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 6, Issue 6, October 2026
Impact Factor: 8.2

A Risk-Based Layered Framework for Cloud Security: A Focused Review

P. S. Ghode, Yakshit Prashant Pandav, Om Dattatray Asmar
Department of Information Technology
Government Polytechnic, Awasari (Kh.), Maharashtra, India
Corresponding author: yaxitprashant@gmail.com

Abstract: *Cloud computing enables scalable access to infrastructure, platforms, and software, but it changes how security responsibilities are distributed between providers, customers, and third parties. Research published since the late 2000s has examined data confidentiality and integrity, virtualization, service-model risks, and cloud-provider trust. More recent guidance continues to highlight operational weaknesses, including misconfiguration, identity and access management (IAM), insecure application programming interfaces (APIs), third-party exposure, and limited security visibility. This paper presents a focused review of foundational research and selected standards and threat reports published from 2007 to 2025. The review synthesizes recurring risks and proposes a risk-based layered framework comprising governance and shared responsibility, identity and access, data protection, workload and configuration security, and detection, response, and recovery. Continuous assurance connects the layers through asset inventory, risk assessment, monitoring, testing, and improvement. The framework is a conceptual synthesis rather than an empirically validated system; it therefore supplies implementation priorities and candidate evaluation measures, not measured performance claims. The paper concludes with a practical adoption sequence and research directions for validating the framework across cloud service models and providers*

Keywords: Cloud Security, Identity and Access Management, Data Protection, Cloud Misconfiguration, Zero Trust, Continuous Monitoring.

I. INTRODUCTION

Cloud computing provides on-demand access to configurable computing resources and supports rapid provisioning, elasticity, and measured service [1], [2]. These characteristics can reduce capital requirements and simplify deployment, but they also move data, applications, identities, and operational dependencies across organizational boundaries. Cloud security is therefore not only a technical matter; it also involves governance, contractual responsibility, architecture, supplier assurance, and incident response [3], [4].

Early research documented concerns about web-service interfaces, virtualization, data location, multi-tenancy, and reliance on providers [2], [5]. Work on storage integrity explored ways to verify remotely held data without downloading complete datasets [6], [7]. Later reviews organized risks across software, platform, and infrastructure service models, emphasizing that customer control differs according to the layer being consumed [3], [8]. These findings remain relevant, although the operating environment has evolved toward managed services, containers, infrastructure as code, automated deployment, and multi-cloud configurations.

Recent cloud threat guidance places persistent attention on misconfiguration and change control, IAM, insecure APIs, third-party resources, insecure software development, accidental disclosure, vulnerabilities, and limited visibility [9]. Zero trust guidance adds that access decisions should not rely on network location alone; they should be based on verified users, devices, and resource context [10]. A contemporary security approach must therefore combine preventive safeguards with evidence collection, detection, response, and recovery.

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/568

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 6, Issue 6, October 2026 Impact Factor: 8.2

This paper addresses the following question: Which cloud-security risks recur across foundational research and contemporary guidance, and how can they be organized into an actionable layered control framework? The paper contributes (i) a focused synthesis of representative older and newer sources, (ii) a mapping from recurring risks to practical control groups, and (iii) a phased implementation sequence with proposed measures for future evaluation. The framework is not presented as a new cryptographic protocol or as a tested product; its value lies in organizing established controls around risk and operational ownership.

II. REVIEW METHODOLOGY

A focused narrative literature review was conducted on 27 October 2026. The search was directed at traceable scholarly records and authoritative publications discoverable through publisher and bibliographic pages, including ACM, IEEE, Springer, ScienceDirect, the National Institute of Standards and Technology (NIST), and the Cloud Security Alliance (CSA). Search terms included “cloud computing security,” “cloud security issues,” “cloud data integrity,” “service delivery models,” “zero trust architecture,” “cloud misconfiguration,” “IAM,” “cloud threat report,” and “multi-cloud security review.” The review window prioritized foundational work published from 2007 onward and incorporated relevant guidance and reviews through 2025.

