Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2021, 8(7):113-117

Research Article ISSN: 2394 - 658X

Cloud Identity and Access Management

Venkata Soma

JetBlue Airlines

ABSTRACT

Cloud-based identity & access management is a strategic solution designed mainly for different cloud-based related operations with many advantages including constructive security mechanisms, swift identity management, and authenticated access controls. It manages the identities of users from provisioning to denial while upholding critical compliance as well as security standards. This study analyses the effective efficient cloud-based identity & access management solutions that ensure compliance, assist scalability, and enhance security in cloud environments. It has been found that through the integration of information technology infrastructures with cloud-based identity & access management, companies can manage compliance with existing regulatory standards. Therefore, it can be concluded that this management system is significant for protecting cloud-based sensitive information.

Keywords: Cloud, Management, System, Organization, Scalability, Artificial Intelligence, Security, Data, and Authentication

INTRODUCTION

Project Specification

The cloud identity and access management system consist of the policies, processes, and tools that safeguard critical resources of the company across cloud platforms & services. This cloud security is important as it lets organizations manage which cloud-based information and applications employees might access [1]. This project mainly concentrates on the constructive integration and analysis of cloud identity and access management systems in a critical cloud infrastructure. It primarily includes deploying and designing a strong identity and access management framework to address security issues, scalability concerns, and compliance requirements.

Aim and Objectives

Aim: This study aims to determine efficient cloud identity and access management solutions that ensure compliance, assist scalability, and enhance security in cloud environments.

Objectives: the objectives of this study are as follows.

- To evaluate the efficiency of advanced identity and access management trends in cloud environments
- To analyze the main functionalities and components of cloud identity and access management
- To contrast identity and access management solutions and determine the best possible practices for integration
- To assess the incorporation of multi-cloud services with identity and access management and its associated effect on security

Research Questions

The questions of this study have arisen from the objectives, which are as follows.

- What is the effectiveness of advanced identity and access management trends in cloud environments?
- What are the main functionalities and components of cloud identity and access management?
- What is the association of identity and access management solutions regarding its best possible practices?
- What is the incorporation of multi-cloud services with identity and access management and what is its associated effect on security?

Research Rationale

Data is kept remotely and accessed over the internet within cloud computing as users can associate with the internet from any device and any location, most of the cloud services are location- and device-agnostic [2]. Furthermore, as companies increasingly operate in cloud environments, therefore making sure secure access to all resources becomes significant. It has been observed that conventional security models are generally lacking in recognizing the cloud infrastructure complexities, where companies span multiple services and platforms [3]. Furthermore, this research intends to offer a constructive comprehension regarding the way companies can use identity and access management in a cloud environment to safeguard sensitive information by managing regulatory compliance while preventing unauthorized access.

LITERATURE REVIEW

Research Background

Identity and access management is a significant cloud service that users must generally pass through to obtain the rest of the cloud infrastructure of the organizations. It can also be employed on the internal network premises of an organization. It has been observed that the fast integration of cloud computing has critically revolutionized infrastructures of information technology by offering flexibility, cost-efficiency, and scalability [4]. Regardless of the benefits, there are also critical security issues, mainly in handling controlling and identity access to sensitive information. The inclination towards cloud-based identity and access management solutions is guided by the requirement for scalable, adaptive, and centralized access management mechanisms that execute across diverse cloud services.

Critical Assessment

Cloud-based access and identity management solutions typically address significant components, for instance, resources, roles, members, groups, and permissions. It offers more protection compared to its conventional counterpart [5]. It supervises access across different platforms while minimizing insider threats by offering seamless offboarding, onboarding, and role changes. Organizations can contract and expand their usage as per their requirements which makes cloud-based identity and access management cost-effective compared to on-prem solutions [6]. Contrarily, it has been observed that companies generally encounter issues regarding configuration permission at the time of shifting to cloud-based identity and access management.

Linking with Aim

This study primarily seeks to determine efficient cloud identity and access management solutions that ensure compliance, assist scalability, and enhance security in cloud environments. It also intends to define critical areas for innovation and improvement by evaluating the limitations of the present cloud-based identity and access management model while analyzing the incorporation of technologies for instance machine learning and artificial intelligence. In the meantime, it also explored the possibility of emerging cloud-based identity and access management technologies to offer more adaptive access control mechanisms.

Encapsulation of Applications

There has been a major burst in this competitive market with advanced applications and the need for the organization to utilize these modern applications has enhanced drastically. This cloud-based technology can be utilized to capture, initiate, manage, and record user identities with their access permissions. All the users are authorized, evaluated, and authenticated as per the roles & policies [7]. Conversely, it has been observed that poor execution of identity and access management might guide non-compliance to regulations; when the company is audited, the responsible management might not be capable of justifying that its sensitive data is risk-free.

