

Prerequisites include:

- Basic understanding of Security concepts (CIA, Risk Management, IT infrastructure, Business Continuity, etc.)
- Basic understanding of networks (VPN, Protocols, Network Topology, Network Devices, etc.)

Outlining a specific course framework will rely on sources, Purpose, Targeted learning or competencies, and Intention (Travers et al., 2019). Educational frameworks are essential and varied; selecting one based on analyzing needs using the four factors mentioned will yield the best results. Work-based learning is an instructional strategy that enhances learning by connecting it to the workplace (The U.S. Department of Education, 2017). A well-designed WBL comprises three key components: the alignment of classroom and workplace learning, the application of academic, technical, and employability skills in a work setting, and support from classroom or workplace mentors (The U.S. Department of Education, 2017). This model would provide students with academic, real-world experience and access to industry professionals.

## Course Outline

This proposal consists of two courses covering the previously discussed objectives.

These are:

- **Cloud Architecture and Implementation**
- **Safe Cloud Management.**

The student is expected to have met the basic requirements mentioned in the previous section, have foundational knowledge of security-related topics, and be familiar with networks, including architecture and protocols. Once the student meets the requirements, they can take the course to learn to apply these foundational concepts in cloud computing.

## ***Cloud Architecture and Implementation***

In this course, students will work with the practical application of foundational network knowledge within cloud computing. The CSA critical domains guide the topics proposed in each module and the content is based on reading material references from various books and publications. Each module's contents were expanded using the book *Cloud Computing: Concepts, Technology & Architecture* (Mahmood & Erl, 2013). This book covers all topics discussed in this course and provides depth to the proposed modules. Table 2 shows each module's title, briefly describing the objectives. This course is divided into 12 modules, each building the foundation of the next section. This course aims to provide an overview of cloud computing,

introducing key concepts and terminologies. After establishing a clear baseline, the course moves into topics related to specific implementations, such as cloud service and deployment models. After this primer, students can move on to more hands-on technical topics, such as cloud architecture fundamentals, where they will cover the general principles of designing reliable cloud systems.

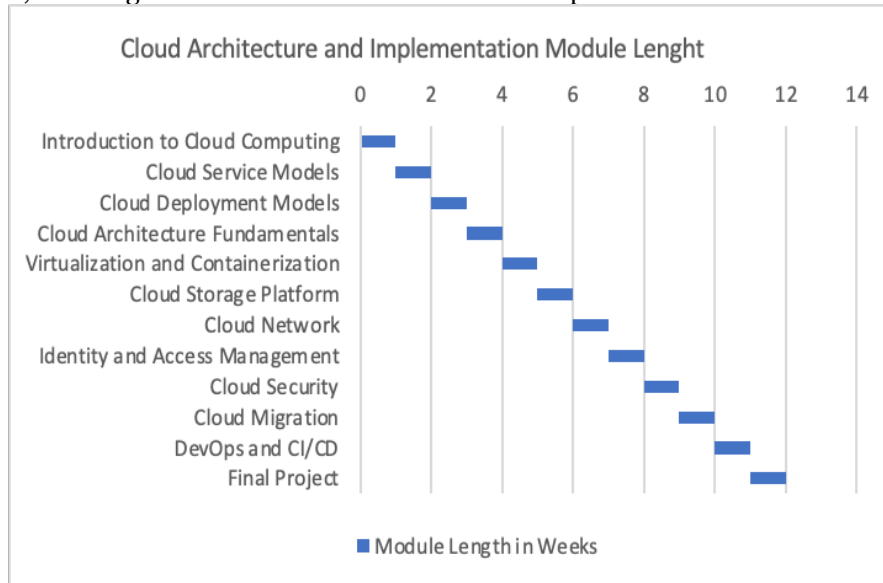
Virtualizations and Containerization are separated into their module due to the importance of resource management in a cloud environment. Continuing with topics related to resource management, the course covers cloud storage solutions and the scalability considerations required by each. The prerequisite knowledge of networks comes into play when covering cloud networks; this includes topics such as VPN, Subnets, etc. Identity and Access Management to ensure students can apply authentication, authorization, and auditing. The final three modules of the course cover topics directly related to cloud security, such as the considerations required for cloud migration and DevOps principles. Finally, students must submit a final project reflecting their acquired skills and knowledge.

