## **CYBR 415: Cloud Security and Privacy (3 credits)**

The course provides a deep and critical understanding of the Cloud security architecture. The learners explore the guiding security design principles, design patterns, industry standards, applied technologies and addressing regulatory compliance requirements critical to design, implement, deliver, and manage secure cloud-based services. The course instills the specialist skills into the learners to dive into the secure cloud architectural aspects. It is regarding identifying and mitigating risks, protection and isolation of physical & logical infrastructures including compute, network and storage, comprehensive data protection, end-to-end identity management & access control, monitoring and auditing processes and meeting compliance with industry and regulatory mandates. *(Prerequisite: CMPE 215)*

**Course Learning Outcomes:**

By the end of the course, students will be able to:

A1. Demonstrate Critical knowledge of the specialized concept and theories related to cloud security and privacy.

A2. Apply specialized techniques, tools and standards to assure the security of cloud-based services.

B1. Critically analyse the problems of administration, usage and control of resources on cloud to formulate specialized customizable security profile for ensuring privacy of the cloud tenant.

B2. Implement specialist strategies to provide effective data protection, intrusion preventive and incident response to counter sophisticated attacks on cloud premises.

B3. Exhibit the specialist skills of expressing and communicating cloud security compliance effectively in written and oral.

C1. Demonstrate effective teamwork and collaboration skills in the context of cloud security, working collaboratively to provide specialist solutions to private cloud security problems.

**Course Learning Materials:**

* Eyal Estrin, “Cloud Security Handbook: Find out how to effectively secure cloud environments using AWS, Azure, and GCP”, (2022), Packt Publishing, ISBN: 978-1800569195.
* Mike Chapple, David Seidl, “CCSP Certified Cloud Security Professional Official Study Guide”, 3rd Edition (2022), Sybex, ISBN: 978-1119909378.
* Chris Binnie, Rory McCune, “Cloud Native Security”, 1st edition (2021), Wiley, ISBN: 978-1119782230

**Course Content:**

1. Introduction to Cloud Computing
2. Cloud Vulnerabilities, Attacks and Security Approaches
3. Cloud Security Compliance
4. Isolation in Cloud
5. Identity Management in Cloud Computing
6. Identity and Access Management (IAM)
7. Compute and Configuration Management
8. Compute and Configuration Management
9. Data Protection and Automation
10. Logging Network/cloud services for Monitoring
11. Cloud Monitoring and Auditing
12. Incidence Response and Forensics
13. Cloud Security Compliance Services and Standards
14. Cloud Security Regulatory Compliance