Active Learning in Cloud Security Course Design

Xaymarie N. García Collazo
Master in Computer Science
Advisor: Alfredo Cruz, Ph.D.
Polytechnic University of Puerto Rico
Graduate Project EXPO, May 2025

Abstract *— Cloud computing has transformed how data is accessed, managed, and protected across industries, offering flexible and scalable solutions particularly beneficial to small and medium-sized enterprises (SMEs). However, its rapid adoption introduces novel cybersecurity vulnerabilities that require specialized expertise. This project proposes the design of two cybersecurity courses, Cloud Architecture and Implementation and Safe Cloud Management, integrating active learning methodologies. By embedding hands-on labs, role-playing, collaborative projects, and scenario-based exercises grounded in constructivist and experiential learning theories, the curriculum aims to strengthen technical, analytical, and adaptive capabilities. Alignment with the Cloud Security Alliance's Crucial Domains ensures that graduates are prepared to meet the evolving cloud security challenges and contribute effectively to securing digital infrastructures.*

Key Terms *— Active Learning, Cloud Computing, Cloud Security Alliance, and Cybersecurity Education.*

INTRODUCTION

Cloud computing has become a fundamental pillar of modern digital transformation, offering flexible, scalable, and cost-effective solutions for managing data and services [1]. Its adoption has accelerated across industries, enabling organizations to innovate rapidly and operate more efficiently. Through models like Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), businesses gain access to powerful resources without the burden of maintaining physical infrastructure [1].

However, the complexity and unique vulnerabilities of cloud environments introduce new cybersecurity challenges. Misconfigurations, insufficient identity and access management (IAM) controls, insecure storage practices, and misunderstandings of the shared responsibility model are common issues threatening cloud-based systems [2]. As organizations increasingly rely on clouds, the need for security professionals with specialized cloud expertise becomes critical.

Despite the growing demand for such professionals, traditional cybersecurity education often remains anchored in lecture-based methodologies that emphasize theoretical understanding without cultivating applied technical skills [3]. Active learning approaches—such as scenario-based simulations, hands-on labs, and collaborative projects—are increasingly recognized as effective strategies to prepare students for securing cloud systems [5] and [9].

This paper proposes a curriculum design integrating active learning into cloud-focused cybersecurity education. The objective is to bridge the existing skills gap by providing students with practical, adaptive, and critical-thinking competencies essential for modern cybersecurity roles.

PROBLEM

Although cloud services offer unparalleled advantages in terms of scalability and operational efficiency, they also present significant security risks that traditional IT models did not anticipate [2]. The transition to the cloud has outpaced the development of corresponding educational models, leaving a severe shortage of adequately prepared cybersecurity professionals.

According to Forrest and Posey [4], 44% of organizations report difficulties finding qualified candidates for cloud security roles. Additional challenges include the increasing complexity of cloud platforms and the rapid introduction of new

technologies. Graduates often lack the practical skills necessary for designing secure cloud architectures, implementing identity and access management strategies, and responding effectively to cloud-specific security incidents.

The impact of this skills gap is tangible: organizations experience higher vulnerability rates, operational disruptions, increased regulatory risks, and financial losses due to data breaches [5]. Traditional education methodologies—predominantly based on passive learning—have proven insufficient for preparing students to address these dynamic, real-world challenges [5].

Figure 1 illustrates the major reasons organizations struggle to hire skilled cloud security professionals, emphasizing the urgency of integrating more effective, application-driven educational strategies [4].

