Network Security in Hybrid Cloud Environments

Anurag K More (2101CS84), Harsh Loomba (2101CS32), Pragya Harsh (2101AI23)

April 22, 2025

Word count: 3543

1 Introduction

Cloud computing has transformed IT infrastructure by allowing organizations to scale rapidly without holding physical resources. Hybrid cloud models are now used by many to achieve balance between security and flexibility. Hybrid cloud integrates on-premises, private, and public clouds so that workload can be distributed according to security, performance, and cost. IT and business experts utilize hybrid cloud for its agility and scalability as 77% of them use hybrid cloud, as reported by the IBM Transformation Index: State of Cloud (IBM, 2023).

But hybrid cloud defies traditional security, with perimeter defenses no longer adequate. Security teams need to implement end-to-end strategies to provide visibility and control in all environments.

This paper looks at hybrid cloud security from a network point of view, examining existing and new approaches—such as Zero Trust Architecture—to enable organizations to address risks in hybrid deployments.

2 Literature Review

Hybrid cloud security has become a key area of research as more organizations embrace blended models of infrastructure. There have been many studies examining the security issues and solutions for safeguarding these intricate environments.

Emmanni (2024) has carried out in-depth research on the deployment of Zero Trust Architecture in hybrid cloud environments, underscoring the way this strategy fundamentally changes security paradigms from location-based trust to continuous verification. The research points out that Zero Trust principles are most effective in hybrid situations where classical network boundaries are indistinct, offering a model for uniform protection across different platforms.

Nedzelskỳ (2015) broke down the security implications and challenges of hybrid cloud computing into analysis, pointing out the points of integration between public and private clouds as weak points that need specialized security controls. The research laid building blocks for understanding the special security considerations in hybrid deployments.

Donadio et al. (2014) analyzed network security frameworks tailored for hybrid cloud environments, suggesting architectural models that ensure security across diverse infrastructure elements. Their research highlighted the need for single security policies and uniform enforcement mechanisms that function irrespective of where workloads are executed.

The Cloud Security Alliance has released comprehensive research on hybrid cloud security, recording important application scenarios and security threats unique to hybrid deployments (Cloud Security Alliance, 2021). Their research points out that "hybrid clouds are now often the starting point for organizations in their cloud journey" and describes the security advantages of hybrid methods when properly implemented.

Ahmad and Garko (2019) examined hybrid cryptography algorithms for cloud computing, showing how blended encryption methods can offer better security for information transferring between environments in hybrid implementations. Their findings show that hybrid encryption models yield greater security than single-algorithm solutions.

Pravin and Malik (2019) introduced a hybrid cloud security model that is particularly aimed at securing data both in transit and at rest, utilizing several cryptographic services such as user authentication, access control policies, encryption, and integrity verification. This multi-pronged approach targets several attack vectors at once, making it especially useful for hybrid environments.

Raza, Imtiaz and Shoaib (2019) undertook a comprehensive review of security problems in hybrid cloud computing systems, examining how these problems affect enterprise adoption. Their study revealed trust management, identity authentication, and compliance to be important issues needing special attention within hybrid implementations.

3 Hybrid Cloud Fundamentals

To learn what a hybrid cloud is, first learn what a cloud is. Cloud computing is nothing but people and companies are able to use computer resources (such as storage, servers, applications) over the internet, rather than possessing and running these resources in a physical sense. Cloud service providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud host these resources in data centers.

There are various kinds of clouds:

- **Public Cloud**: Resources are shared over the internet with numerous customers. It's similar to leasing an apartment in a building in which other tenants reside.
- **Private Cloud**: The whole infrastructure is reserved for a single organization. It's similar to owning your own home.
- **Hybrid Cloud**: Both public and private clouds combined. Organizations utilize private cloud for critical operations and public cloud for non-critical or scalable operations.

A hybrid cloud infrastructure integrates on-premises infrastructure (what an organization physically owns and controls) with public and/or private clouds. This configuration enables data and applications to be transferred between these infrastructures, giving more flexibility and optimization, as shown in Figure 1.

