ASSIGNMENT 3: PART B

<u>TASK</u>: Read the paper: "Identity and access management in cloud environment: Mechanisms and challenges [1]" and write a summary.

Cloud computing is a collection of various reconfigurable computing resources that aids in giving cloud consumers easy, on-demand access. However, the CSP dominates the identity management system in cloud environments. The three types of cloud environments are private, public, and hybrid/federated. Additionally, there are several cloud environments that are created especially to support certain services, such as Internet of Things (IoT) cloud services and mobile cloud services.

The paper presents a comparative study of various identity and access management mechanisms in the cloud environment, overview of access governance policies, overview of the market's top identity and access control suite of products and solutions, analysis of security threats in the cloud environment, and recommendations on governance policies and industry best practises.

<u>Mainly it has following components discussed in depth</u>:

1. *Authentication mechanisms include:*
   - Physical security mechanisms like access cards and biometrics ensure security of cloud resources and facilities by denying unauthorized access.
   - Digital security mechanisms include Secure Shell (SSH) keys, Multifactor authentication, Chip and PIN, SSO techniques, OpenID, OAuth and SAML.

2. *Authorization mechanisms include:*
   - Access Control Mechanisms: MAC, DAC, RBAC, and ABAC.
   - Access Control Governance: Certification & Risk Control, Life cycle management, and Segregation of duties.

3. *Identity and access management (IAM).*

4. *Security threats in cloud environment* like virus or malware, apts and malicious outsiders, password and key compromises and many more.

5. *Security Analysis in cloud environment:* MITM attacks, Insider attacks, Session and cookie hijacking, guessing attacks and many others.

In my opinion, the paper has thoroughly introduced through every important aspect of the cloud environment which is very helpful for beginners who are about to embark their journey as a cloud or DevOps engineer. This paper analysed and summarized the current security aspects, potential threats and mitigations involved in cloud services.

To give academics and even the business professionals a thorough introduction of IAM systems, the various identity and access control models are compared, and the security implications of each model are thoroughly examined. It is advocated to use multifactor authentication, chip and pin, the OpenID Connect framework, role-based access control, and the ABAC architecture.

REFERENCE:

[1] I. Indu, P. Anand and V. Bhaskar, "Identity and access management in cloud environment: Mechanisms and challenges", *Engineering Science and Technology, an International Journal*, vol. 21, no. 4, pp. 574-588, 2018.