International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cloud Access Security Brokers: Strengthening Cloud Security

Latika Kharb and Deepak Chahal

Professor, Jagan Institute of Management Studies, Sector-5, Rohini, Delhi-110085, India
latika.kharb@jimsindia.org

DOI: https://doi.org/10.55248/gengpi.4.823.50412

ABSTRACT

As organizations increasingly migrate their applications and data to the cloud, the need for robust cloud security solutions becomes paramount. Cloud Access Security Brokers (CASBs) have emerged as a vital component in ensuring the secure and compliant adoption of cloud services. This paper provides an in-depth exploration of Cloud Access Security Brokers, their architecture, features, benefits, and challenges. By analysing CASBs' role in enhancing cloud security, this paper aims to demonstrate their importance in safeguarding sensitive information and mitigating risks associated with cloud-based operations.

Keywords: Cloud access, security brokers, risks, data breaches, security tool.

1. Introduction

The rapid expansion of cloud computing has revolutionized the way businesses operate and manage their data. However, this digital transformation has also introduced numerous security challenges related to data breaches, unauthorized access, and compliance violations. Cloud service providers offer some built-in security features, but many enterprises require an additional layer of security control. Cloud Access Security Brokers have emerged as a critical solution to bridge the security gap between cloud services and organizations' security policies.

2. Understanding Cloud Access Security Brokers (CASBs)

A Cloud Access Security Broker (CASB) is a security tool or service that acts as an intermediary between cloud service users and cloud service providers. CASBs are designed to enforce security policies, monitor activities, and extend security controls over cloud-based applications. They provide a unified approach to address security challenges associated with cloud adoption, enabling organizations to maintain visibility, compliance, and data protection.

CASB Architecture

CASBs typically operate through two main deployment models:

- API-based CASBs: These CASBs integrate with cloud services through their application programming interfaces (APIs). By using APIs, CASBs can gain visibility into cloud activities, enforce security policies, and analyze data without requiring any on-premises hardware or software.
- Proxy-based CASBs: These CASBs act as a proxy or gateway between users and cloud services. Traffic between users and the cloud is routed through the CASB, allowing it to inspect, control, and secure data in real-time. Proxy-based CASBs may require configuration changes or the installation of agents on users' devices.

Key Features of CASBs

CASBs offer a wide range of security features to address different aspects of cloud security, including:

- Data Loss Prevention (DLP): CASBs scan data in real-time, identifying and preventing the sharing or storage of sensitive information outside the organization's defined policies.
- User and Entity Behavior Analytics (UEBA): By monitoring user behavior, CASBs can detect unusual activities that may indicate potential security threats or insider attacks.
- Encryption and Tokenization: CASBs can encrypt data before it is uploaded to the cloud and store the encryption keys separately, enhancing data protection.

- Access Control and Authentication: CASBs enforce multi-factor authentication (MFA) and other access control measures to ensure authorized access to cloud services.
- Shadow IT Discovery: CASBs identify unauthorized cloud applications and services being used within an organization, allowing IT administrators to take appropriate action.
- Compliance Monitoring: CASBs assess cloud services for compliance with industry standards and regulatory requirements, helping organizations maintain data privacy and meet legal obligations.

3. Benefits of CASBs

The adoption of CASBs provides numerous benefits for organizations:

Enhanced Cloud Security

CASBs enable organizations to extend their security policies and controls to cloud services, reducing the risk of data breaches and unauthorized access. The real-time monitoring and threat detection capabilities of CASBs contribute to the early identification and mitigation of security incidents.

Increased Visibility and Control

CASBs offer comprehensive visibility into cloud activities, giving organizations insights into data usage, user behavior, and potential security gaps. This visibility empowers IT administrators to make informed decisions and take proactive measures.

Compliance and Data Governance

With CASBs, organizations can enforce consistent security policies across different cloud services, ensuring compliance with regulations and industry standards. CASBs facilitate data governance by helping organizations classify and protect sensitive data appropriately.

Protection against Insider Threats

CASBs' user and entity behavior analytics capabilities can detect unusual activities and unauthorized access attempts, mitigating the risk of insider threats and data leaks.

4. Challenges and Considerations

While CASBs offer significant advantages, organizations should be aware of certain challenges and considerations:

Performance Impact

Proxy-based CASBs may introduce latency due to the additional traffic routing. Careful consideration and testing are necessary to ensure minimal impact on user experience.

Data Privacy Concerns

As CASBs intercept and analyze data, organizations must ensure that sensitive information is appropriately handled and not exposed to any security risks.

Integration Complexity

API-based CASBs may require complex integration with various cloud services, necessitating expertise in cloud security and integration.