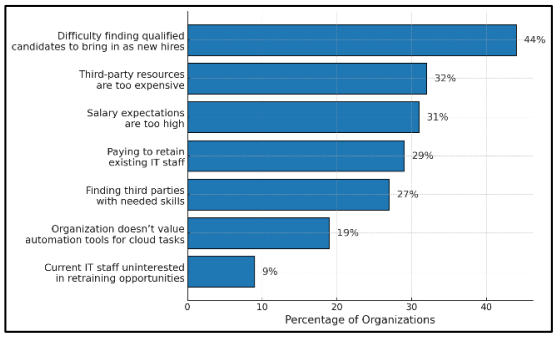


Figure 1
Cloud Security Hiring Difficulties [4]

LITERATURE REVIEW

The methodological framework adopted integrates two fundamental pillars: cloud computing security principles and active learning strategies. This integration is designed to establish a curriculum that not only reinforces technical competencies but also cultivates critical thinking, adaptability, and problem-solving skills. By merging theoretical foundations with experiential learning practices, the curriculum prepares students to address the evolving challenges inherent in securing contemporary cloud environments.

Cloud Security

Cloud computing has fundamentally reshaped the cybersecurity landscape by introducing a paradigm in which computing resources—such as servers, storage, applications, and services—are accessed remotely and dynamically scaled across distributed infrastructures. This model, while offering organizations unprecedented flexibility, scalability, and cost-efficiency, simultaneously introduces new layers of complexity and risk in the management of digital assets.

Cloud computing services are typically categorized into three primary delivery models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [1]. Each model delegates distinct responsibilities to cloud service providers and customers, requiring a clear understanding of the shared responsibility framework to implement effective security controls.

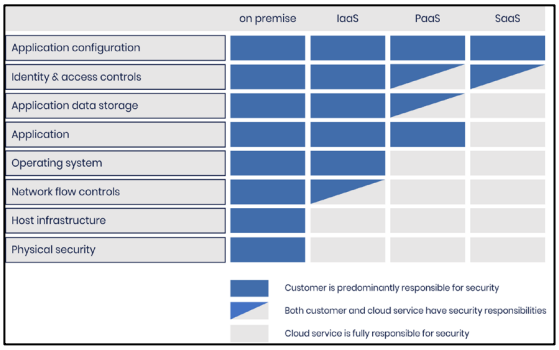
The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources" [1]. Within this paradigm, understanding the differences among cloud service models is critical to deploying secure environments. For example:

- In IaaS, customers are responsible for operating system patches, data security, and network configurations.
- In PaaS, customers manage only applications and data.
- In SaaS, the provider manages most layers, while customers secure access and user-level configurations.

Table 1 (Cloud Environment Responsibility Testing) in the broader study outlines these shared responsibilities, illustrating the importance of training students to recognize and manage them appropriately.

Table 1

Cloud Environment Responsibilities



Furthermore, research by Guanco, et al. emphasizes that cloud-specific attack vectors—including misconfigured workloads, unsecured encryption, and exploitable IAM policies—require a specialized skillset not adequately addressed by traditional IT security training. Students must be prepared to navigate risks associated with virtualization layers, federated identity management, and multi-tenant architecture [2].

Therefore, integrating cloud security competencies into cybersecurity education is not optional—it is essential for ensuring graduates can effectively assess and mitigate risks in modern digital infrastructures.

Active Learning

The traditional lecture-based model of education, centered on passive transmission of information, has shown significant limitations in preparing graduates for dynamic fields like cybersecurity. Active learning addresses this gap by promoting direct student engagement through hands-on practice, collaboration, critical reflection, and real-world problem-solving.

Active learning is grounded in constructivist educational theory, where knowledge is constructed actively through experiences and social interaction [7]. Learning is most effective when students engage deeply with the material, work collaboratively, and receive continuous feedback to refine their understanding [8]. In cybersecurity education, especially cloud-focused areas—where environments evolve rapidly and decision-making is critical, active learning is not only advantageous but essential.

Figure 2 shows Empirical evidence overwhelmingly supports the effectiveness of active learning. A meta-analysis by Freeman et al. [5] found that active learning:

- Reduces failure rates by 55%,
- Improves exam performance by 6%,
- Enhance critical thinking, problem-solving, and knowledge retention.

These gains demonstrate the clear advantage of active engagement strategies over passive lecture methods in technical education settings.