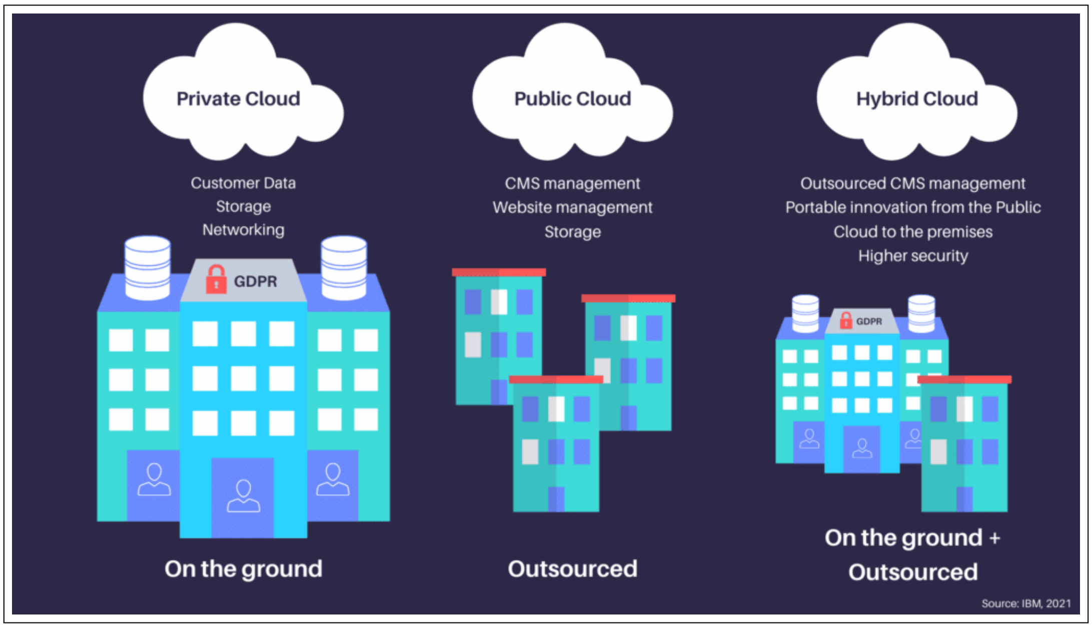

Figure 1: Basic Hybrid Cloud Architecture showing integration between on-premise, public, and private cloud components

Public clouds make use of publicly shared virtualized resources and are intended to host multiple customers by offering connectivity via the internet, thus being perfect for processing less confidential resources. Private clouds, by contrast, provide privately shared virtualized resources to a committal cluster of customers with options for connectivity via internet, fiber, and private networks. Such a setup is best suited to organizations that need secure management of confidential information and core systems, enabling more control and improved security than public cloud environments, as illustrated in Figure 2 (Fortinet, 2025).

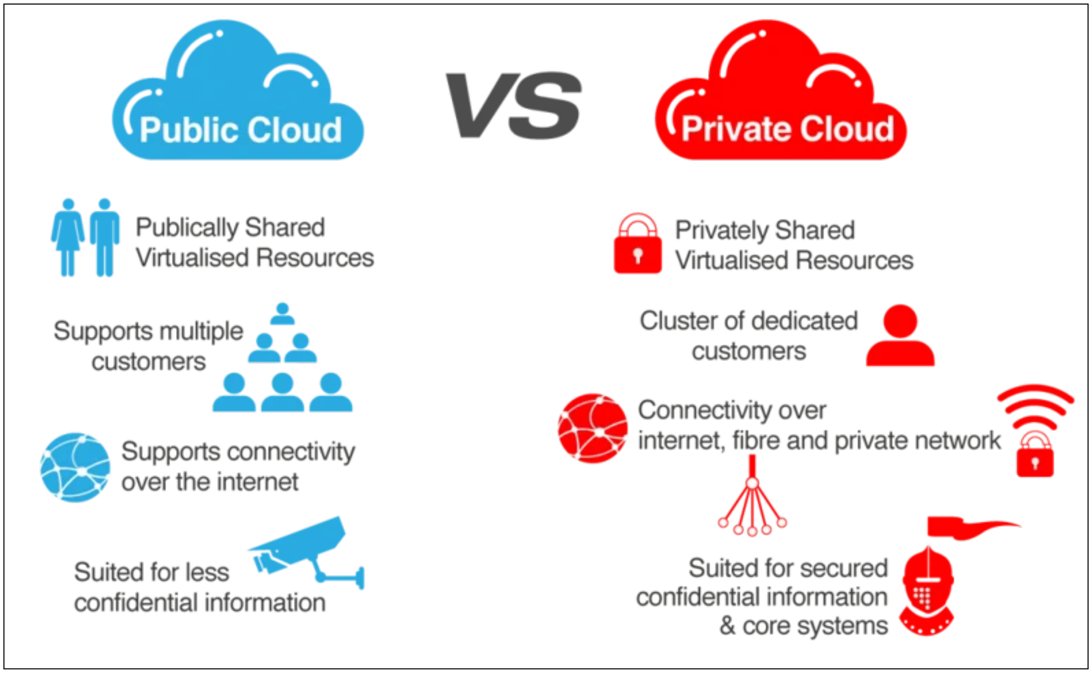
Public Cloud
VS
Private Cloud
Publically Shared Virtualised Resources
Supports multiple customers
Supports connectivity over the internet
Suited for less confidential information
Privately Shared Virtualised Resources
Cluster of dedicated customers
Connectivity over internet, fibre and private network
Suited for secured confidential information & core systems

Figure 2: Private Cloud vs Public Cloud

4 Advantages of Hybrid Cloud Environments

- **Scalability:** The hybrid cloud offers organizations flexibility to scale their computing resources on demand. For example, an e-commerce website could take advantage of excess computing resources from the public cloud during its peak hours or for special occasions where significant online sales are expected. This would allow an e-commerce website to take on additional traffic to avoid crashing the system and flow seamlessly for the user without having to make a new permanent investment in hardware (IBM, 2023).

