# COURSE DESCRIPTION CARD - SYLLABUS

Course name
Cloud computing [S1MiKC1>ChO]

## Course

Field of study
Microelectronics and digital communications

Year/Semester
2/3

Area of study (specialization)
–

Profile of study
general academic

Level of study
first-cycle

Course offered in
Polish

Form of study
full-time

Requirements
compulsory

## Number of hours

Lecture
15

Laboratory classes
15

Other
0

Tutorials
0

Projects/seminars
0

## Number of credit points

2,00

## Coordinators

dr hab. inż. Mariusz Żal
mariusz.zal@put.poznan.pl

## Lecturers

## Prerequisites

• Basic knowledge of computer networking concepts (protocols, OSI/TCP-IP model). • Ability to use operating systems (Windows, Linux) for software installation and basic network commands. • Fundamental understanding of virtualization and/or server solutions. • Basic programming skills in any language (Python, C, Java).

## Course objective

The aim of this course is to introduce students to the fundamental principles of cloud computing, virtualization techniques, and the design of applications and services in a distributed cloud environment. Students will learn how to use cloud platforms (AWS, Azure, Google Cloud), configure computing and networking services, and deploy highly available and scalable applications. Special emphasis will be placed on cloud security, deployment automation, and application monitoring. The course will prepare students for effective work with modern cloud technologies and the design of IoT applications in cloud environments.

## Course-related learning outcomes

Knowledge:
• Understands the fundamental concepts and models of cloud computing (IaaS, PaaS, SaaS) as well as

deployment models (public, private, and hybrid cloud). [K1_W10]
• Is familiar with basic computing, networking, and database services offered by leading cloud platforms (AWS, Azure, Google Cloud). [K1_W08]
• Understands the architecture of cloud computing, including containerization concepts and microservices. [K1_W10]
• Knows security techniques in cloud environments, including authentication mechanisms, encryption, and access control. [K1_W24]
• Is aware of the impact of the availability of cloud services on the digital society.. [K1_W14]

Skills:
• Is able to configure a cloud environment and deploy and manage virtual machines and containers. [K1_U26]
• Can deploy web applications using the IaaS and PaaS models, configure networking services, and manage cloud databases. [K1_U26]
• Is capable of designing and deploying an IoT application in a cloud environment, utilizing tools for application lifecycle management. [K1_U26]
• Is able to use available tools and information sources for planning and implementing self-education. [K1_U32]

Social competences:
• Understands the significance of cloud computing in modern IT and can consciously utilize cloud technologies while ensuring security and regulatory compliance. [K1_K04]
• Is capable of working in project teams, effectively communicating work results, problems, and solutions. [K1_K03]
• Is aware of the necessity for continuous development and staying up to date with trends in cloud computing. [K1_K01]

## Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Knowledge: A written test with questions related to cloud services and applications. The minimum passing threshold is 50% of the total possible points.
Skills: Ongoing assessment of laboratory task completion. The minimum passing threshold is 50% of the total possible points.

## Programme content

As part of this course, students will gain knowledge about cloud computing architecture, service models (IaaS, PaaS, SaaS), and fundamental virtualization and containerization techniques. They will also learn the principles of operation and configuration of cloud platforms such as AWS, Azure, and Google Cloud, including computing, database, and networking services.
The course covers cloud security topics, including authentication mechanisms, encryption, and identity management. Special emphasis will be placed on cloud service management and orchestration systems, such as Docker Swarm, Kubernetes, and OpenStack, including service monitoring, failure handling, and application lifecycle management.
Students will learn how to deploy web and IoT applications in cloud environments, utilizing deployment automation (CI/CD) and performance and cost monitoring tools. During laboratory sessions, participants will have the opportunity to practically configure a cloud environment, launch virtual machines and containers, and deploy applications using the PaaS model.
The course will conclude with a team project where students will design and deploy a complete cloud-based application, considering its scalability, security, and reliability.

