SYLLABUS

Cloud Application and Infrastructure Security

University year 2025-2026

1. Information regarding the programme

1.1. Higher education institution	Babeş-Bolyai University
1.2. Faculty	Faculty of Mathematics and Computer Science
1.3. Department	Department of Computer Science
1.4. Field of study	Computer Science
1.5. Study cycle	Master
1.6. Study programme/Qualification	Cyber Security
1.7. Form of education	Full time

2. Information regarding the discipline

2.1. Name of the discipline	**Cloud Application and Infrastructure Security**					Discipline code	**MME8202**
2.2. Course coordinator	C.d.asoc. Ing. Andrei Petru Ştefănie						
2.3. Seminar coordinator	C.d.asoc. Ing. Andrei Petru Ştefănie						
2.4. Year of study	**2**	2.5. Semester	**3**	2.6. Type of evaluation	**C**	2.7. Discipline regime	**Mandatory**

3. Total estimated time (hours/semester of didactic activities)

3.1. Hours per week	**4**	of which: 3.2 course	**2**	3.3 laboratory/project	**2**
3.4. Total hours in the curriculum	**56**	of which: 3.5 course	**28**	3.6 laboratory/project	**28**
Time allotment for individual study (ID) and self-study activities (SA)					**hours**
Learning using manual, course support, bibliography, course notes (SA)					20
Additional documentation (in libraries, on electronic platforms, field documentation)					30
Preparation for seminars/labs, homework, papers, portfolios and essays					30
Tutorship					6
Evaluations					8
3.7. Total individual study hours	**94**				
3.8. Total hours per semester	**150**				
3.9. Number of ECTS credits	**6**				

4. Prerequisites (if necessary)

4.1. curriculum	Computer network, databases, web applications, encryption
4.2. competencies	Good programming skills in at least one programming language (Java, JavaScript, C#, etc.)

5. Conditions (if necessary)

5.1. for the course	Projector and internet access
5.2. for the seminar /lab activities	Projector and internet access

6.1. Specific competencies acquired

Professional/essential competencies	• Know and understand the main paradigms related to data protection: confidentiality, integrity and data availability; • Ability to create distributed applications in the Cloud, respecting the ethical and secure policies;
Transversal competencies	• Professional communication skills; concise and precise description, both oral and written, of professional results. • Entrepreneurial skills; working with economical knowledge; continuous learning;

6.2. Learning outcomes

Knowledge	• The student / graduate knows the architecture of cloud applications and the security models used in such applications; • The student / graduate knows the basic mechanisms that define the security of the system and the software environment in which an application runs, such as: access permissions, security policies, interaction with the external environment;
Skills	• The student / graduate is able to use security techniques in the software systems development process; • The student/graduate is able to provide specialized advice and develop specialized materials; • The student / graduate is able to assess the security risk using at least one of the established methods;
Responsibility and autonomy:	• The student/graduate assumes responsibility for the product of his / her work, requests feedback and uses it constructively; • The student/graduate demonstrates teamwork capabilities and develops communication skills;

7. Objectives of the discipline (outcome of the acquired competencies)

7.1 General objective of the discipline	• To provide students with a comprehensive understanding of the security principles, risks, and controls associated with cloud computing. • To develop the ability to design, deploy, and secure cloud applications and infrastructures across different service models (IaaS, PaaS, SaaS). • To build an awareness of shared-responsibility models and how they influence security design and incident response in the cloud. • To promote a critical perspective on how cloud adoption affects compliance, governance, and threat exposure.

7.2 Specific objective of the discipline	• Gain practical experience in securing workloads on major public cloud platforms (e.g., AWS, Azure, GCP). • Understand and apply key cloud-security services such as identity and access management, encryption, monitoring, and vulnerability management. • Analyze real-world security incidents and misconfigurations to derive best practices for prevention and remediation. • Evaluate cloud compliance frameworks (CIS Benchmarks, NIST 800-53, ISO 27017, etc.) and model them using cloud-native policies and controls. • Integrate security into the full lifecycle of cloud-native applications using automation and managed services.

8. Content

8.1 Course	Teaching methods	Remarks
1. Introduction to Cloud Security • Cloud computing models (IaaS, PaaS, SaaS) • Shared Responsibility Model • Cloud threat landscape and common attack vectors • Benefits and risks of cloud adoption • Overview of compliance frameworks (CIS, NIST, ISO 27017, FedRAMP)	Exposure: description, explanation, examples, debate	
2. Cloud Security Architecture • Cloud-native security principles • Defense-in-depth and Zero Trust • Security responsibilities across layers (application, network, data, identity) • Secure design patterns in cloud applications	Exposure: description, explanation, examples, debate	
3. Identity and Access Management (IAM) Part I • Principles of authentication and authorization • Users, roles, and policies • Federation and SSO • IAM in AWS, Azure, and GCP	Exposure: description, explanation, examples, debate	
4. Identity and Access Management (IAM) Part II • Privilege management and least privilege • Role chaining and cross-account access • Common IAM misconfigurations and attack paths • Detection and remediation of IAM risks	Exposure: description, explanation, examples, debate	
5. Cloud Networking and Perimeter Security Part I • Virtual networks, subnets, routing tables • Security groups and network ACLs • Ingress/egress control • Private vs. public connectivity	Exposure: description, explanation, examples, debate	
6. Cloud Networking and Perimeter Security Part I • Hybrid connectivity (VPNs, Direct Connect, ExpressRoute) • Network segmentation • Zero Trust networking • Network monitoring and reachability analysis	Exposure: description, explanation, examples, debate	