- **Cost Efficiency:** Cost savings is one of the biggest advantages of hybrid cloud. Organizations can avoid avoiding large capital expenditures in hardware and use public cloud services for temporary or less critical tasks instead. Because cloud providers usually serve as utility companies and use a pay-as-you-go pricing model, organizations are only charged for actual resources consumed when using the cloud, and are not wasting money on an idle resource (IBM, 2023).

- **Flexibility and Agility:** The hybrid model provides business agility to determine where to execute workloads. Sensitive and critical data can remain on private servers, while workloads that are less sensitive can be executed from the public cloud; this gives organizations the ability to make changes quickly to meet changing needs, while pursuing innovation quickly without reverse the current infrastructure in place (F5, 2024).

- **Disaster Recovery:** Disaster recovery is paramount for business continuity. Hybrid cloud can be used by organizations to mirror critical data in various locations, including in the cloud. In case one system collapses because of a cyberattack or natural calamity, the data is still secure and may be recovered rapidly, limiting downtime and data loss (IBM, 2023).

- **Data Localization:** Some regulations and industry standards mandate data to be hosted within certain geographical areas. Hybrid cloud assists businesses in complying with these regulations as sensitive or regulated data can be hosted on-premise or private cloud, while non-sensitive data can be hosted anywhere in public cloud servers (Fortinet, 2025).

5 Challenges Faced in Hybrid Cloud Environments

- **Security Risks:** ith information flowing across different environments, it becomes easier for someone to observe, gain unauthorized access, or breach this information. The company will have serious threats if they do not secure the interfaces. Hackers could exploit any vulnerabilities in the cloud or on-premise infrastructure. Therefore, strong encryption and access controls are needed (Raza, Imtiaz and Shoaib, 2019).

- **Integration Complexity:** Merging systems and applications within private and public clouds is not always seamless. Various platforms will employ varying technologies, protocols, and stan- dards. This can cause compatibility problems, uneven performance, or challenges with data sharing. Consequently, integration tends to involve custom development and meticulous planning (Ahmad and Garko, 2019).

- **Visibility and Monitoring:** Administrators should be in possession of clear insight into whatever is transpiring in their systems at any time. Under a hybrid deployment, monitoring devices must monitor activity from multiple platforms, networks, and vendors. Underlying the presence of holistic visibility, performance anomalies or likely threats can be missed (F5, 2024).

- **Compliance and Regulation:** Companies that are doing business across borders or in regulated sectors need to adhere to multiple legal and data protection requirements. It is harder to ensure that every component of a hybrid setup is compliant with these requirements compared to running a single environment. Any compliance gap may result in legal fines or damage to reputation (Raza, Imtiaz and Shoaib, 2019).

- **Latency Issues:** Latency is when there is a delay in transferring data. Data could be travelling great distances from a local server to a cloud provider within a hybrid environment. If the system is poorly designed, these delays can impact application performance, particularly for real-time applications such as video conferencing or online banking (F5, 2024).

The different issues encountered in hybrid cloud environments are illustrated in Figure 3, showing the interrelatedness of these problems.

