



Comparative Analysis of Cloud Computing Security Techniques for Secure Data Management

Deepansh Chaisiri

Department of Computer Science and Engineering, Daehan Institute of Management and Logistics, South Korea

deepansh.chaisiri@diml-kr.org

Peer Review Information

Submission: 05 Jan 2019

Revision: 08 Feb 2019

Acceptance: 11 March 2019

Keywords

Cloud Computing, Data Security, Encryption, Access Control, Secure Data Management

Abstract

Cloud computing enables organizations to store, process, and share large volumes of data through scalable third-party infrastructure, but outsourcing data also expands the attack surface and reduces the data owner's direct control over confidentiality, integrity, access, and processing. This methodology paper comparatively analyzes major security techniques used for secure cloud data management, with the evidence base restricted to research published up to 2019. The study synthesizes literature on conventional encryption, attribute-based encryption (ABE), identity and access management (IAM), role/attribute-based access control, integrity auditing and provable data possession, privacy-preserving processing, and trusted virtualization. A structured comparative method is applied using six criteria: confidentiality protection, access-control granularity, integrity assurance, scalability/manageability, performance efficiency, and breadth of threat coverage. Each technique is assigned an ordinal literature-derived score from 1 (weak) to 5 (strong), and weighted scores are used only as an analytical synthesis rather than as experimentally measured benchmarks. The comparative results show that no individual mechanism adequately protects all stages of the cloud data life cycle. Encryption provides strong confidentiality; ABE offers fine-grained sharing; auditing mechanisms are strongest for integrity verification; and trusted virtualization reduces infrastructure-level risk. The highest overall protection is obtained from a layered hybrid approach combining encryption, fine-grained access control, integrity verification, multi-factor authentication, logging, and infrastructure isolation. The study therefore recommends defense-in-depth as the most suitable security strategy for secure cloud data management.

Introduction

Cloud computing has transformed information technology by providing elastic computing, storage, platform, and software resources as services. Its economic value comes from rapid provisioning, shared infrastructure, remote access, and pay-per-use operation; however, these same characteristics alter the traditional security boundary. Data may be stored outside

the organization, replicated across locations, processed on shared virtualized infrastructure, and accessed through Internet-facing interfaces. Early cloud-security studies therefore identified confidentiality, privacy, authentication, multi-tenancy, virtualization, availability, and accountability as fundamental concerns that vary across SaaS, PaaS, and IaaS models [1]-[4].

For secure data management, the central problem is not merely protecting files at rest. A cloud data life cycle includes creation, transmission, storage, sharing, processing, backup, auditing, recovery, and deletion. A weakness at any stage can undermine the entire protection scheme. Encryption can make stolen data unreadable, but it does not independently determine who should receive decryption rights, verify that a remote copy remains intact, stop denial-of-service, or isolate a compromised virtual machine. Similarly, access-control rules are ineffective if a privileged administrator can read unencrypted storage. This interdependence explains why cloud security research progressively moved from isolated countermeasures toward multi-layer protection [5]-[10].

By 2019, the literature had expanded from identifying risks to comparing privacy-preserving technologies, access-control models, cryptographic approaches, integrity techniques, and end-to-end countermeasures. Studies emphasized that sensitive cloud data requires technical controls that preserve confidentiality and integrity while still supporting useful processing and manageable access policies [11]-[16]. The practical research question is therefore: which security techniques are strongest for particular security objectives, what limitations prevent them from operating as complete solutions, and what combination is most appropriate for secure cloud data management?

The objective of this paper is to provide a compact, reproducible comparative methodology rather than propose a new cryptographic primitive. The analysis (i) identifies major cloud data-security techniques reported up to 2019, (ii) evaluates them against common data-management security criteria, (iii) compares their strengths and limitations, and (iv) derives a layered framework suitable for organizations that must balance security, performance, scalability, and administrative complexity. Because the paper is literature-based, the numerical results are explicitly treated as ordinal analytical scores supported by the reviewed evidence and not as laboratory measurements.

