CSCI 5410: Assignment 3

Part B: Paper Review

Identity and access management in cloud environment: Mechanisms and challenges [1]

As the name suggests, the paper focuses on Identity and Access Management in various Cloud Environments. The primary aim is to cover the mechanisms and the challenges faced in identity and access management. In the Introduction, the authors explain the different cloud architectures and highlight all the cloud's vulnerabilities. Other types of attacks and data breaches are possible. The authors describe how the vulnerabilities above can be overcome by using IAM, which provides checks Authorization of the users using the cloud services.

The paper also focuses on the Security of the Cloud environment, starting with the Authentication factor. Physical systems like Biometrics and Face Recognition are used to authenticate workers at Data Centres. Along with these, other security mechanisms like credentials, Multifactor Authentication, SSH, Chip and Pin and OAuth are used and further explained in the paper by the authors. The authorization mechanisms are described in great detail in the paper. I can relate to when my friend's Facebook account got hacked because he had used his Facebook email on some untrusted website. The website had asked him for some access permissions, which he did not realize were malicious and could expose his Facebook credentials, causing his account to be easily hacked. The paper depicts a hierarchical map of the Cloud Services Security bifurcated in Authentication, Authorization and Security.

The IAM (Identity Access Management) helps maintain the integrity of the cloud service systems by monitoring the Federated Identity, Policies and even Environments. These services also use various third-party vendors to verify the identity of the users leading to less overload on the cloud infrastructure. The increase in resource availability has created a different number of security issues for the cloud services infrastructure. The authors in the paper have covered various threats and the percentage of their share affecting the cloud infrastructure. The delicate balance in security and data privacy and performance is critical to considering and maintaining a reliable and profitable system.

Below is a list of general attacks described for the cloud infrastructure:

Attack	Description
Man in the Middle	Interception of the Communication Channel
Insider Attack	Malicious Insider person or application being the trigger
Pass/Key Compromise	The hacker gets hold of your credentials
Replay Attack	The hacker uses some older authentication message
Session Cookie Hijack	A valid ongoing session is compromised and stolen from the client
Guessing Attack	The hacker guesses the credentials by either brute-force or by guessing algorithms
Denial of Service (DoS)	A tremendous amount of fake requests overloads the server

Based on the topics covered in the paper, specific recommendations such as using multi-factor authentication, Open ID, Role-based mechanisms and many more could be used to prevent all of the above attacks. The paper infers that the Cloud service infrastructure is a fundamental

concept. To maintain Integrity, Security and Privacy, the IAM services are one of the key pillars of its architecture.

My views on the "Identity and access management in cloud environment: Mechanisms and challenges" paper are that the Cloud Services are integral in shaping digital solutions, bringing down any organization's overall expenditure and operational costs. But adopting Cloud Services has its fair share of threats and difficulties that the organizations need to deal with to protect their operations and data from vulnerabilities. To overcome these vulnerabilities and threats, Cloud Services provides Identity and Access Management mechanisms. The research compares the different topics with their commonly used mechanisms and significant issues associated with each other. The need of the hour is to enhance the Identity and Access Management mechanisms along with the different services offered by the cloud technology. The authors have covered various attacks that could be attempted in the cloud as mentioned above in the table, to get a detailed view of the types of attacks. These attacks emphasize how important it is to have IAM-enabled cloud services to protect user information and company operations. The impact and adoption of the cloud have been quite aggressive, so considering these threats and ways to overcome them is the need of the hour. The improvements are needed as the IAM is mainly CSP-centered which hardly meets users' requirements of flexible and fine-grained access control policy.

References

[1] I. Indu, P. M. Rubesh Anand and V. Bhaskar, "Identity and access management in cloud environment: Mechanisms and challenges" in E*ngineering Science and Technology, an International Journal, Volume 21, Issue 4*, Chennai, India | CA, USA, 2018.