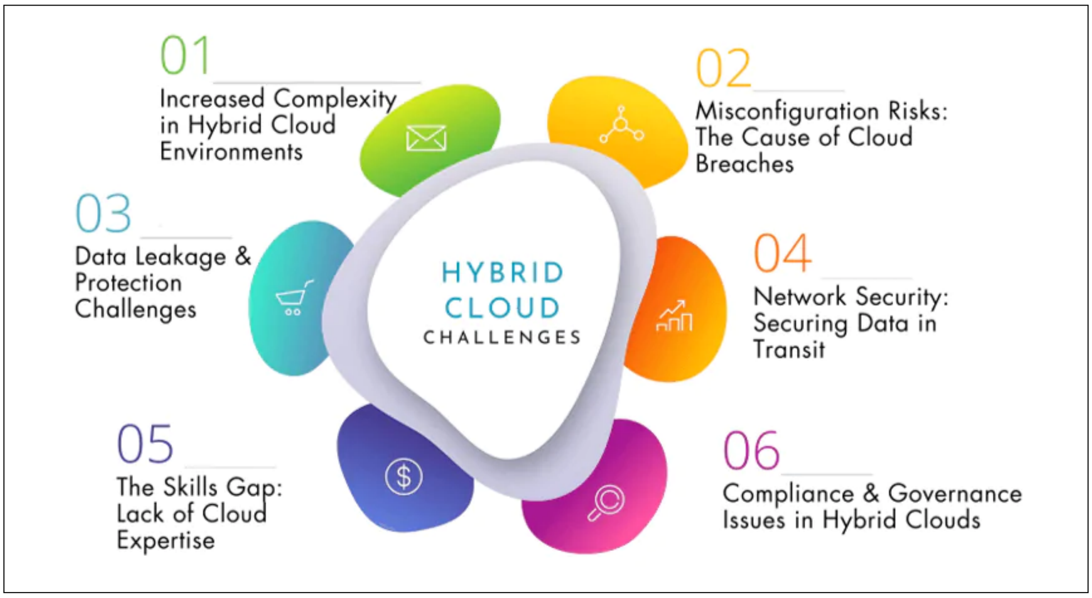
01
Increased Complexity in Hybrid Cloud Environments
02
Misconfiguration Risks: The Cause of Cloud Breaches
03
Data Leakage & Protection Challenges
04
Network Security: Securing Data in Transit
05
The Skills Gap: Lack of Cloud Expertise
06
Compliance & Governance Issues in Hybrid Clouds
HYBRID CLOUD CHALLENGES

Figure 3: Challenges faced in a Hybrid Cloud Environment

6 Network Security in Hybrid Cloud Environments

Network security is the process of protecting data and systems from unauthorized access or attacks while in transit across networks. In a hybrid cloud, the diversity of systems and providers adds to the number of potential weak points, so robust security procedures are necessary.

6.1 Identity and Access Management (IAM)

IAM tools assist in managing who can see what information within a system. It entails authenticating a user's identity (e.g., passwords or biometric verification) and limiting their access to the data or services required for their function. This minimizes the likelihood of internal abuse or inadvertent data disclosure (Fortinet, 2025). As per Pravin and Malik (2019), efficient IAM in hybrid environments should involve "user authentication and authorization using OTP or authenticator application" as well as strong "user access control policy" to secure cloud storage during transit and when resting.

6.2 Encryption

Encryption is a process through which readable data is converted into coded format that can be accessed only by the key. Encryption in hybrid cloud is applied to safeguard data on servers (at rest) and data traveling over networks (in transit). Even if intercepted, data is not readable by unauthorized users (Ahmad and Garko, 2019). Studies by Ahmad and Garko (2019) identify that hybrid encryption schemes, which apply multiple cryptographic techniques, provide enhanced security

for sensitive information in cloud environments as opposed to implementations based on single algorithms.

6.3 Firewalls and Gateways

Firewalls are similar to checkpoints that restrict what information moves in or out of a network. In a hybrid cloud configuration, firewalls secure the private-to-public connection. Gateways control data exchange and only permit safe, approved traffic to transit (F5, 2024).

6.4 Intrusion Detection and Prevention Systems (IDPS)

These devices watch for traffic and system behavior on a network to identify threats or attacks. When anomalous behavior is detected—like strange login patterns or excessive data transfers—an alert is generated. Certain systems will even block malicious activity automatically to avoid breaches (F5, 2024). Pravin and Malik (2019) suggested integrating monitoring systems as a key component within hybrid cloud security models to detect abnormal behavior from legitimate users or would-be hackers trying to reach private data in real time.

6.5 Microsegmentation

Microsegmentation consists of segmentation of a network into small isolated parts. The rules for each segment are administered individually. The attacker, after penetrating one of them, will be unable to simply move over to others easily. This makes it harder to wreak havoc that would result from a breach, as well as being simpler to monitor for any strange behavior (Fortinet, 2025).

7 Application Areas of Hybrid Cloud with Network Security

Hybrid cloud environments are being actively adopted in numerous sectors. The combination of public and private cloud solutions, enhanced with robust network security protocols, is proving to be an ideal setup for organizations that require both flexibility and control.

- **Government:** Government agencies handle vast amounts of citizen data, some of which is highly sensitive and classified. Hybrid clouds allow them to run essential services using public cloud infrastructure, while national security and legal data remain strictly within private, on-premise environments (F5, 2024).

- **Finance:** Banks and financial institutions are rapidly adopting hybrid cloud models to manage their vast workloads. Transaction processing, customer data management, and fraud detection systems often run on private infrastructure for maximum security, while customer-facing services leverage the public cloud to scale with demand. Enhanced network security ensures data is encrypted and protected across all points of access (Raza, Imtiaz and Shoaib, 2019).

