IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, November 2025
Impact Factor: 7.67

Data Loss Prevention Strategies in Cloud Computing

Shreya Gupta and Nikita Shekhar
Department of Computer Science and Applications
Sharda School of Computer Science and Engineering Sharda University, Greater Noida, UP, India
2023207161.shreya@ug.sharda.ac.in, 2023474506.nikita@ug.sharda.ac.in

Abstract: *Cloud computing offers scalable, cost-effective, and flexible computing resources, but storing sensitive data in shared third-party infrastructures introduces new risks of accidental or malicious data loss. Data Loss Prevention (DLP) is a critical discipline that ensures confidentiality, integrity, and availability of cloud data. This paper provides an extensive study of cloud data loss threats, analyzes cloud shared responsibility, and presents a multi-layered DLP framework. Preventive, detective, corrective, and compensating controls are discussed in detail, including encryption, access control, cloud-native DLP scanning, anomaly detection, zero-trust networks, immutable backups, and confidential computing. The paper concludes with emerging research trends and challenges in multi-cloud DLP, AI-driven analytics, and homomorphic encryption.*

Keywords*:* Data loss in the cloud can be due to misconfig- urations, malicious insiders, ransomware, insecure APIs, multi- cloud complexity, and supply-chain vulnerabilities

I. INTRODUCTION

Cloud computing has transformed enterprise IT through its elasticity, global availability, and cost-efficiency. However, shifting sensitive data to cloud environments introduces challenges, including data breaches, misconfigurations, insider attacks, and ransomware. Data Loss Prevention (DLP) aims to prevent unauthorized exposure, exfiltration, or destruction of cloud data. This paper examines modern DLP strategies and their effectiveness. Research in the domain of data loss prevention strategies in cloud computing has become a vital aspect of This is an inquiry due to increasing reliance on cloud services for data storage and processing, coupled with amid growing security threats and regulatory imperatives [5].Cloud computing has evolved from simple infrastructure services starting in the early 2010s to more complex, multitenant envi- ronments, further exacerbating concerns about data confiden- tiality and integrity. The practical significance of this research is underlined by the rising frequency and cost of data breaches, incidents that have caused billions in losses and undermined organizational trust, Kaur et al. 2017, Montano et al. 2022. While cloud adoption is expanding across sectors, securing sensitive information remains quintessential for compliance and operational ends.[9]But despite the extensive research in this direction, data leakage has still remained a great concern in cloud environments. These attacks are driven by insider threats, misconfigurations, and sophisticated cyber-attacks in nature.[7]It improves the models by increasing their accuracy and adaptability to constantly evolving threats Another major advantage of using multimodal fusion is This knowledge gap exists in integrating behavioral analytics, machine learning, and metadata-based processes.[2]Controls that give total pro- tection in real-time Controversies arise regarding the trade- offs between detection accuracy and system overhead, as well as balancing data protection with user privacy[10]Failure to address these gaps results in significant financial penal- ties and reputational damage, emphasizing the urgency for advanced, adaptive solutions[2] The aim of this systematic review is therefore to critically assess state-of-the-art, recent advances in data loss. The prevention strategies in cloud computing deal more with emerging technologies involving machines.[1]The review follows a structured approach with a comprehensive literature search, the in of peer-reviewed studies from 2010 to 2025, and thematic analysis according to Conceptual framework. Findings are organized to reflect technological innovations, challenges, and Future research di- rections also include enabling a coherent understanding of the ever-changing landscape of clouds. data loss prevention[4]The

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, November 2025 Impact Factor: 7.67

value lies in consolidating fragmented knowledge and high- lighting integrative approaches that enhance detection accuracy while minimizing operational costs[6]

II. THREAT LANDSCAPE

The breaches in public clouds are are often linked to misconfigured storage buckets or exposed credentials Security experts find that migration from on-premise infrastructures to cloud-based environments increases the attack surface and adds further complexity. These cloud platforms introduce new attack vectors through virtualization, shared resources, and multi-tenancy, including API-driven architectures that intro- duce new areas where data can be compromised. This section will look at some of the major threats contributing to data loss, leakage, or corruption in cloud environments.[12]