Sources were retained when they met at least one of three criteria: (1) peer-reviewed research addressing cloud security threats or mechanisms; (2) a traceable research review synthesizing cloud security risks; or (3) an official security standard or threat report offering control guidance. Preference was given to papers with a persistent DOI and to standards hosted by the issuing organization. General promotional material and sources without identifiable publication details were not used as evidence. Findings were compared qualitatively across threat categories, proposed controls, and the degree to which responsibility lies with the cloud provider, customer, or both.

This method is intentionally described as a focused narrative review, not a systematic review. The search was not an exhaustive database query with a preregistered protocol, formal duplicate-removal process, or independent quality scoring. No statistical meta-analysis was conducted. Consequently, the selected literature is illustrative rather than exhaustive, and the framework should be treated as a synthesis requiring empirical evaluation.

III. LITERATURE REVIEW AND EVOLUTION

Foundational work establishes that cloud security inherits familiar distributed-system risks while creating additional questions about control and accountability. Jensen et al. examined technical security issues in cloud environments, including the consequences of delivering resources through network-accessible services [2]. Subashini and Kavitha later organized security concerns by SaaS, PaaS, and IaaS, showing that the service model changes which controls a customer can directly operate [3]. Mahalle and Jaiswal’s 2015 survey provides another historical synthesis of cloud-security concerns [15]. Jansen and Grance emphasized the need to evaluate public-cloud security and privacy before outsourcing data, applications, and infrastructure [4].

Research on data integrity provides a more specific example of cloud trust. Ateniese et al. introduced provable data possession, enabling a client to check that an untrusted storage service retains data without retrieving the full dataset [6]. Wang et al. developed privacy-preserving public auditing techniques for cloud storage, balancing integrity verification and the privacy of outsourced content [7]. Later work on privacy-preserving certificateless public auditing continues this line of inquiry [16]. These approaches address a narrow but important problem: encryption can limit unauthorized reading, yet it does not by itself prove that data remains intact or available.

Subsequent reviews connected technical vulnerabilities to threats and countermeasures. Zissis and Lekkas examined cloud security requirements and proposed a trust-oriented approach based on public-key infrastructure and identity mechanisms [8]. Hashizume et al. analyzed vulnerabilities inherited from technologies used in cloud systems and linked threats to possible solutions [5]. Such work remains useful as a threat taxonomy, but modern deployments also require continuous configuration assessment, automated identity lifecycle controls, and telemetry across managed services and cloud accounts.

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 6, Issue 6, October 2026 Impact Factor: 8.2

The emphasis in current guidance is more operational. NIST zero trust architecture discourages implicit trust based solely on network location or ownership [10]. NIST Cybersecurity Framework 2.0 organizes cybersecurity outcomes around governance and risk management as well as identification, protection, detection, response, and recovery [11]. CSA's 2024 report identifies misconfiguration and inadequate change control, IAM, insecure interfaces and APIs, inadequate strategy, third-party resources, and limited visibility among its top cloud threats [9]. A 2025 systematic review of multi-cloud security reports recurring research themes involving data, cryptography, authentication and authorization, service availability, confidential computing, and virtualization [12]. Together, these sources suggest that controls must be designed as a connected operating system rather than isolated point solutions.

TABLE I. REPRESENTATIVE LITERATURE AND ITS IMPLICATIONS

Source	Main focus	Implication for this review
Ateniese et al. (2007) [6]	Provable data possession for untrusted storage	Data integrity needs verification in addition to access restriction.
Jensen et al. (2009) [2]	Technical risks in cloud services	Interfaces, virtualization, and distributed operation expand the threat surface.
Wang et al. (2010) [7]	Privacy-preserving public auditing	Auditing should protect confidentiality while checking integrity.
Subashini and Kavitha (2011) [3]	Threats across SaaS, PaaS, and IaaS	Control ownership depends on the service model.
Hashizume et al. (2013) [5]	Threats, vulnerabilities, and countermeasures	Security analysis should connect weaknesses to specific mitigations.
NIST Zero Trust (2020) [10]	Resource-centric access control	Verify access based on identity, context, and resource sensitivity.
CSA Top Threats (2024) [9]	Operational cloud threat priorities	Misconfiguration, IAM, APIs, and visibility need sustained attention.
Diningrat et al. (2025) [12]	Multi-cloud systematic literature review	Cross-provider data, identity, and availability controls remain active research issues.