Literature Review

Takabi et al. [1] described how cloud delivery and deployment models intensify security and privacy challenges, especially because identity, trust, authorization, and data protection must operate across organizational boundaries. Subashini and Kavitha [2] similarly mapped security risks to cloud service delivery models and showed that SaaS, PaaS, and IaaS expose different combinations of application, platform,

virtualization, and data-security concerns. Zissis and Lekkas [3] proposed a trusted-third-party-oriented security approach using public-key infrastructure, single sign-on, and directory services, illustrating an early move toward coordinated security services rather than isolated controls.

Hashizume et al. [4] systematically related cloud vulnerabilities, threats, and countermeasures and highlighted storage, networks, and virtualization as major problem areas. Modi et al. [5] reviewed security issues across multiple cloud layers, including authentication, data protection, virtualization, and network attacks. Fernandes et al. [7] provided a broad taxonomy of cloud vulnerabilities, threats, and attacks, showing that security must be designed across the infrastructure and service stack. These surveys establish that a cloud data-security comparison should evaluate more than confidentiality alone.

Fine-grained access to encrypted outsourced information became a major research direction. Li et al. [6] demonstrated the use of multi-authority attribute-based encryption for scalable sharing of personal health records, providing cryptographically enforced access policies, user revocation, and controlled sharing. ABE is especially relevant to cloud data management because authorization is bound to user attributes and ciphertext policies rather than relying only on a storage provider's discretionary access-control list. Its main trade-offs are cryptographic computation, key management, policy complexity, and revocation overhead.

Ali et al. [8] reviewed cloud security opportunities and challenges and emphasized risks created when data and applications move beyond the user's administrative control. Khan [9] categorized threats and remediation methods and compared trusted computing, intrusion detection, and compliance mechanisms, while Singh et al. [10] surveyed threats and solutions and argued for layered security management. Together, these studies support evaluation criteria that include threat breadth, manageability, and performance in addition to the confidentiality-integrity-availability triad.

Virtualization and multi-tenancy introduce infrastructure-level risks that data encryption by itself cannot remove. Ristenpart et al. [11] experimentally demonstrated information-leakage possibilities associated with co-resident virtual machines in third-party compute clouds. Later work on cloud hypervisors showed that hypervisor hardening, isolation, monitoring, and trusted-computing mechanisms are necessary to reduce attacks that cross virtual-machine boundaries. Consequently, secure data

management must consider both the data object and the execution environment in which that data is processed.

The 2019 literature consolidated these themes. Kumar and Goyal [12] mapped cloud security requirements to threats, vulnerabilities, and countermeasures and reinforced the need for end-to-end controls. Domingo-Ferrer et al. [13] compared privacy-preserving cloud methods for sensitive data, including cryptographic protection, anonymization, and data splitting, while noting trade-offs between privacy, supported operations, accuracy, and overhead. Sun [14] reviewed access control, ABE, proxy re-encryption, searchable encryption, trust, and reputation mechanisms, showing that privacy protection increasingly depends on combinations of techniques. Rady et al. [15] specifically analyzed confidentiality, integrity, and query processing for outsourced databases, and Amamou et al. [16] summarized data-protection risks during transfer and recovery. These studies motivate the comparative methodology used in this paper.

Methodology

This study uses a structured comparative-review methodology. It does not claim new experimental measurements; instead, it converts consistent findings from the literature into an explicit evaluation matrix. The method is designed so that another researcher can repeat the comparison with the same technique groups and criteria.

Step 1: Literature Selection and Scope

Peer-reviewed journal and conference literature on cloud security and secure outsourced data was selected with a publication cut-off of 2019. Priority was given to widely cited surveys, security taxonomies, and representative technique papers with verified DOI identifiers. Studies after 2019 were excluded. The final evidence set covers service-model security, encryption and key management, fine-grained access control, privacy-preserving processing, integrity verification, multi-tenancy/virtualization, and integrated cloud countermeasures [1]-[16].

Step 2: Security Technique Grouping

The reviewed mechanisms were grouped into seven functional categories: (T1) conventional encryption and PKI for data at rest/in transit; (T2) attribute-based encryption for cryptographically enforced fine-grained sharing; (T3) IAM with RBAC/ABAC and multi-factor authentication for identity-centered authorization; (T4) remote integrity auditing and provable-data-possession-style verification; (T5) privacy-preserving processing such as masking, anonymization, data splitting, and encrypted processing; (T6) hypervisor hardening, virtual-machine isolation, and trusted-computing mechanisms; and (T7) a layered hybrid framework that combines complementary controls. The grouping reflects the fact that cloud attacks can target data, identities, interfaces, storage, or the shared infrastructure [4], [7], [11], [12].

