**International Journal of Emerging Trends in Computer Science and Information Technology**
ISSN: 3050-9246 | https://doi.org/10.63282/3050-9246.IJETCSIT-V1I2P104
Eureka Vision Publication | Volume 1, Issue 2, 26-36, 2020

*Original Article*

# Hybrid Cloud Security: A Multi-Layered Approach for Securing Cloud-Native Applications

Sathish Srinivasan[1] Suresh Bysani Venkata Naga[2] Krishnaiah Narukulla[3]
[1]Member of Technical Staff | PayPal, Core Platforms & Infrastructure, San Francisco Bay Area, California, USA.
[2]Engineering Leader SAAS and Distributed systems Cohesity, San Francisco Bay Area, California, USA.
[3]Principal Engineer | Roku and Cohesity, Distributed Systeems, Cloud & Machine Learning Expert, Sanfrancisco Bay Area, California, USA.

*Abstract - While organizations advance in using cloud-native solutions, ensuring security in applications running on hybrid clouds has become very important. Hybrid clouds let organizations manage systems themselves and also access functions from the public cloud to benefit from high flexibility, scalability and lower spending. At the same time, cloud computing adds many new security issues due to its distributed design, mix of equipment and fast-changing threats. We offer in this paper a multi-tier defense system designed for hybrid cloud applications that focuses primarily on protecting cloud-native applications. This framework covers security for five important layers. Efforts include infrastructure protection, managing user access, application-level security, data security and privacy and remaining on watch and handling incidents instantly. Customers have the assurance that their applications are safe, thanks to network separation, secured containers, micro services-based authenticity, encryption methods and automated observations of threats. The framework also supports the use of DevSecOps and monitoring compliance at all times. By comparing several cases and analyzing them together, the paper shows how this strategy ensures that hybrid cloud systems are secure and still flexible and perform well. We have seen strong improvements in how fast threats are detected, how compliance is automated and how risks are managed. The research concludes that layered, adaptive security architecture is essential for protecting cloud-native workloads and ensuring secure digital transformation in hybrid environments.*

*Keywords - Hybrid Cloud Security, Cloud-Native Applications, Identity and Access Management (IAM), Container Security, DevSecOps, Incident Response.*

## 1. Introduction

The fast pace of cloud computing has transformed the development, deployment and management of applications by organisations. Enterprises have found that balancing scalability, cost-efficiency and security of important workloads works best when they combine public and private cloud infrastructure. As a result, businesses can host their key systems on local networks and use public clouds for flexible or new IT projects.  But using micro services, containers and Kubernetes in hybrid deployments can also cause many security risks for cloud-native applications. These applications are not fixed; they make use of distributed functions, short-lived services and continual integration/deployment. Working with a hybrid cloud system brings new issues such as ensuring security is kept the same on different platforms, with various cloud companies and over network limits. [1-3] Traditional defenses that rely on boundaries are not enough anymore, since risks can come from within the network, outside or due to security holes in APIs and configuration.

Furthermore, since cloud service providers use a shared responsibility model, companies are expected to look after their application workloads, identities and data. Because of these challenges, more attention is being placed on using a security strategy that covers infrastructure, the platform and applications. The policy is zero-trust, which means never to trust and always to check the trustworthiness. Training software developers on security (DevSecOps) and making sure continuous monitoring, compliance, and threat detection are always present in the environment. For hybrid cloud security to be effective, it needs both the right tools and close cooperation between security experts, developers and cloud architects. The paper discusses a security framework that is intended for both hybrid cloud and cloud-native applications. The suggested framework looks at real-life security issues to help cybersecurity teams harden all levels of the system. The plan is to give groups the ability to construct cloud-native systems that can withstand new threats and remain flexible and compliant.

## 2. Background and Related Work

### *2.1. Cloud-Native Applications Overview*

Cloud-native applications are designed with cloud-based flexibility, scaling power and distributed capability in mind. Micro services are the key method used in cloud-native applications to support their separate, modular nature, instead of the rigid codebases systems found in traditional monolithic software architectures. The components, which are micro services, are not directly connected and manage their operations independently, transmit requests with API calls and are often run in lightweight, mobile containers. Due to this new style of architecture, businesses can quickly create new solutions, update them easily and adjust to user changes swiftly.

A variety of important characteristics recognize cloud-native applications. The ability to scale up and down automatically means these apps work at their best even when usage is highest. Services are made resilient by providing redundancy, designing for fault tolerance and putting in place mechanisms that help them heal after difficulties. Micro services are flexible, since they can be built, deployed and scaled apart from one another, helping to add CI/CD processes more easily. Portability is an important benefit of cloud-native applications, made possible by container technologies such as Kubernetes, which make distributing them easy no matter where they are deployed.

The properties of cloud-native applications ensure they can operate well in areas that require high adaptability and constant availability, like e-commerce, financial data systems, media streams, healthcare details analysis and live data processing. As businesses move faster into digital transformation, cloud-native ways have become essential in IT planning. Cloud-native applications are suitable for use in e-commerce, financial services, streaming media, healthcare analysis or processing data in real-time because these industrial areas need products that can move swiftly and be always accessible. With digital transformation spreading rapidly in all industries, cloud-native approaches are now a key part of modern IT strategies for companies.