IV. RECURRING CLOUD SECURITY RISKS

A. Identity and Access Management

Cloud control planes expose high-impact operations through consoles, command-line tools, APIs, service accounts, and automation. Stolen credentials, excessive permissions, long-lived access keys, and unreviewed privileged identities can enable data access or infrastructure changes. Authentication alone is insufficient when authorization is overly broad. A practical baseline combines phishing-resistant multi-factor authentication for privileged access where feasible, least-privilege roles, separation of duties, short-lived credentials, managed workload identities, periodic access reviews, and alerts for unusual privilege escalation. These controls are consistent with resource-centric zero trust principles [10] and access-control guidance for cloud systems [13].

B. Data Confidentiality, Integrity, and Recovery

Cloud data may be exposed through weak access policies, public storage permissions, compromised credentials, insecure application logic, or mismanaged encryption keys. Encryption in transit and at rest is necessary but not sufficient: the organization must also govern key access, rotate secrets, classify data, limit retention, validate backups, and test restoration. Integrity mechanisms and independent audit trails can help detect unauthorized alteration or loss [6], [7]. Data-protection controls should cover the entire lifecycle, including collection, transfer, processing, sharing, archival, and deletion.

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 6, Issue 6, October 2026
Impact Factor: 8.2

C. Misconfiguration and Insecure Interfaces

Cloud resources can be created rapidly through templates, APIs, and infrastructure-as-code pipelines. This speed also allows incorrect access policies, public endpoints, permissive network rules, disabled logs, or unencrypted storage to propagate across environments. Insecure APIs create a related risk because they may expose sensitive functions or data when authentication, authorization, validation, rate limiting, or inventory management is weak [14]. Recommended controls include approved baselines, peer review for infrastructure changes, automated policy checks, vulnerability scanning, API inventory, secret scanning, and drift detection. Findings should be prioritized by exposure and business impact rather than merely counted.

D. Shared Responsibility, Third Parties, and Compliance

Security responsibility varies with service and deployment model. A provider may operate physical facilities and underlying infrastructure while the customer remains responsible for identity policy, data classification, application logic, or resource configuration. The boundary is not identical across providers or services and must be documented per workload [3], [4]. Third-party software, managed services, supply-chain dependencies, and cross-border data handling introduce further dependencies. Contracts and compliance statements are useful inputs, but they do not substitute for customer-side validation of actual configurations and operating practices.

E. Limited Visibility and Incident Readiness

Distributed workloads and multiple administrative planes can fragment logs and security alerts. Without centralized, time-synchronized, tamper-resistant records, an organization may struggle to identify what happened, determine scope, or preserve evidence. Monitoring must include relevant identity events, control-plane changes, workload activity, data-access events, and security-tool health. A response plan should specify ownership, escalation, isolation, evidence preservation, provider engagement, communication, and recovery. Recovery objectives should be tested; a backup that has never been restored is not demonstrated resilience.

