Cybersecurity Challenges and Solutions in Cloud Computing

Akanksha Korhale[1], Shivam Salunkhe[2]

Student, Department of Computer Applications (MCA),D. Y. Patil Institute of Master of Computer Applications and Management, Maharashtra, India.

Dr Sanket Lodha

Assistant Professor and Research Guide, Department of Computer Applications (MCA),D. Y. Patil Institute of Master of Computer Applications and Management, Maharashtra, India.

Abstract**—***Cloud computing has become the default delivery model for enterprise, government and consumer services because of its elasticity, pay-per-use economics and global reach. The same properties, namely multi-tenancy, resource pooling, internet-facing management interfaces and shared responsibility between provider and customer, enlarge the attack surface and blur accountability. This paper presents a structured review of cybersecurity challenges in cloud computing and of the solutions proposed in the literature and in industry guidance. Threats are organised along the three service models (IaaS, PaaS, SaaS) and along five cross-cutting concerns: data security and privacy, identity and access management, virtualization and multi-tenancy, application and interface security, and governance and compliance. Each threat class is mapped to technical and organisational countermeasures, including encryption and searchable or homomorphic schemes, attribute-based access control, multi-factor authentication, Zero Trust architecture, micro-segmentation, remote data auditing, intrusion detection, secure DevOps and continuous compliance monitoring. A layered defence framework with a misconfiguration-focused feedback loop is proposed, together with an evaluation plan for future empirical validation. The paper is a secondary-source, literature-based study; no new experimental measurements are claimed, and no vendor is endorsed. The findings are intended as a reference for students, practitioners and researchers planning secure cloud adoption.*

Index Terms**—***Cloud Computing; Cybersecurity; Data Privacy; Identity and Access Management; Multi-Tenancy; Zero Trust; Encryption; Shared Responsibility; Compliance.*

I. INTRODUCTION

Cloud computing is defined by the U.S. National Institute of Standards and Technology (NIST) as a model for enabling ubiquitous, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned with minimal management effort [1]. Its essential characteristics are on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service, delivered through the Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) models and deployed as public, private, community or hybrid clouds [1], [2], [3].

These characteristics are also the source of its security difficulties. Customers hand over physical control of servers, networks and storage to a provider, share hardware with unknown tenants, and manage their resources through web consoles and application programming interfaces (APIs) that are reachable from the internet [4], [5]. A single misconfigured storage bucket, a leaked access key or a weakly protected administrator account can expose very large volumes of data. Security in the cloud is therefore not simply traditional security hosted elsewhere; it requires a re-examination of trust boundaries, responsibility and control [6], [7].

The aim of this paper is to organise the cybersecurity challenges of cloud computing into a coherent taxonomy and to connect each challenge with practical solutions drawn from peer-reviewed research, standards and industry guidance.

1.1 Research Gap and Problem Statement

Three limitations in existing treatments motivate this work: (i) many surveys describe threats and defences separately, which leaves readers without a clear mapping from a specific threat to a specific control; (ii) discussions often ignore the shared-responsibility model, so customer-side misconfiguration, which is among the most common causes of cloud incidents, receives less attention than provider-side vulnerabilities [11], [12]; and (iii) newer concerns such as Zero Trust, API security and regional data-protection law are scattered across separate sources [16], [27], [28]. The research problem is therefore to consolidate these threads into a reproducible, service-model-aware review and a layered defence framework.

1.2 Objectives

- Describe the cloud service and deployment models and the associated trust boundaries.
- Classify major cybersecurity threats in cloud environments by service model and by concern.

- Review technical, architectural and organisational solutions for each threat class.
- Propose a layered defence framework that includes a continuous feedback loop.
- Summarise regulatory and ethical considerations, including Indian and European data-protection law.
- Identify limitations and future research directions.

