DOI: 10.2507/35th.daaam.proceedings.xxx

SECURITY PRINCIPLES IN CLOUD COMPUTING

Damir Josic, Matej Basic*, Luka Zgrablic

This Publication has to be referred as: Josic, D[amir]; Basic, M[atej] & Zgrablic, L[uka] (2024). Security Principles in Cloud Computing, Proceedings of the 35th DAAAM International Symposium, pp.xxxx-xxxx, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-xx-x, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/35th.daaam.proceedings.xxx

Abstract

This paper provides a comprehensive overview of cloud security principles, highlighting the critical areas of data confidentiality, identity security, access controls, and the role of monitoring and event logging in maintaining secure cloud environments. It addresses organizations' everyday challenges, such as improper identity and access management, insecure APIs, and potential unauthorized access risks. The discussion includes detailed strategies for mitigating these issues, such as implementing robust authentication protocols, network segmentation, continuous security assessments, and robust employee training programs. The paper also highlights the importance of multifactor authentication (MFA) and the innovative use of passwordless authentication to enhance security and user experience. It explores using SIEM (Security Information and Event Management) and SOAR (Security Orchestration Automation and Response) technologies to bolster cybersecurity through real-time analysis and automated incident response.

Keywords: cloud security; data confidentiality; Multi-Factor Authentication; identity security; Security Information and Event Management; Security Orchestration Automation and Response; network segmentation; passwordless authentication.

1. Introduction

Many businesses are adopting cloud computing for its flexibility and growth potential. However, this comes with challenges in maintaining data security. This paper will explain cloud security principles, focusing on data privacy, ensuring authorized access, and using tools to monitor for potential issues. When companies use the cloud, they must protect their critical information. It's not solely the cloud service provider's job; it is a shared responsibility. In discussing data security in the cloud, one must consider the challenges of ensuring that only the right people have access to data and the potential risks involved.

This paper aims to present these challenges to readers and demonstrate ways to enhance their cloud security. It will explore strategies for managing access permissions, implementing advanced security tools, and the importance of real-time monitoring. The following sections will delve into critical areas such as Identity and Access Management (IAM), the importance of data privacy, and the necessity of monitoring security events as businesses navigate the complexities of cloud security.

2. Important Cloud Security Concepts

As cloud computing becomes an increasingly popular choice for organizations, they face various challenges concerning data, identity, architecture security, and more. One of the primary challenges for organizations is taking accountability for their data. Users must manage access controls, implement best security practices, and monitor what is happening within their organizations and with their data. Many cloud security threats can be mitigated using proper configurations, correct security settings, cloud-native authentication protections, and various other security features [1]. Cloud security is an evolving sub-domain of computer security, encompassing network security and information security. It involves a broad set of policies, technologies, and controls to protect data, applications, and the associated cloud computing infrastructure. Users must ensure proper measures are in place to prevent unauthorized access, which can be achieved through data encryption, access controls, and regular monitoring.

In the following sections, this paper will focus on access controls, data security, and identity security, using multifactor authentication to manage identity security. It will also explore the importance of event logging and how event-driven security can help detect, mitigate, and improve the overall security of cloud computing.

2.1. Access Controls and Identity Management in Cloud Environments

Access controls are implemented through an access management system that includes identity and credential management. These systems utilize various tools and policies to manage and define access to valuable resources such as data, systems, or physical assets. Effective access management is crucial to protecting these resources from unauthorized access. Familiar IAM (Identity and Access Management) challenges in cloud environments include improper provisioning or de-provisioning of services and users, maintaining inactive assigned users, managing numerous admin accounts, and users bypassing IAM controls. Implementing role-based access controls can also be challenging. Best practices to address IAM challenges in the cloud include developing governance strategies for identity management and using central directory services like Microsoft Active Directory to facilitate the provisioning, auditing, and de-provisioning of accounts.

All SaaS (Software as a Service) applications should support single sign-on (SSO) technology, requiring users to authenticate through SSO to ensure secure access. Organizations often need help safely and effectively providing employees access to systems and data. Access request management systems can help overcome these challenges, ensuring the organization operates securely and efficiently [2][3]. Unauthorized access often occurs for several reasons, including weak authentication mechanisms, insider threats, insecure APIs, insufficient access controls, and social engineering or phishing attacks. To mitigate these and other unwanted scenarios, organizations should consider the following strategies:

- Strong Authentication and Access Controls: Implement robust authentication mechanisms and stringent access controls to ensure only authorized users can access cloud resources [2][3].
- Network Segmentation and Firewalls: Implement firewall controls for both inbound and outbound traffic, segment critical resources, and allow only authorized communication [2][3].
- Continuous Security Assessments: Perform regular security assessments to identify and address any improper access controls or configurations that could result in unauthorized access.
- Employee Training: Educate employees about security best practices, the risks associated with data breaches, and the importance of following security policies and procedures to prevent unauthorized access [2][3].

