CSCI 5410

Assignment 3 – Part B

Name: Benny Daniel Tharigopala
Banner ID: B00899629

Research Paper Critique

The article - “Identity and access management in cloud environment: Mechanisms and challenges” seeks to address security issues in the Cloud environment and compares existing techniques for identity and access management. It provides a comparison of various identity and access management strategies in a cloud environment, an overview of access management principles and the market's top authentication and session control suite of products and solutions, analysis of security threats in a cloud environment, and recommendations on management policies and standards. In a typical cloud system, businesses or outside providers assist in the processing and storage of data and applications by ensuring that only the appropriate individuals are permitted access to cloud systems, Identity and Access Management (IAM) solutions offer security for cloud services. The paper first introduces the domain of cloud security by providing an overview of the modules which compose Cloud security services, namely, Authentication, Authorization and Security along with their sub-components. Subsequently it articulates each of the sub-components before describing various threats in the Cloud environment and methodologies attackers implement to breach systems hosted on the Cloud. Finally, the paper offers recommendations and lists best practices for implementing secure models and preventing cyber-attacks on the cloud infrastructure [1].

The physical and digital authentication mechanisms discussed in the paper primarily include access cards and biometrics, which deny unauthorized access to resources and facilities, credentials and secure shell keys, which prevent the interception or cracking of passwords and help establish connection to servers without the need for individual passwords for each system, and multifactor authentication, where a secondary layer of authentication takes place in the form of patterns, One-time passwords or security questions. Other digital mechanisms like Single Sign-on (SSO) techniques, open standard authentication protocols (OpenId), mutual authentication (OAuth) and token-based request and response techniques (SAML) are also detailed in the article. SSO techniques allow uninterrupted services by storing one credential for each user while enterprise SSO facilitates the transmission of credentials by encrypted session cookies across web-based applications. OAuth is a great access delegation protocol since it allows users on one website to access users on another without revealing the credentials from an application or website that needs authentication. SAML allows to encrypt and encode data communication between the identity provider and service provider thereby promoting interoperability. Next, Access control mechanisms like Mandatory access control, discretionary access control and role-based access control are elaborated in the paper. These methods implement access rights and policies to determine the privileges of each user and subsequently grant or deny access to resources or services.

Subsequent chapters involve the explanation of Access control governance approaches. Certification is one such approach and is performed by managers, who review and certify the access privileges of the users and resources under their administration. User, Resource, and account certifications are a few examples. Segregation of duties is another approach, and it helps prevent frauds by requiring the participation of two or more persons. It helps avoid intentional frauds and aids in identifying harmless mistakes that may occur during the process workflow. Next the paper describes identity management which guarantees the secure management of credentials, ensures privacy and authenticity of data, and determines whether the authenticated entity is permitted to carry out any operations within a specific application. By regulating each user's access permission, IAM systems lower the hazards related to the cloud environment.

IAM systems offer capabilities for managing passwords, complying with regulations, governing data access, granting access requests, automating provisioning, and Single Sign-On. The paper then lists out the security threats to the cloud environment, including threats to data in motion and rest, malicious software which can access confidential information, cause serious damage to the performance of cloud based systems or cause unavailability of resources or Denial of Service, like Ransomware [2]. Cloud system attacks can range from Insider attacks wherein someone within the security perimeter compromises the system, to guessing attacks where hijackers can regenerate weak passwords by collecting valid information of users. The paper finally recommends best practices such as multifactor authentication mechanisms, role-based access control, identity and account certification, lifecycle management and segregation of duties. It concludes by highlighting the need for enhancements to existing Identity and Access management systems.

To conclude, the paper offers a plethora of information, which is useful especially for novices in the Cloud computing environment. The authors have performed extensive research in the domain of cloud security and have consolidated information from numerous sources. In addition, the summary tables at the end of each chapter present vital information in a concise manner. However, more statistics relevant to cloud security could have been furnished. The paper could have also dwelled on the combination of multiple existing approaches for an enhanced cloud security model. Also, unencountered approaches to cloud security, as discussed in other papers [3], could have been articulated in the paper.

Citations

[1] Indu, I., et al. "Identity and Access Management in Cloud Environment: Mechanisms and Challenges." *Engineering Science and Technology, an International Journal*, vol. 21, no. 4, Aug. 2018, pp. 574–588, www.sciencedirect.com/science/article/pii/S2215098617316750, 10.1016/j.jestch.2018.05.010. Accessed 1 Oct. 2019.

[2] Fruhlinger, Josh. "What Is Ransomware? How These Attacks Work & How to Recover from Them." *CSO Online*, 19 June 2020, www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html. Accessed 20 June 2022.

[3] Juels, Ari, and Alina Oprea. "New Approaches to Security and Availability for Cloud Data." *Communications of the ACM*, vol. 56, no. 2, 1 Feb. 2013, p. 64, 10.1145/2408776.2408793.