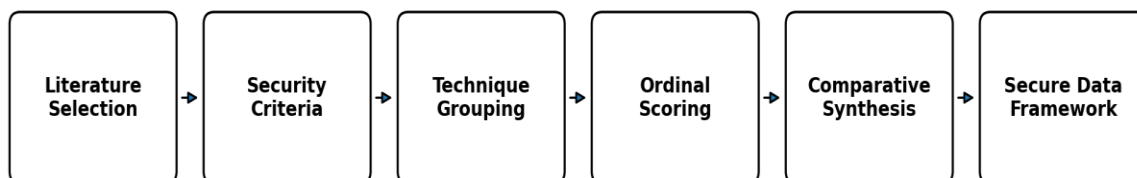


Figure 1. Methodology workflow for the comparative analysis

Step 3: Comparative Criteria and Weighting

Six criteria were used. C1 Confidentiality Protection (25%) assesses resistance to unauthorized data disclosure. C2 Access-Control Granularity (20%) evaluates how precisely privileges can be expressed and enforced. C3 Integrity Assurance (20%) measures the ability to detect unauthorized modification or loss. C4 Scalability and Manageability (15%) evaluates key, policy, user, and multi-tenant administration. C5 Performance Efficiency (10%) reflects relative computational and operational overhead, where a higher score means lower overhead. C6 Threat-Coverage Breadth (10%) measures how many clouds attack surfaces the

technique addresses. The weighting gives 65% of the total score to confidentiality, access control, and integrity because these properties are primary requirements for secure data management [12], [15].

Step 4: Literature-Derived Ordinal Scoring

Each technique received a score from 1 to 5 for each criterion: 1 = very weak, 2 = weak, 3 = moderate, 4 = strong, and 5 = very strong. Scores were assigned by comparing the mechanisms and limitations repeatedly reported in the literature. For example, conventional encryption receives a very strong confidentiality score but only a weak access-granularity score when used alone; ABE receives high confidentiality and granularity

scores but lower performance efficiency because policy evaluation and key operations add overhead [6], [14]. Integrity auditing receives a very strong integrity score but limited confidentiality coverage. Virtualization security receives high infrastructure threat coverage but does not replace object-level encryption [11].

Step 5: Weighted Score Calculation and Interpretation

For each technique, the overall score S was calculated as $S = 0.25C1 + 0.20C2 + 0.20C3 + 0.15C4 + 0.10C5 + 0.10C6$. The score is not a percentage of real-world security and should not be interpreted as a measured probability of preventing an attack. It is a transparent ordinal synthesis used to rank how completely each technique addresses the defined requirements. The qualitative advantages and disadvantages were retained alongside the numerical score so that a high overall score would not hide operational trade-offs.

Step 6: Validity Controls

Three controls were applied to reduce over-interpretation. First, all references were limited to 2019 or earlier, matching the study scope. Second, the comparison separates security coverage from performance efficiency, preventing a computationally expensive

mechanism from being labeled universally superior. Third, the final recommendation is based on complementarity across mechanisms, consistent with review findings that cloud security contains multiple interacting threat classes and no single countermeasure addresses all of them [5], [8], [10], [12].

Results

The literature-derived scoring matrix is shown in Table 1. The hybrid framework receives the highest overall score (4.70/5) because it combines object-level confidentiality, identity and policy control, integrity verification, logging, and infrastructure protection. ABE ranks highest among single specialized mechanisms for secure data sharing because it couples encryption with fine-grained authorization. Conventional encryption remains the most efficient strong baseline for confidentiality, while remote auditing is the most focused mechanism for integrity assurance. Privacy-preserving processing offers strong protection for sensitive outsourced computation but incurs greater overhead and may restrict supported operations. Infrastructure isolation addresses multi-tenancy threats but requires complementary data and identity controls.

Table 1. Literature-derived comparative scoring of cloud security techniques (1 = very weak; 5 = very strong).

