BIRZEIT UNIVERSITY

Computer Science Department

Cloud Computing and Data Security (COMP 4381)

Second Semester 2023/2024

Project: Cloud computing and data security *Due Date 1/06/2024*

Project Overview:

This project involves conducting a detailed case study on the secure migration of a fictional company's IT infrastructure to the cloud. Throughout the project, students will explore various aspects of cloud computing and data security, including definitions, security challenges, data protection mechanisms, and strategies for mitigating data breaches and vulnerabilities.

Project explanation:

The fictional company ***"TechSolutions Inc."*** is a mid-sized technology company looking to migrate its on-premises IT infrastructure to the cloud to improve scalability, accessibility and cost-effectiveness. However, the company is concerned about the potential security risks associated with cloud adoption and wants to ensure data security.

You work in the IT department of a giant company like Google, Microsoft, or Azure, and you have been asked to create a proposal for this company, ***TechSolutions Inc.*** With a product available in one of these giant companies. You must give a complete proposal explaining all the features and services provided by the cloud company you work for. Also, this proposal must explain some security flaws and vulnerabilities that could cause data breaches. Finally, a security strategy must be developed to solve all these security vulnerabilities using appropriate security countermeasures for each vulnerability.

Then you should cover the following in your project:

1- Understanding Cloud Computing Definitions: Select one of these giant companies and explain critical characteristics and different cloud service and deployment models. Analyze how cloud computing aligns with ***TechSolutions Inc.'s*** business objectives and IT requirements.

2- Assessing Cloud Computing Security: Identify security risks and challenges associated with cloud computing and explain **three** security vulnerabilities that cause those risks. Discuss the shared responsibility model and the roles of cloud service providers and clients in ensuring security. Finally, evaluate security measures provided by your cloud company and their suitability for ***TechSolutions Inc.'s*** needs.

3- Implementing Data Security in Cloud Computing: Develop a data security strategy for ***TechSolutions Inc.'s*** cloud data processing, considering **at least three** data security requirements: privacy, confidentiality, integrity, authentication, authorization, accountability and availability. Discuss the importance of data classification and lifecycle management in maintaining data security. Explore cloud-native security services and tools for securing data in the cloud environment.

4- Address data breaches, vulnerabilities, and security requirements: Summarize your security proposal using a flowchart. Firstly, it identifies data breaches and potential vulnerabilities that may arise in the cloud. Second, it develops security requirements and policies specifically designed for ***TechSolutions Inc.'s*** cloud environment. Finally, security controls and countermeasures are implemented to mitigate identified risks.

Your project must follow the following requirements:

1- Your proposal meets at least three security requirements.
2- Your proposal discusses three vulnerabilities.
3- Your proposal's security requirements, vulnerabilities, and countermeasures are limited to class discussion.
4- The proposal is an individual work, and any work based on artificial intelligence sites will be marked Zero and referred to a control committee.
5- Submissions should be made before the specified deadline, 01/06/2024, at 10:00 p.m. Any late submission will be marked out of 50%.