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 1, June 2026
Impact Factor: 8.2

Hybrid Cloud Security and Use Cases

Divya Bhogawade
Student, MCA, Sadhu Vaswani Institute of Management Studies, Pune, India

Abstract: *Hybrid cloud has become a common deployment model where enterprises keep sensitive databases on local or on premise servers while moving applications, analytics, and customer facing services to public cloud platforms. This setup creates a data bridge or a link between the on premise environment and the cloud, which becomes a prime target for attackers when it is poorly designed or poorly configured. This review paper summarizes security risks on this bridge, focusing on misconfigurations in hybrid connection, API and integration leaks, and identity and access management (IAM), and discusses governance practices that enterprises can adopt to reduce these risks based on existing research and reports.*

Keywords: Hybrid Cloud, Cloud Security, API Security, Identity and Access Management, Data Breach, Hybrid Integration

I. INTRODUCTION

Hybrid cloud is a deployment model where a business or an enterprise uses both on-premise infrastructure and public cloud services and connects them so that data and applications can work together as a single environment. Many organizations keep critical or sensitive databases on-premise for reasons such as regulatory compliance, legacy systems, or perceived control, while shifting applications, user interfaces, and analytics work loads to public cloud platforms to gain flexibility and scalability.

Several studies and research note that cloud security risks often arise from the nature of cloud service delivery models and the way data is exposed across multiple environments, rather than from a single technology alone. Recent cloud threat landscape reports also show that misuse of valid credentials, insecure APIs, and misconfigured cloud resources are among the most common attack paths in modern enterprises. In a hybrid setting, these problems directly affect the bridge between on-prem and cloud.

II. PROBLEM STATEMENT AND OBJECTIVES

Many organizations focus on securing individual components, such as the on-premise database or the cloud application, but underestimate the risks in the hybrid connection itself. The central problem is that the integration path between on-prem and cloud is often treated as “plumbing” and joining and fixing and not as a primary security asset, which leads to gaps in design, configuration, and monitoring.

Problem statement:

This paper addresses the problem that many enterprises underestimate the security risks of the hybrid bridge between on-prem databases and cloud applications, especially misconfigured connectivity, insecure APIs, and weak identity management, leading to potential data exposure and unauthorized access and compromise of data.

Objectives:

- To explain typical hybrid cloud architectures and data flows connecting on-prem databases with cloud applications.
- To identify common misconfiguration and API leak scenarios that affect the hybrid data bridge.
- To study identity and access management issues specific to hybrid environments.

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 1, June 2026
Impact Factor: 8.2

- To summarize observed and noted threat patterns from research and industry reports related to hybrid and multi-cloud environments.

III. RESEARCH METHOD

This paper is based on secondary research and functions as a literature review. It does not include experiments, measurements, or new statistical studies. Instead, it synthesizes findings from academic articles, conference papers, and industry reports that discuss cloud security, big data privacy, identity and access management, and hybrid cloud threat patterns.

The recurring points from these sources are grouped into the following themes:

- Cloud service models like SaaS, PaaS and IaaS and security issues
- Big data and privacy and security in cloud computing
- IAM challenges in cloud and hybrid environments and platforms
- Hybrid cloud-specific threats and misconfigurations
- Governance and best practices for hybrid and multi-cloud security

IV. LITERATURE REVIEW

A. Cloud Service Models and Security Issues:

Subashini and Kavitha survey security issues across cloud service delivery models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) and highlight that different layers introduce different risk types. They discuss how multitenancy, virtualization, and shared infrastructure can affect confidentiality, integrity, and availability of data, particularly when customers rely on the provider for underlying security. Their work shows that misconfigurations in service delivery and unclear responsibility of a responsible person between provider and consumer are key contributors to security incidents.

B. Big Data and Privacy in Cloud Computing:

Gholami and Laure review security and privacy of sensitive and big data in cloud computing, and emphasize that large-scale data processing in the cloud introduces new privacy threats due to broad access and complex data flows. They categorize cloud security concerns across different layers of a cloud reference architecture and identify privacy threat modelling and privacy enhancing mechanisms for enhancement as key research areas. Their work notes that storing and processing big data in cloud environments requires careful control of who can access what data and how data is transferred between systems.

C. Identity and Access Management Challenges:

Identity and Access Management (IAM) has been identified as a critical issue in cloud computing, since cloud users rely on authentication, authorization, and auditing (often referred to as AAA) to control who can access cloud resources. Reviews of IAM management in cloud computing, such as the work attributed to Alansari and colleagues, highlight challenges like managing identities across multiple cloud providers, handling federated identity, and avoiding over-privileged accounts. These studies show that IAM misleads can directly lead to unauthorized access, data breaches, and abuse of delegated permissions.

