Journal of Science Research International (JSRI)
ISSN: 2456-6365 (Online)

OPEN ACCESS

CLOUD COMPUTING SECURITY: CHALLENGES AND SOLUTIONS

Anuradha Singh*, Chirag Chavan,

Omkar Jadhav, Atharv Fakke and Harsh Dubey

Department of Computer Science,

Pillai College of Arts, Commerce and Science (Empowered Autonomous), New Panvel

**Corresponding author E-mail: anuradhasingh@mes.ac.in*

Received: 21 January 2026	Revised: 17 February 2026	Accepted: 20 March 2026	Published: 13 April 2026

DOI: **https://doi.org/10.5281/zenodo.19555707**

Abstract:

Cloud computing has become an essential technology that enables organizations and individuals to store, manage, and process data through internet-based services rather than relying on local infrastructure. It offers significant advantages including scalability, cost savings, and convenient access to data from distributed locations. However, storing information on remote cloud servers also introduces a variety of security concerns that require systematic attention (1,2). Typical security threats in cloud environments include data breaches, unauthorized access, malware attacks, denial-of-service incidents, and insecure application interfaces. These threats can result in data leakage, service interruptions, and exposure of confidential information. Since cloud systems operate over shared networks, implementing strong security mechanisms is both necessary and challenging (3). This study explores the major security challenges in cloud computing and the protection mechanisms used to safeguard cloud data. Techniques such as encryption, access control mechanisms, multi-factor authentication, intrusion detection systems, and continuous monitoring tools play critical roles in maintaining security. Applying effective protection strategies helps ensure the confidentiality, integrity, and availability of data stored on cloud platforms—the three pillars of the CIA triad foundational to information security (4).

Keywords: *Cloud Computing, Security, Challenges, Solutions.*

1. Introduction

Cloud computing has fundamentally changed how organizations store, process, and manage their information systems. Instead of maintaining physical servers and on-premises infrastructure, users can access computing resources through remote servers connected via the internet. This model helps organizations reduce capital expenditure on hardware while enabling flexible, on-demand access to applications and data from any location (1).

Cloud services are generally categorized into three primary deployment models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Each model introduces distinct security responsibilities shared between the cloud provider and the customer—a division known as the shared responsibility model. Understanding this division is critical for designing comprehensive security architectures (2,3).

Despite the benefits of cloud adoption, organizations face significant security challenges. Since cloud services operate through internet-based networks, they are continuously exposed to cyber threats that may compromise sensitive information. Data breaches—where confidential information becomes accessible to unauthorized parties—represent one of the most critical risks. Such breaches may arise from weak passwords, poor configuration of cloud systems, or unpatched vulnerabilities within cloud applications, potentially leading to financial loss and reputational damage (3,4).

Other prominent threats include unauthorized access through stolen credentials or weak authentication systems, malware attacks delivered via phishing or compromised software, and denial-of-service (DoS) attacks that overwhelm cloud resources to disrupt legitimate operations. This paper examines these threats systematically and evaluates the security mechanisms organizations can deploy to address them.

2. Literature review

Several studies have analyzed the security challenges associated with cloud computing environments. Researchers consistently identify data protection and privacy as major concerns when information is stored on remote servers accessible through shared, multi-tenant infrastructure (1,2).

Mell and Grance (1) established foundational definitions of cloud computing and identified inherent security considerations within each service model. Their work underscores that the transition from on-premises systems to cloud environments fundamentally alters the threat landscape, requiring security strategies tailored to distributed architectures.

Stallings (2) emphasizes the critical importance of network security protocols and encryption techniques in protecting cloud-stored data. Encryption converts readable information into encoded form so that unauthorized users cannot interpret data even if access is achieved. Modern cloud environments typically employ AES-256 encryption for data at rest and TLS/SSL protocols for data in transit.

Singh and Chatterjee (3) conducted a comprehensive review of cloud security issues, identifying misconfiguration of cloud settings as the leading cause of data breaches—a finding corroborated by subsequent industry reports. Their research evaluates the role of access control frameworks and highlights that role-based access control (RBAC) significantly reduces unauthorized access incidents. The ISO/IEC 27001 standard (4) provides a widely adopted framework for information security management in cloud environments. It prescribes systematic risk assessment, security controls, and continuous monitoring practices that organizations should apply to maintain compliance and resilience. Together, the existing literature establishes that no single security measure is sufficient; instead, a layered, multi-mechanism approach is essential for effective cloud security.