A. Misconfiguration of Cloud Resources

Common issues include publicly exposed storage buckets, incorrect access control lists, disabled encryption settings, and unrestricted inbound/outbound firewall rules. Attackers routinely scan for misconfigured services, which makes such errors highly susceptible to hacking.[15]

B. Insider Threats

Both malicious insiders-cloud provider employees or tenant staff-and unintentional insiders-employees making mistakes-pose significant DLP risks. Overprivileged accounts, inade- quate auditing, and long-lived credentials increase the possible impact of insider misuse.[9]

C. Account Hijacking and Credential Theft

Attackers compromise user and service identities through phishing, brute force, token theft, or OAuth abuse. Once inside, they may exfiltrate data, deploy malicious workloads, or disable logging. Inadequate IAM policies and a lack of MFA further magnify this risk.[3]

D. API and Cloud Interface Vulnerabilities

Web-based APIs control cloud services. Insecure APIs, insufficient rate limiting, missing input validation, or poorly designed authentication might allow an adversary to manipu- late cloud resources or access sensitive data. API-based attacks in multi-cloud deployments are becoming more common.[14]

E. External Cyberattacks

Traditional attack vectors of malware, ransomware, DDoS, and man-in-the-middle attacks are still very active. Ran- somware targeting cloud storage and backups could lead to disastrous data loss if versioning or immutability is dis- abled.[19]

F. Multi-Tenancy Risks

In shared cloud environments, several customers coexist on shared hardware. Vulnerabilities in hypervisors, container engines, or isolation mechanisms may allow for cross-tenant attacks that enable unauthorized access to memory or storage of neighboring virtual machines or containers.[20]

III. DLP REQUIREMENTS

A cloud-based DLP framework should guarantee the pro- tection of sensitive data throughout its lifecycle, which cov- ers creation, storage, transmission, processing, and deletion. The following requirements define an effective DLP architec- ture.[20]

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, November 2025 Impact Factor: 7.67

A. Data Classification Context Awareness

DLP systems must:Identify and classify sensitive data: PII, PHI, PCI, and confidential IP. Apply metadata tags for automatic policy enforcement.Perform contextual analysis on user role, location, device, and access pattern.[16]

B. Confidentiality Requirements

To maintain data confidentiality,Encryption should be en- forced at rest, in transit, and in use.Keys need to be protected by using secure KMS, HSM, or customer-managed keys.Policies should prevent unauthorized access through least privileges and zero trust.[18]

C. Integrity Requirements

Data integrity means that nothing will be altered maliciously or by accident. DLP must:Implement hashing, integrity checks, versioning, and logging.Detect unauthorized modifications by identifying anomalies.Provide rollback mechanisms through version-controlled backups.[14]

D. Availability Requirements

DLP strategies must:Ensure uninterrupted access with re- dundancy and multi-zone replication.This includes maintaining disaster recovery and business continuity plans.Provide RTO/RPO guarantees for critical workloads.[16]

E. Access Control Identity Requirements

Cloud DLP shall enforce:Strong IAM: MFA, RBAC/ABAC, JIT access.Identity governance with lifecycle management.Privileged Access Management: utilized for sensitive operations[19.

F. Monitoring Audit Requirements

Continuous monitoring is necessary:Track all data flows, API calls, and privileged operations.Generate immutable audit logs. Use UEBA and AI-based analytics to detect abnormal exfiltration patterns.[20]

IV. PREVENTIVE CONTROLS

Such preventive controls are the very foundation of reducing data leakage in cloud environments. These proactive controls prevent data leakage through access restrictions, policy en- forcement, and data protection across its lifecycle.[3]