D. Hybrid Cloud Threat Patterns and Vulnerabilities:

Hybrid cloud-specific analyses show that the interconnection between public and private environments introduces additional risk because traffic, policies, and identities must span multiple domains. Leavitt notes that hybrid clouds gained popularity as businesses wanted to combine the flexibility of public clouds with the control of private

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 1, June 2026 Impact Factor: 8.2

infrastructure, but this combination requires careful planning to avoid new security gaps. Studies on hybrid and multi-cloud threats, like those by Mishra et al., observe that misconfigurations, inconsistent policies, and lack of unified monitoring are common in such environments.

Industry reports from Thales, IBM X-Force, SentinelOne platform, and others consistently highlight misconfigured cloud storage, insecure APIs, misuse of credentials, and limited visibility as leading causes of cloud incidents. These reports emphasize that attackers often exploit trust relationships between cloud services and on-prem systems, using one side as a stepping stone to the other. Hybrid cloud guidance from the Cloud Security Alliance similarly stresses that hybrid environments demands strong cross-cloud security capabilities across perimeter, transmission, storage, and management layers as it is.

V. HYBRID CLOUD PLATFORM EXAMPLES

This section presents simple, generic examples of how enterprises connect on-prem databases to cloud applications and where security weaknesses can appear.

VPN-based connectivity:

1. An enterprise runs its master customer database in an on-premise data centre and connects a cloud-hosted application server using a site-to-site VPN tunnel.

2. The VPN allows the cloud app to query the on-prem database over a private IP range. If firewall rules or VPN access lists are too broad, other cloud resources in the same virtual network may also reach the on-prem database, exposing it if those resources are compromised.

Dedicated private link or direct connect:

1. A critical financial database remains on-prem, and the organization uses a dedicated private link service from a cloud provider to establish a high-bandwidth connection.

API-based integration using an integration platform:

2. The on-prem database exposes a set of REST APIs via an API gateway, and cloud applications call these APIs over HTTPS, possibly through an integration platform.

3. If these APIs lack proper authentication, use weak API keys, or do not enforce rate limits, an attacker who gains access to the cloud environment or the API endpoint can query or modify on-prem data.

VI. FINDINGS AND DISCUSSION

This section connects the literature themes to concrete risks in hybrid cloud environments, especially where an on-prem database is bridged to cloud applications.

Misconfigured Connectivity and Storage:

Studies on cloud security consistently show that misconfigurations are a leading cause of incidents, particularly misconfigured security groups, open storage buckets, and weak network controls. In a hybrid context:

- Misconfigured VPNs or private links can expose internal address ranges to cloud networks more broadly than intended.
- Incorrect routing tables or network peering rules can allow lateral movement from less sensitive cloud workloads to the network segment where the hybrid connector resides.
- Misconfigured cloud storage (e.g., object storage used as a staging area between on-prem and cloud) can be left publicly accessible, allowing attackers to download data that was meant to remain internal.

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 1, June 2026
Impact Factor: 8.2

Because hybrid environments need consistent policies across on-prem and cloud, any mismatch or drift can create a path that attackers exploit. For example, a strict firewall on-prem combined with a permissive security group in the cloud still results in a weak link on the cloud side.

Insecure and Poorly Managed APIs:

The literature on cloud security and big data privacy emphasizes that APIs are central to modern cloud services and integration. At the same time, industry analyses list insecure or unprotected APIs as a major risk factor, especially in multi-cloud and hybrid scenarios. In the hybrid bridge:

- APIs that expose the on-prem data to cloud applications may use static API keys, basic authentication, or weak tokens.
- If these credentials are stored in code repositories, misconfigured secret stores, or cloud metadata, attackers who gain access to a cloud workload can extract them and call the API directly.
- Lack of proper input validation, authorization checks and scans, or rate limiting can allow attackers to enumerate data, perform mass downloads, or attempt injection attacks through the API.

Research on cloud-backed enterprise applications shows that integration logic often assumes that calls from the cloud side are trusted, especially when IP whitelists or network-based controls are used instead of strong identity-based mechanisms. This assumption fails if attackers compromise a cloud instance or use stolen credentials.

Identity and Access Management Weaknesses:

IAM challenges highlighted by Alansari et al., Ha and Kim, and other researchers become more severe in hybrid environments where identities must work across on-prem directories and cloud identity providers. Key problems include:

- Over-privileged service accounts for hybrid connectors, which have broad read/write edit access to the on-prem database or multiple cloud resources.
- Weak or missing least-privilege design for roles and policies associated with VPN gateways and pathways, integration services, or sync agents.
- Poor handling of federated identities and tokens, where long-lived tokens or poorly validated SSO sessions can be reused by attackers to access hybrid resources.

Industry reports repeatedly show that misuse of valid credentials is one of the most common techniques used by attackers in cloud environments. In a hybrid setup, stolen admin credentials or compromised service account keys can grant direct access to both cloud workloads and on-prem systems, effectively bypassing network-level controls.