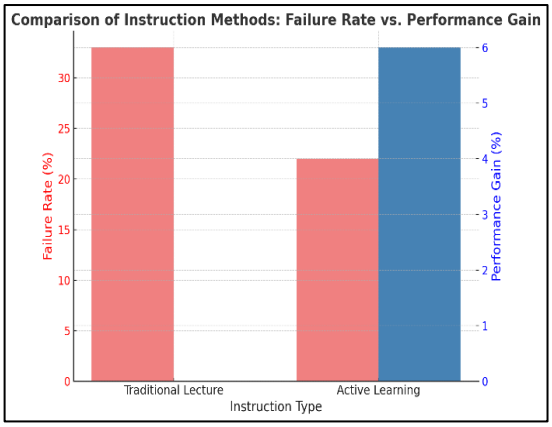


Figure 2

Performance with Active Learning vs Traditional Lecture

Beyond theoretical support, recent studies provide strong empirical evidence on the benefits of active learning in cybersecurity education.

A systematic review conducted by Lombardi, et al. [9] found that:

- 70% of studies reported increased student engagement and participation,
- 60% demonstrated measurable learning gains (e.g., better exam scores, higher project quality),
- 50% showed improved student confidence and industry readiness.

Figure 3 visually summarizes these findings. The bar chart shows the percentage of studies that reported improvements across three critical outcome categories: engagement and participation, learning gains, and confidence and readiness. The data highlights that active learning not only enhances

academic performance but also plays a crucial role in fostering the practical competencies and professional attitudes necessary for success in the cybersecurity industry. These metrics strongly support the integration of active learning as a central pedagogical strategy for cloud security education.

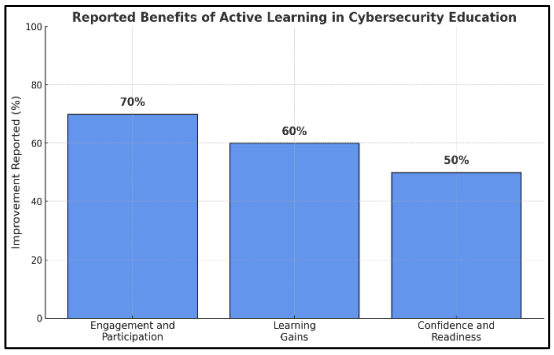


Figure 3
Benefits of Active Learning in Cybersecurity Education

These outcomes are particularly significant in cloud security, where rapidly evolving environments demand adaptable, self-directed professionals capable of critical analysis and quick action.

Cloud security is a field characterized by complexity, unpredictability, and interdisciplinary collaboration. These characteristics align naturally with active learning methodologies because:

- Authenticity: Labs and simulations expose students to real-world cloud service configurations, compliance requirements, and security threats.
- Adaptability: Students learn how to think critically and adjust strategies dynamically, just as they would in a real cloud security role.
- Collaboration: Group-based exercises simulate professional cybersecurity teams, fostering teamwork, communication, and
- Shared problem-solving.

Thus, active learning not only enhances technical competence but also prepares students for the nuanced demands of the modern cybersecurity workforce.

METHODOLOGY

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

This course introduces students to the practical application of network fundamentals in cloud environments. Organized into twelve modules, the curriculum follows the Cloud Security Alliance (CSA) critical domains and is based on the material presented in Cloud Computing: Concepts, Technology & Architecture [10].

Students' progress from basic cloud concepts to service and deployment models, followed by technical topics such as cloud architecture design, virtualization, secure networking, and Identity and Access Management (IAM). The final modules address cloud security practices, migration strategies, and DevOps principles, culminating in a final project that integrates all acquired skills.

Table 2 summarizes the modules of the Cloud Architecture and Implementation course, progressing from foundational cloud concepts to advanced topics such as virtualization, security, and DevOps. The course concludes with a final project that integrates all acquired skills.