- **Healthcare:** The healthcare sector deals with highly sensitive patient information that is protected by regulations like HIPAA. Hybrid clouds allow hospitals and clinics to store confidential patient records securely in a private cloud while utilizing public cloud services for tasks like analytics and appointment scheduling. For example, patient data collected in real-time from wearable devices can be analyzed in the public cloud while the actual records remain secure and localized, as illustrated in Figure 4 (IBM, 2023).

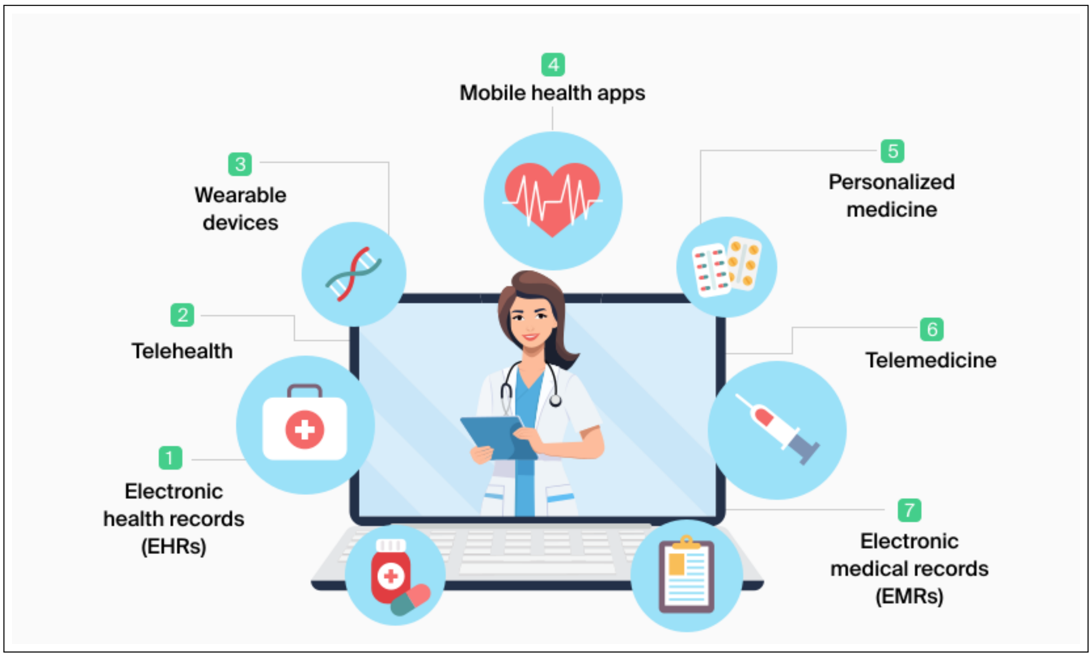

Figure 4: Healthcare hybrid cloud model: public cloud for analytics and private cloud for patient data.

- **Retail and eCommerce:** Retailers face fluctuating traffic, especially during holiday seasons or promotional sales. Hybrid clouds help manage this by allowing front-end websites and recommendation engines to run on the public cloud, while backend operations such as inventory management, payment processing, and customer records are kept secure in a private environment (IBM, 2023).

- **Manufacturing and IoT:** Modern factories rely heavily on IoT devices to track machine performance and optimize production. Hybrid clouds allow immediate operational data to be processed locally, ensuring low latency, while long-term data can be stored and analyzed in the cloud (F5, 2024).

- **Education and Research:** Educational institutions benefit from hybrid cloud by hosting virtual classrooms and online portals on scalable public cloud platforms. Sensitive academic records remain in a secure private cloud. Figure 5 illustrates a cloud-based architecture for education that integrates multiple layers to deliver resources across devices (Fortinet, 2025).

