IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 13, Issue 2, April-May 2025
ISSN: 2320 – 8791 (Impact Factor: 2.317)
www.ijreat.org

Intrusion Detection System for Identity Access Management via Hashing over Cloud Platform

Yashini P[1], Divya A[2], Neikesha D[3], Ponmaniraj S[4] and Soundhariya S[5]

[1] **Department of Artificial Intelligence and Data Science, DMI College of Engineering, Chennai, Tamil Nadu 600123, India**
yashinipatchamal@gmail.com

[2] **Department of Artificial Intelligence and Data Science, DMI College of Engineering, Chennai, Tamil Nadu 600123, India**
akshu.bharathi93@gmail.com

[3] **Department of Artificial Intelligence and Data Science, DMI College of Engineering, Chennai, Tamil Nadu 600123, India**
neikeshadhakshna@gmail.com

[4] **Department of Computational Intelligence, Saveetha School of Engineering, SIMATS, Chennai, Tamil Nadu 600123, India**
ponmaniraj@gmail.com

[5] **Department of Information Technology, DMI College of Engineering, Chennai, Tamil Nadu 600123, India**
soundhariya0493@gmail.com

Abstract

With the growth of cloud computing, data and application security have emerged as top concerns. Cloud security solutions offer elastic protection against cyber-attacks such as unauthorized access, data leakage, and malware. This paper delves into prominent challenges and solutions in securing the cloud, namely cloud access security brokers (CASBs), cloud-based firewalls, and encryption, with reference to their strengths and weaknesses. It also considers how identity and access management (IAM) fits into cloud security, pointing to best practices like multi-factor authentication, access control, and robust encryption. The paper further offers a case study of a cloud security solution, illustrating how it can thwart attacks and maintain compliance. Finally, this paper emphasizes the necessity of cloud security in contemporary cybersecurity measures and gives recommendations to organizations looking to secure their cloud applications and data.

Keywords: *IDS, Cloud, Network attacks, Authentication, CASB, IAM.*

1. Introduction

Cloud security is the practice of protecting cloud- based applications, data, and infrastructure from unauthorized access, theft, and other cyber threats. With the increasing adoption of cloud computing, cloud security has become an increasingly critical concern for organizations of all sizes and industries. Cloud security involves a range of technologies, processes, and best practices that are designed to protect against a wide range of threats, including malware, data breaches, denial-of-service attacks, and other types of cyber-attacks. Some of the key challenges associated with cloud security include ensuring the confidentiality, integrity, and availability of cloud-based resources, as well as maintaining compliance with regulatory requirements [1].

Cloud security solutions include a wide range of tools and technologies, such as cloud access security brokers (CASBs), cloud-based firewalls, and cloud-based encryption, as well as identity and access management (IAM) solutions, network security tools, and threat intelligence solutions [2]. Effective cloud security requires a holistic approach that includes both preventative and responsive measures, as well as ongoing monitoring and management of cloud-based resources.

In this context, it is essential for organizations to implement a robust and comprehensive cloud security strategy that takes into account their unique security requirements, risk profile, and compliance obligations [3]. By adopting the right cloud security tools and best practices, organizations can help ensure the security and privacy of their cloud-based applications and data, while reducing the risk of cyber-attacks and other security incidents.

2. Survey on Cloud Security

Cloud computing refers to the delivery of on-demand computing resources over the internet, including applications, data storage, and computing power, without requiring the user to have direct control over the underlying infrastructure. In cloud computing, the service provider is responsible for managing the underlying infrastructure, including hardware, software, and network resources, while the user can access these resources through a web browser or other client interface [4].

Cloud computing is typically organized into three service models: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). IaaS provides the user with access to basic computing resources, such as servers, storage, and networking, which can be used to build and deploy applications. PaaS provides a more complete development and deployment environment, including application frameworks and middleware. SaaS provides the user with access to complete applications, such as email, customer relationship management (CRM), and enterprise resource planning (ERP) software [5, 6].

Some of the key security challenges in cloud computing include securing data at rest and in transit, securing cloud infrastructure, controlling access to cloud resources, and ensuring compliance with regulatory requirements. To address these challenges, cloud security measures typically include firewalls, intrusion detection and prevention systems, encryption, access controls, vulnerability management, and threat intelligence [7].