These strategies can help organizations protect their cloud resources from unauthorized access and other security threats. Effective access control and identity management are critical to maintaining the security and integrity of cloud environments.

2.2. Identity Security and Multifactor Authentication

Identity security in the cloud encompasses measures, policies, actions, and mechanisms to protect user and service account identities. This includes ensuring that only authorized users can access specific resources while maintaining the confidentiality and integrity of user and company data. Since cloud computing relies on the Internet to deliver services and resources, it is vulnerable to numerous security threats. Therefore, identity security in the cloud is essential for protecting users, company data, and other valuable resources.

To significantly reduce security risks, several policies can be implemented, including:

- Using strong and unique passwords for accounts and enabling multifactor authentication (MFA), especially for privileged accounts. This makes it significantly harder for attackers to gain unauthorized access [4].
- Allowing access to cloud accounts only through HTTPS and VPN. This ensures that data is encrypted during transmission, protecting it from interception [2].

- Regularly reviewing and updating security controls and settings in cloud accounts. This helps identify and mitigate vulnerabilities in real time [5].
- Monitor cloud accounts for any unusual activity and investigate immediately if any occur. Continuous monitoring allows quick detection and response to potential security breaches [6].
- Staying informed about the latest security threats and best practices for managing identity security in the cloud. Keeping up-to-date with new threats and defenses is crucial for maintaining robust security [7].

Multifactor authentication (MFA) is a core component of a strong identity and access management policy. MFA requires one or more verification factors, significantly decreasing the possibility of a successful cyber-attack. By requiring users to provide multiple verification factors, MFA minimizes the potential for unauthorized access. Common authentication factors used in MFA include OTP (one-time passwords) generated by authenticator apps, software tokens, SMS-based passwords, physical USB tokens, and biometric authentication such as facial or fingerprint recognition. Less secure methods include personal security questions [7]. Implementing more secure methods and multifactor authentication makes it more challenging for unauthorized individuals to gain access to systems. MFA is also crucial in resisting brute-force attacks, phishing attacks, and other cyber-attacks. This extra layer of security operates on the principle that a user must present a username and password, approve the login using something they have (e.g., a phone), and provide something they are (e.g., fingerprint or facial recognition). Additional factors include time and location, where the time factor expects actions within an established time frame, and the location factor verifies if the user logs in from a known location [2].

Passwordless authentication is another method to enhance user security and simplify IT operations by eliminating the need to store, maintain, and rotate passwords. This method allows users to access applications or systems without entering a password, instead providing another form of evidence such as fingerprint, facial recognition, or hardware token code. It is often used alongside SSO to improve the user experience [5].

2.3. Data Security

As mentioned earlier, the Internet-based or public cloud model implies that data is transmitted over the Internet. Data losses or leakages can severely impact an organization's reputation and lead to legal consequences. Therefore, data storage in remote data centers must be done with the utmost care. Key data security challenges include maintaining confidentiality, integrity, locality, etc. Classifying and treating confidential data appropriately is crucial to protect it from various attacks, such as cross-site scripting. Implementing robust encryption methods alongside access controls and monitoring suspicious activities is essential. Data should be encrypted both while stored ("data at rest") and while being transmitted ("data in transit"). Encrypting data during transmission prevents eavesdropping and unauthorized interception, while at rest, encryption ensures data protection even if physical storage media are compromised [4][2].

Maintaining data integrity is also vital to prevent data loss. Only authorized personnel should be able to modify the data, ensuring that unauthorized persons keep digital information unaltered. This guarantees that data is kept private, consistent, safe, and complete throughout its lifecycle [5][6]. Data locality is another significant challenge for organizations and cloud service providers. Data distributed across various regions can lead to compliance issues due to differing laws and regulations governing data. As data moves across different zones, the applicable laws may change, causing potential customer compliance issues. Data replication or backups for business continuity and disaster recovery can further complicate these issues [7].

