PRIVACY CHALLENGES IN CLOUD COMPUTING UNDER IT LAW

[1]Davesh Grover, [2]Dr. Ramveer Singh

[1]Research Scholar, School of Law, MVN University, Palwal
[2]Associate Professor, School of Law, MVN University, Palwal

Abstract

Cloud computing has become a central part of digital governance, business operations, education, health services, banking, e-commerce and public service delivery. Its technical advantages arise from on-demand access, shared resources, rapid elasticity and measured services, but the same features create serious privacy challenges because personal data may be stored, processed, replicated and accessed across multiple systems, jurisdictions and service providers. In India, these challenges must be examined under the Information Technology Act, 2000, the SPDI Rules, 2011, the Digital Personal Data Protection Act, 2023, the Digital Personal Data Protection Rules, 2025, CERT-In cyber-security obligations, and the constitutional right to privacy recognised in Justice K.S. Puttaswamy v. Union of India. This paper analyses the major privacy risks in cloud computing, including unclear data control, cross-border transfer, breach notification, weak consent management, vendor lock-in, government access, metadata exposure, misconfiguration and accountability gaps. The paper concludes that Indian IT law has moved from a limited compensation-based model under section 43A of the IT Act toward a rights-and-obligations model under the DPDP framework, but cloud-specific governance still requires stronger contractual controls, technical safeguards, auditability, encryption, data minimisation, incident response and risk-based compliance.

***Keywords*: cloud computing, privacy, IT Act 2000, DPDP Act 2023, SPDI Rules, data protection, CERT-In, data fiduciary, cyber law, India.**

1. INTRODUCTION

Cloud computing is commonly understood as a model that enables convenient and on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications and services. The NIST definition is important for legal analysis because it shows that cloud computing is not merely remote storage; it is a complex service model built on shared infrastructure, resource pooling, elasticity, automated provisioning and measured use. In privacy terms, these features mean that personal data can move through several layers of infrastructure without the individual user seeing where it is stored, who administers it, or how long copies are retained.[1]

The legal relevance of cloud computing arises because cloud service providers, customer organisations, intermediaries, data centres and processors may all participate in the life cycle of personal data. Under Indian IT law, liability and compliance may arise from failure to maintain reasonable security practices, unauthorised access, wrongful disclosure, intermediary due diligence, incident reporting and data protection obligations.

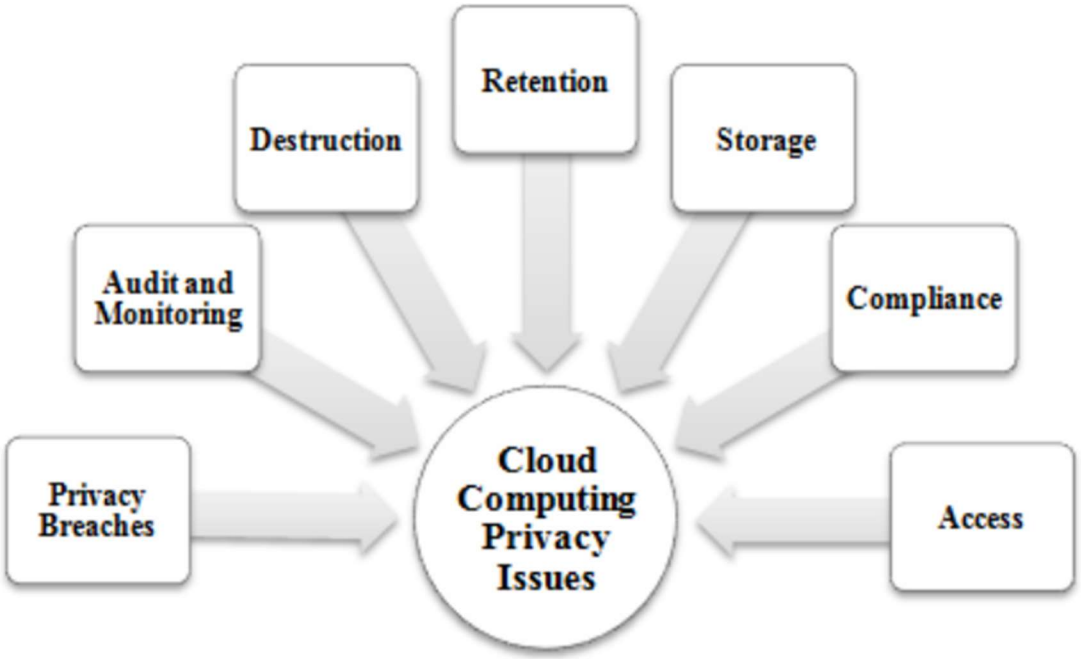
[1] Pei-Jen Sun, Security and Privacy Protection in Cloud Computing: Discussions and Challenges, 160 Journal of Network & Computer Applications 102642 (2020), https://doi.org/10.1016/j.jnca.2020.102642.

Therefore, privacy in cloud computing cannot be reduced to one technical control; it requires a combined analysis of law, contract, governance and security architecture.[2]

The right to privacy has a constitutional foundation in India after the Supreme Court recognised privacy as part of the right to life and personal liberty under Article 21 in Justice K.S. Puttaswamy v. Union of India. The judgment is especially relevant to cloud computing because it recognised informational privacy and noted that risks to privacy can arise from both the State and non-State actors. Cloud environments are often operated by private actors but may also involve government access, public-sector outsourcing and law-enforcement requests, making constitutional values relevant to statutory interpretation and compliance design.

India's legal framework has also changed substantially after the enactment of the Digital Personal Data Protection Act, 2023 and the notification of the Digital Personal Data Protection Rules, 2025. The DPDP framework focuses on lawful processing, notice, consent, duties of data fiduciaries, rights of data principals, security safeguards, breach intimation and regulatory oversight. For cloud computing, these provisions create a practical need to identify whether the cloud customer, cloud provider, managed service provider or another entity is acting as data fiduciary, data processor, intermediary or service provider in each processing activity.[3]

The first objective of this paper is to identify the main privacy challenges created by cloud computing in the Indian legal environment. The second objective is to examine how the IT Act, SPDI Rules, DPDP Act, DPDP Rules, IT Rules and CERT-In directions respond to those challenges. The third objective is to propose practical legal and technical safeguards that can help organisations adopt cloud services without weakening privacy rights, data protection compliance or cyber-security accountability.