Theoretical Framework

The integration of cloud-based identity and access management can be understood through the applications of theories. In the context of this, the control theory mainly concentrates on the way of system regulation to accomplish stability and manage desired performance regardless of any external disturbances. This theory can help to understand the regulation of identity and access management to cloud services by making sure that solely authorized users can access services or data [8]. This significant theory goes with the requirement for automated responses to protection breachers, the requirement for real-time, and modification of access control depending on user behavior. Furthermore, a role-based access control model can be used to comprehend the management of identities and access right within cloud systems.

Literature Gap

There are still significant gaps within the existing literature regardless of advancements within cloud-based identity and access management. The gap mainly concerns the efficiency and integration of identity and access management solutions within hybrid & multi-cloud environments. Furthermore, it is evident that there is a critical gap in the thorough analysis analyzing the influence of machine learning and artificial intelligence in this cloud-based mechanism, mainly regarding algorithm fairness, privacy concerns, and interpretability [9]. This study intends to abridge the identified gaps with critical analysis regarding the integration of cloud-based identity and access management system.

METHODOLOGY

Research Philosophy

Research philosophy is an important part of proposing prime beliefs and assumptions regarding the subject matter. It is a significant methodological paradigm that supervises the type of information to be assessed and collected to justify the research objectives. Determination of a related research philosophy based on the knowledge to be gained from the research as its managers the ways to objectify the ascertained benefits [10]. Moreover, the interpretivism research philosophy has been used here which mainly concentrates on illustrating defined research components by maximizing associated theories. The reason behind the selection of this philosophy lies in its focus on gathering qualitative information which is supported by theories.

Research Approach

Research approaches are important procedures utilized to analyze the related steps for conducting interpretation, assessment, and collection of necessary data. Based on the determined approaches, the process of information collection, interpretation, and analysis can be identified [11]. The prime admiration of the research approach is to supervise systematic procedures which can guide the directions of the methodology in the study. Here, the inductive research approach has been selected to maximize the critical patterns which helps to collect needed data. The utilization of the inductive approach has assisted in connecting models and theories by which information has been arranged to accomplish stated objectives.

Research Design

The notion of research design relates to the achievement of study plans and designs by arranging gathered data in a particular manner. It is a constructive process of methodology that assists in generating practical answers to the research questions on the subject matter [12]. It permits in establishment of critical processes which can fulfil objectives & aims by assisting the data analysis process. This study has integrated the explanatory research design that seeks to find out the main reason, results, and associated results behind the presence of a particular error by analyzing it critically which can impact existing data. This selected research design has assisted in gathering needed information and arrange in different segments by compiling defined objectives.

Data Collection Method

The data collection process can be viewed as an inclusive strategy that helps in collecting needed data from various resources. It is a significant systematic process that makes sure better accuracy, adaptiveness, and quality of the collected data in a definite manner by which framed research objectives can be accomplished [13]. The secondary qualitative method of data collection has been used in this study which also assisted in analyzing data collected from existing resources on the subject matter [14]. This method of data collection has assisted in collecting needed information from relevant articles, online journals, publishing, news, and others.

Ethical Consideration

Appropriate ethical considerations have been maintained due to the integration of the identified methodological process. To gather relevant information, significant secondary resources have been used which have swift access and help to meet the stated objectives. E-books, articles, online journals, and other related sources published before 2021 have been used to gather up-to-date data which assist the critical research outcomes.

RESULTS

Critical Analysis

It has been evident that cybercriminals are becoming smarter in their approach to stealing data, breach networks, and utilizing ransomware to cause havoc. Cloud-based identity and access management is a significant security framework employed within the cloud which is utilized to confirm users and monitor their rights of access including denying and issuing access privileges [15]. It has been observed that nearly 15 billion stolen information permitting account takeovers which are accessible on the dark web with password and username pairs for social media accounts, services regarding music streaming, and online banking [16]. In this context, cloud-based identity and access management permits organizations or individuals to confirm users no matter where they are and also secure access to sensitive resources across the cloud, all the while enhancing agility, effectiveness and speed. Therefore, it can be stated that the critical analysis of this advanced mechanism exhibits that while it permits strategic improvements in handling cloud resource access, efficiency is critically associated with the ongoing management and configuration of the system.

Findings and Discussion

Theme 1: Incorporation of cloud-based identity and access management with legacy systems

Cloud-based identity and access management are fundamental for businesses steering the complications of cloud-dependent various operations. Although, incorporating this mechanism with present legacy systems poses a critical challenge [17]. The critical findings from the existing studies highlight that legacy systems typically lack the needed standards for swift integration which causes unforeseen security gaps and manual intervention. It also highlights the significance of executing and planning a phased incorporation approach where critical legacy systems are typically replaced or modernized.