A. Encryption Mechanisms

Data should be encrypted at rest, during transmission, and, where possible, when used. Encryption at Rest: Employment of strong cryptographic standards assures encryption of disks, object storages, and databases (AES-256). Encryption in Tran- sit: TLS 1.2+ and mutual TLS secure communications between services. Encryption in Use: Confidential Computing enables protection of data during processing with hardware-based TEEs. Key Management: Enforce centralized KMS, automated key rotation, least-privilege key access, and customer-managed keys for sensitive datasets.[6]

B. Identity and Access Management (IAM)

Strong IAM restricts unauthorized access to cloud assets. RBAC or ABAC (Role-Based Access Control or Attribute-Based Access Control) Multi-Factor Authentication (MFA) Just-In-Time privilege elevation Short-lived, automatically ro- tated access tokens Service accounts with minimal permis- sions[3]

C. Network Security Controls

Segmentation and restricted connectivity reduce exposure. Private endpoints and VPC service controls Firewall rules, security groups, and network ACLs Zero-trust architecture Egress filtering to detect or block unauthorized data exfiltration.[8]

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, November 2025 Impact Factor: 7.67

D. Data Classification and Minimization

Categorization of data based on sensitivity enables the implementation of precise DLP. Minimization reduces risk by retaining only essential data and getting rid of unnecessary sensitive information.[3]

E. Secure Configuration and Hardening

Preventive measures include: Detect misconfigurations using Cloud Security Posture Management - CSPM Infrastructure-as-Code scanning Automated baseline policies allow encryption by default, with no public buckets. Patch and vulnerability management[9]

F. Tokenization and Anonymization

Tokenization replaces sensitive fields with surrogate values, whereas anonymization techniques prevent linkage to subjects. These methods limit the risk of exposure when doing analytics or sharing data.

V. DETECTIVE CONTROLS

The detective controls help in early detection of anomalous behavior, unauthorized data access, or a potential breach, forming part of cloud DLP.[18]

A. Logging and Audit Trails

Comprehensive logging of administrative actions, data ac- cess events, and API calls enables rapid detection and forensic investigations. Immutable log storage prevents tampering.[20]

B. Security Information and Event Management (SIEM)

Centralized SIEM platforms perform correlation across cloud sources to identify suspicious patterns, unusual traffic, or unauthorized file transfers. SIEM tools generate compliance- ready reports[14]

C. User and Entity Behavior Analytics (UEBA)

Machine learning models monitor deviations in normal user behavior-such as large data downloads and access at unusual hours. UEBA is effective against insider threats.[11]

D. Cloud Security Posture Management (CSPM)

CSPM solutions constantly scan cloud configurations for misconfigurations and send alerts to security teams in real time. They are highly important for multi-cloud visibility.[8]

E. Data Flow Monitoring

Network-based DLP solutions inspect the outgoing traffic for sensitive data signatures or transfers of prohibited content. Real-time monitoring prevents data exfiltration.[4]

F. File Integrity Monitoring (FIM)

Critical file or system configuration tampering is detected, mainly through unauthorized modifications, helping in intru- sion detection.[20]

VI. CORRECTIVE CONTROLS

Corrective controls form an essential component of Data Loss Prevention (DLP) strategies in cloud computing by enabling organizations to contain, mitigate, and recover from data loss incidents after they occur. While preventive and detective controls aim to reduce the likelihood and speed of detection of a data compromise, corrective mechanisms ensure that disruptions do not escalate into long-term or irreversible failures. In cloud environments—characterized by distributed architectures, virtualization, multi-tenancy, and dynamic resource provisioning—corrective controls must be designed to scale seamlessly, integrate across heterogeneous services, and minimize recovery time. This section

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, November 2025 Impact Factor: 7.67

provides a comprehensive analysis of corrective controls, their com- ponents, implementation approaches, and their relevance in modern cloud ecosystems.[5] Purpose of Corrective Controls The main objectives of corrective controls in cloud-based DLP are: Restore lost or corrupted data to the most recent safe state. Limit the impact of ongoing incidents, such as ransomware, accidental deletion, or insider misuse.[19] Re- establish normal operations without major downtime. Iden- tify root causes to prevent recurrence. Ensure compliance, especially when the incident involves sensitive or regulated data. Corrective controls must work both technically (through backups, versioning, failover) and organizationally (incident response plans, forensic procedures).[11]