2. LITERATURE REVIEW

2 Nnaemeka Ukeje, Jairo Gutierrez & Krassie Petrova, Information Security and Privacy Challenges of Cloud Computing for Government Adoption: A Systematic Review, 23 International Journal of Information Security 1459 (2024), https://doi.org/10.1007/s10207-023-00797-6.

3 Subhajit Saha & Surjashis Mukhopadhyay, A New Age of Data Privacy Laws in India: Review of Digital Personal Data Protection Act, 2023, 10 International Journal of Law and Social Sciences 84 (2024), https://doi.org/10.60143/ijls.v10.i1.2024.114.

Author(s) & Year	Paper / Journal	Method	Main Findings
Kaaniche & Laurent (2017)	Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms; Computer Communications[4]	Survey / comparative review of cryptographic mechanisms	The paper shows that outsourced cloud storage creates loss of control, confidentiality risks, and integrity concerns. It compares cryptographic mechanisms such as searchable encryption, proxy re-encryption and auditing approaches for protecting stored cloud data.
Singh & Chatterjee (2018)	Data Privacy Protection Mechanisms in Cloud; Data Science and Engineering[5]	State-of-the-art review and taxonomy	The authors classify privacy-preserving approaches into cryptography, probability, anonymization and ranking. They also stress the need for auditing and accountability mechanisms to monitor data use and provenance in cloud environments.
Domingo-Ferrer et al. (2019)	Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges; Computer Communications[6]	Survey of privacy-enabling technologies	The study reviews masking, data splitting, anonymization and cryptographic techniques that permit cloud processing while reducing exposure of sensitive data. It highlights trade-offs between functionality, overhead, transparency and interoperability.
Sun (2020)	Security and privacy protection in cloud computing: Discussions and challenges; Journal of Network and Computer Applications[7]	Technical review and protection framework	The paper identifies key privacy-security risks in cloud computing and reviews access control, CP-ABE, KP-ABE, proxy re-encryption, searchable encryption, trust mechanisms and multi-tenant protection.
Abdulsalam & Hedabou (2021/2022)	Security and Privacy in Cloud Computing: Technical Review; Future Internet[8]	Technical review	The paper discusses cloud security and privacy problems across cloud layers and notes that adaptive solutions are necessary because threats evolve and may conflict with traditional static security models.
Adee & Mouratidis (2022)	A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and	Model development and security evaluation	The authors argue that encryption alone is insufficient for cloud privacy and propose a layered model combining cryptography and steganography for data at rest and in transit.

4 Nora Kaaniche & Maryline Laurent, Data Security and Privacy Preservation in Cloud Storage Environments Based on Cryptographic Mechanisms, 111 Computer Communications 120 (2017), https://doi.org/10.1016/j.comcom.2017.07.006.
5 Nandita Singh & Amit Chatterjee, Data Privacy Protection Mechanisms in Cloud, 3 Data Science & Engineering 24 (2018), https://doi.org/10.1007/s41019-017-0046-0.
6 Josep Domingo-Ferrer et al., Privacy-Preserving Cloud Computing on Sensitive Data: A Survey of Methods, Products and Challenges, 140-141 Computer Communications 38 (2019), https://doi.org/10.1016/j.comcom.2019.04.011.
7 Pei-Jen Sun, Security and Privacy Protection in Cloud Computing: Discussions and Challenges, 160 Journal of Network & Computer Applications 102642 (2020), https://doi.org/10.1016/j.jnca.2020.102642.
8 Yaseen S. Abdulsalam & Mohammed Hedabou, Security and Privacy in Cloud Computing: Technical Review, 14 Future Internet 11 (2022), https://doi.org/10.3390/fi14010011.

	Steganography; Sensors[9]		
Soveizi et al. (2023)	Security and privacy concerns in cloud-based scientific and business workflows: A systematic review; Future Generation Computer Systems[10]	Systematic review	The review finds that many studies focus on modeling and execution phases, while monitoring and adaptation phases are under-covered. This creates gaps in detecting, preventing and reacting to privacy or security violations in cloud workflows.
Issaoui et al. (2023)	Exploring GDPR compliance in cloud services: insights from Swedish public organizations on privacy compliance; Future Business Journal[11]	Empirical study using LINDDUN privacy threat categories	The study identifies unauthorized access, loss of confidentiality, lack of awareness, lack of trust, legal uncertainties, regulatory challenges and loss of control as major privacy issues in public-cloud use.
Ukeje et al. (2024)	Information security and privacy challenges of cloud computing for government adoption: a systematic review; International Journal of Information Security[12]	PRISMA systematic literature review	The authors screened 758 papers and included 33 studies. Information security and privacy were found to be critical barriers to government cloud adoption, together representing a major portion of identified adoption gaps.
Zandesh (2024)	Privacy, Security, and Legal Issues in the Health Cloud: Structured Review for Taxonomy Development; JMIR Formative Research[13]	Structured review and taxonomy development	The study develops a taxonomy with cloud, data, device and legal dimensions. It identifies 15 components and 57 subcategories, showing that legal issues have a direct impact on cloud privacy in sensitive health-data contexts.
Ali et al. (2025)	Security and privacy in multi-cloud and hybrid cloud environments: Challenges, strategies,	Comprehensive review	The review identifies privacy and security concerns in multi-cloud and hybrid-cloud environments, including data confidentiality, access control, secure communication, regulatory compliance, cross-cloud threats and side-channel risks.

9 Rudy Adee & Haralambos Mouratidis, A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography, 22 Sensors 1109 (2022), https://doi.org/10.3390/s22031109.

10 Nazila Soveizi, Fatih Turkmen & Dimka Karastoyanova, Security and Privacy Concerns in Cloud-Based Scientific and Business Workflows: A Systematic Review, 148 Future Generation Computer Systems 184 (2023), https://doi.org/10.1016/j.future.2023.05.015.