**Table 2:** Cloud Architecture Implementation Course Module Description

Cloud Architecture and Implementation	
Modules	Description
<b>Introduction to Cloud Computing</b>	This module provides an overview of cloud computing, introducing fundamental concepts, key terminology, and the benefits of cloud technology.
<b>Cloud Service Models</b>	Explore the various service models in cloud computing, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).
<b>Cloud Deployment Models</b>	Understand different cloud deployment models such as Public Cloud, Private Cloud, Hybrid Cloud, and Multi-Cloud, examining their characteristics and use cases.
<b>Cloud Architecture Fundamentals</b>	Delve into the basics of cloud architecture, covering design principles, components, and considerations for building scalable and reliable cloud systems.
<b>Virtualization and Containerization</b>	Explore virtualization technologies and containerization, understanding how they optimize resource utilization and simplify application deployment.
<b>Cloud Storage Platform</b>	Learn about cloud storage solutions, including types of storage, scalability considerations, and the use of cloud storage platforms for data management.
<b>Cloud Network</b>	Examine networking in the cloud, covering topics such as virtual networks, subnets, load balancing, and security measures for cloud-based applications.
<b>Identity and Access Management (IAM)</b>	Understand IAM principles in the cloud, focusing on user authentication, authorization, and the implementation of secure access controls.
<b>Cloud Security</b>	Explore principles and best practices for ensuring security in the cloud, including data encryption, threat detection, and compliance with security standards.
<b>Cloud Migration</b>	Learn strategies and considerations for migrating applications and data to the cloud, including assessment, planning, and execution of migration projects.
<b>Cloud-native DevOps and Automated Deployment Practices</b>	Explore the integration of DevOps principles with cloud-native practices, emphasizing continuous integration, continuous deployment, and automation in cloud environments.

Cloud Architecture and Implementation	
Modules	Description
<b>Final Project</b>	Apply the knowledge gained throughout the course to a final project, demonstrating proficiency in designing, implementing, and managing cloud-based solutions.

Figure 3 shows the expected length of the course in weeks. Each module will take a week of class time in a trimester format, meaning the course will take 12 weeks to complete.