A. Continuous Monitoring

Cloud-native monitoring tools such as AWS CloudTrail, Azure Monitor, and Google Cloud Logging capture every administrative and data-related event. SIEM integration enables correlation across services.[2]

B. Anomaly and Behavioral Analytics

Machine learning-based User and Entity Behavior Analytics (UEBA) detect deviations such as unusual download volumes, abnormal access times, or atypical login patterns.[9]

C. DLP Content Inspection

Detective DLP tools scan structured and unstructured data for sensitive fields (PII, PHI, PCI) using pattern recognition, NLP-based classification, or contextual.[2]

D. Cloud Security Posture Management (CSPM)

CSPM solutions continuously inspect cloud configurations for public buckets, disabled encryption, open ports, and over- privileged IAM roles that increase data loss risks.[9]

E. Immutable Audit Logs

Tamper-proof audit logs support forensic investigations and regulatory compliance. Log integrity ensures accurate recon- struction of data-related events.[21]

VII. COMPENSATING CONTROLS

Compensating controls are alternative security measures deployed by an organization when standard or primary controls cannot be implemented because of technological, financial, op- erational, or compliance reasons. Within cloud environments, some native DLP mechanisms might be inherently limited due to multi-tenancy architecture, provider-imposed restrictions, or simply because of the legacy of an application itself. In this case, compensating controls would enable an equivalent level of protection of sensitive data and allow achieving overall data loss prevention objectives.[17] Cloud computing adds many complexities, which include limited visibility of the provider infrastructure, encryption mechanisms that are controlled by vendors, and storage systems that are distributed. Compensating controls help reduce exposure, minimize the impact of data leakage, and add an extra layer of assurance to address such gaps. These controls do not replace primary controls but help achieve comparable security outcomes when the primary controls cannot be fully applied.[11]

A. Application-Level Encryption

This may not be appropriate in all cases due to organiza- tional or regulatory requirements. Application-level or client-side encryption acts as a compensating control wherein data gets encrypted before going into the cloud, ensuring that the attacker is not able to get plaintext data from any compromise of the storage layer or the CSP environment.[2]

B. Tokenization and Data Masking

When encryption is not practical—as in certain legacy systems or applications that cannot handle ciphertext—tokenization and masking can limit exposure. Sensitive information such as credit card numbers or personal identifiers

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, November 2025 Impact Factor: 7.67

is replaced with harmless tokens. These tokens retain format similarity, enabling systems to operate normally while minimizing risk.[8]

C. Confidential Computing with Usage

Confidential Computing environments, such as hardware- based Trusted Execution Environments (TEEs), allow data to be processed in encrypted memory. This compensates for lim- itations in native DLP mechanisms that cannot inspect or con- trol data in use. TEEs protect against hypervisor-level attacks, insider threats, and cloud infrastructure compromises[10].

D. Network Isolation and Out-of-Band Monitoring

When enforcing strict DLP rules at the application or storage layer is not possible, network-based isolation can serve as an alternative. Private subnets, isolated VPCs, and controlled routing paths restrict data movement, while out- of-band monitoring tools analyze traffic patterns and detect potential exfiltration. This compensates for limitations in host- level or application-level monitoring capabilities.[3]

E. Improved Logging and Auditing

If real-time DLP tools cannot be integrated due to system constraints, detailed logging with centralized monitoring can compensate by enabling rapid detection of suspicious activi- ties. Immutable audit logs and SIEM-based correlations act as secondary protections, helping investigate incidents and reducing the overall impact of potential data loss.[20]