Table 2
Cloud Architecture Implementation Course Module Description

Cloud Architecture and Implementation	
Modules	**Description**
Introduction to Cloud Computing	Overview of fundamental concepts, terminology, and benefits of cloud technology.
Cloud Service Models	Study of IaaS, PaaS, and SaaS models and their applications.
Cloud Deployment Models	Examination of public, private, hybrid, and multi-cloud deployment models.
Cloud Architecture Fundamentals	Principles for designing scalable, reliable cloud systems.
Virtualization and Containerization	Concepts of virtualization and containers for efficient resource management.
Cloud Storage Platform	Types of cloud storage, scalability, and data management solutions.
Cloud Network	Networking concepts in the cloud, including VPCs, subnets, and security measures.
Identity and Access Management (IAM)	Authentication, authorization, and secure access control in cloud environments.
Cloud Security	Best practices for data protection, threat detection, and regulatory compliance.
Cloud Migration	Strategies for planning and executing secure migrations to the cloud.
Cloud-native DevOps and Automated Deployment Practices	Integration of DevOps principles for automation and CI/CD in cloud systems.
Final Project	Capstone project applying all learned concepts in a practical cloud solution.

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.

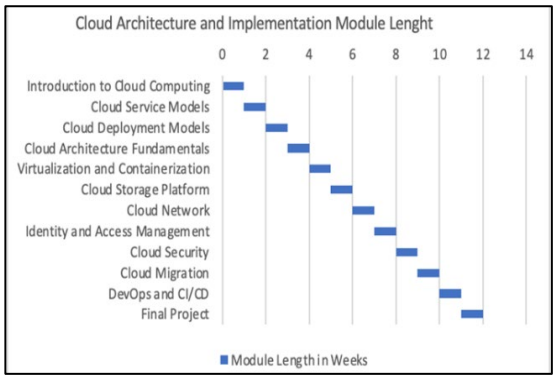


Figure 4
Cloud Architecture and Implementation Module Length

Cloud Architecture and Implementation Exercise

The Cloud Architecture and Implementation exercises consist of a practical laboratory conducted in Microsoft Azure for Students, where participants deploy and secure cloud infrastructure components. Additionally, the course includes a case study that challenges students to solve real-world cloud performance issues using Azure services. To reinforce learning, a series of quizzes at beginner, intermediate, and advanced levels are provided, testing theoretical and practical knowledge across key cloud concepts.

Laboratory: Configuring a Secure Virtual Network in Microsoft Azure

The goal of this exercise is to enable students to develop hands-on skills in cloud network configuration, subnet segmentation, virtual machine deployment, and the implementation of network security controls within Azure environments.

In this laboratory exercise, students are guided through the process of creating and configuring a secure virtual network within the Microsoft Azure cloud environment. Initially, students set up an Azure for Students account to obtain free credits necessary for the lab activities. They proceed to create a Virtual Network (VNet) named CloudNetworkingVNet, specifying the address space and selecting an appropriate region. Subsequently, the network is segmented into two subnets: a PublicSubnet for externally accessible resources and a PrivateSubnet for internal services. Students then deploy a Windows Server 2019 Virtual Machine (VM) within the created VNet, ensuring proper network interface attachment. To secure the environment, they configure Network Security Groups (NSGs) by setting rules to allow Remote Desktop Protocol (RDP) access and restricting external access to private subnet resources. The lab concludes with connectivity validation between the deployed VMs and testing security rules, reinforcing foundational concepts of cloud networking and security best practices.

Case Study: Slow Performance During Peak Usage

This case study challenges students to address performance degradation during high traffic periods for an e-commerce website hosted on a single Azure Virtual Machine. Students analyze the scenario and recommend solutions such as implementing horizontal scaling through multiple VM instances behind a Load Balancer, migrating the web application to Azure App Service with autoscaling capabilities, and relocating the database to Azure SQL Database with performance tuning. Through critical analysis, students compare horizontal and vertical scaling strategies, discuss the role of load balancers in availability improvement, and propose database isolation techniques to enhance both security and performance.

Students will learn to design resilient, scalable architectures and propose effective cloud-native solutions to enhance system performance and business continuity during periods of increased demand.