1.3 Contributions

- A threat taxonomy that links service models, attack vectors and affected security properties (confidentiality, integrity, availability).
- A threat-to-solution mapping table suitable for design reviews and teaching.
- A six-layer defence framework that treats misconfiguration, identity and monitoring as first-class concerns.
- An evaluation plan with metrics for future empirical validation.

II. BACKGROUND AND RELATED WORK

2.1 Cloud Service and Deployment Models

In IaaS the provider supplies virtualised compute, storage and networking, while the customer controls operating systems, middleware and applications. In PaaS the provider also manages the runtime, and the customer controls applications and data. In SaaS the provider manages nearly the entire stack, and the customer controls mainly data, user access and configuration [1], [3]. Public clouds serve many tenants on shared infrastructure; private clouds are dedicated to one organisation; hybrid clouds combine both and add the complexity of securing the links between them [2], [26].

2.2 Shared Responsibility

Major providers describe security as a shared responsibility: the provider secures the underlying facilities, hardware and virtualization layer, and the customer secures what it deploys and configures. The boundary moves with the service model, and misunderstanding it is a frequent cause of gaps [12], [13]. Table I summarises a typical division.

TABLE I. TYPICAL SHARED-RESPONSIBILITY DIVISION

Layer	IaaS	PaaS	SaaS
Physical / hypervisor	Provider	Provider	Provider
OS and patching	Customer	Provider	Provider
Application code	Customer	Customer	Provider
Data and classification	Customer	Customer	Customer
Identities and access	Customer	Customer	Customer

2.3 Prior Surveys

Early work by Armbrust et al. identified data confidentiality, availability and auditability among the top obstacles to cloud adoption [2]. Takabi et al. highlighted multi-tenancy, trust and policy integration [4], and Zissis and Lekkas proposed addressing cloud security through a trusted third party and cryptographic protection [5]. Subashini and Kavitha analysed issues by service delivery model [7], while Modi et al. reviewed vulnerabilities and countermeasures layer by layer [18]. Later surveys by Khalil et al. [14], Ali et al. [13], Singh and Chatterjee [25] and Xiao and Xiao [26] expanded the coverage to include privacy, forensics and mobile cloud issues. Grobauer et al. argued that cloud vulnerabilities should be understood in terms of the essential cloud characteristics rather than as generic IT weaknesses [24]. The Cloud Security Alliance (CSA) periodically publishes ranked lists of top threats and guidance for critical focus areas [11], [12]. This paper builds on these sources and adds a threat-to-solution mapping and a feedback-oriented framework.

III. MATERIALS AND METHODS

3.1 Study Design

This is a secondary-source, qualitative review. No new participant data, system logs or experimental benchmarks were collected. Sources were selected from peer-reviewed journals and conference proceedings, standards from NIST, guidance from the Cloud Security Alliance, and primary legal texts. Preference was given to widely cited foundational papers and to standards that are publicly available. Readers are advised to verify current editions of standards and legislation before applying them.

3.2 Classification Approach

Threats were grouped by (a) the service model most affected, and (b) one of five concerns: data security and privacy; identity and access management (IAM); virtualization and multi-tenancy; application and interface security; and governance, risk and compliance. Each threat was assigned the security property primarily at risk (confidentiality, integrity or availability) and matched with countermeasures that appear in the literature or in NIST control catalogues [29].

3.3 Limits of the Method

A literature review reflects the state of published knowledge, which lags the threat landscape. Incident statistics change yearly and are therefore not tabulated here; readers should consult current threat reports. Severity ranking is qualitative and context dependent.

IV. CYBERSECURITY CHALLENGES IN CLOUD COMPUTING

4.1 Data Security and Privacy

Data breaches and data loss are consistently ranked among the most serious cloud risks [11]. In the cloud, data may be replicated across regions, handled by sub-processors and persist after deletion requests, which complicates confidentiality and retention [4], [15]. Customers may lack visibility into where data is stored, creating jurisdictional and sovereignty concerns [26]. Insider misuse at the provider or customer, insecure backups and weak key management further threaten data. Integrity and

availability are also at risk: a client has to be assured that outsourced files remain intact and retrievable without downloading them in full [19], [20].