VIII. PROPOSED MULTI-LAYER DLP FRAMEWORK

A robust Data Loss Prevention(DLP) armature in pall computing must admit the distributed, elastic, andmulti-tenant nature of pall surroundings. Traditional enterprise DLP results follow border- grounded models, but these approaches come inadequate in pall ecosystems where data flows across virtual networks, serverless workflows, storehouse pails, APIs, and third- party SaaS operations. To address these complications, this exploration proposes aMulti-Layer DLP Framework that integrates security controls across five logical layers Data Layer, Identity Layer, Network Layer, Application Layer, and Monitoring/ Analytics Subcaste. Each subcaste contributes unique defensive capabilities, and together they establish a defense- in- depth armature able of precluding, detecting, and responding to data loss incidents in dynamic pall surroundings. [21]

A. Layer 1: Data Governance and Classification

The foundation of the frame is strong data governance. Or- ganizations must classify data grounded on perceptivity(e.g., public, internal, nonpublic, defined) and assign metadata mark- ers to support automated enforcement. Clear power, retention schedules, and handling procedures help align DLP operations with nonsupervisory and organizational conditions.[2]

B. Layer 2: Preventive Security Controls

This subcaste focuses on minimizing the probability of unauthorized data access or leakage. crucial mechanisms in- clude encryption(at rest, in conveyance, and in use), least- honor access control, secure crucial operation, and network segmentation. preventative controls insure that indeed if bush- whackers gain access to the terrain, data exposure remains delicate.[6]

C. Layer 3: Detective Monitoring and Analytics

nonstop monitoring is critical for relating anomalous geste and implicit exfiltration attempts. This subcaste integrates pall- native logging, stoner and reality Behavior Analytics(UEBA), SIEM systems, CSPM tools, and DLP pattern- matching machines. The thing is to enable early discovery of suspicious data movements and misconfigurations before they escalate into major incidents.[14]

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, November 2025 Impact Factor: 7.67

D. Layer 4: Corrective and Recovery Mechanisms

When incidents do, rapid-fire constraint and recovery are essential. This subcaste includes backup and restoration mech- anisms, inflexible storehouse for critical data, credential can- cellation , security robotization, and well- defined incident response playbooks. The ideal is to restore normal operations while minimizing data loss and business impact.[12]

E. Layer 5: Compensating and Advanced Security Controls

This subcaste provides indispensable or supplementary con- trols where standard security measures are inadequate. exem- plifications include operation- position encryption, tokeniza- tion, nonpublic computing, and format- conserving encryption. These controls enhance data security in scripts involving heritage operations,cross-border data transfers, or untrusted surroundings.[11]

F. Layer 6: Continuous Audit and Compliance Management

The final subcaste ensures that all DLP conditioning mis- behave with nonsupervisory norms similar as GDPR, HIPAA, or PCI- DSS. Regular checkups, security assessments, vul- nerability scanning, and automated compliance reporting help maintain alignment with evolving legal and assiduity condi- tions.[20]

IX. CHALLENGES

Despite advancements in pall security technologies, enforc- ing effective Data Loss Prevention(DLP) remains grueling for associations. These challenges arise from the dynamic, distributed, andmulti-tenant nature of pall surroundings. [16]

A. Multi-Tenancy and Shared Responsibility

Cloud platforms operate on a multi-tenant architecture where computing resources are shared among multiple users. Ensuring strict data isolation while depending on the cloud provider's internal controls is complex. Additionally, the shared responsibility model can cause confusion regarding which controls are managed by the customer versus the CSP, potentially leaving security gaps.[18]

B. Misconfigurations and Human Error

A significant percentage of cloud data loss incidents stem from misconfigured storage buckets, weak access permis- sions, or improper key handling. As cloud environments scale rapidly, configuration drift becomes common, making it difficult to maintain consistent security posture across all resources.[21]

C. Data Visibility and Control Limitations

Organizations often lack full visibility into cloud provider infrastructure, which restricts their ability to monitor data movement and enforce DLP policies at deeper levels. Tradi- tional on-premise monitoring tools are not always compatible with cloud APIs, leading to blind spots in data flow monitor- ing.[14]

