Detailed Analysis of Security Challenges in the Domain of Hybrid Cloud

Dhanashri Ravi Patil[1], Pratik Sarjerao Gaikwad[2]

[1,2]Reserach Student, Department of Computer Science and Engineering
[1,2]Sanjay Ghodawat University, Kolhapur, Maharashtra, India.

---***---

Abstract - Private and public hybrid clouds are a Concept that is frequently debated in the current times. Because most data must be maintained on-premise hardware and cannot be migrated to any public cloud, the hybrid solution is the only method for major corporations and governmental institutions to participate in cloud computing innovation. Even if there are no legal limits inside the hybrid situations, businesses are concerned about information leakage or other constraints that may develop when they do not have control over their data. The use of outplacement infrastructure, about which the user should not bother, or of services in the areas of machine learning, business intelligence, stream analytics, and other SaaS features, on the other hand, is highly tempting. From a cost-savings perspective, migrating to cloud solutions is a very attractive idea. However, some cloud service functionalities that cannot be combined with local, on-premise servers provide a challenge for public cloud solutions. Recent studies have tended to concentrate solely on the topic of private or public clouds.

This study is concerned with security in hybrid clouds. It explores numerous security measures and challenges within the context of IaaS and SaaS, as well as various authentication and security concepts and security-related difficulties.

Key Words: Hybrid Cloud, Cloud Security, Security Challenges, Threats in Cloud

1. INTRODUCTION

Today, 94 percent of firms utilize some sort of cloud, with 58 percent adopting a hybrid cloud architecture. The term "hybrid cloud" refers to an IT infrastructure that includes some level of workload migration, and management across two or more connected but independent environments, such as physical servers, virtualized, private cloud, and public cloud. We can execute applications in any of the interconnected environments, transfer it across them, and use resources from those environments interchangeably using a hybrid cloud architecture.

Although implementing IaaS through a hybrid architecture allows a flexible, on-demand method for meeting organizational computing needs, there are still several difficulties that need to be resolved. Security is the main barrier to IaaS adoption in the company. Due to the division of resources into different clouds, software complexity and configuration increase as an organization migrates its resources to hybrid clouds. In addition to this complexity, there are multiple security concerns, such as controlling the communication link between the two sites when delivering IT infrastructure from the cloud to businesses, creating firewall rules that only permit authorized traffic from the cloud, and incompatible network policies. Security is a major concern no matter where you are in your hybrid cloud journey. In fact, 81 percent of businesses identify cloud security as a threat. Hybrid cloud security vulnerabilities often manifest as loss of resource monitoring and control, which might include unauthorized usage of the public cloud, a lack of resource visibility, insufficient change control, poor configuration management, and ineffective access controls. These holes can be exploited by unauthorized individuals to have access to confidential information and corporate resources. Security lapses can be expensive. A data breach typically costs US$3.92 million, with lost revenue accounting for 36.2% of this expense.

The rest of the paper is organized as follows. In Section 2, we provide an overview on the different service models being used and cloud architectures which can be deployed according to the enterprise requirements. Section 3 presents the challenges involved while deploying hybrid cloud architecture for enterprise needs, Section 4 describes the solutions which help in enterprises to operate efficiently and securely in hybrid environment. Section 5 discusses on differences in the mentioned solutions. We conclude and give future work in Section 5 and Section 4 respectively.

2 HYBRID CLOUD ARCHITECTURE

The hybrid cloud is one system that combines different cloud environments, typically private and public. A hybrid cloud is usually supported by software that helps manage and automate workloads, allowing them to operate seamlessly across on-premise and public cloud environments. The concept of hybrid cloud is closely related to multi-cloud, which is the combination of two or more public clouds operated by different vendors. The architecture of a hybrid cloud typically includes an Infrastructure-as-a-Service (IaaS) platform. The main IaaS platforms are Amazon Web Services (AWS), Microsoft Azure and Google Cloud platform.