Technique	C1	C2	C3	C4	C5	C6	Weighted	Main interpretation
Conventional encryption / PKI	5	2	3	4	4	3	3.65	Strong confidentiality baseline; depends on key and access management.
Attribute-based encryption (ABE)	5	5	3	3	2	4	4.00	Excellent fine-grained encrypted sharing; higher cryptographic/policy overhead.
IAM + RBAC/ABAC + MFA	2	5	2	4	4	3	3.20	Strong authorization and identity assurance; does not protect exposed plaintext alone.
Integrity auditing / PDP-style verification	1	1	5	4	3	2	2.70	Best for remote integrity checking; narrow confidentiality/access coverage.
Privacy-preserving processing / masking	5	3	3	2	1	4	3.40	Strong privacy for outsourced analytics; overhead and operation limits remain.
Hypervisor isolation / trusted computing	3	3	4	3	3	5	3.45	Reduces infrastructure and co-residency risk; needs data-level controls.
Layered hybrid framework	5	5	5	4	3	5	4.70	Most complete coverage; complexity and governance must be managed.

The ranking should be interpreted by security objective. If the principal requirement is bulk confidentiality for backups or object storage, conventional authenticated encryption with strong key management is efficient and mature. If the requirement is controlled sharing among many users or organizations, ABE is more expressive because authorization can be embedded in cryptographic policy [6], [14]. For databases and analytical workloads, privacy-preserving methods can reduce exposure to the cloud provider, but Domingo-Ferrer et al. [13] and Rady et al. [15] show that query functionality, computational cost, and data-management flexibility become important trade-offs.

Integrity is a separate requirement. A cloud provider can possess encrypted data that are incomplete, corrupted, or stale; consequently, integrity auditing mechanisms are valuable even when confidentiality is already provided. Conversely, a perfect integrity check does not prevent unauthorized disclosure. This explains the lower overall score of specialized auditing despite its high C3 value. The same specialization effect appears in IAM: strong authentication and RBAC/ABAC can prevent unauthorized logical access, but they cannot preserve confidentiality after a storage-layer breach unless the data are encrypted.

Virtualization security is important because shared infrastructure can create attack paths below the application and storage-control layers. Co-residency research [11] and later cloud-security surveys [7], [12] demonstrate that hypervisor hardening, isolation, patching, monitoring, and trusted execution complement rather than replace data-centric controls. Therefore, the highest-ranked architecture is layered: encrypt sensitive data; protect and rotate keys separately; apply MFA and fine-grained authorization; audit data integrity and administrative activity; harden APIs and virtual infrastructure; and use privacy-preserving processing when the cloud must operate on highly sensitive data.

Conclusion and Discussion

This comparative methodology demonstrates that cloud security techniques should be selected according to the security property they protect and the stage of the data life cycle they control. Encryption is indispensable for confidentiality, but conventional encryption alone has limited policy granularity. Attribute-based encryption strengthens secure sharing by joining cryptography with fine-grained authorization, although its computational and key-management requirements can affect large dynamic deployments. IAM, RBAC/ABAC, and MFA remain

essential for user and service authorization; remote auditing strengthens integrity; privacy-preserving techniques reduce exposure during outsourced processing; and virtualization/trusted-computing controls reduce risks arising from shared infrastructure. The principal finding is that secure cloud data management is a defense-in-depth problem. Reviews up to 2019 consistently show that cloud threats span identities, interfaces, networks, storage, virtualization, and service-provider trust [7], [10], [12], [16]. A layered hybrid model therefore provides the strongest overall protection because compromise of one control does not automatically expose the data. In practical deployments, the security stack should combine authenticated encryption, independent key management, least-privilege access control, MFA, tamper-evident logging, integrity checking, secure backup/recovery, hardened virtualization, and appropriate privacy-preserving processing. The methodology has two limitations. First, the scores are ordinal literature-derived judgments rather than measurements from a common experimental platform. Second, performance varies with dataset size, cryptographic parameters, cloud provider, workload, and implementation quality. Future experimental work can extend this study by implementing representative techniques on the same public-cloud testbed and measuring encryption latency, policy-evaluation time, audit overhead, throughput, recovery time, and attack-resistance under controlled scenarios. Within the 2019 evidence boundary, however, the comparative analysis supports a clear recommendation: organizations should not search for one universal cloud-security technique; they should engineer complementary controls around data confidentiality, integrity, authorization, privacy, and infrastructure trust. For practical adoption, the comparative scores can be used as a selection guide rather than a universal ranking. Low-complexity workloads such as encrypted archival storage may obtain adequate protection from strong encryption, independent key management, authenticated transfer, and integrity checks. Collaborative environments with changing users require stronger identity governance and fine-grained policies; in such cases, ABE or ABAC can reduce the risk of over-privileged access, although revocation and policy administration must be engineered carefully [6], [14]. When sensitive information must be processed by an external cloud, privacy-preserving computation, masking, or data splitting can reduce provider visibility, but the acceptable method depends on the operations that must remain available and the