11 Abdelhakim Issaoui, Johan Ortensjo & M. S. Islam, Exploring the General Data Protection Regulation (GDPR) Compliance in Cloud Services: Insights from Swedish Public Organizations on Privacy Compliance, 9 Future Business Journal 107 (2023), https://doi.org/10.1186/s43093-023-00285-2.

12 Nnaemeka Ukeje, Jairo Gutierrez & Krassie Petrova, Information Security and Privacy Challenges of Cloud Computing for Government Adoption: A Systematic Review, 23 International Journal of Information Security 1459 (2024), https://doi.org/10.1007/s10207-023-00797-6.

13 Zeinab Zandesh, Privacy, Security, and Legal Issues in the Health Cloud: Structured Review for Taxonomy Development, 8 JMIR Formative Research e38372 (2024), https://doi.org/10.2196/38372.

	and future directions; Computers & Security[14]		
Junior et al. (2025)	Cloud data privacy protection with homomorphic algorithm: a systematic literature review; Journal of Cloud Computing[15]	Systematic literature review	The authors examine homomorphic algorithms for cloud data privacy and note that these techniques allow computation on encrypted data, but computational overhead and complexity remain important barriers for real-time use.
Hao (2026)	Data security strategies and technologies for robust cloud computing; Discover Applied Sciences[16]	Review with real-world case analysis	The paper reviews encryption, access control and privacy-preserving computation, emphasizing practical trade-offs between security, performance and cost in complex or multi-cloud environments.

2.1 Research Gap

Existing studies discuss privacy issues in cloud computing mainly from a technical point of view, such as encryption, access control, authentication and data security mechanisms. However, limited research focuses on cloud privacy challenges under Indian IT law. Important legal issues such as user consent, data misuse, unauthorized access, cross-border data storage, jurisdiction and liability of cloud service providers are still not explained in depth. There is also limited discussion on the role of the DPDP Act, 2023 in protecting cloud users' personal data. Therefore, this study addresses this gap by examining whether the present Indian legal framework is sufficient to protect privacy in cloud computing.

3. RESEARCH METHODOLOGY

This paper follows a doctrinal legal research method supported by technical standards analysis. Primary legal sources include the Information Technology Act, 2000, subordinate rules made under the IT Act, the Digital Personal Data Protection Act, 2023, the Digital Personal Data Protection Rules, 2025, CERT-In directions and the Supreme Court privacy judgment. Technical and policy sources include NIST publications on cloud computing and cloud privacy, Cloud Security Alliance security guidance and OECD principles on government access to privately held personal data.

The study is limited to privacy challenges under Indian IT law and allied data protection law. It does not provide legal advice for any specific cloud contract, nor does it assess the compliance position of a particular provider. The analysis is based on statutory provisions, official rules, government notifications, judicial principles and recognised cyber-security standards available up to June 2026.

4. CONCEPTUAL BACKGROUND OF CLOUD PRIVACY

Cloud computing changes the traditional assumption that an organisation directly controls the physical location, hardware and administrative access to its data. In infrastructure as a service, platform as a service and software as a service models, operational control may be divided between the customer and provider. This

14 Shoukat Ali et al., Security and Privacy in Multi-Cloud and Hybrid Cloud Environments: Challenges, Strategies, and Future Directions, 157 Computers & Security 104599 (2025), https://doi.org/10.1016/j.cose.2025.104599.
15 Manuel A. Junior et al., Cloud Data Privacy Protection with Homomorphic Algorithm: A Systematic Literature Review, 14 Journal of Cloud Computing 84 (2025), https://doi.org/10.1186/s13677-025-00774-5.
16 Hao Hao, Data Security Strategies and Technologies for Robust Cloud Computing, 8 Discover Applied Sciences 91 (2026), https://doi.org/10.1007/s42452-025-08091-x.

division creates a shared-responsibility problem: the customer may remain legally answerable for personal data while the provider controls many technical measures that affect confidentiality, integrity, availability, deletion and audit evidence.[17]

Privacy in the cloud includes more than secrecy. It includes lawful collection, transparency, purpose limitation, retention control, access governance, deletion, portability, accountability, incident response and limits on onward disclosure. A privacy breach may occur even when data is not publicly leaked, for example where data is retained beyond the purpose, processed without valid notice, transferred to an unauthorised processor, exposed to excessive administrator access or made available to government agencies without lawful safeguards.[18]

The technical features of public cloud services intensify privacy risks because data may be replicated for redundancy, stored in backups, cached in content delivery systems, logged for security monitoring and processed by multiple sub-processors. Such processing can be legitimate and useful, but it must be mapped clearly because privacy compliance depends on knowing the categories of personal data, processing purposes, access roles, retention periods and legal basis for transfer or disclosure.[19]

5. INDIAN LEGAL FRAMEWORK APPLICABLE TO CLOUD PRIVACY

The Information Technology Act, 2000 remains the foundation of India's cyber law. For privacy in cloud computing, section 43A is significant because it provides compensation where a body corporate handling sensitive personal data or information is negligent in implementing and maintaining reasonable security practices and procedures, causing wrongful loss or wrongful gain. Section 72A is also relevant because it deals with punishment for disclosure of information in breach of lawful contract, while other IT Act provisions address unauthorised access, cyber offences and lawful interception or monitoring.[20]

The SPDI Rules, 2011 operationalised section 43A by defining sensitive personal data or information and requiring privacy policies, collection limitation, consent, purpose limitation, disclosure controls, transfer conditions and reasonable security practices. Although the DPDP framework has now become the central personal data protection framework, the SPDI Rules remain important in understanding the historical development of Indian privacy compliance and the way cloud customers traditionally assessed security, consent, policy publication and grievance handling.[21]

The Digital Personal Data Protection Act, 2023 gives India a broader statutory structure for digital personal data. It regulates the processing of digital personal data, recognises data principals and data fiduciaries, requires notice and consent except in permitted situations, imposes security safeguards, and creates rights and duties connected with digital personal data. For cloud computing, this means that organisations using cloud services