2.1 Cloud Service Models –

Currently, there are more service models available than the four fundamental ones that helped establish cloud computing. Organizations continue to develop new concepts that may be offered as a service. However, NIST [National Institute of Standards and Technology] states that the following are the fundamental four (without SECaaS)

- SaaS - Software as a Service - Application Layer
- IaaS - Infrastructure as a Service - Hardware Layer
- PaaS - Platform as a Service - Middleware Layer
- DaaS - Data as a Service, or Database as a Service
- SECaaS - Security as a Service

2.2 Cloud Deployment Models –

It is necessary to discuss the fundamental cloud service deployment capabilities of each architecture right away. Four fundamental types of cloud computing are defined by NIST [National Institute of Standards and Technology]:

1. Public - Cloud infrastructure is owned by a service provider and its entire administration.
2. Private - Infrastructure is owned by a company or hosted by a provider, but it is always developed and Managed by the customer or third parties.
3. Community - Cloud infrastructure is shared by several companies / organizations and it is managed by one of the companies or a third party.
4. Hybrid - This model is the interconnection of previous models, combines them, but also creates a custom entity

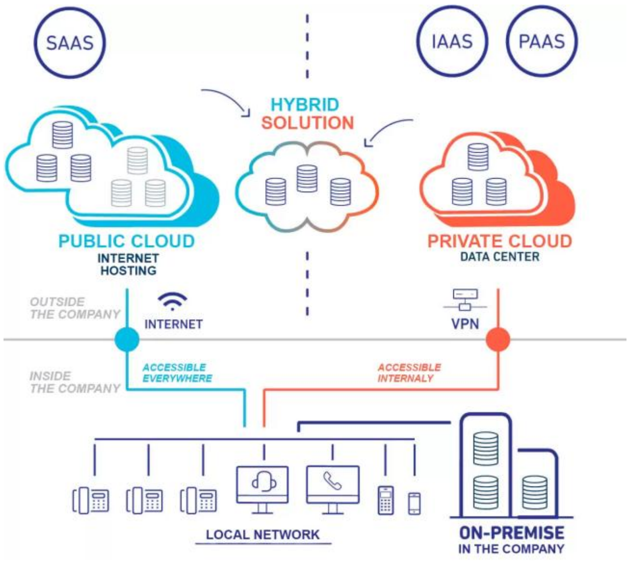

Figure 1 [Hybrid Cloud Architecture]
Source: https://www.padok.fr/

2.3 Hybrid Cloud Management –

Beyond the technical aspects that are involved, it requires an in-depth understanding of security, governance, and end user requirements. Following are a few essential considerations for successful hybrid cloud management.

- Security and governance - We need to prepare security for your hybrid cloud from the beginning with today's DevSecOps attitude. Utilize solutions like Identity and Access Management (IaM) to build uniform security interfaces across environments as you determine the security needs for on-premises and cloud environments. Verify that performance is not impacted by security needs like encryption

- Workload inventory - learn about the workloads that will be used in the hybrid cloud and how they will make use of both on-premises and public cloud resources. Understand the importance of apps to users, anticipated loads, data needs, integrations, networking, and everything else that can affect availability or performance by mapping out the applications.

- Service level agreements (SLA) - Due to the high sensitivity of hybrid clouds to performance, SLAs are a crucial component of planning. To easily fulfil user performance expectations, build public-private interfaces, data transfer pipelines, and latencies. To achieve high availability and be able to meet uptime needs, use public and private cloud resources effectively.

- Visibility across multiple cloud environments - Using dashboards or interfaces for every individual cloud environment may get complex rather quick. Utilize a device or technology that can gather information from both private and public cloud systems and present it all on a single piece of glass. Management will be lot simpler if everything is visible in one location and there is a consistent system for measurements and reporting.

3. SECURITY CHALLENGES IN HYBRID CLOUD –

The majority of corporate apps available today are multi-tiered and frequently comprise several different parts. Businesses may deploy their apps partially on-premises and partially in the cloud due to hybrid architecture. Since data is often the backbone of businesses, it is crucial to manage access permissions and safeguard it. Any data security breach will not be tolerated, hence several methods have been developed to safeguard such data and information. In addition to this, businesses must adhere to a number of laws to ensure data governance. Enterprises will lose some control over their own data set by putting the data into the cloud. To ensure the security of their data, they must rely on the service providers.