Quizzes: Beginner, Intermediate, and Advanced Levels

Throughout the module, students' complete quizzes categorize into beginner, intermediate, and advanced levels. These quizzes test their knowledge of fundamental cloud services, Azure-specific functionalities, networking principles, storage solutions, and infrastructure management tools. Each question is accompanied by explanations that reinforce learning objectives and clarify practical applications within Azure environments.

Students will consolidate theoretical knowledge of Azure components and cloud architecture best practices, ensuring foundational competency for more complex design and security tasks.

Safe Cloud Management

The Safe Cloud Management course focuses on the secure administration of daily operations within cloud environments. Structured into twelve progressive modules, the curriculum covers essential topics such as secure cloud administration practices, risk assessment and mitigation specific to cloud settings, and regulatory and governance frameworks. Further modules delve into Identity and Access Management (IAM) governance, data, network, and application security, as well as security monitoring.

The course culminates in developing an organization-wide incident response plan, encompassing incident identification, containment, eradication, recovery, post-incident analysis, and disaster recovery planning. A final project requires students to demonstrate the skills acquired throughout the course. The modules are developed based on the book Cloud Computing Security: Foundations and Challenges [11], which offers comprehensive insights into cloud security challenges and solutions. In addition to theoretical instruction, the course integrates applied learning strategies such as case studies, Microsoft Azure-based labs, and tiered quizzes to reinforce technical skills. These activities enable students to simulate real-world scenarios, assess cloud risks, and apply access controls effectively. This hands-on approach strengthens their ability to respond to cloud security threats with practical expertise and confidence.

Table 3 provides concise summaries of the twelve modules in the Safe Cloud Management course, each focusing on key aspects of securing cloud environments.

Table 3
Cloud Architecture Implementation Course Module Description

Safe Cloud Management	
Modules	**Description**
Foundations of Secure Cloud Administration	Introduces core principles and best practices for securely managing cloud environments.
Cloud Risk Analysis and Mitigation Strategies	Focuses on identifying, assessing, and mitigating risks in cloud environments to proactively manage potential threats.
Cloud Regulatory Compliance and Governance	Frameworks and policies ensuring regulatory adherence in cloud services.
Ethics and Policies in Cloud Security	Ethical considerations and policy development for cloud security.

Safe Cloud Management	
Modules	**Description**
Cloud Identity Governance and Security Access	Covers Identity and Access Management (IAM) in cloud environments, focusing on secure management of user identities and access controls.
Cloud Data Security	Techniques for protecting data through encryption and access controls.
Cloud Network Security	Securing cloud networks via virtual networks, subnets, and firewalls.
Cloud Incident Response and Recovery	Strategies for responding to and recovering from cloud security incidents.
Cloud Application Security	Ensuring application security through secure development practices.
Cloud Security: Monitoring and Audit Protocols	Implementing continuous monitoring and auditing in cloud environments.
Cloud Disaster Recovery Planning	Planning for business continuity and disaster recovery in the cloud.
Final Project	Applying course knowledge to design and manage secure cloud solutions.

Figure 5 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.

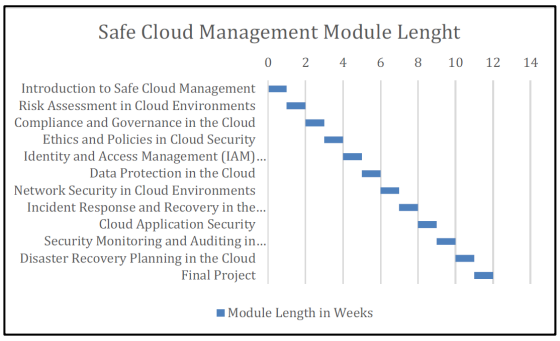


Figure 5
The distribution of Course Topics for the course Safe Cloud Management

Safe Cloud Management Exercise

The Safe Cloud Management section is designed to strengthen students' ability to securely manage cloud environments. Through a combination of a hands-on lab, a real-world case study, and targeted quizzes, students gain practical experience in implementing governance policies, securing data, monitoring cloud environments, and applying compliance strategies using Microsoft Azure.