17 Nora Kaaniche & Maryline Laurent, Data Security and Privacy Preservation in Cloud Storage Environments Based on Cryptographic Mechanisms, 111 Computer Communications 120 (2017), https://doi.org/10.1016/j.comcom.2017.07.006.
18 Nandita Singh & Amit Chatterjee, Data Privacy Protection Mechanisms in Cloud, 3 Data Science & Engineering 24 (2018), https://doi.org/10.1007/s41019-017-0046-0.
19 Josep Domingo-Ferrer et al., Privacy-Preserving Cloud Computing on Sensitive Data: A Survey of Methods, Products and Challenges, 140-141 Computer Communications 38 (2019), https://doi.org/10.1016/j.comcom.2019.04.011.
20 Graham Greenleaf, India's 2023 Data Privacy Act: Business/Government Friendly, Consumer Hostile, 185 Privacy Laws & Business International Report 1 (2023), https://doi.org/10.2139/ssrn.4666389.
21 Acharaj Kaur Tuteja & Digvijay Singh, Data Protection in India: Privacy, Personal Data, and the Saga of a Legislative and Economical Approach, 6 GNLU Journal of Law & Economics 92 (2023), https://gjle.in/wp-content/uploads/2024/03/Paper-5.pdf.

must not only secure data but also ensure that processing through cloud infrastructure remains tied to a lawful purpose and valid governance mechanism.[22]

The Digital Personal Data Protection Rules, 2025 provide implementation details and were notified by the Government of India in November 2025. The official PIB note states that the rules give full effect to the DPDP Act and form a citizen-centred framework for privacy protection and responsible data use. For cloud-based processing, the rules make compliance more operational because organisations must design notices, consent processes, breach procedures and accountability mechanisms that can work even when data is handled through outsourced or distributed systems.

CERT-In directions and advisories are also highly relevant because cloud privacy failures often begin as cyber-security failures. CERT-In has issued directions covering incident reporting, log maintenance, point-of-contact designation and information sharing, while its advisory on data breaches identifies misconfiguration, weak credentials, exposed tokens, inadequate access control, insecure APIs and poor cloud storage configuration as common causes of data leakage. These points directly connect cloud security controls with legal duties to prevent, detect and report incidents.[23]

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 may become relevant where the cloud-related entity also acts as an intermediary or stores/transmits third-party information on behalf of users. The intermediary framework emphasises due diligence and grievance redressal, but it does not fully resolve cloud privacy issues because enterprise cloud providers may operate in several roles depending on the service model and contract. Legal classification is therefore a key step in cloud privacy compliance.

Table 2: Key Indian Legal Provisions Relevant to Cloud Privacy

Legal source	Main relevance to cloud privacy	Cloud issue addressed
Information Technology Act, 2000	Cyber offences, compensation for negligence, wrongful disclosure, interception and CERT-In powers	Unauthorised access, disclosure, liability and incident handling
SPDI Rules, 2011	Privacy policy, consent, collection limitation, disclosure, transfer and reasonable security practices	Sensitive personal data handling and security safeguards
DPDP Act, 2023	Digital personal data processing, data principal rights, data fiduciary duties and breach governance	Lawful processing, notice, consent, security and accountability
DPDP Rules, 2025	Operational rules for DPDP implementation	Notice, consent management, breach processes and regulatory mechanisms
CERT-In Directions and Advisories	Incident reporting, logs, point of contact and breach-prevention guidance	Misconfiguration, tokens, encryption, IAM, logs and breach response
IT Rules, 2021	Intermediary due diligence and grievance redressal	Relevant when cloud-related entities act as intermediaries

6. MAJOR PRIVACY CHALLENGES IN CLOUD COMPUTING UNDER IT LAW

22 Subhajit Saha & Surjashis Mukhopadhyay, A New Age of Data Privacy Laws in India: Review of Digital Personal Data Protection Act, 2023, 10 International Journal of Law and Social Sciences 84 (2024), https://doi.org/10.60143/ijls.v10.i1.2024.114.

23 Pei-Jen Sun, Security and Privacy Protection in Cloud Computing: Discussions and Challenges, 160 Journal of Network & Computer Applications 102642 (2020), https://doi.org/10.1016/j.jnca.2020.102642.

- The major challenge is loss of direct control over data. When organisations move data to cloud platforms, they may still decide the purpose of processing, but the provider controls data centre operations, virtualization layers, identity management features, encryption tools, backups and logging systems. Under Indian privacy law, this creates a compliance gap if the organisation remains responsible to data principals but lacks contractual rights to audit, delete, restrict access or obtain incident evidence from the provider.[24]
- The challenge is uncertainty about data location and cross-border processing. Cloud services may allow customers to choose regions, but data may still be replicated, backed up, supported or accessed from other jurisdictions depending on the service architecture. Indian law increasingly treats personal data governance as a fiduciary responsibility, and cross-border handling requires organisations to understand where data is processed, which laws may apply, and whether foreign government access or contractual disclosure obligations could affect privacy expectations.[25]
- The challenge is consent and notice in complex cloud ecosystems. A cloud user may give consent to a business, but the actual processing may involve the business, cloud provider, analytics service, backup provider, customer support tool and security monitoring service. If the notice does not explain processing clearly, or if consent is used for purposes that are broader than necessary, cloud adoption can become inconsistent with privacy principles of transparency, purpose limitation and data minimisation.[26]
- The challenge is cloud misconfiguration. CERT-In specifically identifies misconfigured cloud instances, public accessibility of storage buckets, exposed access tokens, poor segregation of production and testing environments, weak access controls and lack of encryption as causes of data breach and leakage. From a legal perspective, such failures may indicate absence of reasonable security practices and may trigger duties relating to incident reporting, user intimation, compensation or regulatory scrutiny. [27]
- The challenge is identity and access management. Cloud platforms permit fine-grained access control, but privacy risk increases when organisations use excessive privileges, shared administrator accounts, weak passwords, lack of multi-factor authentication or poor key management. These failures can convert a technical weakness into a legal problem because unauthorised access may expose personal data, trade secrets, health records, financial information or other sensitive categories stored in cloud applications.[28]
- The challenge is data retention and deletion. Cloud services often retain data in backups, logs, snapshots, disaster recovery systems and archives. Even when a user requests erasure or a processing purpose ends, deletion may not be immediate across every copy. Indian data protection compliance therefore requires retention schedules, deletion workflows, backup expiry policies and provider commitments that align with legal duties and can be demonstrated through records or audit trails.[29]

---

24 Nora Kaaniche & Maryline Laurent, Data Security and Privacy Preservation in Cloud Storage Environments Based on Cryptographic Mechanisms, 111 Computer Communications 120 (2017), https://doi.org/10.1016/j.comcom.2017.07.006.

