DOI: 10.2507/35th.daaam.proceedings.028

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.0210-0215, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-44-0, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/35th.daaam.proceedings.028

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.

1. Introduction

Cloud computing has developed as a revolutionary technology, altering how corporations store, analyse, and manage data. It provides scalable resources, cost-effectiveness, and adaptability, enabling enterprises to adjust to evolving requirements. Nevertheless, these benefits are accompanied by considerable security challenges. The centralised structure of cloud services and the substantial volumes of data they manage render them a prime target for hackers. Maintaining data security, integrity, and availability is crucial for sustaining trust and promoting the broader adoption of cloud computing. This article examines essential security principles in cloud systems, concentrating on important aspects such as data encryption, identity and access management, and multi-factor authentication. Additionally, it analyses the significance of monitoring and event logging in improving cloud security. It addresses developing trends in applying Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) systems for real-time threat mitigation. 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 increasingly popular for organisations, they face various challenges concerning data, identity, architecture security, and more. One of the primary challenges for organisations is taking accountability for their data. Users must manage access controls, implement best security practices, and monitor what is happening within their organisations 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 computing security encompasses multiple layers, including infrastructure, data encryption, and identity management. A fundamental problem is data security, encompassing hazards such as data breaches and illegal access [2]. Numerous firms use encryption to guarantee data security, integrity, and availability. A multi-tiered encryption framework employing hybrid cryptographic methods, including RSA and Data Encryption Standard (DES), enhances security by implementing encryption at both user and server levels, substantially mitigating the risk of data breaches [3]. Alternative encryption techniques, such as attribute-based encryption (ABE) and proxy re-encryption (PRE), enhance the security of data exchange and storage across diverse settings [4]. A significant area for improvement in cloud security is data privacy, which is stored in shared environments. In public cloud installations with shared resources, safeguarding privacy becomes increasingly complex, necessitating sophisticated access controls and encryption technologies. Privacy-preserving methodologies, such as multi-factor authentication (MFA) and secure critical management systems, assist in mitigating concerns [5]. Cloud security also involves addressing vulnerabilities in Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) models. A prominent issue in IaaS and SaaS deployments is unauthorised access through weak authentication systems. Robust identity and access management solutions have been proposed to address these concerns, including federated identity systems and biometric authentication [6]. However, the challenge of securing virtual machines (VMs) against attacks like hyperjacking remains, as malicious users can exploit vulnerabilities in the hypervisor [7].

Implementing hybrid cloud models, which integrate public and private cloud environments, presents other security concerns, such as adhering to data protection rules and maintaining cross-cloud data integrity. Researchers have proposed alternatives to solve these difficulties, including end-to-end encryption and decentralised trust models [8]. Notwithstanding progress in cloud security technologies, human factors, including an inadequate understanding of security best practices, remain a substantial obstacle. Enhanced user knowledge, training, and improved governance norms can mitigate cloud security concerns [9].

This paper will focus on access controls, data security, and identity security in the following sections, 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 utilise 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 unauthorised 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. Organisations often need help safely and effectively providing employees access to systems and data. Access request management systems can help overcome these challenges, ensuring the organisation operates securely and efficiently [10][11]. Unauthorised 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, organisations should consider the following strategies:

- Strong Authentication and Access Controls: Implement robust authentication mechanisms and stringent access controls to ensure only authorised users can access cloud resources [10][11].
- Network Segmentation and Firewalls: Implement firewall controls for both inbound and outbound traffic, segment critical resources, and allow only authorised communication [10][11].
- Continuous Security Assessments: Perform regular security assessments to identify and address any improper access controls or configurations that could result in unauthorised 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 unauthorised access [10][11].

These strategies can help organisations protect their cloud resources from unauthorised 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 authorised 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 unauthorised access [12].
- Allowing access to cloud accounts only through HTTPS and VPN. This ensures that data is encrypted during transmission, protecting it from interception [10].
- Regularly reviewing and updating security controls and settings in cloud accounts. This helps identify and mitigate vulnerabilities in real-time [13].
- Monitor cloud accounts for any unusual activity and investigate immediately if any occur. Continuous monitoring allows quick detection and response to potential security breaches [14].
- 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 defences is crucial for maintaining robust security [15].

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 minimises the potential for unauthorised 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 [15]. Implementing more secure methods and multifactor authentication makes it more challenging for unauthorised 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 [10]. 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 organisation’s reputation and lead to legal consequences. Therefore, data storage in remote data centres 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 unauthorised interception, while at rest, encryption ensures data protection even if physical storage media are compromised [10][12].

Maintaining data integrity is also vital to prevent data loss. Only authorised personnel should be able to modify the data, ensuring that unauthorised persons keep digital information unaltered. This guarantees that data is kept private, consistent, safe, and complete throughout its lifecycle [13][14]. Data locality is another significant challenge for organisations 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 [15].

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. Organisations can recognise unusual activity and improve security by monitoring environmental traffic.

Organisations 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 organisations to analyse, manage, and monitor the health, security, performance, and availability of their infrastructures and applications. It allows organisations 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. Modern 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) analyses security alerts generated by resources such as applications, networks, and servers [16]. 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, centralised visibility, and compliance management, making detecting, managing, and responding to security events easier [16]. SOAR (Security Orchestration, Automation, and Response) complements SIEM by focusing on task automation and incident response [16]. 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 standardised responses [11]. SIEM and SOAR are often integrated to create comprehensive cybersecurity ecosystems [16]. SIEM allows for initial correlation and anomaly detection based on analysed data, while SOAR automates and orchestrates the response. This combined approach enhances infrastructure security by enabling quicker and more efficient incident response.