V. PROPOSED RISK-BASED LAYERED FRAMEWORK

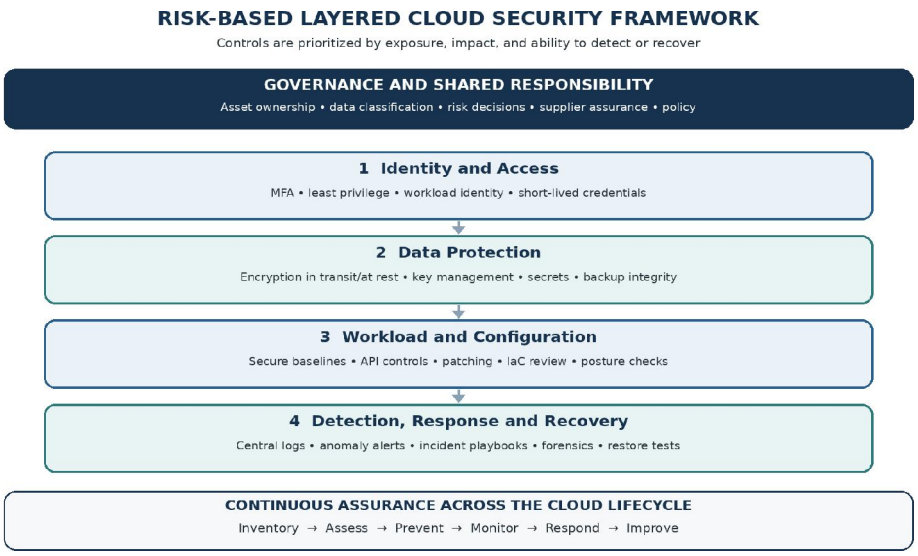

Fig. 1. Risk-based layered cloud security framework synthesized from the reviewed literature and guidance.

The proposed framework groups cloud security into five mutually reinforcing layers. Governance and shared responsibility establish ownership across the other layers; identity, data, and workload controls reduce the likelihood

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 6, Issue 6, October 2026 Impact Factor: 8.2

and impact of compromise; detection, response, and recovery reduce dwell time and support restoration. Continuous assurance links all layers through asset inventory, testing, monitoring, and improvement. This organization synthesizes established controls and does not imply that any single layer can prevent all cloud incidents.

Layer 1 — Governance and shared responsibility. Maintain an inventory of cloud accounts, services, data stores, integrations, owners, and critical business processes. Define the accountable owner for each control, document the division of duties with each provider, classify data, set risk tolerances, and verify supplier and contractual requirements. Risk treatment should consider likelihood, impact, exposure, and the availability of compensating controls. NIST CSF 2.0 provides a useful outcomes-oriented structure for connecting these decisions to organizational governance [11].

Layer 2 — Identity and access. Centralize identity where practical, enforce strong authentication, minimize standing privilege, and prefer short-lived or federated credentials over static keys. Separate human identities from workload identities, constrain administrative actions, review role assignments, and alert on unusual access. Apply zero-trust principles to sessions and resources rather than granting trust based only on network position [10].

Layer 3 — Data protection. Classify data and define handling rules; use appropriate encryption in transit and at rest; tightly govern key management and secret storage; restrict sharing; and apply integrity checks, retention limits, and verified backups. Use independent auditing where the data sensitivity and service model justify it. Access to audit records should itself be restricted to reduce the risk that an attacker can alter or misuse evidence.

Layer 4 — Workload and configuration security. Build from hardened baselines, apply least privilege to networks and services, maintain inventories of externally reachable endpoints, scan images and dependencies, patch supported assets, review infrastructure-as-code changes, and test API authorization. Run continuous or risk-triggered posture checks to identify configuration drift. Correct publicly exposed or high-impact misconfigurations first; generate tickets with an owner, severity, due date, and evidence of closure.

Layer 5 — Detection, response, and recovery. Collect and normalize relevant logs across accounts and services, monitor identity and configuration events, create actionable detections, and test response playbooks. Preserve evidence and know when provider support is required. Define recovery time and recovery point objectives for critical services, then test restoration and failover. Feed incident findings and recurring near misses back into policy, architecture, and training.