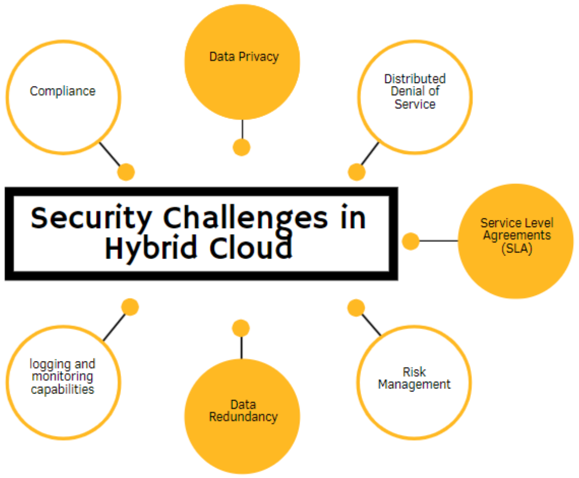
Compliance
Data Privacy
Distributed Denial of Service
Security Challenges in Hybrid Cloud
Service Level Agreements (SLA)
logging and monitoring capabilities
Data Redundancy
Risk Management

Figure 2 [Security Challenges in hybrid cloud]

3.1 Compliance –

Data travels between highly secure private cloud networks and less secure public cloud networks in a hybrid cloud computing approach. This frequently puts data and compliance at risk. Additionally, the introduction of data security standards like GDPR has raised awareness of legal and compliance requirements. Therefore, companies must go above and beyond to guarantee that compliance needs are satisfied. Make that the data transmission mechanism complies with legal requirements and that the public and private cloud networks both comply with industry standards like GDPR.

3.2 Data Privacy –

This is another significant security issue that a hybrid cloud approach may encounter. Data transfer between public and private clouds must be flexible when using hybrid clouds. Your data may be vulnerable to hacker assaults in these circumstances, violating the organization's data privacy policies.

During security breach incidents, measures like endpoint verification protocol, a strong VPN, and a strong encryption policy may encrypt and safeguard your data.

3.3 Risk Management –

To safeguard the organization's secrets from possible dangers, appropriate risk management and preventative safety measures must be implemented in light of the vulnerabilities and threats. This may entail maintaining a log monitoring system with cutting-edge firewall and security management capabilities and employing technologies like IDS/IPS to detect harmful traffic.

3.4 Distributed Denial of service –

The Distributed Denial of Service (DDoS), one of the most dangerous kind of cyber-attack, is a crucial problem that often originates from several sources to target a single place. These assaults often provide a high risk factor since they have several origins, making it difficult to identify and detect them.

Maintaining a stringent monitoring system that can track input and outflow is necessary to deal with this. In a perfect world, this system would be scalable, quick, and capable of defending against multi-vector assaults.

4. SECURITY SOLUTIONS FOR CHALLENGES IN HYBRID CLOUD –

In IaaS, there is a requirement to investigate the solution that aids in offering safe transfer of IT infrastructure services from cloud to corporate internal network since the cloud gives the whole computing and storage capability as a service to the companies and end-users. Encryption and providing safe transmission are crucial techniques for defending business data from intruders.

4.1 Virtual private cloud [VPC] –

Since Amazon developed this solution, it is considered that the public cloud used is Amazon Web Services. Organizations may use Amazon Virtual Private Cloud (VPC) to build their own virtual cloud inside of Amazon Public Cloud, hosting their IT infrastructure within a specified subnet. A VPN connection is provided by VPC between business IT infrastructure and the business virtual cloud (present inside public cloud). To prevent data eavesdropping and manipulation, the VPN connection use IPsec tunnel mode. All security measures put in place for organizations may be extended to virtual clouds. It is evident from figure 3 that the business has built its own virtual cloud called VPC inside an Amazon public cloud. A VPN connection is made between a corporate network and the Amazon public cloud through the internet with the assistance of the VPN gateway and the customer gateway.