### *2.2. Hybrid Cloud Architecture*

A hybrid cloud design uses public cloud and either private cloud or on-site data centers to unite and improve IT flexibility. This approach helps organizations map their workloads according to how much security, speed, compliance and cost are required. More important business information or systems may be kept secure inside the organization, but publicly accessible systems can use the public cloud to make use of its scalability and cost-saving options. Several patterns of architecture have developed in the hybrid cloud framework. [4-6] Private clouds handle sensitive tasks, while public clouds take care of the need for more computing resources using the hybrid model.

This model lets you rely on your current on-premises hardware while using the public cloud only for special cases, such as recovery from disruptions or managing high workloads. By including several public cloud services and internal infrastructure, multi-cloud deployments give increased options and reduce the danger of becoming stuck with a single vendor. Organizations can manage every cloud and physical environment in one place by using hybrid host platforms. For a hybrid cloud to function, robust connections should be made by Virtual Private Networks (VPNs), dedicated lines, or Software-Defined Networking (SDN). Virtualization and containerization are essential because they support moving workloads, standard deployment and better resource utilization in various computing areas.

### *2.3. Security Challenges in Cloud Environments*

Security in cloud and hybrid environments does not look the same as security in traditional IT. Because cloud-native applications are usually distributed, temporary and connect with various systems, they increase the risk of cyber-attacks and make simple security tactics ineffective. In hybrid environments, since resources use different policies and tools, it is much harder to achieve a consistent level of security. Based on the 2020 Cloud Security Report, incorrect configuration of systems represents the top cyber threat to 68% of organisations. If storage buckets are not set up properly, access rights are too generous, or the default settings aren’t secure, unauthorised users may access sensitive data or infrastructure.

Organisations are most concerned about unauthorised access, as seen in 58% of their responses, mainly triggered by poor IAM systems. Insecure APIs and interfaces, as pointed out by 52% of respondents, are risky since they are generally the most common way cloud services share data. Web attackers can use API vulnerabilities to get into systems or change data. Half of the organisations in the report indicated that account hijacking often results when a threat actor gains access to usernames and passwords using any of these techniques and can take over the entire cloud infrastructure. Besides, 69% of the respondents stated that data loss or leakage is a serious problem in places where data is not properly protected. Compliance with privacy laws also adds challenges, especially when global operations mean organisations must stick to systems like GDPR, HIPAA or PCI-DSS.

In cloud computing, with its decentralized and dynamic resources, using traditional perimeter security may not work well. It was found that 82% of organisations admit their legacy security solutions do not effectively shield their cloud systems. By using hybrid and multi-cloud, companies must manage several security solutions, which adds to the complexity and makes things harder to see. As a result, it becomes obvious that organisations should have a comprehensive plan that includes micro-segmentation, automation based on policies, on-the-spot threat detection and continuous compliance checks. Organisations should secure every layer on their hybrid cloud, from the infrastructure down to the applications, to meet the challenges of current threats.

## 3. Threat Landscape in Hybrid Cloud Environments

Organisations that choose hybrid cloud solutions see flexibility, lower costs and scalability. However, this also brings new risks and changes in security requirements. [7-10] Having public, private cloud and on-premises resources connected gives attackers more areas to target, making it difficult to monitor and protect them consistently. Attackers in these environments often target weaknesses in the different layers, apps, identity systems and cloud tools, using clever methods that regular security controls might not block. It is essential to learn about the security risks facing businesses to develop strong mitigation methods that suit current cloud environments.

### *3.1. Attack Vectors and Vulnerabilities*

The enhanced complexity and connection between resources in hybrid cloud environments open various attack vectors. Errors in setup or security policies are very common and often happen in cloud storage, identity management and network settings. Such settings can accidentally give bad actors access to the internet, allowing them access to sensitive data and important services within your organization.

Attackers use phishing to take login details and access cloud systems, which they can then misuse to influence services, steal information or attack victims again. API security is also an important issue to address. Since cloud-native applications communicate with each other through APIs, any unprotected part of the APIs might allow injection, data breaches, or enhanced user privileges.

Cyber attackers can target a supply chain by attacking the third-party software used in CI/CD systems, and they can also target containers, so they can spread to the host machine or influence other containers. If services talk to each other via an unprotected connection, Man-In-The-Middle (MITM) attacks can happen, especially in multi-cloud environments where the traffic goes through internet networks. Having lots of short-lived workloads and many devices creates new challenges for finding and managing threats, so monitoring and alert systems are necessary.

### *3.2. Security Risks in Multi-Tenant Environments*

In hybrid clouds, many organisations or services may benefit from sharing the same infrastructure. By saving resources, this model opens up the system to important security risks if protection is not used. An attacker gaining access to one tenant's network could then move into the networks of nearby tenants that are linked or have the same security flaws and settings.