TABLE II. RISK-TO-CONTROL MAPPING AND CANDIDATE MEASURES

Risk area	Priority controls	Candidate measure	Important caveat
Excessive privilege	MFA, least privilege, short-lived credentials, access reviews	Privileged accounts protected by MFA; stale credentials removed	Measure coverage and exception risk, not only account count.
Data exposure	Classification, encryption, key governance, access restrictions, backup tests	Sensitive stores with verified access policy; restore-test success	Encryption does not fix over-permissive access or compromised endpoints.
Configuration drift	Hardened baselines, policy-as-code, scanning, owner-assigned remediation	Critical findings open beyond target remediation time	Raw alert volume can be misleading without severity and exposure context.
API/workload compromise	API inventory, authorization tests, patching, dependency and image scans	Critical API routes tested; critical vulnerabilities past SLA	Scanner results require prioritization and validation.
Delayed detection	Central logging, alerting, incident playbooks, evidence retention	Log-source coverage; time to detect and contain	A low mean time can hide missed events or incomplete scope.
Service disruption	Resilience design, tested backups, incident and recovery exercises	Recovery exercises meeting defined RTO/RPO	A documented plan is not equivalent to a successful test.

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 6, Issue 6, October 2026
Impact Factor: 8.2

VI. IMPLEMENTATION AND DISCUSSION

A practical adoption sequence should prioritize the controls that reduce the most consequential exposures and establish evidence of operation. The following order is a proposed implementation roadmap, not an empirically measured ranking:

1) Establish scope and ownership. Inventory accounts, services, identities, data stores, externally accessible resources, providers, and critical workloads. Document which party operates each control and identify gaps in visibility. Define a small set of critical business outcomes and data classifications.

2) Reduce immediate exposure. Enforce strong authentication for privileged users, remove unused accounts and keys, prohibit unintended public data access, patch known critical vulnerabilities, and review high-risk network and API exposure. Require explicit approval and traceability for exceptions.

3) Automate repeatable baselines. Encode approved configurations and identity policies as reusable templates or policy checks. Add security review to deployment pipelines, scan dependencies and container images, and detect configuration drift after deployment. Automation should create traceable remediation work rather than only produce dashboards.

4) Establish monitoring and response. Identify required log sources, centralize high-value events, define alert ownership and escalation thresholds, rehearse investigation and isolation, and verify evidence retention. Test incidents involving leaked credentials, exposed storage, and a compromised workload.

5) Validate recovery and improve. Test restore procedures, measure recovery against agreed RTO/RPO, evaluate control exceptions, and review trends with engineering and business owners. Use measures as evidence for decisions, not as targets to optimize in isolation. A rising count of detected issues may reflect improved visibility rather than worsening security; closure time and residual exposure provide additional context.

The framework's primary practical implication is that cloud security must be managed as a continuous cycle. Preventive controls remain essential, but rapid provisioning and frequent change make periodic manual review insufficient on its own. Similarly, monitoring cannot compensate for weak access governance, and encryption cannot compensate for public exposure or poor key management. The layers are intentionally complementary. Service-model boundaries should be rechecked whenever a workload adopts a new managed service, cross-account integration, or additional cloud provider.

The proposed measures are candidate indicators for an eventual evaluation. A field study could compare control coverage and remediation outcomes before and after framework adoption, examine incident simulations, and measure operational overhead across SaaS, PaaS, and IaaS environments. A useful evaluation would report baseline conditions, cloud provider and service model, sample size, measurement window, false-positive handling, and the limitations of each metric. Until such evidence exists, no numerical reduction in breaches, costs, or response time should be attributed to this framework.

VII. LIMITATIONS AND FUTURE RESEARCH

This paper synthesizes a focused selection of literature and official guidance, not the complete cloud-security evidence base. Its search and selection process was not designed to support systematic review claims, and the cited sources differ in purpose: peer-reviewed papers analyze technical mechanisms, while standards and threat reports describe controls or practitioner concerns. Some historical studies address architectures that have evolved since publication. The framework has not been implemented or tested in a live cloud environment, so its effectiveness, cost, and usability remain unverified.