Theme 2: Role-based access control configuration for cloud-based identity and access management

Role-based access control systems control actions and access the role of the individual in the system. In this context, cloud-based identity and access management are significant services and tools designed to supervise digital identities as well as control access of users to various cloud-bound sources. Its prime objective is to assist the company manage access to services, data, and applications within the cloud with comprehensive authorization & authentication protocols [18]. Businesses can use this to enhance their security, manage identities, and ease the pathways of user access across cloud environments. Although, it has been observed that inappropriate configuration regarding role-based access control is a common problem which guides to either insufficient or excessive access rights.

Theme 3: Continual auditing and monitoring of the mechanism

Effective audit procedures offer reporting abilities with management and operational dashboards for identity and access management in cloud environments. This offers information technology auditors the capability to comprehend risks, assess existing issues, establish control, and take required actions. Instances of such control are entitlement creep, orphaned accounts, and visibility into sensitive user accounts. It has been observed that companies sometimes underestimate the significance of real-time management which is indeed for responding and detecting to policy violations and unauthorized access [19]. From the findings of this study, it can be discussed that routine audits of identity and access management policies assist in determining unforeseen security loopholes while managing compliance.

Evaluation

Cloud-based identity and access management can utilise cloud-native automation and architecture to accommodate shifts within resource demands, access requirements, and resource demands [20]. Although, the assessment of this system depending on the findings of this study exhibits that while it improves the operational and security effectiveness, its actual success critically relies on ongoing management and meticulous implementation.

CONCLUSION

In conclusion, cloud-based identity and access management provides organizations with a cost-effective intervention for verifying the identities of users and permitting them access to solely the resources they need. It also supervises access rights, for instance, denying rights to ex-employees or providing access to new employees. In the meantime, it has been found that this system permits security and information technology teams to manage access to the sources within their cloud environments.

RESEARCH RECOMMENDATIONS

It can be recommended from the above findings and discussion.

I. Organizations must incorporate zero-trust security models that scrutinize the authenticity of every device and user until proven.

II. It is important to perform routine audits of this mechanism practice to makes sure compliance with changing regulatory standards.

III. There must be a concentration on incorporating machine learning and artificial intelligence with cloud-based identity and access management to authorize adaptive authentication systems.

FUTURE WORK

Later studies must concentrate on creating cloud-based identity & access management which is controlled by artificial intelligence and able to immediately adaptive access management while identifying any threat. Furthermore, future studies must analyze the incorporation of cloud-based identity & access management with blockchain technology to improve transparency and security.

REFERENCES

[1]. I. A. Mohammed, "Cloud identity and access management–a model proposal," *International Journal of Innovations in Engineering Research and Technology*, vol. 6, no. 10, pp. 1-8, 2019. Available: https://www.researchgate.net/profile/Ishaq-Azhar-Mohammed/publication/353887567_CLOUD_IDENTITY_AND_ACCESS_MANAGEMENT_-_A_MODEL_PROPOSAL/links/61169d070c2bfa282a41f553/CLOUD-IDENTITY-AND-ACCESS-MANAGEMENT-A-MODEL-PROPOSAL.pdf

[2]. I. Indu, P. R. 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. Available: https://www.sciencedirect.com/science/article/pii/S2215098617316750

[3]. C. Anilkumar and S. Sumathy, "Security strategies for cloud identity management—A study," *International Journal of Engineering & Technology*, vol. 7, no. 2, pp. 732-741, 2018. Available: https://www.researchgate.net/profile/Anilkumar-Chunduru-

2/publication/327032449_Security_strategies_for_cloud_identity_management_-_a_study/links/64ed16d59b1cb33d732c64c9/Security-strategies-for-cloud-identity-management-a-study.pdf

[4]. I. A. Mohammed, "Systematic review of identity access management in information security," *International Journal of Innovations in Engineering Research and Technology*, vol. 4, no. 7, pp. 1-7, 2017. Available: https://www.researchgate.net/profile/Ishaq-Azhar-Mohammed/publication/353887659_SYSTEMATIC_REVIEW_OF_IDENTITY_ACCESS_MANAGEMENT_IN_INFORMATION_SECURITY/links/61169c5d1ca20f6f861e4496/SYSTEMATIC-REVIEW-OF-IDENTITY-ACCESS-MANAGEMENT-IN-INFORMATION-SECURITY.pdf