4.2 Identity and Access Management

Because cloud resources are managed over the network, credentials are the new perimeter. Threats include weak or reused passwords, phishing, stolen API keys committed to public code repositories, excessive privileges, orphaned accounts and unmanaged service identities [11], [12]. Federated identity and single sign-on reduce password sprawl but concentrate risk in the identity provider.

4.3 Virtualization and Multi-Tenancy

Virtualization enables resource sharing but introduces hypervisor vulnerabilities, VM escape, VM sprawl and insecure snapshots [6], [18]. Ristenpart et al. showed that an attacker could co-locate a virtual machine with a target in a public cloud and use side channels to gather information [8]. Zhang et al. later demonstrated that cross-VM side channels could be used to extract private cryptographic keys [9]. Providers have since added mitigations, but the underlying risk of shared hardware remains an active research area.

4.4 Application and Interface Security

Cloud services expose APIs for provisioning, storage and management. Insecure interfaces, weak authentication, missing rate limiting and injection flaws can let attackers control resources at scale [11], [17]. Web-application vulnerabilities in SaaS and PaaS offerings, insecure containers and vulnerable third-party libraries add to the exposure. Denial-of-service attacks target availability and can also inflate customer bills through resource exhaustion.

4.5 Misconfiguration and Lack of Visibility

Publicly accessible storage, permissive security groups, disabled logging and default credentials are recurring causes of exposure in customer-managed layers, and the CSA lists misconfiguration and inadequate change control among its top threats [11], [12]. Dynamic, short-lived and multi-account environments make asset inventories hard to keep accurate.

4.6 Governance, Compliance and Vendor Lock-in

Organisations remain accountable for personal data even when it is processed by a provider. Compliance with laws such as the EU General Data Protection Regulation [27] and India's Digital Personal Data Protection Act, 2023 [28] requires lawful processing, security safeguards, breach handling and attention to cross-border transfers. Lock-in, limited portability and unclear exit terms add business continuity risks [2], [3].

TABLE II. THREAT TAXONOMY

Concern	Representative threats	Property at risk
Data security and privacy	Breach, data loss, insecure deletion, weak key management	C, I, A
IAM	Credential theft, over-privilege, API key leakage	C, I
Virtualization / tenancy	Side channels, VM escape, VM sprawl	C, I
Application / API	Insecure APIs, injection, DoS	I, A
Misconfiguration	Public storage, open ports, disabled logs	C, A
Governance	Regulatory non-compliance, lock-in, poor audit trail	A, accountability

C = confidentiality, I = integrity, A = availability.

V. SOLUTIONS AND COUNTERMEASURES

5.1 Cryptographic Protection of Data

Encryption of data at rest and in transit, with strong algorithms and customer-controlled keys managed in hardware security modules or key-management services, is the baseline control [13], [15], [29]. Searchable symmetric encryption allows keyword search over encrypted data without revealing the plaintext to the server [21]. Fully homomorphic encryption, first constructed by Gentry, permits computation on ciphertexts and points towards confidential outsourced computing, although performance overhead still restricts practical use [10]. Attribute-based encryption supports fine-grained, policy-based sharing of encrypted data [22].

5.2 Integrity and Remote Data Auditing

Provable data possession and proofs of retrievability let a client verify that an untrusted store still holds its data, using probabilistic challenges instead of full downloads [19], [20]. Privacy-preserving public auditing allows a third-party auditor to verify integrity without learning the data [23]. A survey by Sookhak et al. classifies remote auditing schemes and discusses open issues such as dynamic updates and batch verification [30].

5.3 Identity and Access Management

Recommended practices include multi-factor authentication for all privileged and remote users, least-privilege role or attribute-based access control, short-lived credentials, automated de-provisioning, secrets management and regular access reviews [12], [16], [29]. Federated identity should be protected with strong assurance levels and monitoring.

