Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 07, NCIRTAI - 2026

Survey on Cloud Data Security Challenges with Solutions

Mrs. R. Meena[1]
Assistant Professor, Department of Computer Science and Engineering,
Sri Bharathi Engineering College for Women,
Kaikkurichi, Pudukkottai.
r.meena.cse.90@gmail.com[1]

Abstract

Cloud computing has become an integral part of modern IT infrastructure, offering organizations scalable, flexible, and cost efficient solutions for data storage and processing. This survey investigates the key challenges in cloud data security and reviews contemporary solutions to mitigate these risks. Techniques such as advanced encryption, multi factor authentication, access control mechanisms and AI&ML driven threat detection are analyzed for their effectiveness in protecting data confidentiality, integrity, and availability. Additionally compliance management strategies are explored to address regulatory requirements in multi cloud and hybrid environments. By examining these challenges and solutions, the survey provides a comprehensive overview for organizations to implement robust cloud security frameworks, ensuring safe and reliable utilization of cloud services while maintaining operational efficiency.

I. INTRODUCTION

Cloud computing has revolutionized the way organizations store, process, and manage data by providing scalable, flexible, and cost-efficient computing resources over the internet. While it offers significant benefits such as on-demand access, reduced hardware costs, and enhanced collaboration, it also introduces critical security challenges. Protecting sensitive data in cloud environments has become a top priority as businesses increasingly rely on multi-cloud and hybrid infrastructures.

Cloud data security challenges arise from several factors, including unauthorized access, data breaches, insider threats, insecure APIs and compliance requirements. Additionally emerging technologies such as Artificial Intelligence (AI) and Machine Learning (ML) introduce new risks like model theft, prompt injection and Shadow AI. These challenges can compromise data confidentiality, integrity and availability if not addressed effectively. This survey aims to explore the key cloud data security challenges and examine practical solutions including encryption techniques, access control mechanisms, AI driven threat detection and compliance management strategies. By understanding these challenges and their solutions, organizations can develop robust security frameworks that safeguard data while enabling the benefits of cloud computing.

Fig.No:1 Cloud Computing Security Challenges

Principles of information security

Data Confidentiality: Ensures that data is accessed or modified only by authorized users or processes, keeping sensitive information private.

Data Integrity: Guarantees that data remains accurate, authentic, and reliable. Measures are implemented to prevent unauthorized modifications, tampering, or deletion.

Data Availability: Ensures that authorized users can access data when needed. Systems, networks, and devices must maintain continuous uptime for uninterrupted access.

Benefits of Cloud Data Security

Enhanced Visibility: Strong security practices provide clear insight into your cloud environment, including what data exists, where it is stored, who accesses it, and how it is being used.

Simplified Backups and Recovery: Cloud security solutions automate and standardize backup processes, reducing the need for manual monitoring. Disaster recovery capabilities allow rapid restoration of data and applications, minimizing downtime.

Regulatory Compliance: Robust cloud security frameworks help organizations meet compliance

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 07, NCIRTAI - 2026

requirements by tracking data storage, access, processing, and protection measures. Data Loss Prevention (DLP) tools enable discovery, classification, and de-identification of sensitive information to mitigate the risk of violations.

II. CLOUD DATA SECURITY THREATS

Data Breaches

Data breaches in cloud environments typically occur due to misconfigurations, weak access controls, or insufficient encryption, which expose sensitive information to unauthorized parties. Unlike traditional on-premise breaches, cloud breaches involve a shared responsibility model, where both the provider and the user must ensure security. Improper storage or transmission of data can allow attackers to access confidential information, potentially leading to financial losses, regulatory penalties, and reputational damage, particularly because cloud services often hold vast amounts of critical data across global locations.

Account Hijacking

Account hijacking happens when attackers gain unauthorized access to cloud accounts by exploiting stolen or weak credentials. Due to the centralized nature of cloud platforms, a compromised account can provide extensive control over cloud resources, enabling data manipulation, malware deployment, or fraudulent activities. Attackers may also escalate privileges, exposing additional sensitive systems, applications, or data repositories across the cloud.

Insecure APIs

Application Programming Interfaces (APIs) enable software systems to communicate. If APIs are not secured properly, they can become entry points for cyber-attacks, granting unauthorized access to cloud services and data.

Denial of Service (DoS) Attacks

In a cloud setting, DoS attacks overwhelm services such as applications, websites, or APIs with excessive traffic, making them unavailable to legitimate users. These attacks can disrupt critical business operations, degrade user experience, and result in substantial financial losses due to prolonged downtime.

Insider Threats

Not all security risks originate externally. Employees or contractors with legitimate access can accidentally or intentionally compromise cloud security by mishandling data or abusing privileges, leading to breaches or unauthorized disclosures.

Misconfigurations

Misconfigured cloud resources such as storage buckets, databases, or virtual machines are a frequent and serious risk. Examples include publicly accessible storage, disabled encryption, or incorrectly set identity and access management (IAM) policies. These misconfigurations expose data and infrastructure to unauthorized access, making them prime targets for attackers.

Weak Identity and Access Management (IAM)

Inadequate IAM practices create vulnerabilities in cloud security. Effective IAM defines user roles, permissions, and authentication protocols. Weak practices, such as insufficient role-based access controls, missing multi-factor authentication (MFA), or not enforcing least-privilege principles, can leave critical cloud resources exposed. APTs are sophisticated, long-term attacks where adversaries infiltrate cloud environments and remain undetected for months or even years. Unlike standard attacks, APTs are designed for stealth, enabling attackers to gather sensitive data or compromise systems over time.