25 Abdelhakim Issaoui, Johan Ortensjo & M. S. Islam, Exploring the General Data Protection Regulation (GDPR) Compliance in Cloud Services: Insights from Swedish Public Organizations on Privacy Compliance, 9 Future Business Journal 107 (2023), https://doi.org/10.1186/s43093-023-00285-2.

26 Abdelhakim Issaoui, Johan Ortensjo & M. S. Islam, Exploring the General Data Protection Regulation (GDPR) Compliance in Cloud Services: Insights from Swedish Public Organizations on Privacy Compliance, 9 Future Business Journal 107 (2023), https://doi.org/10.1186/s43093-023-00285-2.

27 Pei-Jen Sun, Security and Privacy Protection in Cloud Computing: Discussions and Challenges, 160 Journal of Network & Computer Applications 102642 (2020), https://doi.org/10.1016/j.jnca.2020.102642.

28 Pei-Jen Sun, Security and Privacy Protection in Cloud Computing: Discussions and Challenges, 160 Journal of Network & Computer Applications 102642 (2020), https://doi.org/10.1016/j.jnca.2020.102642.

29 Junaid Hassan et al., The Rise of Cloud Computing: Data Protection, Privacy, and Open Research Challenges - A Systematic Literature Review (SLR), 2022 Computational Intelligence & Neuroscience art. 8303504 (2022), https://doi.org/10.1155/2022/8303504.

- The challenge is breach detection and notification. Cloud customers may not discover an incident unless the provider shares logs, alerts and forensic information in time. CERT-In directions require certain entities to report cyber incidents and maintain logs, while the DPDP framework requires appropriate handling of personal data breaches. Organisations must therefore ensure that cloud contracts include timelines, cooperation clauses, evidence preservation, incident classification and notification workflows.[30]
- The challenge is vendor lock-in and audit dependency. Once data, applications and identity systems are deeply integrated into a cloud platform, it may be difficult to move to another provider or independently verify compliance. Privacy accountability can become weak if the customer relies only on marketing claims rather than audit reports, security certifications, contractual warranties, data processing terms and technical testing. Cloud contracts should therefore include portability, exit assistance, audit rights and sub-processor transparency.[31]
- The challenge is lawful government access. Cloud providers may receive lawful orders for access, interception, monitoring, decryption assistance or information sharing depending on applicable laws. Privacy protection requires that government access be based on legality, legitimate aim, necessity, proportionality and procedural safeguards. These principles are consistent with the Puttaswamy judgment and with the OECD declaration on government access to personal data held by private-sector entities.
- The challenge is metadata and behavioural profiling. Cloud services may collect usage logs, device identifiers, IP addresses, security telemetry and interaction records. Even where content is encrypted, metadata can reveal user behaviour, business activity, location patterns and relationships. Under a modern privacy approach, organisations should treat metadata governance as part of personal data governance wherever such data can identify or relate to an individual.[32]

Table 3: Cloud Privacy Challenges and Suggested Controls

Cloud privacy challenge	Legal risk	Suggested control
Unclear control over data	Weak accountability and inability to fulfil data principal rights	Role mapping, data processing agreement, audit rights
Cross-border processing	Unclear applicable law and government access risk	Data map, region selection, transfer assessment, access safeguards
Cloud misconfiguration	Data breach, negligence and regulatory action	Secure configuration baseline, continuous scanning, least privilege
Weak identity management	Unauthorised access and data disclosure	MFA, key rotation, privileged access review, zero-trust controls
Retention and deletion gaps	Processing beyond purpose and failure to erase	Retention schedule, backup expiry, deletion certificate
Delayed breach detection	Late reporting and weak user protection	Log retention, SIEM alerts, incident playbooks, provider cooperation

7. LEGAL ANALYSIS: ALLOCATION OF RESPONSIBILITY

30 Nazila Soveizi, Fatih Turkmen & Dimka Karastoyanova, Security and Privacy Concerns in Cloud-Based Scientific and Business Workflows: A Systematic Review, 148 Future Generation Computer Systems 184 (2023), https://doi.org/10.1016/j.future.2023.05.015.

31 Nnaemeka Ukeje, Jairo Gutierrez & Krassie Petrova, Information Security and Privacy Challenges of Cloud Computing for Government Adoption: A Systematic Review, 23 International Journal of Information Security 1459 (2024), https://doi.org/10.1007/s10207-023-00797-6.

32 Zeinab Zandesh, Privacy, Security, and Legal Issues in the Health Cloud: Structured Review for Taxonomy Development, 8 JMIR Formative Research e38372 (2024), https://doi.org/10.2196/38372.

A central legal question is who is responsible when personal data is processed in the cloud. Under the DPDP framework, the entity that determines the purpose and means of processing is generally placed in the position of a data fiduciary, while another entity may process data on its behalf. In many enterprise cloud arrangements, the customer organisation is likely to determine the business purpose, while the cloud provider supplies technical infrastructure or application services. However, this classification depends on actual control, contractual terms and the nature of the processing.[33]

The practical implication is that cloud customers cannot transfer privacy responsibility merely by outsourcing storage or processing. If the customer collects personal data from users, chooses to use a cloud platform and determines processing purposes, it must ensure that the provider's security, retention, deletion, sub-processing and incident response practices support legal compliance. Outsourcing may transfer operational tasks, but it does not automatically transfer accountability to affected data principals or regulators.[34]

Cloud providers also carry responsibilities where they are covered as body corporates, service providers, intermediaries, data centres or processors under applicable law and directions. CERT-In directions refer to categories such as service providers, intermediaries, data centres, body corporates and government organisations, which is relevant because many cloud businesses fall within one or more of these descriptions. The more control a provider exercises over security, logs, support access and sub-processing, the greater the need for transparent compliance evidence.