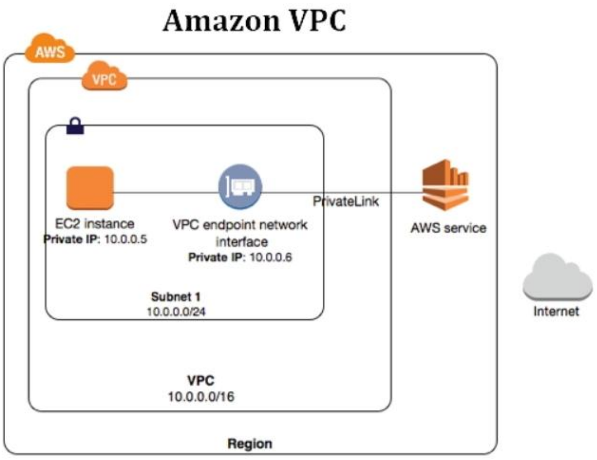

Figure 3 [Amazon VPC]
Source: https://www.testpreptraining.com/

4.2 Open VPN –

This open source VPN technology enables networks to exchange data securely. The data in this case is encrypted using an OpenSSL-based system. For the flow of data Between company IT infrastructure and the cloud, Open VPN creates a secure tunnel. OpenSSH is the protocol used to encrypt tunnel communication. OpenVPN uses the SSL/TLS protocol to offer a secure network. Before establishing a secure connection, it supports a variety of authentication methods, including certificate verification, smart card usage, username/password authentication, firewall access control settings, and more.

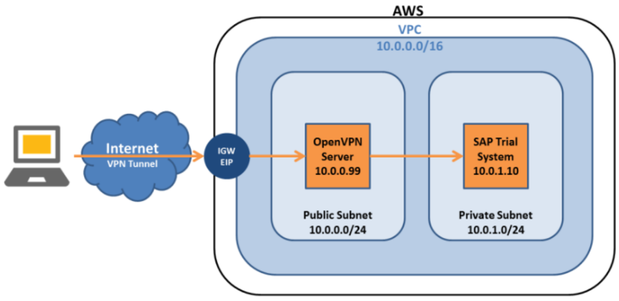

Figure 4 [Open VPN in Cloud Architecture]
Source: https://blogs.sap.com/

4.3 Open Citrix –

Between enterprises and public clouds, cloud bridge solutions offer transparent networks and seamless connection. They need to act as a single integrated network and be securely connected in order to deliver a seamless hybrid cloud. The enterprise's demilitarized zone (DMZ) is safely and openly extended into the cloud using Open Cloud Bridge. Since the cloud bridge solution makes the business and cloud look as unified network, organizations no longer need to worry about altering the network, changing the security and access configurations.

Enterprise customers should be able to access data as if they were using local workstations in order to give them a smooth communication experience when using the cloud. To increase communication speed, Wide Area Network (WAN) performance optimization is crucial.

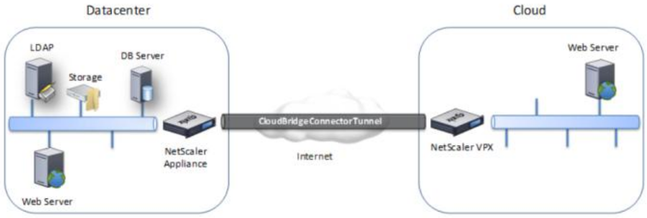

Figure 5 [Open Citrix in Cloud Architecture]
Source: https://docs.citrix.com/

4.4 CloudKnox –

CloudKnox is an identity and access controls supplier that protects the hybrid cloud with its own activity-based authorization architecture. It also serves as a rights management platform, allowing you to see privilege creep, high-risk roles, and unusual activities in real time. CloudKnox is designed specifically for hybrid settings, and it works with all major public clouds as well as virtual machines.