3. Methodology

3.1 Research design

This research adopts a descriptive and analytical approach to study the major security threats in cloud computing and the protection mechanisms used to mitigate them. A systematic review of existing literature was conducted, drawing from cybersecurity journals, cloud computing technical reports, industry white papers, and security

standards documentation. The study synthesizes findings to identify prevalent threat patterns and evaluate the relative effectiveness of available defense strategies (1,2,3,4).

3.2 Data collection

Information was gathered from peer-reviewed cybersecurity journals, cloud service provider security documentation, academic research papers, and international security standards. The key areas of focus included: types of cloud security threats and their prevalence; causes of data breaches and system vulnerabilities; security technologies implemented in major cloud platforms; and protection techniques adopted by organizations to safeguard cloud data.

3.3 Data analysis techniques

The gathered information was analyzed using thematic synthesis to identify recurring security issues in cloud systems and evaluate the effectiveness of different protection mechanisms. The analysis framework involved: identifying and categorizing major security threats in cloud environments; comparing the scope and limitations of different cloud security mechanisms; and evaluating protection strategies adopted by organizations across sectors. Security technologies examined include data encryption techniques, multi-factor authentication (MFA), role-based access control (RBAC), intrusion detection and prevention systems (IDS/IPS), and security information and event management (SIEM) platforms.

4. Dataset description

The dataset used in this study comprises information related to common cloud security threats and the protection techniques used to address them, derived from published security incident reports, cloud provider documentation, and academic studies. The key variables analyzed are organized into three categories:

- **Security threat types:** Data breach, unauthorized access, malware attack, denial-of-service (DoS/DDoS) attack, insecure API exploitation, and man-in-the-middle interception.
- **Causes of security vulnerabilities:** Weak or reused passwords, misconfigured cloud settings, absence of encryption, insecure application programming interfaces (APIs), and insufficient privilege management.
- **Security protection methods:** Encryption technologies (AES-256, TLS/SSL), access control systems (RBAC, IAM), multi-factor authentication (MFA), network monitoring and IDS/IPS tools, firewalls and web application firewalls (WAF), and continuous security auditing via SIEM platforms.

5. Observations

5.1 Data breaches

Data breaches represent one of the most serious risks in cloud computing environments. Industry reports consistently rank misconfiguration of cloud storage as the leading direct cause, followed by compromised credentials. If sensitive data is stored without adequate encryption or access restrictions, attackers may exploit these gaps and obtain unauthorized access. The consequences extend beyond immediate data exposure to include regulatory penalties under frameworks such as GDPR and HIPAA, financial liabilities, and sustained reputational harm (1,3).

5.2 Unauthorized access

Unauthorized access occurs when attackers gain entry to cloud systems without proper authorization. Weak passwords, credential stuffing attacks, stolen session tokens, and poorly configured identity and access

management (IAM) policies are major contributors. Multi-factor authentication (MFA) is among the most effective countermeasures, reducing the probability of unauthorized access significantly even when credentials are compromised. Role-based access control further limits the blast radius of any successful intrusion by restricting what authenticated users can access (2,3).

5.3 Malware attacks

Malware attacks involve malicious software designed to disrupt cloud services, exfiltrate sensitive information, or serve as entry points for broader attacks. These threats commonly arrive through phishing emails targeting cloud users, infected file uploads to shared storage, or compromised third-party software integrated with cloud platforms. Cloud environments are particularly susceptible to cryptojacking—where attackers hijack cloud computing resources for cryptocurrency mining—due to the scalable, always-on nature of cloud infrastructure (3,4).

5.4 Denial-of-Service (DoS) attacks

DoS and distributed denial-of-service (DDoS) attacks overwhelm cloud resources with traffic, making services unavailable to legitimate users. These attacks exploit the internet-facing nature of cloud deployments and can cause significant downtime and SLA violations. Cloud providers typically address this through auto-scaling, traffic filtering, and content delivery networks (CDNs) that absorb volumetric attack traffic before it reaches origin infrastructure (2,4).

5.5 Insecure APIs

Application programming interfaces (APIs) are the primary means through which cloud services communicate internally and externally. Insecure APIs that lack proper authentication, input validation, or rate limiting create direct pathways for attackers to access backend systems. The Cloud Security Alliance consistently lists insecure interfaces and APIs among the top cloud security threats. Implementing web application firewalls (WAF) and regular API security testing are critical countermeasures (3,4).