Cloud service providers (CSPs) also have a role to play in ensuring the security of cloud environments. They typically offer a range of security features, such as data encryption, multi-factor authentication, and network segmentation, and are responsible for managing and maintaining the underlying cloud infrastructure [8]. However, it is ultimately the responsibility of the cloud customer to implement appropriate security measures and controls to protect their data and applications in the cloud.

Cloud security solutions can be provided by third-party vendors, including cloud access security brokers (CASBs) that provide additional security controls and monitoring of cloud environments. Additionally, security standards and frameworks such as ISO 27001, NIST Cybersecurity Framework, and Cloud Security Alliance's Cloud Controls Matrix can provide guidance for organizations to assess and enhance the security of their cloud environments [9].

3. Cloud Based Security Architecture

A cloud-based security architecture typically consists of multiple layers of security controls designed to protect data, applications, and infrastructure in the cloud. These layers may include:

1. Perimeter security: This layer provides the first line of defense for a cloud environment and typically includes firewalls, intrusion detection and prevention systems (IDPS), and other security appliances that protect the network from external threats.
2. Identity and access management (IAM): This layer controls access to cloud resources and typically includes authentication and authorization mechanisms, such as multi-factor authentication and role-based access controls.
3. Data security: This layer protects data stored in the cloud from unauthorized access, disclosure, or modification. Data security controls may include encryption, data loss prevention (DLP) tools, and backup and recovery mechanisms.
4. Application security: This layer secures the applications running in the cloud, including web applications, mobile apps, and APIs. Application security controls may include vulnerability scanning, web application firewalls, and secure coding practices.
5. Infrastructure security: This layer protects the underlying cloud infrastructure, including servers, storage, and networking resources. Infrastructure security controls may include patch management, network segmentation, and virtualization security.

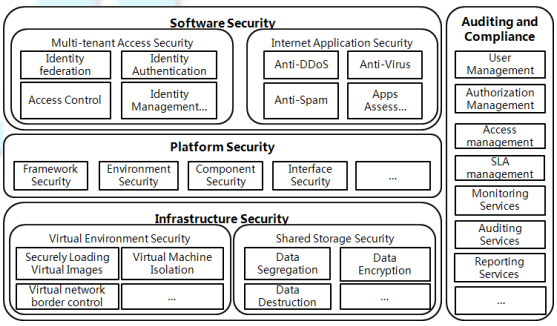

Fig 1 Cloud based intrusion detection system architecture.

6. Monitoring and response: This layer provides continuous monitoring of cloud resources for security threats and anomalies. Monitoring tools may include security information and event management (SIEM)

systems and threat intelligence platforms. In the event of a security incident, this layer also includes incident response and recovery mechanisms.

In addition to these layers, a cloud-based security architecture may also include compliance and governance controls, such as auditing and reporting tools, to ensure that the cloud environment is in compliance with applicable regulatory requirements.

4. Procedure to Implement Cloud Security

A cloud security program typically consists of the following steps:

1. Define security requirements: Identify the security requirements of the cloud environment, taking into account the data, applications, and infrastructure that will be stored and processed in the cloud.
2. Perform risk assessment: Conduct a risk assessment to identify potential security threats and vulnerabilities, and prioritize the risks based on their likelihood and impact.
3. Develop security policies and procedures: Develop security policies and procedures that address the identified risks and provide guidance on how to secure the cloud environment.
4. Implement security controls: Implement security controls to address the risks and comply with the security policies and procedures. This may include deploying firewalls, access controls, encryption, and other security technologies.
5. Train and educate users: Train and educate users on the security policies and procedures, and provide guidance on how to securely use the cloud environment.
6. Monitor and audit: Continuously monitor the cloud environment for security threats and anomalies, and conduct periodic security audits to ensure compliance with security policies and procedures.
7. Respond to incidents: Establish incident response procedures and prepare for security incidents, including identifying the incident response team, defining the roles and responsibilities, and developing a communication plan.
8. Test and improve: Regularly test the security controls and procedures to ensure they are effective, and continuously improve the security program based on the results of the testing and incidents that occur.

By following these steps, organizations can establish a comprehensive cloud security program that addresses the unique security risks and requirements of their particular cloud environment.