Reasonable security practices should be interpreted dynamically in the cloud context. Static policies are not enough where cloud risks include exposed buckets, stolen tokens, vulnerable APIs, insecure development pipelines, excessive permissions and weak monitoring. Reasonable security should include encryption in transit and at rest, strong identity controls, key management, logging, monitoring, least privilege, vulnerability management, backup governance, incident response and regular audits.[35]

8. COMPARATIVE STANDARDS AND BEST PRACTICES

NIST SP 800-144 is a useful standard for cloud privacy because it treats public cloud computing as a model that creates security and privacy concerns requiring risk assessment before outsourcing. It highlights governance, compliance, trust, architecture, identity and access management, software isolation, data protection, availability and incident response. These themes match Indian legal concerns because privacy law increasingly asks organisations to demonstrate that processing is controlled, secure, limited and accountable.

Cloud Security Alliance guidance adds a practical cloud-native perspective by organising controls around governance, risk, compliance, identity, infrastructure, application security, data security and incident response. It is particularly helpful for organisations translating Indian legal duties into operational control measures. For example, a legal requirement to protect personal data can be implemented through encryption, access review, zero-trust design, secure configuration, key rotation and continuous monitoring.

OECD principles on government access to personal data are also useful because cloud data may be stored with private-sector providers that receive access requests from public authorities. The OECD declaration emphasises legal basis, legitimate aims, approvals, handling, transparency, oversight and redress. These concepts help

33 Abdelhakim Issaoui, Johan Ortensjo & M. S. Islam, Exploring the General Data Protection Regulation (GDPR) Compliance in Cloud Services: Insights from Swedish Public Organizations on Privacy Compliance, 9 Future Business Journal 107 (2023), https://doi.org/10.1186/s43093-023-00285-2.

34 Nnaemeka Ukeje, Jairo Gutierrez & Krassie Petrova, Information Security and Privacy Challenges of Cloud Computing for Government Adoption: A Systematic Review, 23 International Journal of Information Security 1459 (2024), https://doi.org/10.1007/s10207-023-00797-6.

35 Pei-Jen Sun, Security and Privacy Protection in Cloud Computing: Discussions and Challenges, 160 Journal of Network & Computer Applications 102642 (2020), https://doi.org/10.1016/j.jnca.2020.102642.

Indian organisations evaluate whether contractual and technical measures can respond to access requests without undermining privacy expectations recognised under constitutional and statutory law.

9. DISCUSSION

The first finding is that Indian IT law has moved from a narrow security-negligence approach toward a broader personal data protection approach. Section 43A and the SPDI Rules focused mainly on sensitive personal data, reasonable security practices and compensation for negligence. The DPDP Act and DPDP Rules now create a wider framework based on lawful processing, notices, consent, data principal rights, data fiduciary obligations and breach governance. This shift is important for cloud computing because privacy risk often arises even before a breach occurs.[36]

The second finding is that cloud privacy depends on accurate role mapping. The same entity may be a cloud customer in one transaction, a processor in another and an intermediary or service provider in a third. Without role mapping, an organisation may fail to identify who must provide notice, obtain consent, maintain logs, report incidents, implement security controls, respond to erasure requests or cooperate with regulators. Role clarity should therefore be included in every cloud data protection impact assessment and cloud service agreement.[37]

The third finding is that misconfiguration is one of the most legally significant cloud privacy risks because it is preventable and well recognised by authorities. CERT-In's advisory directly warns about public cloud storage exposure, exposed tokens, testing environments, weak access control and lack of encryption. Where a known cloud risk is ignored, it becomes difficult for an organisation to claim that reasonable security practices were maintained.

The fourth finding is that cross-border and multi-jurisdictional processing remain challenging. Cloud architecture often separates data storage, technical support, security monitoring and legal control across jurisdictions. Even where Indian law allows a transfer, organisations must still ensure notice, contract, security, accountability and lawful access safeguards. A formal data map and transfer assessment are therefore essential for cloud privacy governance.[38]

The fifth finding is that cloud contracts are privacy instruments, not merely commercial documents. Service level agreements, data processing agreements, support terms, sub-processor terms, audit clauses, retention schedules, incident response clauses and exit provisions collectively determine whether the customer can comply with Indian IT law. A weak contract can make a technically secure cloud service legally risky because the customer may not have timely access to logs, deletion evidence or breach information.[39]

10. RECOMMENDATIONS

Organisations should begin cloud adoption with a data inventory that identifies personal data, sensitive categories, processing purposes, users, systems, cloud regions, sub-processors, retention periods and legal bases. This inventory should be maintained throughout the cloud life cycle because privacy obligations cannot

36 Subhajit Saha & Surjashis Mukhopadhyay, A New Age of Data Privacy Laws in India: Review of Digital Personal Data Protection Act, 2023, 10 International Journal of Law and Social Sciences 84 (2024), https://doi.org/10.60143/ijls.v10.i1.2024.114.

37 Abdelhakim Issaoui, Johan Ortensjo & M. S. Islam, Exploring the General Data Protection Regulation (GDPR) Compliance in Cloud Services: Insights from Swedish Public Organizations on Privacy Compliance, 9 Future Business Journal 107 (2023), https://doi.org/10.1186/s43093-023-00285-2.

38 Shoukat Ali et al., Security and Privacy in Multi-Cloud and Hybrid Cloud Environments: Challenges, Strategies, and Future Directions, 157 Computers & Security 104599 (2025), https://doi.org/10.1016/j.cose.2025.104599.

39 Zeinab Zandesh, Privacy, Security, and Legal Issues in the Health Cloud: Structured Review for Taxonomy Development, 8 JMIR Formative Research e38372 (2024), https://doi.org/10.2196/38372.

be satisfied unless an organisation knows what data exists, why it is processed, where it is stored and who can access it.

Cloud contracts should expressly address privacy and cyber-security obligations. Essential clauses include processing purpose, confidentiality, encryption, access control, breach notification timelines, CERT-In cooperation, data principal request support, sub-processor approval, audit rights, data localisation or region commitments where needed, deletion certificates, backup retention, portability and exit assistance. These clauses help connect legal responsibility with technical control.