Table 1: Cloud Security Threats — Types, Causes, and Impacts

Threat Type	Description	Primary Cause	Impact
Data Breach	Unauthorized access to confidential stored data	Weak passwords, misconfiguration	Financial loss, reputational damage
Unauthorized Access	Attackers gain entry without valid credentials	Stolen credentials, poor IAM	Data theft, privilege escalation
Malware Attack	Malicious software disrupts or steals data	Phishing, infected files	Service disruption, data loss
DoS/DDoS Attack	Overwhelms cloud resources to deny service	Unprotected endpoints	Downtime, SLA violations
Insecure APIs	Vulnerable interfaces expose backend systems	Lack of input validation	Unauthorized data access
Man-in-the-Middle	Interception of data between client and server	Unencrypted channels	Data interception, credential theft

6. Results and Discussion

The analysis confirms that data breaches remain the most critical threat in cloud environments. Organizations lacking strong encryption policies, proper configuration management, and access controls are significantly more vulnerable. The findings align with industry reports indicating that over 80% of cloud security incidents involve misconfiguration or human error rather than sophisticated technical exploits—highlighting the importance of security training and automated compliance tools (5,6).

Authentication mechanisms play a crucial role in preventing unauthorized access. Implementing MFA reduces account compromise incidents substantially by requiring additional verification beyond passwords. Coupled with RBAC, which enforces least-privilege principles, organizations can significantly limit both the likelihood and impact of unauthorized access events (7).

Intrusion detection and prevention systems (IDS/IPS), when combined with SIEM platforms, provide organizations with near-real-time visibility into suspicious activity. This continuous monitoring capability is essential given the dynamic, multi-tenant nature of cloud environments where threats evolve rapidly. Runtime anomaly detection has been shown to identify a significant proportion of novel attack patterns before they escalate to full breaches (8).

Table 2: Security Mechanisms — Description, Threats Addressed, and Effectiveness

Security Mechanism	Description	Threat Addressed	Effectiveness
Encryption (AES-256)	Encrypts data at rest and in transit	Data breach, MitM	Very High
Multi-Factor Authentication	Adds extra verification layer beyond passwords	Unauthorized access	High
Role-Based Access Control	Restricts user permissions by role	Unauthorized access	High
IDS/IPS	Monitors and blocks suspicious network activity	Malware, DoS	Moderate–High
Firewall & WAF	Filters unauthorized traffic and API abuse	DoS, insecure APIs	High
Security Auditing & SIEM	Aggregates logs for real-time threat detection	All threat types	High

The comparative analysis in Table 2 illustrates that no single mechanism is universally sufficient. Encryption addresses data confidentiality but does not prevent unauthorized logical access. MFA and RBAC strengthen access control but are ineffective against malware delivered through authorized user sessions. A layered approach—combining preventive, detective, and corrective controls—is therefore essential for comprehensive cloud security (1,2,3,4).

Conclusion

This research examined the major security challenges in cloud computing alongside the protection techniques used to safeguard cloud data. The study identified several significant threats including data breaches, unauthorized access, malware attacks, denial-of-service incidents, and insecure APIs. These threats exploit the inherent characteristics of cloud environments—shared infrastructure, internet-facing services, and multi-tenant architectures—making them structurally distinct from on-premises security challenges (1,3).

The findings highlight the importance of implementing a comprehensive, layered security approach. Encryption protects data confidentiality at rest and in transit. Multi-factor authentication and role-based access control reduce the risk of unauthorized access. Intrusion detection systems and SIEM platforms provide continuous visibility into threats. Web application firewalls and DDoS mitigation tools protect public-facing interfaces. Together, these mechanisms support the confidentiality, integrity, and availability of information stored within cloud platforms (2,4).

Future cloud security efforts should address emerging challenges including zero-trust architecture adoption, container and microservices security, supply-chain risks associated with third-party cloud integrations, and quantum-computing threats to current encryption standards. As cloud adoption accelerates across sectors, embedding security into the design of cloud systems—rather than treating it as an afterthought—will be critical for sustainable and resilient digital infrastructure.

Acknowledgement

The authors would like to express their sincere gratitude to their faculty mentor for providing valuable guidance and support during the development of this research work. The authors also thank Pillai University for offering the resources and academic environment necessary to complete this study.

References

1. Mell, P., & Grance, T. (2018). *Cloud computing security guidelines* (NIST Special Publication 800-144). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-144
2. Stallings, W. (2019). *Network security essentials: Applications and standards* (6th ed.). Pearson Education.
3. Singh, A., & Chatterjee, K. (2020). Cloud security issues and challenges: A comprehensive review. *Journal of Information Security, 11*(2), 45–62. https://doi.org/10.4236/jis.2020.112004
4. International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection—Information security management systems—Requirements* (ISO/IEC 27001:2022).
5. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*(1), 1–11. https://doi.org/10.1016/j.jnca.2010.07.006
6. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications, 4*(1), 1–13.
7. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems, 28*(3), 583–592. https://doi.org/10.1016/j.future.2010.12.006
8. Behl, A., & Behl, K. (2017). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.