**Albanese, M., De Benedictis, A., de Macedo, D. D. J., & Messina, F. (2020). Security and trust in cloud application life-cycle management. Future Generation Computer Systems, 111, 934–936.** [**https://doi.org/10.1016/j.future.2020.01.025**](https://doi.org/10.1016/j.future.2020.01.025)

The research conducted by Albanese, Benedictis, Macedo, and Messina is regarding the Security and Trust Enforcement in the Cloud Applications Software Development Lifecycle Management. This research was conducted mainly with the goal highlighting the unique solutions and techniques for the more secured and authenticated cloud-based applications and enforcing the trust and security in the Cloud Infrastructure. Some of the key elements discussed in the article were focused on the Performance metrics and Security Modelling in the Cloud Applications. Highlighting few of them were SLA-based trust management and authorization and Trust-based Cloud Services Selections in Cloud Federations. The article also discussed the various techniques developers need to adopt in assessing the security level permissions and Policies in the existing cloud infrastructure. Data Integrity and Data Protection was one of the biggest concerns which disinclines the trust and authenticity on the Cloud Infrastructures.

**Indu, I., Anand, P. M. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. Engineering Science and Technology, an International Journal, 21(4), 574–588.** [**https://doi.org/10.1016/j.jestch.2018.05.010**](https://doi.org/10.1016/j.jestch.2018.05.010)

The above research was carried out by Indu and Vidhyacharan on the Identity and Access Management (IAM) in cloud environment. The research paper focuses majorly on the 3 sub-domains namely Authentication, Authorization and Security with sub-domains of Physical Security Mechanisms, Digital Security Mechanisms, Access Control Mechanisms, Access Control Governance Mechanisms, Threat in the Cloud Infrastructure and Threats in the Cloud Services. It do discussed some real-time scenarios where the cloud securities are compromised and opens up a channel for the threats and cyber-attacks. In the process of data transmission, access , and storage in Cloud based services have many securities compromised, and how to avoid those compromission and malicious attacks different measures were revealed to adopt in the Cloud based Applications to make it more authentic and authorized guaranteeing security of identities and attributes of the cloud IAM users and groups.

Various Digital Security Mechanisms like Credentials Management on popular LDAP and AD technologies, SSH Keys or challenge-response authentication, Multifactor Authentications adding a top layer on the traditional credential-based authentication, Chip and Pin( commonly used in banking transactions), Single-Sign-On and Federations; if adopted can make your Cloud Infrastructure Services more robust. The smart-pie-chart visualization on the different issues in the Cloud Environment with numerical percentage depicts out in summary the domains which are highly vulnerable to outsider attacks.