Laboratory: Secure Cloud Management: IAM, Encryption, and Monitoring in Azure

In this practical lab, students are tasked with applying governance and security controls within an Azure cloud environment. They begin by creating a new resource group (RG_SafeCloudMgmt) under their Azure for Students account. Afterward, they assign a built-in Azure Policy ("Allowed Locations") to restrict resource deployment to a specific region, reinforcing compliance and resource governance best practices.

Students are then instructed to intentionally attempt to deploy a storage account in an unauthorized region to trigger a policy violation, experiencing firsthand how Azure enforces resource compliance. The lab concludes with students reviewing policy compliance results in Azure Policy, where they can observe compliant and non-compliant resources. This exercise emphasizes how organizations can use policy management and compliance tools to enhance security and maintain organizational standards in multi-cloud environments.

Case Study: Data Leak from Misconfigured Storage Account

Students analyze a real-world scenario where a law firm accidentally exposed sensitive client documents due to misconfigured Azure blob storage settings. As a solution, they propose securing storage by setting private access levels, applying Role-Based Access Control (RBAC) with the least privilege model, enabling Microsoft Defender for Storage, enforcing IP restrictions, using Multi-Factor Authentication (MFA), and implementing storage monitoring and logging to detect suspicious activities.

Quizzes: Beginner, Intermediate, and Advanced Levels

The quizzes incorporated in the Safe Cloud Management module are structured to progressively

challenge students' understanding of fundamental and advanced cloud security concepts.

At the Beginner level, quizzes focus on essential security constructs such as the definition and purpose of Role-Based Access Control (RBAC), the function of Microsoft Defender for Storage, the role of Multi-Factor Authentication (MFA), and basic preventive strategies for avoiding public data exposure.

At the Intermediate level, quizzes assess deeper knowledge of cloud security practices, including customer-managed key storage in Azure Key Vault, the implementation of Conditional Access policies based on user location or IP address, audit logging for user activity, and real-time threat detection tools like Microsoft Defender for Storage.

At the Advanced level, students are tested on strategic security models such as Zero Trust principles, the application of Azure Sentinel for threat detection and incident response, the utility of Just-in-Time (JIT) VM access to reduce attack surfaces, the role of Azure Policy in enforcing compliance standards across subscriptions, and the use of Conditional Access to automatically block high-risk sign-ins.

Each question is accompanied by a detailed explanation, fostering not only memorization but deep comprehension of security frameworks, threat mitigation practices, and regulatory compliance standards in cloud environments.

FINDINGS

The curriculum design process revealed several significant pedagogical and instructional insights. First, active learning methodologies, including scenario-based labs, tiered assessments, and collaborative exercises—are conceptually well-suited to cloud security education. These methods reinforce theoretical knowledge while fostering technical proficiency, adaptability, and collaborative problem-solving skills. Literature reviewed throughout this study supports their effectiveness in enhancing engagement, retention, and applied learning outcomes [5], [9].

Moreover, the alignment of both courses with the Cloud Security Alliance's critical domains [6] ensures that students engage with the core competencies needed to manage risk, enforce cloud governance, and respond to security incidents. The modular design of Cloud Architecture and Implementation and Safe Cloud Management facilitates logical progression from foundational concepts to advanced cloud security strategies, supporting student growth across technical and analytical dimensions. These findings affirm the relevance of active learning as a strategic and evidence-based approach to bridging the cybersecurity skills gap in cloud environments.

CONCLUSION

The implementation of active learning methodologies within cloud security education constitutes a critical advancement in bridging the persistent gap between academic preparation and professional industry demands. This project demonstrated that embedding experiential strategies—such as scenario-based simulations, hands-on laboratories, collaborative case studies, and role-playing exercises—provides a more robust development of technical competencies, critical thinking abilities, and adaptive skills essential for modern cybersecurity roles. The redesign of the courses Cloud Architecture and Implementation and Safe Cloud Management aligns directly with both constructivist and experiential learning theories, emphasizing knowledge construction through authentic tasks, reflective processes, and applied problem-solving. Furthermore, the curriculum strategically addresses the specific technical challenges found in cloud security, such as risk assessment, secure architecture design, identity governance, incident response, and compliance management, ensuring that students acquire not only theoretical understanding but also operational proficiency.