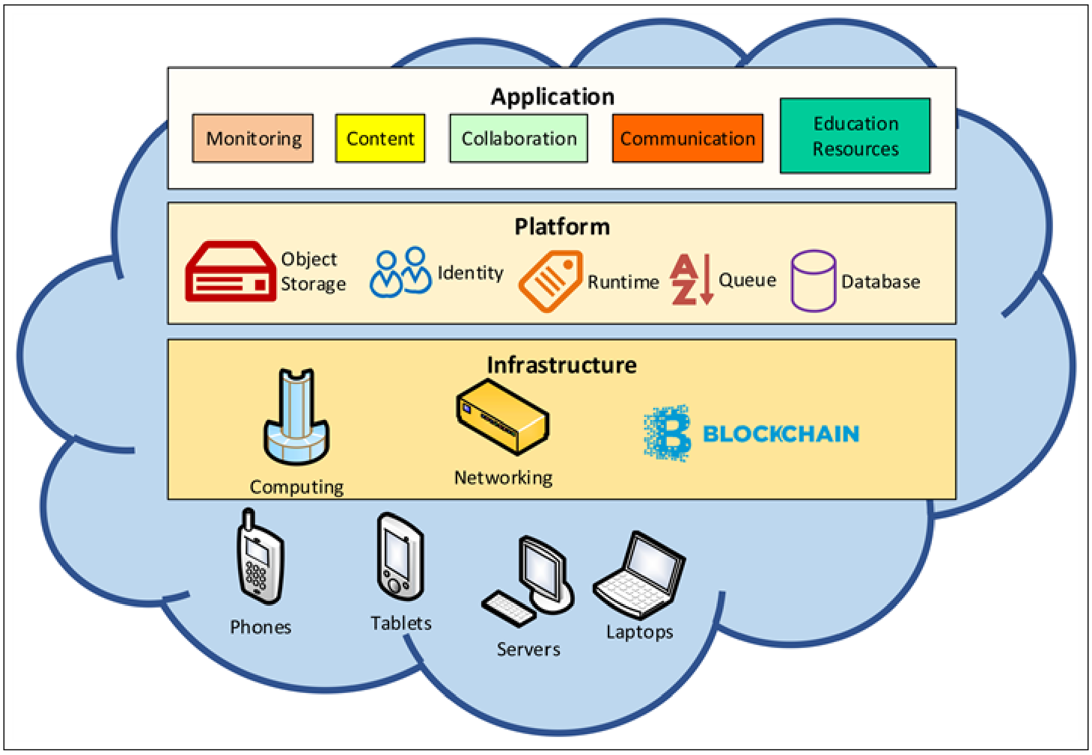

Figure 5: Cloud-based architecture for education: Integrating infrastructure, platform, and application layers to deliver educational resources across devices

- **Media and Entertainment:** Streaming services and game developers rely on hybrid clouds for both storage and delivery. Rendering high-definition content can be outsourced to the public cloud for speed, while the original assets are securely stored in a private repository. Secure content delivery networks (CDNs) ensure that only authorized users can access digital content (IBM, 2023).

8 Mitigating the Risks in Hybrid Cloud Environments

Hybrid cloud environments pose special security risks due to their distributed nature. But risk can be controlled if organizations are prepared and adopt certain measures.

- **Unified Security Policies:** Organisations must have a unified security set of policies that cover all environments (on-premise, private cloud, or public cloud), and must be able to access the data and applications housed within it, without security gaps when moving between these environments (Cloud Security Alliance, 2021).

- **Automation and Orchestration:** Manual security processes are slow and can involve human error. By utilizing automation tools, organizations can automate their normal workloads, including the processes of applying software updates, scanning for vulnerabilities, and responding to a security incident automatically (Ahmad and Garko, 2019).

- **Endpoint Security:** The more devices that connect to the hybrid cloud, the more potential entry points there are for a cyber attacker. Endpoint security refers to protecting these devices including the use of antivirus software, firewalls and EDRs (endpoint detection and response) (F5, 2024).

- **Regular Auditing and Compliance Checks:** On a routine basis, organizations must execute audits to ensure security and compliance with the legal requirements they must adhere to. Audits involve checking access logs for suspicious activity, reviewing configuration settings, and ensuring sensitive data is appropriately protected in accordance with the industry (Raza, Imtiaz and Shoaib, 2019).

- **Advanced Threat Protection:** Advanced Threat Protection (ATP) employs the power of artificial intelligence, machine learning, and behavioral analytics to catch and react to threats that conventional solutions may not detect (F5, 2024).

- **Training and Awareness:** Most cyberattacks capitalize on user error, for example, clicking on phish-ing emails or using poor passwords. Continuous training helps employees see up-to-date threats and be aware of how to sidestep them (F5, 2024).

9 Zero Trust Architecture as a Solution

Zero Trust Architecture (ZTA) is more and more viewed as a critical security model for hybrid cloud infrastructures, where perimeter-based protections are insufficient because resources and users are dynamic and distributed (Cloud Security Alliance, 2021). Zero Trust is required because hybrid clouds blur the distinctions between trusted internal networks and possibly untrusted external environments and make it hard to depend on location-based trust models.

Zero Trust resolves such threats by effectively reversing the security model: it follows the ethos of "never trust, always verify." There is no user, device, or application— whether inside or outside the perimeter of the network— that automatically receives trust. Each access attempt is formally authenticated, authorized, and repeatedly proven based on multiple context elements (Fortinet, 2025). Figure 6 demonstrates the Zero Trust Architecture flow.