overhead that the application can tolerate [13], [15]. A second implication is that governance is as important as cryptographic strength. Key rotation, administrator separation of duties, audit-log review, backup testing, incident response, and service-level requirements determine whether technical controls remain effective over time. The 2019 surveys emphasize mappings between threats, vulnerabilities, requirements, and countermeasures rather than a single protective algorithm [12], [16]. Therefore, organizations should classify data by sensitivity, identify the cloud service model and trust boundary, choose the minimum necessary privileges, and then layer controls according to the expected threat model. This approach preserves the advantages of cloud elasticity while reducing the likelihood that failure of one mechanism becomes a complete compromise.

References

- H. Takabi, J. B. D. Joshi, and G.-J. Ahn, "Security and privacy challenges in cloud computing environments," *IEEE Security & Privacy*, vol. 8, no. 6, pp. 24–31, 2010. DOI: 10.1109/MSP.2010.186.
- S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, 2011. DOI: 10.1016/j.jnca.2010.07.006.
- D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583–592, 2012. DOI: 10.1016/j.future.2010.12.006.
- K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," *Journal of Internet Services and Applications*, vol. 4, art. 5, 2013. DOI: 10.1186/1869-0238-4-5.
- C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey on security issues and solutions at different layers of cloud computing," *The Journal of Supercomputing*, vol. 63, no. 2, pp. 561–592, 2013. DOI: 10.1007/s11227-012-0831-5.
- M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131–143, 2013. DOI: 10.1109/TPDS.2012.97.
- D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M. Freire, and P. R. M. Inácio, "Security issues in cloud environments: A survey," *International Journal of Information Security*, vol. 13, no. 2, pp. 113–170, 2014. DOI: 10.1007/s10207-013-02087.
- M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Information Sciences*, vol. 305, pp. 357–383, 2015. DOI: 10.1016/j.ins.2015.01.025.
- M. A. Khan, "A survey of security issues for cloud computing," *Journal of Network and Computer Applications*, vol. 71, pp. 11–29, 2016. DOI: 10.1016/j.jnca.2016.05.010.
- [10] S. Singh, Y.-S. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," *Journal of Network and Computer Applications*, vol. 75, pp. 200–222, 2016. DOI: 10.1016/j.jnca.2016.09.002.
- T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds," in *Proc. ACM CCS*, pp. 199–212, 2009. DOI: 10.1145/1653662.1653687.
- R. Kumar and R. Goyal, "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey," *Computer Science Review*, vol. 33, pp. 1–48, 2019. DOI: 10.1016/j.cosrev.2019.05.002.
- J. Domingo-Ferrer, O. Farràs, J. Ribes-González, and D. Sánchez, "Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges," *Computer Communications*, vols. 140–141, pp. 38–60, 2019. DOI: 10.1016/j.comcom.2019.04.011.
- P. Sun, "Privacy protection and data security in cloud computing: A survey, challenges, and solutions," *IEEE Access*, vol. 7, pp. 147420–147452, 2019. DOI: 10.1109/ACCESS.2019.2946185.
- M. Rady, T. Abdelkader, and R. Ismail, "Integrity and confidentiality in cloud outsourced data," *Ain Shams Engineering Journal*, vol. 10, no. 2, pp. 275–285, 2019. DOI: 10.1016/j.asej.2019.03.002.
- S. Amamou, Z. Trifa, and M. Khemakhem, "Data protection in cloud computing: A survey of the state-of-art," *Procedia Computer Science*, vol. 159, pp. 155–161, 2019. DOI: 10.1016/j.procs.2019.09.170.