Supported by empirical evidence from recent studies, the active learning approach proposed in this project has been shown to enhance student

engagement, improve learning outcomes, and foster greater confidence and readiness for the workforce. Additionally, by embedding real-world scenarios and emphasizing team-based learning, the curriculum mirrors the interdisciplinary, dynamic, and collaborative nature of professional cybersecurity environments. However, successful implementation requires addressing known institutional challenges, including the provision of appropriate cloud lab infrastructure, faculty training, and continuous curriculum updates to keep pace with rapidly evolving cloud technologies. Although this study is conceptual and not yet supported by primary experimental data, it is strongly grounded in educational theory and supported by secondary research, offering a scalable and adaptable model for other institutions seeking to modernize their cloud security instruction.

Ultimately, this project highlights the urgent need for a pedagogical shift toward active, student-centered learning in technical disciplines. It provides a replicable and theoretically sound framework that not only prepares graduates for the complexity and fluidity of contemporary cloud security roles but also advances the broader goal of creating resilient, adaptable, and critically engaged cybersecurity professionals. Future research will be crucial in empirically validating these findings, exploring the integration of AI-enhanced adaptive learning environments, and ensuring equitable access to transformative cloud security education.

REFERENCES

[1] P. Mell and T. Grance, *The NIST Definition of Cloud Computing*, NIST Special Publication 800-145, National Institute of Standards and Technology, U. S. Department of Commerce, Sept. 2011. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-145. [Accessed: November 15, 2024].

[2] F. Guanco, C. Lehnert, and S. Lumpe, *Understanding Cloud Attack Vectors: IaaS & PaaS Perspective*. Cloud Security Alliance, 2023.

[3] C. C. Bonwell and J. A. Eison, *Active Learning: Creating Excitement in the Classroom,* ASHE-ERIC Higher Education Report No. 1, *George Washington University*, 1991. [Online]. Available: https://files.eric.ed.gov/fulltext/ED336049.pdf [Accessed: December 10, 2024].

[4] C. Forrest and M. Posey, "Closing the cloud skills gap: A perennial problem for businesses," *S&P Global Market Intelligence*, 2023. [Online]. Available: https://www.spglobal.com/marketintelligence/en/news-insights/research/closing-the-cloud-skills-gap-a-perennial-problem-for-businesses. [Accessed: December 10, 2023].

[5] S. Freeman, S. L. Eddy, M. McDonough, M. K. Smith, N. Okoroafor, H. Jordt, and M. P. Wenderoth, "Active learning increases student performance in science, engineering, and mathematics," *Proceedings of the National Academy of Sciences*, vol. 111, no. 23, pp. 8410–8415, 2014. [Online]. Available: https://doi.org/10.1073/pnas.1319030111. [Accessed: February 5, 2025].

[6] Cloud Security Alliance (CSA), *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*, 2017. [Online]. Available: https://anskaffelser.no/sites/default/files/csa_security_guidance_v4.0.pdf. [Accessed: February 5, 2025].

[7] D. A. Kolb, *Experiential Learning: Experience as the Source of Learning and Development*, Prentice Hall, 1984.

[8] L. S. Vygotsky, *Mind in Society: The Development of Higher Psychological Processes*, Harvard University Press, 1978.

[9] A. R. Lombardi, L. L. Gebhardt, C. M. Stefaniak, and L. M. Krieger, "Active Learning in Cybersecurity Education: A Systematic Review," *ACM Transactions on Computing Education (TOCE*), vol. 22, no. 2, Art. no. 15, 2022.

[10] Z. Mahmood and T. Erl, *Cloud Computing: Concepts, Technology & Architecture*, Pearson Education, 2013.

[11] J. R. Vacca (Ed.), *Cloud Computing Security: Foundations and Challenges*, 1st ed., CRC Press, 2016.