D. Scalability and Performance Constraints

DLP technologies, especially those involving deep content inspection or real-time scanning, can introduce latency. In large-scale cloud systems that handle massive data through- put, maintaining a balance between security and performance becomes difficult.[11]

E. Encryption and Key Management Complexity

Although encryption is essential for protecting cloud data, managing encryption keys in distributed cloud environments is challenging. Multi-cloud and hybrid architectures further complicate key lifecycle management, rotation policies, and compliance requirements.[13]

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, November 2025 Impact Factor: 7.67

F. API and Integration Risks

Cloud services rely heavily on APIs for management and data access. Weak API authentication, insufficient rate lim- iting, or insecure integrations with third-party SaaS applica- tions can become vectors for data leakage. Ensuring secure API consumption across multiple platforms is operationally demanding.[19]

G. Compliance and Data Sovereignty

Different countries enforce unique data protection laws, requiring strict controls over where data is stored and pro- cessed. Ensuring compliance across geographically distributed clouds—while preventing unlawful data movement—adds complexity to DLP strategy design.[22]

H. Insider Threats

Both malicious insiders and careless employees pose sig- nificant risks. Detecting subtle insider threat patterns in cloud environments requires advanced behavioral analytics, which many organizations lack. Insider activity is even harder to detect in federated multi-cloud systems.[17]

I. Lack of Standardization Across CSPs

Each cloud provider (AWS, Azure, GCP) offers different security models, logging formats, and policy enforcement mechanisms. This lack of standardization makes it difficult to design uniform DLP policies, especially in multi-cloud setups.[11]

J. Cost and Resource Constraints

Comprehensive DLP deployment—including cloud-native tools, SIEM integration, encryption, and monitoring—can be expensive. Smaller organizations often struggle to allocate re- sources for continuous monitoring, staff training, and incident response capabilities. Despite advancements in cloud security technologies, implementing effective Data Loss Prevention (DLP) remains challenging for organizations. These challenges arise from the dynamic, distributed, and multi-tenant nature of cloud environments.[18]

X. LITRETURE REVIEW

Data Loss Prevention (DLP) in cloud computing has gained significant academic attention due to the rapid migration of organizational workloads to distributed cloud infrastructures. Various studies highlight that cloud environments introduce unique risks such as unauthorized access, insider threats, misconfigurations, and loss of control over data residency. (2013), cloud computing security challenges arise primarily from multi-tenancy, virtualization vulnerabilities, and unclear trust boundaries between cloud service providers (CSPs) and clients.[1] Several researchers have emphasized encryption as a foundational control for data loss prevention. (2019) argue that encryption must be tightly integrated with access policies to remain effective in scalable cloud environments. (2018) observe that encrypted data remains vulnerable to insider sabo- tage, policy mismanagement, and weak identity governance.[4] The role of access control and identity management has been examined extensively. (2012) present a distributed access con- trol architecture that enforces fine-grained policy enforcement across multiple clouds. Their work demonstrates that central- ized access models often fail in distributed infrastructures, motivating the need for federated identity management and Zero Trust principles.[7] (2020) highlight that Zero Trust Architecture (ZTA) provides continuous verification and least- privilege enforcement, significantly reducing the likelihood of accidental or malicious data exposure.[2] Another significant area in DLP literature is anomaly detection and monitoring. (2020) suggests that integrating behavioral analytics with contextual access policies improves detection precision.[4] Recent literature also highlights policy-based DLP and cloud- native security. Sabahi (2011) emphasizes that policy-driven monitoring, combined with automated enforcement through CSP-native tools (e.g., CASB, CSPM), significantly enhances visibility and real-time protection.[8] Overall, the literature shows that while individual DLP techniques—such as encryp- tion, access control, anomaly detection, or backups—provide partial protection, researchers widely acknowledge that a multi-layer, integrated DLP framework is essential for robust security in cloud environments.[1] This conclusion motivates the