2.4. Monitoring and Event Logging

Monitoring and event logging is crucial for IT teams to understand what is happening within their infrastructure. Significant actions or occurrences, known as events, can originate from networks, servers, firewalls, databases, operating systems, hardware infrastructures, or other sources. Event logging and monitoring are essential for auditing, compliance, security, troubleshooting, and alerting. Organizations can recognize unusual activity and improve security by monitoring environment traffic. Organizations address risks by setting up monitoring, logging, and alerting configurations to enhance cloud infrastructures' security, performance, and management, allowing security incidents to be detected before valuable data is stolen. Cloud monitoring encompasses a set of strategies and practices that will enable organizations to analyze, manage, and monitor the health, security, performance, and availability of their infrastructures and applications. It allows organizations to identify and address vulnerabilities or issues, preventing them from impacting business or end users. Regular audits through cloud monitoring ensure security standards and regulatory compliance. Common cloud monitoring solutions include virtual network monitoring, machine monitoring, application performance monitoring, security and compliance monitoring, website monitoring, database monitoring, storage monitoring, and many others [1].

Some benefits of cloud monitoring include:

- Improving the security of cloud applications and networks.

- Enhancing service or application availability and performance due to quick issue reporting and solutions.
- Avoiding unexpected cloud costs.
- Usability on multiple devices.

SIEM (Security Information and Event Management) analyzes security alerts generated by resources such as applications, networks, and servers [8]. Its essential functions are:

- Log collection – SIEM collects logs and event data from various sources.
- Data correlation and analysis – SIEM correlates data to identify patterns, anomalies, and security incidents.
- Alerts – SIEM generates alerts based on activities or events that may indicate a security threat.
- Compliance reporting – SIEM supports compliance efforts by providing reports based on security events and activities.

SIEM benefits include forensic analysis, threat detection, centralized visibility, and compliance management, making detecting, managing, and responding to security events easier [8]. SOAR (Security Orchestration, Automation, and Response) complements SIEM by focusing on task automation and incident response [8]. SOAR aims to automate security operations, identify specific events or threats in advance, and eliminate them through automated responses based on predefined workflows. This approach is known as a triggered outcome. SOAR can isolate infected systems, block malicious IP addresses, and deliver consistent and standardized responses [3]. SIEM and SOAR are often integrated to create comprehensive cybersecurity ecosystems [8]. SIEM allows for initial correlation and anomaly detection based on analyzed data, while SOAR automates and orchestrates the response. This combined approach enhances infrastructure security by enabling quicker and more efficient incident response.

5. Future Works

Future studies could explore the integration of artificial intelligence (AI) with Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) systems to enhance threat detection capabilities and automate responses more effectively. This integration could leverage machine learning models to detect anomalies and predict potential security threats in real time, thus improving overall cybersecurity posture. Improving multifactor authentication (MFA) is another vital area for future research. New forms of MFA that are secure and user-friendly, such as advanced facial recognition, behavioral biometrics, and wearable technology for authentication, should be investigated. Additionally, the impact of these technologies on user experience and security should be evaluated to ensure they balance usability and protection.

6. Conclusion

One significant challenge for organizations is taking accountability for their data and configurations. Users must manage access controls, implement best security practices, and oversee their organizations' and information systems' activities. Access control is managed through systems that use identity and identification information, incorporating various tools and principles to safeguard critical resources, such as data, systems, and physical assets. A centralized directory service, like Microsoft Active Directory, is recommended to facilitate accounting, auditing, and de-provisioning, ensuring centralized control and visibility.

To mitigate undesirable scenarios, organizations should consider the following strategies:

- Strong Authentication and Access Control Measures: Ensure cloud resources are accessed only by authorized users.
- Network Segmentation and Firewalls: Implement firewalls for inbound and outbound traffic, segment critical resources, and permit only authorized communications.
- Continuous Security Assessments: Conduct security assessments regularly to identify and rectify any improper access control measures or configurations that could lead to unauthorized access.
- Employee Training: Educate employees on information security best practices, the risks of security breaches due to unauthorized access, their role in preventing breaches, and the importance of adhering to security policies and procedures.