**Figure 3:** Cloud Architecture and Implementation Module Length

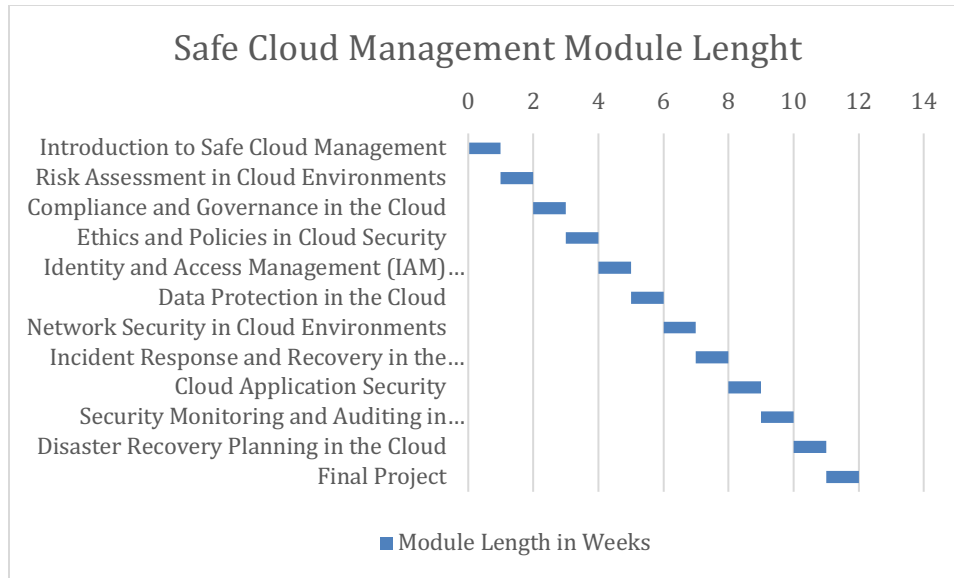
### ***Safe Cloud Management***

This course focuses on the secure management of day-to-day operations in a cloud environment. The contents of each module were expanded on using the book: *Cloud Computing Security: Foundations and Challenges* (Vacca, 2013). This book covers all topics discussed in this course and provides depth to the proposed modules. Table 3 shows the title of each module, along with a description of the topics covered. This course is divided into 12 modules, each building the foundation of the next section. This course aims to establish an understanding of secure cloud administration practices and essential topics related to this topic. With that covered, the course moves on to risk assessment and mitigation related explicitly to cloud environments, which leads nicely into cloud regulatory and governance frameworks. The course then moves on to IAM governance and topics related to security concepts, such as data security, network security, application security, and security monitoring. Finally, the curriculum goes over developing an organizational-wide incident response plan, including incident identification, containment, eradication, recovery, post-incident security controls and analysis, and disaster recovery planning, where recovery strategies for cloud environments are discussed. The student must submit a final project demonstrating skills learned.

**Table 3:** Safe Cloud Management Course Module Description

Safe Cloud Management	
Modules	Description
<b>Foundations of Secure Cloud Administration</b>	Establish a solid understanding of secure cloud administration practices, covering essential concepts, principles, and foundational skills required for managing cloud environments securely.
<b>Cloud Risk Analysis and Mitigation Strategies</b>	Explore the identification, assessment, and mitigation of risks in cloud environments, with a focus on strategies to proactively manage and minimize potential threats.
<b>Cloud Regulatory Compliance and Governance</b>	Examine compliance requirements and governance frameworks applicable to cloud services, emphasizing the establishment of policies and procedures to ensure regulatory adherence.
<b>Ethics and Policies in Cloud Security</b>	This targeted educational module is designed to provide a deep understanding of the ethical considerations and policy frameworks essential for maintaining security in cloud computing environments. It explores the intersection of ethical principles, regulatory requirements, and industry standards within the context of cloud security practices.
<b>Cloud Identity Governance and Security Access</b>	Focus on Identity and Access Management (IAM) in cloud environments, emphasizing the secure management of user identities, access controls, and authentication mechanisms.
<b>Cloud Data Security</b>	Explore strategies and techniques for securing data in the cloud, including encryption, access controls, and data loss prevention measures to safeguard sensitive information.
<b>Cloud Network Security</b>	Examine networking in the cloud, covering topics such as virtual networks, subnets, load balancing, and security measures for cloud-based applications.
<b>Cloud Incident Response and Recovery</b>	Develop skills in responding to and recovering from security incidents in the cloud, including incident identification, containment, eradication, recovery, and post-incident analysis.
<b>Cloud Application Security</b>	Explore security considerations specific to cloud-based applications, covering secure development practices, code reviews, and application-level security controls.
<b>Cloud Security: Monitoring and Audit Protocols</b>	Focus on the implementation of security monitoring and audit protocols in the cloud, emphasizing continuous surveillance and assessment of cloud environments.
<b>Cloud Disaster Recovery Planning</b>	Learn the principles and strategies for disaster recovery planning in cloud environments, ensuring business continuity and minimizing downtime in the face of unexpected disruptions.
<b>Final Project</b>	Apply the knowledge gained throughout the course to a final project, demonstrating proficiency in designing, implementing, and managing cloud-based solutions.

Figure 4 shows the expected length of the course in weeks. Each module will take a week of class time in a trimester format, meaning the course will take 12 weeks to complete.



**Figure 4:** The distribution of Course Topics for the course Safe Cloud Management

## Rational Analysis

Cloud computing has revolutionized data storage, access, and management. Cloud solutions particularly benefit Small and Medium-Sized Enterprises (SMEs) because of their cost-effective, dynamic resource allocation and elasticity. Cybersecurity-related issues are prevalent in a cloud environment. There exists a need for a robust security architecture while deploying cloud solutions to mitigate attack vectors. The courses outlined are needed to address the increasing reliance on cloud computing technologies for storing and managing data and the corresponding need for robust measures to safeguard sensitive information. Training upcoming experts to address the nuance of vulnerabilities within cloud security will create well-rounded graduates who can navigate the complex world of cloud security.

## Future Work

Students would learn to solve problems practically by including real-world case studies and simulations. Simulations would enable them to handle challenging cybersecurity issues in cloud environments. Developing a continuous update mechanism would keep the content current, involving collaborations with industry experts and responsive adjustments to address evolving threats. Examining how to incorporate widely accepted credentials into the curriculum, including those provided by big cloud service providers, can give the training more legitimacy and value. Collaborating across disciplines with domains such as ethical hacking and data science would offer a comprehensive understanding of the always-changing obstacles in cloud-based system security. Deviating from the standard module evaluation and embedding an evaluation framework into the pedagogical design would allow for a self-correcting course that ensures the students keep up with the course objectives. The evaluation framework would be implemented on a need-basis using the four-factor (Travers et al., 2019) model mentioned in the objective outline section.