7. Data Security - Protection and Encryption • Data classification and lifecycle • Encryption at rest and in transit • Key management systems (AWS KMS, Azure Key Vault, GCP KMS) • Secrets management and token-based access	Exposure: description, explanation, examples, debate	
8. Data Security – Backup and Recovery • Backup and snapshot strategies • Continuous backups vs. point-in-time recovery • Disaster recovery (RPO/RTO concepts) • Immutability and WORM storage	Exposure: description, explanation, examples, debate	
9. Governance and Multi-Account Management Part I • Multi-account structure and best practices • Service Control Policies (SCPs) • Centralized billing and audit • Organizational security posture management	Exposure: description, explanation, examples, debate	
10. Governance and Multi-Account Management Part II • Azure Management Groups and Blueprints • GCP Folders and Organization Policies • Cross-cloud policy enforcement • Managing compliance at scale	Exposure: description, explanation, examples, debate	
11. Monitoring and Logging Part I • Importance of observability for security • Cloud-native logging services (CloudTrail, CloudWatch, Azure Monitor, GCP Cloud Logging) • Centralized log storage and retention • Detecting anomalies in logs	Exposure: description, explanation, examples, debate	
12. Monitoring and Logging Part II • Integration with SIEM/SOAR tools • Correlation of logs and alerts • Case studies of incident investigation • Continuous compliance monitoring	Exposure: description, explanation, examples, debate	
13. Cloud Security Tools and Platforms • Overview of CNAPP, CSPM, CWPP, CIEM, KSPM • Agent-based vs. agentless approaches • Benchmarking and compliance automation (CIS, STIG) • Runtime protection and emerging trends	Exposure: description, explanation, examples, debate	
14. Recap and Final Evaluation • Review of key topics • Integrative discussions • Final evaluation and student presentations	Exposure: description, explanation, examples, debate	

Bibliography

1. Chris Dotson - Practical Cloud Native Security, O'Reilly Media, 2nd edition, 2023
2. Ross Anderson – Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley, 3rd edition, 2020
3. Yuri Diogenes, Nicholas DiCola, Jonathan Trull – Azure Security Handbook: A Comprehensive Guide for Defending Your Enterprise Environment, Microsoft Press, 1st edition, 2021
4. Center for Internet Security (CIS) – CIS Benchmarks for AWS, Azure, and GCP, latest online edition
5. NIST Special Publication 800-144 – Guidelines on Security and Privacy in Public Cloud Computing, U.S. Department of Commerce, 2011

8.2 Seminar / laboratory	Teaching methods	Remarks

1. Introduction to Cloud Security Foundations • Overview of the AWS Academy platform and course structure • Access and navigation of the AWS Academy Learner Lab environment • Review of shared responsibility model and AWS global infrastructure • Introduction to lab submission and evaluation process	Demonstration, guided setup, Q&A	
2. Using Resource-Based Policies to Secure an S3 Bucket • Create and configure S3 buckets with different access policies • Use bucket policies and IAM policies to manage access • Implement least-privilege principles	Demonstration, guided setup, Q&A	
3. Securing VPC Resources by Using Security Groups • Configure a VPC with public and private subnets • Create and apply security groups to control inbound/outbound traffic • Test connectivity scenarios and verify network isolation • Review best practices for network segmentation	Demonstration, guided setup, Q&A	
4. Encrypting Data at Rest by Using AWS KMS • Create and manage encryption keys in AWS KMS • Encrypt and decrypt S3 objects and EBS volumes • Understand key rotation and policy management	Demonstration, guided setup, Q&A	
5. Monitoring and Alerting with CloudTrail and CloudWatch • Enable and configure AWS CloudTrail for account activity monitoring • Set up CloudWatch Alarms and Logs • Create metric filters for detecting security-relevant events	Demonstration, guided setup, Q&A	
6. Remediating an Incident by Using AWS Config and Lambda • Use AWS Config to detect non-compliant resources • Develop a Lambda function for automated remediation • Simulate a compliance drift and observe automatic correction	Demonstration, guided setup, Q&A	
7. Final Evaluation and Recap	Demonstration, guided setup, Q&A	

Bibliography

1. AWS Academy Cloud Security Foundations – Learner Lab Manual, AWS Academy, latest edition
2. AWS Documentation – Identity and Access Management (IAM), Amazon S3 Security, AWS KMS, AWS Config, CloudTrail, CloudWatch, available at https://docs.aws.amazon.com/
3. Center for Internet Security (CIS) – CIS Amazon Web Services Foundations Benchmark, latest online edition

9. Corroborating the content of the discipline with the expectations of the epistemic community, professional associations and representative employers within the field of the program

- The discipline aligns with current trends in academic curricula on Cloud Security and Secure Cloud Architecture, as offered by leading universities in Europe and worldwide.
- The course content is consistent with international frameworks and guidelines promoted by professional and standardization bodies such as NIST, ENISA, and the Center for Internet Security (CIS).
- The practical component, delivered through the AWS Academy Cloud Security Foundations program, ensures alignment with industry-recognized best practices and certifications (e.g., AWS Certified Security - Specialty, Azure Security Engineer Associate).
- Software organizations recognize the importance of the concepts discussed during this course.

10. Evaluation

Activity type	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Percentage of final grade
10.4 Course	Individual research and presentation on a topic related to what has been taught at the course.	Colloquium	70%
10.5 Seminar/laboratory	Being able to implement course concepts and presented technologies	Test	30%
10.6 Minimum standard of performance			
• At least grade 5 (from a scale of 1 to 10) at both presentation and laboratory project.			

11. Labels ODD (Sustainable Development Goals)[1]

Not applicable.

Date:	Signature of course coordinator	Signature of seminar coordinator
15.04.2025	**C.d.asoc. Ing. Andrei Petru Ştefănie**	**C.d.asoc. Ing. Andrei Petru Ştefănie**

Date of approval:

...

Signature of the head of department

Assoc.prof.phd. Adrian STERCA