Cloud Resource Hijacking

Cloud resource hijacking occurs when attackers exploit vulnerabilities to gain control of computing resources for their own purposes, such as cryptocurrency mining, launching DDoS attacks, or hosting illicit content. Due to the elastic nature of cloud environments, attackers can covertly use significant computational power without immediate detection.

III. CLOUD SECURITY SOLUTIONS

SentinelOne

SentinelOne provides an autonomous, AI-driven cybersecurity platform designed for advanced threat detection and protection. Its comprehensive Cloud-Native Application Protection Platform (CNAPP) delivers holistic security, supporting both internal and external cloud audits. SentinelOne offers agentless and agent-based vulnerability assessments, with its patented **Storylines** technology reconstructing historical events for detailed analysis. The **Purple AI** feature acts as a generative AI cybersecurity analyst, providing contextual insights after analyzing threat intelligence.

Check Point CloudGuard

Check Point CloudGuard enables organizations to evaluate and manage their cloud security posture with a simple interface. It supports scaling for growing businesses and dynamic cloud environments, ensuring protection against evolving threats. It is particularly useful for organizations transitioning from traditional IT setups or migrating between cloud providers.

Wiz

Wiz provides security for cloud assets across hybrid and multi-cloud ecosystems. It offers visibility into databases with sensitive data, detects excessive administrative privileges, blocks critical attack paths, and continuously monitors and remediates cloud threats to maintain a secure posture.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 07, NCIRTAI - 2026

Tenable Cloud Security

Tenable Cloud Security focuses on safeguarding cloud workloads by monitoring threats and identifying vulnerabilities before they escalate. It helps organizations enforce compliance policies, assess regulatory adherence, and adapt to dynamic cloud environments, offering customizable security controls for evolving infrastructures.

CrowdStrike Falcon

CrowdStrike Falcon is a CNAPP solution that strengthens cloud security strategies by connecting to cloud ecosystems, identifying risks, and remediating threats. It protects against misconfigurations, secures data, prevents API exposures, and mitigates potential security incidents across multi-cloud environments.

Aqua Security

Aqua Security is a specialized security platform designed for containerized applications and cloud native environments. It provides comprehensive protection for Kubernetes, Docker and serverless workloads. The platform emphasizes runtime security, vulnerability management, and compliance enforcement, enabling organizations to deploy scalable applications securely. Aqua Security integrates seamlessly with CI/CD pipelines and DevSecOps workflows, offering proactive threat detection and mitigation without disrupting development processes. It is widely adopted by enterprises to maintain robust security while supporting agile and continuous deployment practices.

IV. CONCLUSION

Selecting the right cloud security solution is a critical and nuanced decision that depends on the unique requirements of an organization. Key considerations include understanding the type and sensitivity of the data being protected, evaluating the business model to match security needs with organizational scale, and ensuring compliance with relevant regulations such as HIPAA or GDPR. Additionally, scalability is essential an effective cloud security solution should be able to grow alongside the organization, allowing the addition of advanced security features as demands evolve. By carefully assessing these factors, organizations can implement a cloud security strategy that protects data, supports business growth, and ensures long term resilience in dynamic cloud environments.

REFERENCES

[1] Mohamed Magdy Mosbah, “Current Services in Cloud Computing: A Survey ,” International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.3,No.5,October 2013

[2] Armbrust, M. et. al., (2009), “Above the clouds: A Berkeley view of Cloud Computing”, UC Berkeley EECS, Feb 2010.

[3] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., “Scientific Cloud Computing: Early Definition and Experience,” 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.

[4] B. R. Kandukuri, R. Paturi V, A. Rakshit, “Cloud Security Issues”, In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009

[5] National Institute of Standards and Technology, NIST Definition of Cloud Computing, Sept 2011.

[6] D. Jamil and H. Zaki, “Security Issues in Cloud Computing and Countermeasures,” International Journal of Engineering Science and Technology, Vol. 3 No. 4, pp. 2672-2676, April 2011 http://www.infoworld.com/article/3041078

[7] Rittinghouse JW, Ransome JF: Security in the Cloud. In Cloud Computing. Implementation, Management, and Security, CRC Press; 2009.

[8] Garfinkel T, Rosenblum M: When virtual is harder than real: Security challenges in virtual machine based computing environments. In Proceedings of the 10th conference on Hot Topics in Operating Systems, Santa Fe, NM. volume 10. CA, USA: USENIX Association Berkeley; 2005:227–229.

[9] Wayne A. Pauley, “Cloud Provider Transparency – An empirical evaluation”, the IEEE computer and reliability societies, IEEE, November 2010, pp: 32 – 39.

[10] Cong Wang, Ning Cao, Kui Ren, Wenjing Lou, “Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data”, IEEE transactions on parallel and distributed systems, IEEE, Digital Object Indentifier 10.1109/TPDS.2011.282, 2011, pp: 1 – 14.

[11] Rosa Sánchez, Florina Almenares, Patricia Arias, Daniel Díaz-Sánchez and Andrés Marín, “Enhancing Privacy and Dynamic Federationn IdM for Consumer Cloud Computing”, IEEE Transactions on Consumer Electronics, Vol. 58, No. 1, February 2012, pp: 95 – 10.