5.4 Zero Trust Architecture

NIST SP 800-207 describes Zero Trust as moving defences from static network perimeters to users, assets and resources, with no implicit trust granted based on network location [16]. In cloud settings this translates into per-request authentication and authorisation, device posture checks, micro-segmentation and continuous monitoring. Zero Trust suits hybrid and multi-cloud environments where a single perimeter does not exist.

5.5 Virtualization and Network Security

Defences include hardened and promptly patched hypervisors, isolation of sensitive workloads on dedicated hosts, VM image scanning, virtual firewalls, micro-segmentation and network intrusion detection and

prevention systems [6], [18], [26]. Placement policies and constant-time cryptographic implementations reduce exposure to side channels [8], [9].

5.6 Secure Development and API Security

Secure software development life-cycle practices, static and dynamic testing, dependency scanning, container image signing, API gateways with authentication, authorisation and rate limiting, and web application firewalls address application-layer threats [12], [17]. Infrastructure-as-code templates can be scanned before deployment to prevent insecure configurations from reaching production.

5.7 Monitoring, Detection and Response

Centralised logging, security information and event management (SIEM), cloud security posture management and anomaly detection provide visibility and early warning [13], [14]. Incident response plans should cover cloud-specific evidence handling and provider coordination, and backups should be tested and kept isolated from production credentials to limit ransomware impact.

5.8 Governance and Compliance

Organisations should classify data, record processing activities, choose regions consistent with legal requirements, review provider certifications and contracts, define exit strategies and use control frameworks such as NIST SP 800-53 for traceable control selection [27], [28], [29]. Continuous compliance checking is preferable to annual audits in fast-changing environments.

TABLE III. THREAT-TO-SOLUTION MAPPING

Threat	Primary solution	Refs.
Data breach	Encryption, key management, DLP, access control	[10], [13], [15], [22]
Data tampering / loss	PDP, PoR, public auditing, backups	[19], [20], [23], [30]
Credential theft	MFA, least privilege, secrets vaults	[12], [16], [29]
Side channels / VM escape	Patching, isolation, placement policy	[8], [9], [18]
Insecure APIs	API gateway, WAF, secure SDLC	[12], [17]
Misconfiguration	Posture management, IaC scanning, change control	[11], [12], [29]
Non-compliance	Data mapping, regional hosting, audits	[27], [28], [29]

VI. PROPOSED LAYERED DEFENCE FRAMEWORK

Building on the preceding analysis, a six-layer framework is proposed. It is conceptual and has not been implemented or experimentally validated in this study.

- Governance layer: policies, data classification, shared-responsibility matrix, regulatory mapping and vendor assessment.
- Identity layer: central identity provider, MFA, least privilege, privileged access management and secrets management.
- Data layer: encryption at rest and in transit, customer-managed keys, tokenisation or masking, backup isolation and integrity auditing.
- Network and workload layer: micro-segmentation, hardened images, container and VM isolation, and web application and DDoS protection.
- Application and pipeline layer: secure SDLC, dependency and image scanning, infrastructure-as-code checks and API protection.
- Monitoring and response layer: centralised logs, SIEM, posture management, alerting, tested incident response and recovery.

A feedback loop connects the monitoring layer back to governance: findings from posture scans, incidents and audits update policies, baselines and training. Zero Trust principles are applied across layers rather than as a separate component [16]. The framework explicitly places misconfiguration control and identity at the centre because these are customer-controlled and commonly exploited [11], [12].

6.1 Proposed Evaluation Plan

Future empirical work could evaluate the framework in a laboratory cloud tenancy using intentionally vulnerable but isolated workloads. Suggested metrics are: number of misconfigurations detected and mean time to remediate; mean time to detect and respond to simulated incidents; proportion of identities protected by MFA; encryption coverage of data stores; performance overhead of controls (latency and throughput); and cost overhead. Experiments must be performed only on systems owned by the researchers or explicitly authorised, with results reported with sample sizes and uncertainty estimates. No such results are claimed in this paper.