Hybrid cloud guidance strictly suggest that attackers increasingly exploit trust relationships and delegated permissions rather than breaking hardened perimeters. This means that the integration path and identity fabric form the primary attack surface.

VII. RECOMMENDATIONS AND GOVERNANCE PRACTICES

Based on the reviewed literature and industry guidance, this section provides practical recommendations for securing the hybrid bridge and related identities.

Strengthen IAM and Enforce Least Privilege

1. Use dedicated identities (service principals, service accounts) for hybrid connectors with **least privilege** access, limited to the specific databases, schemas, and operations they require.

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 1, June 2026 Impact Factor: 8.2

2. Separate administrative identities for cloud computing and on-prem environments where practical, and avoid using general admin accounts for integration tasks.
3. Apply multi-factor authentication (MFA) and strong password policies for all human administrators and critical service accounts.
4. Regularly review IAM policies and roles for hybrid components to remove unused permissions and detect privilege creep.

Secure APIs and Integration Layers:

1. Place an API gateway or integration platform in front of on-prem APIs exposed to cloud applications, and enforce strong, token-based authentication (for example, OAuth 2.0) and fine-grained and well tailored authorization at this layer.
2. Implement rate limiting, input validation or authentication, and logging for all hybrid APIs to detect unusual access patterns and reduce the impact of abuse.
3. Store API keys and secrets in secure vaults or managed secret stores and avoid hard-coding them into applications or configuration files.
4. Use mutual TLS or equivalent secure channels for data in transit between the cloud and on-prem environments.

Improve Monitoring, Logging, and Incident Response:

1. Centralize logs from cloud and on-prem components related to the hybrid bridge, including VPN gateways, API gateways, IAM events, and database logs, into a security information and event management (SIEM) system.
2. Define alerts for suspicious patterns, such as unusual data transfer volumes, access from new locations, failed login attempts, or changes to IAM roles linked to hybrid connectors.

Clarify Governance and Ownership:

1. Establish clear ownership for the hybrid bridge, with defined responsibilities between cloud teams and on-prem teams for design, configuration, integration, and monitoring.
2. Align hybrid security policies with enterprise-wide cloud governance frameworks, ensuring consistent standards for encryption, IAM, logging, and compliance.
3. Provide regular training to operations and development teams on hybrid security patterns, common misconfigurations, and how attackers exploit trust relationships.

VIII. CONCLUSION

The key message is that hybrid cloud security is largely about securing the integration path and identities. Enterprises should give the hybrid bridge the same level of design, control, and monitoring as critical internal systems, with strong IAM, secure and well-governed APIs, hardened network configurations, and clear ownership. By applying least privilege, which is a very important feature, consistent configuration management, and unified visibility across on-prem and cloud, organizations can significantly reduce the risk that attackers will use the hybrid bridge as a route to compromise sensitive on-prem databases or cloud workloads.

REFERENCES

1. **Subashini, S., & Kavitha, V. (2011).**
A survey on security issues in service model of cloud computing. *Journal of Network and Computer Applications, 34(1), 1–11.* At:
https://www.sciencedirect.com/science/article/pii/S1084804510001281

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 1, June 2026
Impact Factor: 8.2

2. **Gholami, A., & Laure, E. (2016).**
Security and Privacy of Big Data in Cloud Computing. *International Journal of Computer Science and Information Security.* At:
https://arxiv.org/abs/1601.01498
3. **Thales Group. (2025).**
Thales Cloud Security Study: Securing a Hybrid and Multi cloud World. *Thales CPL Research Reports.*
PDF of the 2025 cloud security study :
https://cpl.thalesgroup.com/sites/default/files/content/cloud-security/2025/2025-thales-cloud-security-study.pdf
4. **IBM X-Force. (2025).**
Cloud Threat Landscape Report: Evolving Attack Vectors. *IBM Think Security.*
IBM X-Force cloud threat content :
https://www.youtube.com/watch?V=n5wwtmg79h0
5. **Fernandes, E., Rahmati, A., & Prakash, A. (2020).**
Security analysis of cloud-backed enterprise applications. *IEEE Transactions on Dependable and Secure Computing.*
https://openaccess.city.ac.uk/id/eprint/12199/7/revisedpaperbychirag.pdf
6. **Alansari, Z., et al. (2019).**
Identity and Access Management in Cloud Computing: A Review. *International Journal of Advanced Computer Science and Applications.*
Survey on IAM in cloud:
https://www.ijert.org/research/a-survey-on-identity-and-access-management-in-cloud-computing-IJERTV3IS040880.pdf
7. **Ha, T., & Kim, H. (2021).**
Analysis of security vulnerabilities in hybrid cloud identity management systems. *IEEE Access.*
Hybrid cloud identity vulnerabilities and IAM:
https://cloudsecurityalliance.org/research/topics/hybrid-cloud-security