## Acknowledgment

This material is based upon work supported by, or partly by, the National Science Foundation (NSF-SFS) under contract/award 2140638.



## References

- Alhebaishi, N., Wang, L., Jajodia, S., & Singhal, A. (2017). *Threat Modeling for Cloud Data Center Infrastructures*. In: Cuppens, F., Wang, L., Cuppens-Boulahia, N., Tawbi, N., Garcia-Alfaro, J. (eds) *Foundations and Practice of Security. FPS 2016. Lecture Notes in Computer Science()*, vol 10128. Springer, Cham. [https://doi.org/10.1007/978-3-319-51966-1\\_20](https://doi.org/10.1007/978-3-319-51966-1_20)
- John, S., Noma-Osaghae, E., Olajide, F., & Okokpujie, K. (2020). *Bridging the Gap: Developing Cloud Computing Security Courses for Recent Graduates*. *Journal of Cybersecurity Education*, 8(1), 45-58
- Forrest, C., & Posey, M. (2023). *Closing the cloud skills gap: A Perennial Problem for Businesses*. <https://www.spglobal.com/marketintelligence/en/news-insights/research/closing-the-cloud-skills-gap-a-perennial-problem-for-businesses>
- Foundry. (2023). *The Balancing Act of Cloud Expansion*. <https://foundryco.com/tools-for-marketers/research-cloud-computing/>
- Guanco, F., Lehnert, C., & Lumpe, S. (2023). *Understanding Cloud Attack Vectors The IaaS & PaaS Perspective*. Cloud Security Alliance. <https://cloudsecurityalliance.org/artifacts/understanding-cloud-attack-vectors/>
- Islam, M. M., Morshed, S., & Goswami, P. (2013). *Cloud Computing: A Survey on its Limitations and Potential Solutions*. *International Journal of Computer Science Issues*. 10. 159-163.
- Mahmood, Z., & Erl, T. (2013). *Cloud Computing: Concepts, Technology & Architecture (1st ed.)*. Pearson.
- Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing*. (Department of Commerce, Washington, D.C.), NIST SP 800-14, Change Notice September 28, 2011. <https://doi.org/10.6028/NIST.SP.800-145>
- Mousavi, S., Mosavi, A., Varkonyi-Koczy, A., & Fazekas, G. (2017). *Dynamic Resource Allocation in Cloud Computing*. *Acta Polytechnica Hungarica*. 14.
- Mogul, R., Arlen, J., Gilbert, F., Lane, A., Mortman, D., Peterson, G., & Rothman, M. (2017). *Security Guidance for Critical Areas of Focus in Cloud Computing*. [https://cloudsecurityalliance.org/artifacts/security-guidance-v4#related\\_resources](https://cloudsecurityalliance.org/artifacts/security-guidance-v4#related_resources)
- National Cyber Security Centre. (2022). *Cloud Security Shared Responsibility Model*. <https://www.ncsc.gov.uk/collection/cloud/understanding-cloud-services/cloud-security-shared-responsibility-model>
- Puzas, D. (2024). *12 Cloud Security Issues: Risks, Threats & Challenges*. <https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-security-risks-threats-challenges/>
- Thales Group. (2023). *2023 Cloud Security Report Shows Many Data Breaches - press release*. <https://cpl.thalesgroup.com/about-us/newsroom/2023-cloud-security-cyberattacks-data-breaches-press-release>
- The U.S. Department of Education. (2017). *Components of Comprehensive Work-Based Learning (WBL) programs*. <https://cte.ed.gov/wbltoolkit/index.html>

*Miguel A. Rodriguez Delgado; Xaymarie N. Garcia Collazo*

Travers, N., Jankowski, N., Bushway, D., & Duncan, A. (2019). *Learning Frameworks: Tools for Building a Better Educational Experience*. <https://www.luminafoundation.org/wp-content/uploads/2019/05/learning-frameworks.pdf>

Vacca, J. (2016). *Cloud Computing Security: Foundations and Challenges (2nd ed.)*. CRC Press