VII. DISCUSSION

The review shows that cloud security failures arise from a combination of inherent platform properties and everyday operational lapses. Technical research has produced strong cryptographic and virtualization defences, yet surveys repeatedly note that customer misconfiguration, identity weaknesses and unclear responsibility dominate real-world exposure [11], [12], [14], [25]. Advanced techniques such as homomorphic encryption and proofs of retrievability are valuable for specific high-assurance cases, but they carry performance costs, whereas MFA, least privilege, logging and configuration scanning are comparatively inexpensive and address a large portion of practical risk.

Small and medium organisations, including educational institutions, often lack dedicated security staff. For them, managed security services, provider-native controls, templates and automation are realistic options. Skills and awareness training should accompany technology, since phishing and credential misuse bypass technical defences. Regulatory requirements are also increasingly shaping

design choices such as region selection, retention and breach notification [27], [28].

Emerging directions include confidential computing with hardware-based trusted execution environments, machine-learning-based anomaly detection, post-quantum cryptography for long-lived data, secure multi-cloud management and automated compliance as code. These areas need further evaluation of cost, usability and adversarial robustness.

VIII. LIMITATIONS AND FUTURE WORK

- The study is a literature-based review; it contains no new experiments, measurements or case-study data.
- Threat landscapes and provider features change quickly, so conclusions may need periodic revision.
- The proposed framework is conceptual and has not been validated in a production environment.
- Provider-specific implementation details are intentionally omitted to remain vendor-neutral.
- Future work should implement the framework in a controlled test environment, measure the metrics in Section 6.1, compare single-cloud and multi-cloud settings, and examine the cost-effectiveness of controls for small organisations.

IX. ETHICAL AND LEGAL CONSIDERATIONS

This work uses only published literature and public standards. Security knowledge is dual-use; therefore, attack techniques are described at a conceptual level and no exploit procedures are provided. Any future testing must be limited to systems owned by the researchers or authorised in writing, must comply with provider acceptable-use policies and applicable law, and must protect any personal data encountered. The framework is intended to support defensive practice and education and does not guarantee protection against all attacks.

X. CONCLUSION

Cloud computing offers major benefits but changes the security landscape through multi-tenancy, shared responsibility and API-driven management. This paper organised the main cybersecurity challenges into data, identity, virtualization, application, misconfiguration and governance concerns, mapped them to proven countermeasures and proposed a six-layer defence framework with a monitoring-to-governance feedback loop. The central message is that effective cloud security depends on combining strong cryptography and architecture, such as Zero Trust, with disciplined identity management, configuration control, continuous monitoring and regulatory awareness. The effectiveness of the proposed framework remains to be established through the evaluation plan described; no unperformed experimental results are claimed.

DECLARATIONS

- Funding: The authors should confirm the funding status. If no external funding supported this work, state: “This research received no external funding.”
- Conflict of interest: The authors should confirm that no relationships could have influenced the work. If accurate, state: “The authors declare that they have no competing interests.”
- Ethics approval and consent: This is a secondary-source review with no human participants or primary data collection. The authors should verify target-journal requirements before submission.
- Data availability: No new datasets were generated. All sources are listed in the references.
- Author contributions (proposed, for confirmation): Akanksha Korhale – literature review, methodology, writing original draft; Shivam Salunkhe – taxonomy and framework design, visualization, writing review and editing; Dr. Sanket Lodha – supervision, validation, review of the final manuscript.
- Acknowledgements: The authors may acknowledge their department, institution and research guide after confirming preferred wording.
- Corresponding author: Akanksha Korhale.

REFERENCES

[1] P. Mell and T. Grance, “The NIST definition of cloud computing,” National Institute of Standards and Technology, Gaithersburg, MD, USA, Special Publication 800-145, 2011.