Identity security in the cloud involves all measures, practices, operations, and mechanisms implemented to protect the identity of user and service accounts. Multifactor authentication (MFA) is a critical component of a strong identity and access control policy, requiring additional authentication factors that significantly reduce the likelihood of successful cyber-attacks. Implementing secure methods and MFA makes it more challenging for unauthorized individuals to access systems. MFA is also crucial in combating brute-force attacks, phishing attacks, and other cyber threats. Passwordless authentication can further enhance user security and streamline IT operations by eliminating the need for password management. Data loss or leakage can severely impact an organization's reputation and have legal consequences. Data stored in remote data centers must be handled carefully, using robust encryption methods, access controls, and monitoring

for suspicious activities. Data should be encrypted at rest and in transit to prevent unauthorized access and ensure data integrity. Only authorized personnel should be able to modify data to avoid data loss.

Monitoring and event logging are vital for IT teams to understand the activities within their infrastructure. Significant activities or events, considered as events, can originate from various sources, including networks, servers, firewalls, databases, operating systems, and hardware infrastructures. Cloud monitoring involves strategies and practices that allow organizations to analyze, manage, and monitor their infrastructures and applications' health, security, performance, and availability. SIEM systems collect, correlate, and analyze generated data and events, providing real-time analysis and alerts based on potential security threats. SOAR systems complement SIEM by focusing on task automation and incident response, aiming to eliminate threats through automated responses based on predefined workflows. By integrating SIEM and SOAR, organizations can create comprehensive cybersecurity ecosystems that enhance infrastructure security through quicker and more efficient incident response.

7. References

[1] Singh, U.; Tiwari, A. & Sharma, S. (2020). Data Security in Cloud Computing, International Journal of Engineering Applied Sciences and Technology, Published by IJEAST , Vol. 4, No. 10, pp.170-173., ISSN 2455-2143, Rajasthan, India. DOI: 10.33564/IJEAST.2020.v04i10.033, in press.

[2] Dakić, V., & Ribarić, S. (2020). Judicial and Technical Improvement of General Data Protection Regulation, Proceedings of the 31st International DAAAM Symposium 2020, pp.0189-0196, Published by DAAAM International, ISBN 978-3-902734-29-7, ISSN 1726-9679, Vienna, Austria. DOI: 10.2507/31st.daaam.proceedings.025, in press.

[3] Dakić, V., Zaharinov, V., & Nikolov, S. (2020). Linux Security in Physical, Virtual, and Cloud Environments, Proceedings of the 33rd International DAAAM Symposium 2022, pp.0151-0160, Published by DAAAM International, ISBN 978-3-902734-36-5, ISSN 1726-9679, Vienna, Austria. DOI: DOI: 10.2507/33rd.daaam.proceedings.021, in press.

[4] Morić, Z., Branstett, L., & Petrunić, R. (2023). Rust and Webassembly for Fast, Secure, and Reliable Software. Proceedings of the 33rd DAAAM International Symposium, pp.0165-0171, Published by DAAAM International, ISBN 978-3-902734-36-5, ISSN 1726-9679, Vienna, Austria. DOI: 10.2507/33rd.daaam.proceedings.023, in press.

[5] Reithner, I.; Papa, M.; Lueger, B. & Cato, M. (2020). Development and Implementation of a Secure Production Network, Proceedings of the 31st DAAAM International Symposium, pp.0736-0745, Published by DAAAM International, ISBN 978-3-902734-29-7, ISSN 1726-9679, Vienna, Austria. DOI: 10.2507/31st.daaam.proceedings.102, in press.

[6] Blahová, M.; Mikuličová, M. & Hromada, M. (2020). Utilization of Fractal Geometry Possibilities for Information Systems Security, Proceedings of the 31st DAAAM International Symposium, pp.0619-0625, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-29-7, ISSN 1726-9679, Vienna, Austria. DOI: 10.2507/31st.daaam.proceedings.085, in press.

[7] Radinger, T.; Stuja, K.; Wölfel, W. & Markl, E. (2017). Functional Safety Concept for a Handling Robot Built on Optical Systems, Proceedings of the 28th DAAAM International Symposium, pp.0168-0172, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-11-2, ISSN 1726-9679, Vienna, Austria. DOI: 10.2507/28th.daaam.proceedings.022, in press.

[8] Babu, L.D.D.; Krishna, P.V.; Zayan, A.M. & Panda, V. (2011). An Analysis of Security Related Issues in Cloud Computing, Proceedings of the Contemporary Computing - 4th International Conference, IC3 2011, Communications in Computer and Information Science, Published by Springer, Vol. 168, ISBN 978-3-642-22606-9, Berlin, Germany. DOI: 10.1007/978-3-642-22606-9_21, in press.