Technical safeguards should be implemented according to a shared-responsibility model. Customers should configure identity and access management, multi-factor authentication, least privilege, network segmentation, encryption, key management, secure APIs, logging, monitoring, vulnerability management and backup policies. Providers should supply secure infrastructure, transparent configuration options, incident support, resilience controls and reliable compliance documentation.

Privacy notices and consent flows should be rewritten for cloud reality. Notices should explain the categories of data processed, the purpose of processing, the use of processors, retention periods, rights of users and grievance mechanisms in clear language. Where consent is required, it should not be hidden in broad terms that cover unrelated processing. Cloud analytics, profiling and support access should be separately assessed because they may create additional privacy effects.

Organisations should conduct periodic cloud privacy audits. Audits should test whether storage buckets are publicly exposed, access tokens are protected, administrator privileges are justified, encryption is enabled, logs are retained securely, backups follow retention rules, testing environments are segregated, and incident response plans are functional. The audit should produce evidence that can be used to show compliance with reasonable security and data protection obligations.

Public authorities and regulators should consider issuing cloud-specific guidance under Indian data protection and cyber law. Such guidance could clarify data fiduciary and processor roles in cloud services, minimum cloud contract clauses, breach coordination between customers and providers, cross-border support access, deletion standards for backups and expectations for encryption and key management. This would reduce uncertainty and improve compliance consistency across sectors.

11. CONCLUSION

Cloud computing improves scalability, flexibility and cost efficiency, but it also creates serious privacy challenges because personal data may be processed through distributed infrastructure, shared resources, multiple processors and cross-border systems. Under Indian IT law, these challenges are addressed through a combination of the IT Act, SPDI Rules, DPDP Act, DPDP Rules, CERT-In directions, intermediary rules and constitutional privacy principles. However, the effectiveness of these laws depends on practical implementation through contracts, security architecture, audits, notices, consent governance, breach response and role clarity.

The strongest conclusion of this study is that privacy in cloud computing must be treated as a continuous governance obligation rather than a one-time compliance formality. Organisations should adopt privacy-by-design, security-by-design and accountability-by-contract. If Indian organisations combine DPDP compliance with CERT-In readiness, NIST-based risk assessment and cloud-native controls recommended by recognised security bodies, cloud computing can be used responsibly while protecting the dignity, autonomy and informational privacy of individuals.

REFERENCES

1. Pei-Jen Sun, Security and Privacy Protection in Cloud Computing: Discussions and Challenges, 160 Journal of Network & Computer Applications 102642 (2020), https://doi.org/10.1016/j.jnca.2020.102642.

2. Nnaemeka Ukeje, Jairo Gutierrez & Krassie Petrova, Information Security and Privacy Challenges of Cloud Computing for Government Adoption: A Systematic Review, 23 International Journal of Information Security 1459 (2024), https://doi.org/10.1007/s10207-023-00797-6.
3. Subhajit Saha & Surjashis Mukhopadhyay, A New Age of Data Privacy Laws in India: Review of Digital Personal Data Protection Act, 2023, 10 International Journal of Law and Social Sciences 84 (2024), https://doi.org/10.60143/ijls.v10.i1.2024.114.
4. Nora Kaaniche & Maryline Laurent, Data Security and Privacy Preservation in Cloud Storage Environments Based on Cryptographic Mechanisms, 111 Computer Communications 120 (2017), https://doi.org/10.1016/j.comcom.2017.07.006.
5. Nandita Singh & Amit Chatterjee, Data Privacy Protection Mechanisms in Cloud, 3 Data Science & Engineering 24 (2018), https://doi.org/10.1007/s41019-017-0046-0.
6. Josep Domingo-Ferrer et al., Privacy-Preserving Cloud Computing on Sensitive Data: A Survey of Methods, Products and Challenges, 140-141 Computer Communications 38 (2019), https://doi.org/10.1016/j.comcom.2019.04.011.
7. Pei-Jen Sun, Security and Privacy Protection in Cloud Computing: Discussions and Challenges, 160 Journal of Network & Computer Applications 102642 (2020), https://doi.org/10.1016/j.jnca.2020.102642.
8. Yaseen S. Abdulsalam & Mohammed Hedabou, Security and Privacy in Cloud Computing: Technical Review, 14 Future Internet 11 (2022), https://doi.org/10.3390/fi14010011.
9. Rudy Adee & Haralambos Mouratidis, A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography, 22 Sensors 1109 (2022), https://doi.org/10.3390/s22031109.
10. Nazila Soveizi, Fatih Turkmen & Dimka Karastoyanova, Security and Privacy Concerns in Cloud-Based Scientific and Business Workflows: A Systematic Review, 148 Future Generation Computer Systems 184 (2023), https://doi.org/10.1016/j.future.2023.05.015.
11. Abdelhakim Issaoui, Johan Ortensjo & M. S. Islam, Exploring the General Data Protection Regulation (GDPR) Compliance in Cloud Services: Insights from Swedish Public Organizations on Privacy Compliance, 9 Future Business Journal 107 (2023), https://doi.org/10.1186/s43093-023-00285-2.
12. Nnaemeka Ukeje, Jairo Gutierrez & Krassie Petrova, Information Security and Privacy Challenges of Cloud Computing for Government Adoption: A Systematic Review, 23 International Journal of Information Security 1459 (2024), https://doi.org/10.1007/s10207-023-00797-6.
13. Zeinab Zandesh, Privacy, Security, and Legal Issues in the Health Cloud: Structured Review for Taxonomy Development, 8 JMIR Formative Research e38372 (2024), https://doi.org/10.2196/38372.
14. Shoukat Ali et al., Security and Privacy in Multi-Cloud and Hybrid Cloud Environments: Challenges, Strategies, and Future Directions, 157 Computers & Security 104599 (2025), https://doi.org/10.1016/j.cose.2025.104599.
15. Manuel A. Junior et al., Cloud Data Privacy Protection with Homomorphic Algorithm: A Systematic Literature Review, 14 Journal of Cloud Computing 84 (2025), https://doi.org/10.1186/s13677-025-00774-5.
16. Hao Hao, Data Security Strategies and Technologies for Robust Cloud Computing, 8 Discover Applied Sciences 91 (2026), https://doi.org/10.1007/s42452-025-08091-x.
17. Nora Kaaniche & Maryline Laurent, Data Security and Privacy Preservation in Cloud Storage Environments Based on Cryptographic Mechanisms, 111 Computer Communications 120 (2017), https://doi.org/10.1016/j.comcom.2017.07.006.