## Course topics

Lecture:
1. Introduction to Cloud Computing
• Definition of cloud computing, evolution of computing models.
• Service models: IaaS, PaaS, SaaS.
• Deployment models: public, private, hybrid cloud.
2. Cloud Computing Architecture

• Virtualization as the foundation of cloud computing.
• Containerization: Docker, Kubernetes - basics and applications.
3. Virtualization Techniques
• Virtualization as a tool for efficient utilization of physical resources.
• Comparison of virtualization types: Type 1 and Type 2 hypervisors, isolation concepts, architecture, and use cases.
• Virtualization tools: full (KVM, XEN, VMware, VBox), container-based (LXC, Docker), hybrid (Kata Containers).
• Networking techniques for virtual machines and containers ensuring high performance: DPDK, SR-IOV in x86 and ARM architectures.
• Resource allocation and management mechanisms (CPU/GPU, memory, network, energy) and isolation assurance techniques.
• Lifecycle management of virtual machines and containers, specific characteristics of containers (ephemerality), and best practices for creating container images.
4. Cloud Platforms
• Overview of computing, database, and networking services in AWS, Azure, and Google Cloud.
• Edge computing and fog computing - concepts and applications.
5. Cloud Security
• Shared Responsibility Model.
• Authentication, authorization, and data encryption mechanisms.
• Identity and Access Management (IAM).
6. Cloud Service Management and Orchestration Systems
• Comparison of systems: Docker Swarm, Claudify, Kubernetes, OpenStack.
• Core functionalities: image deployment/removal, instance start/stop, resource allocation, virtual machine/container migration, service scaling (scale out & in), load balancing.
• Supporting cloud services: service state monitoring, application mobility management, reliability assurance (failure and anomaly handling).
• Application lifecycle management: software updates, image and container repositories (OSBoxes, Docker Hub).
7. Cloud Resource Management and Monitoring
• Deployment automation: CI/CD.
• Performance and cost monitoring.
8. IoT Application Design in the Cloud
• Utilizing cloud platforms for IoT application development.
• Use case examples: smart homes, industrial applications.
Laboratory:
1. Basic Cloud Environment Configuration
• Creating an account and exploring the user interface of cloud platforms.
2. Deploying Virtual Machines and Containers
• Configuring virtual machines on AWS/Azure.
• Creating and managing containers using Docker.
3. Deploying Applications Using the PaaS Model
• Deploying a web application on a PaaS platform.
4. Cloud Security
• Configuring IAM, firewall rules, and data encryption.
5. Monitoring and Automation
• Creating a CI/CD pipeline using GitHub Actions or GitLab CI.
6. Team Project
• Comprehensive deployment of an application considering scalability, security, and monitoring.

## Teaching methods

Lectures:
a) Multimedia presentation with additional examples presented and explained on the board.
b) Case study based on a presentation utilizing cloud systems.
Laboratory Classes and Projects:
a) Hands-on programming exercises using computers.
b) Short multimedia presentations.

## Bibliography

Basic:
1. Erl, T., Mahmood, Z., Puttini, R. Cloud Computing: Concepts, Technology & Architecture, Prentice Hall, 2013.
2. White papers i dokumentacja techniczna dostawców chmur (AWS, Azure, Google Cloud).
3. Krutz, R. L., Vines, R. D. Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Wiley, 2010.
4. Galkin, B., Chaudhary, A. Beginning Azure DevOps: Leveraging Pipelines, Repos, Boards and More, Apress, 2021.

Additional:
1. Jamsa, K. Cloud Computing: SaaS, PaaS, IaaS, Virtualization, Business Models, Security, Jones & br/ >Bartlett Learning, 2013.
2. Dokumentacja i tutoriale platform chmurowych (AWS, Azure, GCP).
3. Blogi oraz portale branżowe (np. Medium, DevOps.com).
4. Materiały dodatkowe publikowane przez ENISA (European Union Agency for Cybersecurity) dotyczące bezpieczeństwa chmur obliczeniowych.
5. Dokumentacja systemów zarządzania kontenerami (Docker, Kubernetes, OpenStack).
6. Materiały wideo i kursy online (np. Udemy, Coursera) dotyczące automatyzacji i wdrażania aplikacji w chmurze.

## Breakdown of average student's workload

| | Hours | ECTS |
|---|---|---|
| Total workload | 60 | 2,00 |
| Classes requiring direct contact with the teacher | 30 | 1,00 |
| Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation) | 30 | 1,00 |