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, November 2025 Impact Factor: 7.67

development of holistic, defense-in-depth models that combine preventive, detective, corrective, and compensating controls to address the full spectrum of cloud data loss risks.[6]

XI. FUTURE SCOPE

The rapid-fire elaboration of cloud computing, combined with adding data volumes and complex nonsupervisory conditions, indicates that Data Loss Prevention(DLP) will continue to witness significant advancements. The future of DLP in pall surroundings is anticipated to shift toward intelligent, independent, and environment- apprehensive protection mech- anisms able of conforming to dynamic workloads andmulti- cloud ecosystems.

First, AI- driven DLP systems represent a major direc- tion for unborn exploration. Current DLP results frequently struggle with high false-positive rates and limited contextual understanding. Integrating advanced machine literacy mod- els including deep literacy, allied literacy, and underpinning learning — can enable prophetic identification of exfiltra- tion attempts, bigwig anomalies, and high- threat data flows. These intelligent machines may proactively help data exposure without negatively impacting system performance or stoner experience.

Alternate, as associations decreasingly borrowmulti-cloud and cold-blooded pall infrastructures, formalizedcross-platform governance fabrics will come essential. unborn exploration may concentrate on unified policy unity, enabling harmonious DLP rules, encryption programs, and access controls across different pall service providers. also, flawlessmulti-cloud crucial operation and interoperability between miscellaneous security APIs remain open exploration challenges.

Third, the growth of Confidential Computing and translated processing will transfigure how DLP is enforced. Technolo- gies similar as homomorphic encryption, secure multiparty calculation(SMPC), and tackle- grounded Trusted prosecution surroundings(TEEs) can allow sensitive data to be reused without exposure. unborn DLP tools may integrate these mechanisms to secure data " in use, " closing one of the largest gaps in moment's pall security models.

also, with the expansion of edge computing, 5G, and IoT, the future of DLP must address distributed data surroundings in which data is generated, reused, and stored outside centralized pall systems. Research openings live in designing featherlight, decentralized DLP agents able of guarding data across edge bumps, fog layers, and constrained IoT bias. These results must balance strong security with limitations in bandwidth, recycling power, and energy consumption.

Another arising direction involves sequestration- conserving DLP, where associations will need to misbehave with decreas- ingly strict global data protection laws. This motivates unborn results incorporating discriminational sequestration, automated data occupancy enforcement, and real- time nonsupervisory mapping. environment-apprehensive DLP models able of understanding jurisdictional constraints will be critical for transnational associations.

Eventually, the future of DLP will probably include in- dependent remediation and tone- mending security infrastructures. Through robotization and policy- as- law, systems could respond stoutly to data exposure attempts — repealing credentials, rotating keys, segregating workloads, and restoring clean data from inflexible backups without mortal intervention.

XII. CONCLUSION

Data Loss Prevention(DLP) in cloud computing has come a critical demand as associations decreasingly resettle sensitive workloads to pall platforms. The cloud terrain introduces unique pitfalls similar asmulti-tenancy, participated structure, API- driven operations, and frequent configuration changes, all of which increase the chances of data exposure or unau- thorized access. To address these challenges, effective DLP strategies must integrate preventative, operative, corrective, and compensating controls while icing functional effectiveness and nonsupervisory compliance.

preventative controls similar as strong encryption, identity and access operation, network segmentation, and data bracket form the foundation of cloud data protection by minimizing openings for data leakage. operative controls similar as non- stop monitoring, anomaly discovery, inspection logs, and cloud security posture operation — help identify suspicious condi- tioning before they escalate into critical incidents. Corrective controls including backup, disaster recovery, incident response processes, and rapid-fire credential cancellation allow associ- ations to contain and remediate breaches effectively. When traditional controls are limited, compensating controls like tokenization,

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, November 2025 Impact Factor: 7.67

operation- position encryption, and nonpublic computing give fresh layers of protection for high- threat or regulated data.