5. Conclusion

Cloud Access Security Brokers play a vital role in enabling secure cloud adoption for organizations. By providing enhanced security, improved visibility, and compliance enforcement, CASBs serve as a crucial component in the overall cloud security strategy. As the cloud landscape continues to evolve, CASBs are expected to adapt and innovate to meet emerging security challenges, further solidifying their position as a cornerstone of cloud security.

References

[1] Alawadhi, S., & Ali, N. M. (2020). Cloud Access Security Brokers: An Overview and Comparative Study. International Journal of Advanced Computer Science and Applications, 11(12), 108-113.

[2] Chauhan, A., & Singh, V. (2019). A Comprehensive Survey on Cloud Access Security Broker (CASB) Services and Architecture. International Journal of Advanced Research in Computer Science, 10(3), 142-149.

[3] Singh, P., Chahal, D., & Kharb, L. (2020). Predictive strength of selected classification algorithms for diagnosis of liver disease. In Proceedings of ICRIC 2019: Recent Innovations in Computing (pp. 239-255). Springer International Publishing.

[4] Chahal, D., & Kharb, L. (2019). Smart diagnosis of orthopaedic disorders using internet of things (IoT). Int. J. Eng. Adv. Technol, 8, 215-220.

[5] Duggal, S., & Goyal, D. (2018). Cloud Access Security Broker (CASB) and Its Role in Enhancing Cloud Security. International Journal of Computer Applications, 179(40), 1-6.

[6] Chahal, L. D., Kharb, L., Bhardwaj, A., & Singla, D. (2018). A Comprehensive Study of Security in Cloud Computing. International Journal of Engineering & Technology, 7(4), 3897-3901.

[7] Gulati, R., & Bhatia, V. (2019). Cloud Access Security Broker (CASB): A Review. International Journal of Computer Applications, 182(8), 37-41.

[8] Kshetri, N., & Voas, J. (2019). Cloud Access Security Brokers (CASBs) and Security-as-a-Service (SECaaS) for Small and Medium-Sized Enterprises (SMEs). International Journal of Information Management, 46, 259-270.

[9] Menezes, R., & Rao, K. (2018). Cloud Access Security Broker: A Comprehensive Review. International Journal of Computer Sciences and Engineering, 6(7), 239-244.

[10] Kharb, L. (2017). Exploration of social networks with visualization tools. American Journal of Engineering Research (AJER), 6(3), 90-93.

[11] Latika, M. (2011). Software component complexity measurement through proposed integration metrics. Journal of Global Research in Computer Science, 2(6), 13-15.

[12] Singh, R., Singh, P., Chahal, D., & Kharb, L. (2021). “VISIO”: An IoT Device for Assistance of Visually Challenged. In Advances in Electromechanical Technologies: Select Proceedings of TEMT 2019 (pp. 949-964). Springer Singapore.

[13]Nandi, A., & Nath, S. (2020). Enhancing Cloud Security with Cloud Access Security Brokers. International Journal of Advanced Science and Technology, 29(10), 3405-3414.

[14] Rehman, S., Li, J., & Rehman, N. U. (2019). Security and Privacy Challenges of Cloud Access Security Brokers. In Proceedings of the 3rd International Conference on Cloud and Big Data Computing (CBDCom) (pp. 1-6). IEEE.

[15] Kharb, L. (2015). Moving Ahead in Future with Drones: The UA V’s (Unmanned Aerial Vehicle). Journal of Network Communications and Emerging Technologies (JNCET) www. jncet. org, 4(3).

[16] Kharb, L., & Sukic, E. (2015). An agent based software approach towards building complex systems. tEM Journal, 4(3), 287.

[17] Chahal, D., Kharb, L., & Gupta, M. (2017). Challenges and security issues of NoSQL databases. Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol, 2(5), 976-982.

[18] Kharb, L. (2019). Implementing IoT and Data Analytics To Overcome" Vehicles Danger. International Journal of Innovative Technology and Exploring Engineering, 8(11).

[19] Sonowal, G., Sharma, A., & Kharb, L. (2021). Spear-Phishing Emails Verification Method based on Verifiable Secret Sharing Scheme. Journal of Information Assurance & Security, 16(3).

[20] Kharb, L., & Kaur, S. Embedding Intelligence through Cognitive Services. International Journal for Research in Applied Science & Engineering Technology (IJRASET), ISSN, 2321-9653.

[21] Wang, J., & Wen, Q. (2018). A Survey of Cloud Access Security Brokers: Concepts, Architectures, and Challenges. Journal of Network and Computer Applications, 113, 41-54.

[22] Saini, A., Singh, Y., & Gahlot, R. (2021). Cloud Access Security Brokers: A Review and Future Directions. In Proceedings of the 2nd International Conference on Advanced Computational and Communication Paradigms (ICACCP) (pp. 31-36). Springer, Singapore.