Future work should evaluate the framework through a reproducible review protocol and a controlled or field-based implementation. Research questions include whether continuous configuration checks reduce the duration of critical misconfigurations; how least-privilege policies can be maintained across multiple providers; how to audit data integrity while preserving confidentiality; and how confidential computing, workload identity, and automated response affect assurance and operational overhead. Comparative evaluation should report both benefits and trade-offs, including alert

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 6, Issue 6, October 2026
Impact Factor: 8.2

fatigue, deployment latency, implementation cost, and dependence on provider-specific tools.

VIII. CONCLUSION

Cloud security has been a recurring research concern since the first generation of cloud platforms. Earlier research emphasized outsourced data, service interfaces, virtualization, integrity verification, and provider trust. Contemporary guidance continues to emphasize access governance, misconfiguration, insecure APIs, third-party exposure, and visibility. A risk-based response must therefore combine governance, identity and access control, data protection, secure workload configuration, and detection, response, and recovery. This paper organizes these controls into a layered framework and proposes candidate indicators for evaluation. The framework provides an implementation-oriented synthesis, not experimental proof; its next step is validation across real workloads and cloud service models.

REFERENCES

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," NIST Special Publication 800-145, National Institute of Standards and Technology, 2011. doi: 10.6028/NIST.SP.800-145.
[2] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On Technical Security Issues in Cloud Computing," in Proc. IEEE International Conference on Cloud Computing (CLOUD), 2009, pp. 109–116. doi: 10.1109/CLOUD.2009.60.
[3] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1–11, 2011. doi: 10.1016/j.jnca.2010.07.006.
[4] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," NIST Special Publication 800-144, National Institute of Standards and Technology, 2011. doi: 10.6028/NIST.SP.800-144.
[5] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," Journal of Internet Services and Applications, vol. 4, art. no. 5, 2013. doi: 10.1186/1869-0238-4-5.
[6] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. 14th ACM Conference on Computer and Communications Security (CCS), 2007, pp. 598–610. doi: 10.1145/1315245.1315318.
[7] 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. 525–533. doi: 10.1109/INFCOM.2010.5462173.
[8] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, 2012. doi: 10.1016/j.future.2010.12.006.
[9] Cloud Security Alliance, "Top Threats to Cloud Computing 2024," CSA, 2024. Available: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024 (accessed Oct. 27, 2026).
[10] S. W. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST Special Publication 800-207, National Institute of Standards and Technology, 2020. doi: 10.6028/NIST.SP.800-207.
[11] C. Pascoe, S. Quinn, and K. Scarfone, "The NIST Cybersecurity Framework (CSF) 2.0," NIST Cybersecurity White Paper 29, National Institute of Standards and Technology, 2024. doi: 10.6028/NIST.CSWP.29.
[12] D. C. Diningrat, Suhardi, and B. Rahardjo, "Security Issues in Multi-Cloud: A Systematic Literature Review," IEEE Access, vol. 13, pp. 70006–70017, 2025. doi: 10.1109/ACCESS.2025.3561352.
[13] National Institute of Standards and Technology, "General Access Control Guidance for Cloud Systems," NIST Special Publication 800-210, 2020. doi: 10.6028/NIST.SP.800-210.
[14] OWASP Foundation, "OWASP API Security Top 10 – 2023," 2023. Available: https://owasp.org/API-Security/editions/2023/en/ (accessed Oct. 27, 2026).
[15] S. Mahalle and R. Jaiswal, "Cloud Computing Security: A Survey," International Journal of Computer Applications, vol. 115, no. 6, pp. 21–25, 2015. doi: 10.5120/20157-2318.
[16] H. Yan, "Efficient Privacy-Preserving Certificateless Public Auditing of Data in Cloud Storage," Security and Communication Networks, vol. 2021, Art. ID 6639634, 2021. doi: 10.1155/2021/6639634.