Amulti-layer DLP frame that aligns with the cloud par- ticipated responsibility model enables associations to apply a holistic defense- in- depth approach. Such a frame im- proves adaptability against both internal and external pitfalls by integrating specialized measures, governance programs, robotization, and stoner mindfulness programs.

Despite advancements in DLP technologies, challenges re- main — especially in areas likemulti-cloud crucial operation, securing deciduous workloads, reducing false cons in DLP tools, and addressing evolving nonsupervisory conditions. still, arising technologies similar as AI- driven trouble analytics, nonpublic computing, and sequestration-conserving crypto- graphic ways offer significant unborn eventuality for strength- ening pall DLP.

Overall, an effective DLP strategy in pall computing re- quires nonstop adaption, strong governance, and a combination of technological and organizational measures. By espousing a layered and visionary approach, associations can significantly reduce data loss pitfalls and make a secure, secure cloud terrain.

REFERENCES

[1] NIST SP 800-53, “Security and Privacy Controls for Information Sys- tems.”
[2] ISO/IEC 27017, “Cloud Security Guidelines.”
[3] Cloud Security Alliance, “Cloud Controls Matrix.”
[4] 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.
[5] Cloud Security Alliance (CSA), “Top Threats to Cloud Computing,” CSA Research Report, 2020.
[6] K. Hashizume, D. G. Rosado, E. Ferna´ndez-Medina, and E. B. Fernan- dez, “An analysis of security issues for cloud computing,” Journal of Internet Services and Applications, vol. 4, no. 5, 2013.
[7] R. S. Singh and R. K. Yadav, “Data loss prevention in cloud computing: A comprehensive review,” IEEE Access, vol. 8, pp. 116966–116990, 2020.
[8] P. P. Ray, “A survey on data protection techniques in cloud,” ACM Computing Surveys, vol. 52, no. 4, pp. 1–37, 2019.
[9] V. Gupta and M. V. Parmar, “Data loss prevention techniques in cloud computing environment,” International Journal of Computer Applica- tions, vol. 96, no. 18, pp. 6–12, 2014.
[10] D. Chen and H. Zhao, “A survey on data security in cloud computing,” Computer Communications, vol. 47, pp. 1–8, 2014.
[11] M. A. AlZain, B. Soh, and E. Pardede, “A survey on data security issues in cloud computing: From single to multi-clouds,” Journal of Software, vol. 8, no. 5, pp. 1068–1078, 2013.
[12] NIST Special Publication 800-53, “Security and Privacy Controls for Federal Information Systems,” 2020.
[13] D. Fernandes et al., “Security issues in cloud environments: A survey,” International Journal of Information Security, vol. 13, no. 2, pp. 113-170, 2014.
[14] A. Singh and K. Chatterjee, “Cloud security issues and challenges: A survey,” Journal of Network and Computer Applications, vol. 79, pp. 88–115, 2017.
[15] T. Ristenpart et al., “Hey, you, get off of my cloud: Exploring informa- tion leakage in third-party compute clouds,” ACM CCS, pp. 199–312, 2009.
[16] N. Gruschka and M. Jensen, “Attack surfaces: A taxonomy for attacks on cloud services,” IEEE Cloud, 2010.
[17] S. Kamara and K. Lauter, “Cryptographic cloud storage,” Financial Cryptography and Data Security, vol. 6054, pp. 136–149, 2010.
[18] Microsoft Azure Security Documentation, “Data Loss Prevention Best Practices,” 2023.
[19] H. Tabrizchi and M. Rafsanjani, “A survey on security challenges in cloud computing using machine learning,” Journal of Information Security and Applications, vol. 50, 2020.
[20] E. Fernandes et al., “Security implications of cloud-hosted machine learning models,” IEEE Security Privacy, 2019.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, November 2025
Impact Factor: 7.67

[21] J. A. Perez and J. Karlsson, "AI-driven anomaly detection in cloud environments," Future Generation Computer Systems, vol. 108, pp. 247–259, 2020.