[5]. Y. Ren, F. Zhu, J. Qi, J. Wang, and A. K. Sangaiah, "Identity management and access control based on blockchain under edge computing for the industrial internet of things," *Applied Sciences*, vol. 9, no. 10, p. 2058, 2019. Available: https://www.mdpi.com/2076-3417/9/10/2058

[6]. L. Wu, S. Zhou, Z. Zhou, Z. Hong, and K. Huang, "A Reputation-Based Identity Management Model for Cloud Computing," *Mathematical Problems in Engineering*, vol. 2015, p. 238245, 2015. Available: https://onlinelibrary.wiley.com/doi/abs/10.1155/2015/238245

[7]. H. Graupner, K. Torkura, P. Berger, C. Meinel, and M. Schnjakin, "Secure access control for multi-cloud resources," in *2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops)*, Oct. 2015, pp. 722-729. Available: https://ieeexplore.ieee.org/abstract/document/7365920/

[8]. B. P. Gajendra and V. K. Singh, "Achieving cloud security using third party auditor, MD5 and identity-based encryption," in *2016 International Conference on Computing, Communication and Automation (ICCCA)*, Apr. 2016, pp. 1304-1309. Available: https://ieeexplore.ieee.org/abstract/document/7813920/

[9]. C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, and K. Yu, "AuthPrivacyChain: A blockchain-based access control framework with privacy protection in cloud," *IEEE Access*, vol. 8, pp. 70604-70615, 2020. Available: https://ieeexplore.ieee.org/abstract/document/9057456/

[10]. H. Snyder, "Literature review as a research methodology: An overview and guidelines," *Journal of Business Research*, vol. 104, pp. 333-339, 2019. Available: https://www.sciencedirect.com/science/article/pii/S0148296319304564

[11]. M. Patel and N. Patel, "Exploring research methodology," *International Journal of Research and Review*, vol. 6, no. 3, pp. 48-55, 2019. Available: https://www.academia.edu/download/63543152/IJRR001120200605-115829-bxlrli.pdf

[12]. J. Zangirolami-Raimundo, J. de Oliveira Echeimberg, and C. Leone, "Research methodology topics: Cross-sectional studies," *Journal of Human Growth and Development*, vol. 28, no. 3, pp. 356-360, 2018. Available: https://www.revistas.usp.br/jhgd/article/view/152198

[13]. M. Al Kilani and V. Kobziev, "An overview of research methodology in information system (IS)," *Open Access Library Journal*, vol. 3, no. 11, pp. 1-9, 2016. Available: https://www.scirp.org/journal/paperinformation.aspx?paperid=71775

[14]. N. Greening, "Phenomenological research methodology," *Scientific Research Journal*, vol. 7, no. 5, pp. 88-92, 2019. Available: https://www.academia.edu/download/109046401/v7.i5.2019.pdf

[15]. Z. Yan, X. Li, M. Wang, and A. V. Vasilakos, "Flexible data access control based on trust and reputation in cloud computing," *IEEE Transactions on Cloud Computing*, vol. 5, no. 3, pp. 485-498, 2015. Available: https://ieeexplore.ieee.org/abstract/document/7208817/

[16]. K. Xue, Y. Xue, J. Hong, W. Li, H. Yue, D. S. Wei, and P. Hong, "RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 4, pp. 953-967, 2017. Available: https://ieeexplore.ieee.org/abstract/document/7803573/

[17]. S. A. Chaudhry, K. Yahya, F. Al-Turjman, and M. H. Yang, "A secure and reliable device access control scheme for IoT based sensor cloud systems," *IEEE Access*, vol. 8, pp. 139244-139254, 2020. Available: https://ieeexplore.ieee.org/abstract/document/9149883/

[18]. R. Belchior, B. Putz, G. Pernul, M. Correia, A. Vasconcelos, and S. Guerreiro, "SSIBAC: Self-sovereign identity based access control," in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Dec. 2020, pp. 1935-1943. IEEE. Available: https://ieeexplore.ieee.org/abstract/document/9343033/

[19]. N. Naik and P. Jenkins, "uPort open-source identity management system: An assessment of self-sovereign identity and user-centric data platform built on blockchain," in *2020 IEEE International Symposium on Systems Engineering (ISSE)*, Oct. 2020, pp. 1-7. IEEE. Available: https://ieeexplore.ieee.org/abstract/document/9272223/

[20]. M. Akarapu, S. Martha, K. R. Donthamala, B. Prashanth, G. Sunil, and K. Mahender, "Checking for Identity-Based Remote Data Integrity Cloud Storage with Perfect Data Privacy," in *IOP Conference Series: Materials Science and Engineering*, vol. 981, no. 2, p. 022034, Dec. 2020. IOP Publishing. Available: https://iopscience.iop.org/article/10.1088/1757-899X/981/2/022034/meta