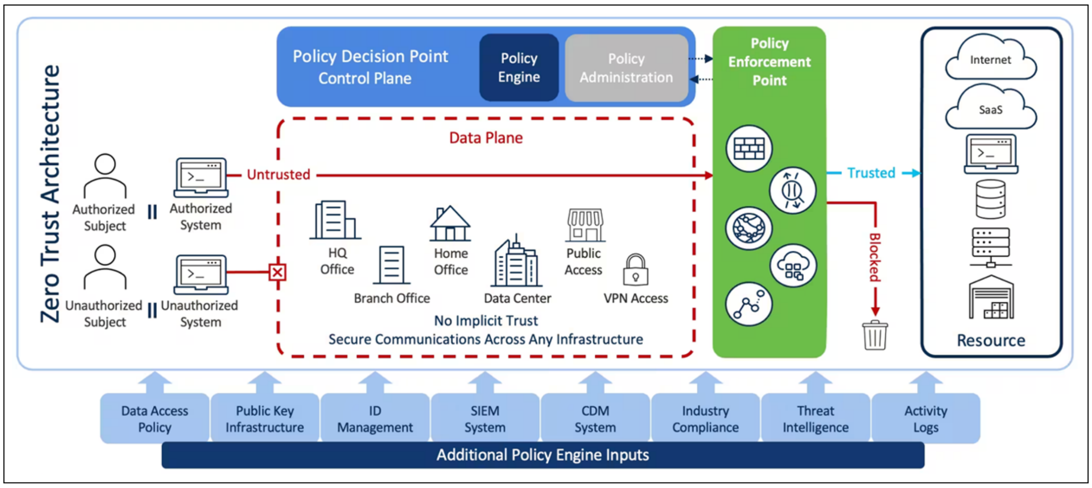

Figure 6: Zero Trust Architecture flow showing verification and access control across cloud endpointss

9.1 Implementation of Zero Trust in Hybrid Cloud Environments

Deploying Zero Trust in a hybrid cloud is complex and needs to be approached holistically and systematically:

- **Strategic Planning and Assessment:** Organizations need to start with an in-depth examination of their current hybrid cloud setup, mapping sensitive data flows, key assets, and likely blind spots (Cloud Security Alliance, 2021).

- **Identity and Access Management (IAM):** Strong IAM is at the heart of Zero Trust. Multi-factor authentication (MFA) and identity federation provide access to only authenticated and approved users and machines, while enforcing least privilege access (Fortinet, 2025).

- **Microsegmentation and Network Design:** The network is separated into divided, isolated segments with fine-grained access controls. Microsegmentation restricts the flow of threats in the environment (F5, 2024).

- **Policy Enforcement and Dynamic Access Control:** Security policies should be dynamic and context-sensitive, dynamically changing based on user behavior, device health, and data sensitivity (F5, 2024).
- **Continuous Monitoring and Response:** Every network traffic, user activity, and system health is monitored round the clock through sophisticated analytics and threat detection tools (Ahmad and Garko, 2019).

9.2 Benefits and Challenges

The implementation of Zero Trust in hybrid clouds provides several advantages: it greatly minimizes the attack surface, maximizes compliance with regulatory requirements, and enhances operational efficiency through automated security processes (Cloud Security Alliance, 2021). Implementation, however, comes with its set of challenges. Organizations can be faced with technical complexities, integration challenges with existing systems, and cultural change necessary to accommodate new security practices. Key principles include:

Key principles include:

1. **Verify Explicitly:** All access requests should be authenticated and authorized using all available data points, including user identity, device health, location, and behavior patterns (Cloud Security Alliance, 2021).
2. **Use Least Privilege Access:** Users, applications, and devices are only given the bare minimum of permissions necessary to carry out their tasks (Fortinet, 2025).
3. **Assume Breach:** Security controls are designed assuming a breach has already taken place—or will take place. This assumption underlies the adoption of network segmentation, robust encryption, and persistent monitoring (F5, 2024).

In hybrid cloud environments, these Zero Trust concepts are especially compelling because they reach beyond traditional network boundaries. Zero Trust combines IAM, network segmentation, encryption, and persistent monitoring to deliver uniform, adaptive security across all platforms.

10 Conclusion

A hybrid cloud infrastructure integrates private and public clouds, allowing organizations to maximize scalability, cost-effectiveness, flexibility, and compliance by hosting sensitive workloads on private clouds and taking advantage of the public clouds for less sensitive or scalable processes. Yet, this in- terconnected infrastructure brings with it special vulnerabilities, including greater attack surfaces, in- con- sistent access controls, integration challenges, and difficulty in providing visibility and com- pliance across heterogeneous platforms (Raza, Imtiaz and Shoaib, 2019).

This study has shown that hybrid cloud environments need to be secured through a multi-faceted strategy that deals with technical as well as organizational security facets. Technical controls like strong IAM, encryption, network segmentation, and ongoing monitoring need to be complemented with organizational controls like centralized security policies, frequent auditing, and employee training (F5, 2024).