18. Nandita Singh & Amit Chatterjee, Data Privacy Protection Mechanisms in Cloud, 3 Data Science & Engineering 24 (2018), https://doi.org/10.1007/s41019-017-0046-0.
19. Josep Domingo-Ferrer et al., Privacy-Preserving Cloud Computing on Sensitive Data: A Survey of Methods, Products and Challenges, 140-141 Computer Communications 38 (2019), https://doi.org/10.1016/j.comcom.2019.04.011.
20. Graham Greenleaf, India's 2023 Data Privacy Act: Business/Government Friendly, Consumer Hostile, 185 Privacy Laws & Business International Report 1 (2023), https://doi.org/10.2139/ssrn.4666389.
21. Acharaj Kaur Tuteja & Digvijay Singh, Data Protection in India: Privacy, Personal Data, and the Saga of a Legislative and Economical Approach, 6 GNLU Journal of Law & Economics 92 (2023), https://gjle.in/wp-content/uploads/2024/03/Paper-5.pdf.
22. Subhajit Saha & Surjashis Mukhopadhyay, A New Age of Data Privacy Laws in India: Review of Digital Personal Data Protection Act, 2023, 10 International Journal of Law and Social Sciences 84 (2024), https://doi.org/10.60143/ijls.v10.i1.2024.114.
23. Pei-Jen Sun, Security and Privacy Protection in Cloud Computing: Discussions and Challenges, 160 Journal of Network & Computer Applications 102642 (2020), https://doi.org/10.1016/j.jnca.2020.102642.
24. Nora Kaaniche & Maryline Laurent, Data Security and Privacy Preservation in Cloud Storage Environments Based on Cryptographic Mechanisms, 111 Computer Communications 120 (2017), https://doi.org/10.1016/j.comcom.2017.07.006.
25. Abdelhakim Issaoui, Johan Ortensjo & M. S. Islam, Exploring the General Data Protection Regulation (GDPR) Compliance in Cloud Services: Insights from Swedish Public Organizations on Privacy Compliance, 9 Future Business Journal 107 (2023), https://doi.org/10.1186/s43093-023-00285-2.
26. Abdelhakim Issaoui, Johan Ortensjo & M. S. Islam, Exploring the General Data Protection Regulation (GDPR) Compliance in Cloud Services: Insights from Swedish Public Organizations on Privacy Compliance, 9 Future Business Journal 107 (2023), https://doi.org/10.1186/s43093-023-00285-2.
27. Pei-Jen Sun, Security and Privacy Protection in Cloud Computing: Discussions and Challenges, 160 Journal of Network & Computer Applications 102642 (2020), https://doi.org/10.1016/j.jnca.2020.102642.
28. Pei-Jen Sun, Security and Privacy Protection in Cloud Computing: Discussions and Challenges, 160 Journal of Network & Computer Applications 102642 (2020), https://doi.org/10.1016/j.jnca.2020.102642.
29. Junaid Hassan et al., The Rise of Cloud Computing: Data Protection, Privacy, and Open Research Challenges - A Systematic Literature Review (SLR), 2022 Computational Intelligence & Neuroscience art. 8303504 (2022), https://doi.org/10.1155/2022/8303504.
30. Nazila Soveizi, Fatih Turkmen & Dimka Karastoyanova, Security and Privacy Concerns in Cloud-Based Scientific and Business Workflows: A Systematic Review, 148 Future Generation Computer Systems 184 (2023), https://doi.org/10.1016/j.future.2023.05.015.
31. Nnaemeka Ukeje, Jairo Gutierrez & Krassie Petrova, Information Security and Privacy Challenges of Cloud Computing for Government Adoption: A Systematic Review, 23 International Journal of Information Security 1459 (2024), https://doi.org/10.1007/s10207-023-00797-6.
32. Zeinab Zandesh, Privacy, Security, and Legal Issues in the Health Cloud: Structured Review for Taxonomy Development, 8 JMIR Formative Research e38372 (2024), https://doi.org/10.2196/38372.
33. Abdelhakim Issaoui, Johan Ortensjo & M. S. Islam, Exploring the General Data Protection Regulation (GDPR) Compliance in Cloud Services: Insights from Swedish Public Organizations on Privacy Compliance, 9 Future Business Journal 107 (2023), https://doi.org/10.1186/s43093-023-00285-2.

34. Nnaemeka Ukeje, Jairo Gutierrez & Krassie Petrova, Information Security and Privacy Challenges of Cloud Computing for Government Adoption: A Systematic Review, 23 International Journal of Information Security 1459 (2024), https://doi.org/10.1007/s10207-023-00797-6.
35. Pei-Jen Sun, Security and Privacy Protection in Cloud Computing: Discussions and Challenges, 160 Journal of Network & Computer Applications 102642 (2020), https://doi.org/10.1016/j.jnca.2020.102642.
36. Subhajit Saha & Surjashis Mukhopadhyay, A New Age of Data Privacy Laws in India: Review of Digital Personal Data Protection Act, 2023, 10 International Journal of Law and Social Sciences 84 (2024), https://doi.org/10.60143/ijls.v10.i1.2024.114.
37. Abdelhakim Issaoui, Johan Ortensjo & M. S. Islam, Exploring the General Data Protection Regulation (GDPR) Compliance in Cloud Services: Insights from Swedish Public Organizations on Privacy Compliance, 9 Future Business Journal 107 (2023), https://doi.org/10.1186/s43093-023-00285-2.
38. Shoukat Ali et al., Security and Privacy in Multi-Cloud and Hybrid Cloud Environments: Challenges, Strategies, and Future Directions, 157 Computers & Security 104599 (2025), https://doi.org/10.1016/j.cose.2025.104599.
39. Zeinab Zandesh, Privacy, Security, and Legal Issues in the Health Cloud: Structured Review for Taxonomy Development, 8 JMIR Formative Research e38372 (2024), https://doi.org/10.2196/38372.