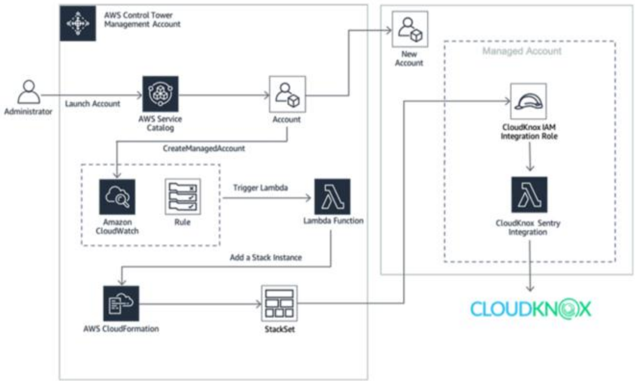

Figure 6 [CloudKnox in AWS Cloud Architecture]
Source: https://aws.amazon.com/

4.4 Guardicore Centra –

Guardicore Centra's software-only design enables advanced network segmentation. This security platform is a smarter alternative to classic firewalls, allowing you to view, segment, and secure your assets across physical data centres, public clouds, and hybrid cloud environments. Guradicore is a powerful policy engine that maps your whole

IT environment and makes suggestions based on the asset classification. Guardicore runs on artificial intelligence.

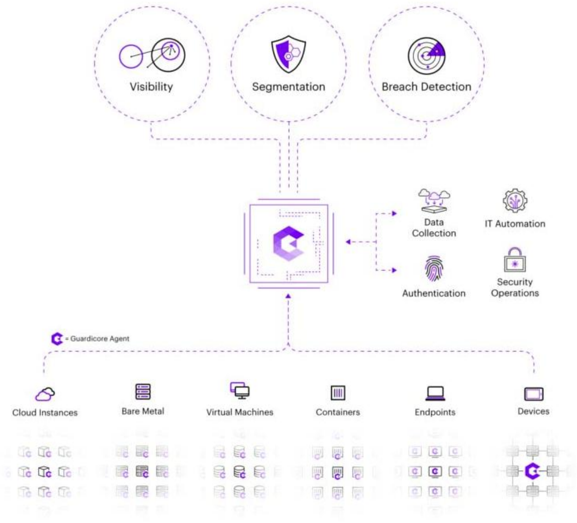

Figure 7 [Guardicore Centra in AWS Cloud Architecture] Source: https://www.guardicore.com/cyber-security-platform/

5. Conclusion–

To avail advantage of the features offered by cloud computing models, the majority of business IT companies intend to implement cloud models in their regular IT operations. Enterprises are free to select from the many cloud deployment and resource options. The hybrid approach is made to fit the needs of the business, enabling them to place some data in the local network and some in the cloud. However, there are various outside concerns that could endanger the sensitive company data. Many businesses have developed solutions, some of which are detailed here, such as building a secure tunnel between a company and the cloud, encrypting the data and storing it there, and setting up a firewall using simple ACL rules.

REFERENCES

[1] https://www.redhat.com/rhdc/managed-files/cl-hybrid-cloud-security-ebook-f18867-202002-en.pdf

[2] Security Risks in Hybrid Cloud https://www.veritis.com/blog/hybrid-cloud-model-6-security-risks-and-ways-to-overcome/

[3] Security Challenges in Hybrid Cloud https://www.csoonline.com/article/3638780/5-top-hybrid-cloud-security-challenges.html

[4] Hybrid Cloud Management https://cloudian.com/guides/hybrid-it/hybrid-cloud-management/

[5] HYBRID CLOUD ARCHITECTURE DESIGN, DEPLOYMENT AND ANALYSIS https://era.library.ualberta.ca/items/b66ad826-fcc9-427e-bf8c-b1b4eb3e165e/view/edb88087-2804-43c1-a987-1ceaa362ebf2/Soliven.pdf

[6] Extending your existing datacenter to the cloud. Technical report. https://docs.citrix.com/en-us/citrix-adc/current-release/system/cloudbridge-connector-introduction.html