5. Result on Cloud Security Implementation

The results of implementing a comprehensive cloud security program can be significant. By following the steps outlined in the program, organizations can achieve several benefits, including:

1. Reduced risk of security breaches: A well-designed cloud security program can help organizations to identify and mitigate potential security risks, reducing the likelihood of security breaches.
2. Improved compliance: Compliance with security and privacy regulations is essential for organizations, and a comprehensive cloud security program can help organizations to achieve and maintain compliance.
3. Increased user confidence: When organizations prioritize cloud security, users can have greater confidence that their data is being handled and stored securely, which can lead to increased trust and adoption of cloud services.
4. Cost savings: By implementing appropriate security measures, organizations can avoid costly data breaches and other security incidents, which can result in significant financial losses.
5. Continuous improvement: A cloud security program should be an ongoing process that includes regular monitoring, testing, and improvement. By continuously improving the security program, organizations can stay ahead of emerging threats and ensure that their security measures remain effective.

It is important to note that the implementation of a comprehensive cloud security program is not a one-time event, but an ongoing process. Organizations should regularly review and update their security policies and procedures to address emerging threats and changes in the cloud environment [10]. By doing so, organizations can ensure the continued protection of their data and infrastructure, and maintain the trust of their users and stakeholders.

6. Conclusion

Cloud security is a critical aspect of cloud computing that organizations must prioritize to protect their data, applications, and infrastructure from cyber threats. A well-designed cloud security program can help organizations to identify and mitigate risks, implement security controls, train and educate users, monitor and audit for security threats, respond to incidents, and continuously improve the security program.

References

[1] D. D. Kshirsagar, D. K. Tagad, S. S. Sale, and G. Khandagale, "Network Intrusion Detection based on Attack Pattern," in *IEEE International Conference on Emerging Trends in Engineering and Technology (ICECTECH)*, 2011, doi:10.1109/ICECTECH.2011.5942003.

[2] M. Grimmer, M. M. Röhling, D. Kreusel, and S. Ganz, "A modern and sophisticated host-based intrusion detection data set," *IT-Sicherheit als Voraussetzung für eine erfolgreiche Digitalisierung*, vol. 11, 2019, pp. 135-145.

[3] M. Pendleton and S. Xu, "A dataset generator for next-generation system call host intrusion detection systems," in *Proceedings of IEEE Military Communications Conference (MILCOM)*, 2017.

[4] S. M. AL-Ghuribi and S. Alshomrani, "Bi-languages Mining Algorithm for Extraction Useful Web Contents (BiLEx)," *Arab Journal of Science and Engineering*, vol. 40, 2015, pp. 501-518. doi:10.1007/s13369-014-1530-8.

[5] N. Kushmerick, D. S. Weld, and R. Doorenbos, "Wrapper Induction for Information Extraction," in *Proceedings of the International Joint Conference on Artificial Intelligence (IJCAI)*, 1997.

[6] A. K. Tripathy, N. Joshi, S. Thomas, S. Shetty, and N. Thomas, "VEDD - A visual wrapper for extraction of data using DOM tree," in *International Conference on Communication, Information & Computing Technology (ICCICT)*, 2012, pp. 1-6.

[7] Q. P. Abdul Rasool and Memon, "Hybrid model of content extraction," *Journal of Computer Science and Systems*, vol. 11, 2012, pp. 135-145.

[8] H. A. Tariq, W. Yang, I. Hameed, B. Ahmed, and R. U. Khan, "Using Black-List and White-List Technique to Detect Malicious URLs," *International Journal of Innovative Research in Information Security*, vol. IV, 2017, pp. 1-7. doi:10.26562/IJIRIS.2017.DCIS10081.

[9] A. K. Jain and B. B. Gupta, "A novel approach to protect against phishing attacks at client-side using auto-updated white-list," *Springer*, 2016. doi:10.1186/s13635-016-0034-3.

[10] T. Karthikeyan, K. Sekaran, D. Ranjith, V. Vinoth Kumar, and J. M. Balajee, "Personalized Content Extraction and Text Classification Using Effective Web Scraping Techniques," *International Journal of Web Portals*, vol. 11, no. 2, 2019, pp. 41–52. doi:10.4018/ijwp.2019070103.

IJREAT
PRDG