3. Future Works

Future research in cloud security is increasingly focused on advancing Zero Trust Architecture (ZTA), which guarantees that no user or device is automatically trusted, whether inside or external to the network. ZTA necessitates additional scrutiny to enhance authentication, access control, and the execution of detailed security policies. Integrating with sophisticated Security Information and Event Management and Security Orchestration, Automation, and Response systems is essential for improving real-time threat detection and automated incident response capabilities. These technologies facilitate expedited response times and enhance risk mitigation, yet their use in multi-cloud setups necessitates optimisation and scalability enhancements.

Artificial Intelligence (AI) and Machine Learning (ML) are essential in forecasting, identifying, and addressing cloud-based threats. Research should concentrate on creating more adaptive and intelligent models capable of detecting sophisticated attacks, including those employing adversarial strategies, while maintaining resource efficiency. Nonetheless, AI-driven solutions have problems regarding transparency and interpretability, requiring further research to ensure these systems are both successful and comprehensible.

Another area of research is the integration of homomorphic encryption and secure multi-party computation (SMPC), which could allow cloud services to process encrypted data without exposing sensitive information. These cryptographic methods hold promise but remain computationally expensive and challenging to scale for large cloud environments, requiring further optimisation.

Further research is needed in data privacy compliance, particularly in global cloud ecosystems where varying regional regulations, such as GDPR, CCPA, and new laws, continually evolve. More research is needed on developing privacy-preserving techniques that seamlessly comply with these regulations across borders, ensuring robust protection of user data while maintaining operational efficiency. Quantum computing is emerging as a potential threat to traditional encryption schemes, necessitating research into post-quantum cryptography. As quantum computers become more viable, securing cloud infrastructures against potential future quantum attacks is essential to avoid catastrophic data breaches.

Moreover, compliance with and enhancement of cloud security standards established by the National Institute of Standards and Technology (NIST) is essential. The NIST framework remains a fundamental resource, especially in risk management and incident response. Future research should investigate the alignment of upcoming technologies, such as AI, quantum computing, and edge computing, with NIST's growing standards to enhance cloud security.

4. Conclusion

One significant challenge for organisations is taking accountability for their data and configurations. Users must manage access controls, implement best security practices, and oversee their organisations' 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 centralised directory service, like Microsoft Active Directory, is recommended to facilitate accounting, auditing, and de-provisioning, ensuring centralised control and visibility.

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

- Strong Authentication and Access Control Measures: Ensure cloud resources are accessed only by authorised users.
- Network Segmentation and Firewalls: Implement firewalls for inbound and outbound traffic, segment critical resources, and permit only authorised communications.
- Continuous Security Assessments: Conduct security assessments regularly to identify and rectify any improper access control measures or configurations that could lead to unauthorised access.
- Employee Training: Educate employees on information security best practices, the risks of security breaches due to unauthorised 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 accessing systems more challenging for unauthorised individuals. 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 organisation's reputation and have legal consequences. Data stored in remote data centres 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 unauthorised access and ensure data integrity. Only authorised 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 organisations to analyse, manage, and monitor their infrastructures and applications' health, security, performance, and availability. SIEM systems collect, correlate, and analyse 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, organisations can create comprehensive cybersecurity ecosystems that enhance infrastructure security through quicker and more efficient incident response.

5. 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] Miryala, N. K.; & Gupta, D. (2019) Security in Cloud Computing, 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), pp. 599-604, IEEE, DOI: 10.17148/ijarcce.2019.81225.

[3] Kumar, S.; Karnani, G.; Gaur, M. S. & Mishra, A. (2021) Cloud Security using Hybrid Cryptography Algorithms, 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM). IEEE, Apr. 28, 2021. doi: 10.1109/iciem51511.2021.9445377.

[4] Sun, P. (2020). Security and Privacy Protection in Cloud Computing: Discussions and Challenges. Journal of Network and Computer Applications, Vol. 160, pp. 102642. ISSN 1084-8045, DOI: 10.1016/j.jnca.2020.102642.

[5] Cherviakova, T. (2020). Information Security of Cloud Computing Technology. The National Transport University Bulletin, ISSN 2308-6645, DOI: 10.33744/2308-6645-2020-1-46-427-436.

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

[7] Zunnurhain, K., & Vrbsky, S. V. (2023). Security in Cloud Computing. International Research Journal of Modernization in Engineering Technology and Science. DOI: 10.56726/irjmets45986.

[8] Seth, B., Dalal, S., Jaglan, V., Le, D. N., Mohan, S., & Srivastava, G. (2020). Integrating Encryption Techniques for Secure Data Storage in the Cloud. Transactions on Emerging Telecommunications Technologies, Vol. 33, DOI: 10.1002/ett.4108.

[9] Alenezi, M. (2021). Safeguarding Cloud Computing Infrastructure: A Security Analysis. Computer Systems Science and Engineering, DOI: 10.32604/csse.2021.015282.

[10] 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.

[11] Dakić, V., Jakobović K., Žgrablić L. (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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.