[2] M. Armbrust et al., “A view of cloud computing,” Commun. ACM, vol. 53, no. 4, pp. 50–58, 2010.

[3] Q. Zhang, L. Cheng, and R. Boutaba, “Cloud computing: State-of-the-art and research challenges,” J. Internet Serv. Appl., vol. 1, no. 1, pp. 7–18, 2010.

[4] H. Takabi, J. B. D. Joshi, and G.-J. Ahn, “Security and privacy challenges in cloud computing environments,” IEEE Secur. Privacy, vol. 8, no. 6, pp. 24–31, 2010.

[5] D. Zissis and D. Lekkas, “Addressing cloud computing security issues,” Future Gener. Comput. Syst., vol. 28, no. 3, pp. 583–592, 2012.

[6] M. Almorsy, J. Grundy, and I. Müller, “An analysis of the cloud computing security problem,” in Proc. APSEC Cloud Workshop, Sydney, Australia, 2010.

[7] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, 2011.

[8] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, “Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds,” in Proc. ACM Conf. Computer and Communications Security (CCS), 2009, pp. 199–212.

[9] Y. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, “Cross-VM side channels and their use to extract private keys,” in Proc. ACM CCS, 2012, pp. 305–316.

[10] C. Gentry, “Fully homomorphic encryption using ideal lattices,” in Proc. ACM Symp. Theory of Computing (STOC), 2009, pp. 169–178.

[11] Cloud Security Alliance, “Top threats to cloud computing: Egregious eleven,” 2019.

[12] Cloud Security Alliance, “Security guidance for critical areas of focus in cloud computing v4.0,” 2017.

[13] M. Ali, S. U. Khan, and A. V. Vasilakos, “Security in cloud computing: Opportunities and challenges,” Inf. Sci., vol. 305, pp. 357–383, 2015.

[14] I. Khalil, A. Khreishah, and M. Azeem, “Cloud computing security: A survey,” Computers, vol. 3, no. 1, pp. 1–35, 2014.

[15] R. Chow et al., “Controlling data in the cloud: Outsourcing computation without outsourcing control,” in Proc. ACM Cloud Computing Security Workshop (CCSW), 2009, pp. 85–90.

[16] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," NIST Special Publication 800-207, 2020.

[17] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Comput., vol. 16, no. 1, pp. 69–73, 2012.

[18] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey on security issues and solutions at different layers of cloud computing," J. Supercomput., vol. 63, no. 2, pp. 561–592, 2013.

[19] G. Ateniese et al., "Provable data possession at untrusted stores," in Proc. ACM CCS, 2007, pp. 598–609.

[20] A. Juels and B. S. Kaliski Jr., "PORs: Proofs of retrievability for large files," in Proc. ACM CCS, 2007, pp. 584–597.

[21] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Security and Privacy, 2000, pp. 44–55.

[22] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACM CCS, 2006, pp. 89–98.

[23] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proc. IEEE INFOCOM, 2010, pp. 1–9.

[24] B. Grobauer, T. Walloschek, and E. Stöcker, "Understanding cloud computing vulnerabilities," IEEE Secur. Privacy, vol. 9, no. 2, pp. 50–57, 2011.

[25] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," J. Netw. Comput. Appl., vol. 79, pp. 88–115, 2017.

[26] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," IEEE Commun. Surveys Tuts., vol. 15, no. 2, pp. 843–859, 2013.

[27] European Parliament and Council, "Regulation (EU) 2016/679 (General Data Protection Regulation)," Official Journal of the European Union, L 119, 2016.

[28] Government of India, "The Digital Personal Data Protection Act, 2023," Act No. 22 of 2023, 2023.

[29] Joint Task Force, "Security and privacy controls for information systems and organizations," NIST Special Publication 800-53, Rev. 5, 2020.

[30] M. Sookhak et al., "Remote data auditing in cloud computing environments: A survey, taxonomy, and open issues," ACM Comput. Surv., vol. 47, no. 4, Art. no. 65, 2015.