The literature review found a number of powerful studies being conducted regarding customized security approaches for hybrid environments and Zero Trust Architecture is an emerging approach (Cloud Security Alliance, 2021). By looking at case studies within specific industries, it proved that there cannot be an all-encompassing security approach for hybrid cloud security. Organizations in regulated sectors such as healthcare, finance, government, and education are expected to customize their security approach based on specific regulatory expectations and/or sensitivity of data expectations.

Securing the hybrid cloud infrastructure is necessary to avoid security breaches, remain regulatory compliant, and maintain business continuity. Based on their organizational needs, one of the best approaches to take in the secure operation of hybrid cloud architecture is the implementation of a Zero Trust architecture based on "never trust, always verify". Future research should explore novel approaches to meet the new challenges of securing ever-more complicated hybrid environments, especially as edge computing and IoT deployments widen the hybrid environment processing capability.

Organizations employing Zero Trust models can effectively meet the high security demands of hybrid clouds, enhance their security posture, and provide resilient environments that can adapt to changing threats and changing business needs (Fortinet, 2025).

References

Ahmad, Sadiq Aliyu and Ahmed Baita Garko. 2019. Hybrid cryptography algorithms in cloud computing: A review. In *2019 15th international conference on electronics, computer and computation (ICECCO)*. IEEE pp. 1–6.

Cloud Security Alliance. 2021. “Hybrid Cloud Security.”. Available at: https://cloudsecurityalliance.org/research/topics/hybrid-cloud-security.

Donadio, Pasquale, Giovanni B Fioccola, Roberto Canonico and Giorgio Ventre. 2014. Network security for hybrid cloud. In *2014 Euro Med Telco Conference (EMTC)*. IEEE pp. 1–6.

Emmanni, Phani Sekhar. 2024. “Implementing a zero-trust architecture in hybrid cloud environments.” *International Journal of Computer Trends and Technology* 72(5):33–39.

F5. 2024. “What is Hybrid Cloud Security?”. Available at: https://www.f5.com/glossary/hybrid-cloud-security.

Fortinet. 2025. “What Is Hybrid Cloud Security and How Does It Protect Your Data?”. Available at: https://www.fortinet.com/resources/cyberglossary/hybrid-cloud-security.

IBM. 2023. “Hybrid Cloud Examples, Applications & Use Cases.”. Available at: https://www.ibm.com/think/topics/hybrid-cloud-use-cases.

Nedzelskỳ, Roman. 2015. “Hybrid cloud computing: Security Aspects and Challenges.” *University of Economics Prague* .

Pravin and Malik. 2019. “Hybrid Cloud Security Model for Data Protection in Cloud Computing.” *International Journal of Computer Sciences and Engineering* 7(3):751–757.

Raza, Mohsin, Ayesha Imtiaz and Umar Shoaib. 2019. “A review on security issues and their impact on hybrid cloud computing environment.” *International Journal of Advanced Computer Science and Applications* 10(3):353–356.

Statutory Declaration

Hiermit versichere ich, dass diese Arbeit von mir persönlich verfasst ist und dass ich keinerlei fremde Hilfe in Anspruch genommen habe. Ebenso versichere ich, dass diese Arbeit oder Teile daraus weder von mir selbst noch von anderen als Leistungsnachweise andernorts eingereicht wurden. Wörtliche oder sinngemäße Übernahmen aus anderen Schriften und Veröffentlichungen in gedruckter oder elektronischer Form sind gekennzeichnet. Sämtliche Sekundärliteratur und sonstige Quellen sind nachgewiesen und in der Bibliographie aufgeführt. Das Gleiche gilt für graphische Darstellungen und Bilder sowie für alle Internet-Quellen. Ich bin ferner damit einverstanden, dass meine Arbeit zum Zwecke eines Plagiatsabgleichs in elektronischer Form anonymisiert versendet und gespeichert werden kann. Mir ist bekannt, dass von der Korrektur der Arbeit abgesehen und die Prüfungsleistung mit nicht ausreichend bewertet werden kann, wenn die Erklärung nicht erteilt wird.

I hereby declare that the paper presented is my own work and that I have not called upon the help of a third party. In addition, I affirm that neither I nor anybody else has submitted this paper or parts of it to obtain credits elsewhere before. I have clearly marked and acknowledged all quotations or references that have been taken from the works of others. All secondary literature and other sources are marked and listed in the bibliography. The same applies to all charts, diagrams and illustrations as well as to all Internet resources. Moreover, I consent to my paper being electronically stored and sent anonymously in order to be checked for plagiarism. I am aware that the paper cannot be evaluated and may be graded “failed” (“nicht ausreichend”) if the declaration is not made.

____

Signature

____

Place, Date