Multi-tenant environments often deal with worries about shared resources and leaked data. Suppose virtual machines or containers are not properly isolated. In that case, Spectre and Meltdown side-channel attacks can be carried out, and such attacks may enable data extraction from other users. Another possibility is that using the same log or monitor infrastructure could let sensitive information about operations be exposed unintentionally.

A problem with identity and access management is another area of vulnerability. Each tenant's users, services and resources should be carefully segmented and isolated on a multi-tenant platform with RBAC, ABAC and policy enforcement points. If administration is not properly implemented, attackers or rogue users could raise their privileges and gain access to other tenants' resources. To protect multi-tenant settings, you should use specific segmentation, secure both moving and stored data, regularly check for risks and implement the least privilege approach. Both cloud providers and customers need to practice their shared responsibilities in security to keep risks low.

### *3.3. Compliance and Data Sovereignty Issues*

In hybrid cloud systems, organisations often struggle the most with meeting legal requirements and respecting data ownership, where laws are not the same for all locations. Data sovereignty is a law that dictates companies and users should store and process their data only in certain locations, such as those required by the General Data Protection Regulation (GDPR), HIPAA or PIPEDA. Compliance is complex in hybrid environments because data could be stored, handled or cached in both private and public clouds in numerous regions.

Organisations have to prevent the cross-border transfer of sensitive and private information when making use of public cloud services that come from international companies. Not complying with laws can cause serious challenges, affect the company's reputation and interrupt operations. All compliance questions must be fully auditable, and data must be classified, properly encrypted and constantly kept for the specified retention period in hybrid networks. It's important to maintain thorough records, create audit logs that cannot be changed and put in place access and breach notification tools for data subjects.

The task of getting separate groups and systems to adjust to changing regulations is difficult. Many organisations find it challenging to manage and oversee their hybrid environments, meaning compliance is not well managed. Monitoring for compliance, coordinating policies from one location, and regular audits are important elements in proper data governance. Hybrid cloud platforms need to be built and operated according to the compliance-by-design principle to ensure that compliance with laws is easy.

## 4. Multi-Layered Security Framework

Hybrid cloud security requires a full defense plan that covers each level of the technology setup. An extra layer of security in the system can still hold back threats even if others are breached. [11-14] .The model fits with important practices, including not trusting anyone or anything without constant checks. Starting with the main infrastructure layer, the framework moves forward to address identity management and other important tasks.

### *4.1. Layer 1: Infrastructure Security*

Infrastructure security creates the root of the security framework, making sure that hybrid cloud systems protect both digital and physical hardware resources. This means including virtual machines, container hosts, storage devices and network systems which are typically found in on-premises locations as well as on public clouds.

#### *4.1.1. Network Segmentation*

Network segmentation helps to decrease the chances of an attack and blocks threat actors from moving laterally within a system. Splitting the network into different sections, which are usually classified by their purpose, sensitivity, or hazard level, helps organisations focus targeted security measures on each group. No access is allowed from a less secure network to prevent unintentional attacks on the development and production environments. With software-defined networking, micro-segmentation allows administrators to handle application or workload traffic in a more detailed way. Doing this allows businesses to regulate communication strictly and change their security strategies whenever new threats emerge.

#### *4.1.2. Virtual Private Clouds (VPCs)*

Virtual Private Clouds (VPCs) set up private clouds within the infrastructure already offered by the public cloud provider. They enable users to specify IP ranges, subnets, routing tables and gateways to direct how resources within their organization communicate with the outside world. Using VPCs, companies can set up safe, insulated spaces on the cloud that look and function like on-site networks, but offer more flexibility and room to grow. With VPC peering and VPN links, it becomes possible to securely attach these separated environments to private data centers. Appropriately setting up and watching VPCs is very important to stop private services from being seen on the public internet.

#### *4.1.3. Firewall Configurations*

Hybrid cloud systems rely heavily on both traditional and modern firewalls. Organisations can use cloud firewalls to apply rules at the subnet, host and application levels. Access Control Lists (ACLs) and security groups are used to control what can enter or leave your network according to IP addresses, ports and protocols. For more complex settings, application-layer firewalls can scan traffic to find known attacks, enforce the usage of HTTPS and defend against distributed denial-of-service attacks. The use of firewall rules needs to be checked often and through routine audits to ensure critical networks aren't left open to threats.

### *4.2. Layer 2: Identity and Access Management (IAM)*

Identity and Access Management (IAM) is the second most important section in security because it restricts access to specific resources to authorised users and services. When there are so many services in a hybrid cloud environment, it becomes difficult and vital to have secure policies for identity. A centralized IAM strategy that spans across cloud and on-premises environments is vital for maintaining consistent access control.

#### *4.2.1. Role-Based Access Control (RBAC)*

Role-Based Access Control (RBAC) allows administrators to grant permissions according to someone's role instead of to specific individuals. In effect, it means managing access rights can be handled the same way regardless of the number of people. [15-17] Access to environments may vary: developers may not have permission to development or live systems, but system administrators may control many of them. Reducing risks of improper access is made possible by RBAC, as it applies the least privilege principle, so users and services are given only what they need to do their work. Using RBAC at the cloud provider side, as well as within apps, is essential for strong access governance.

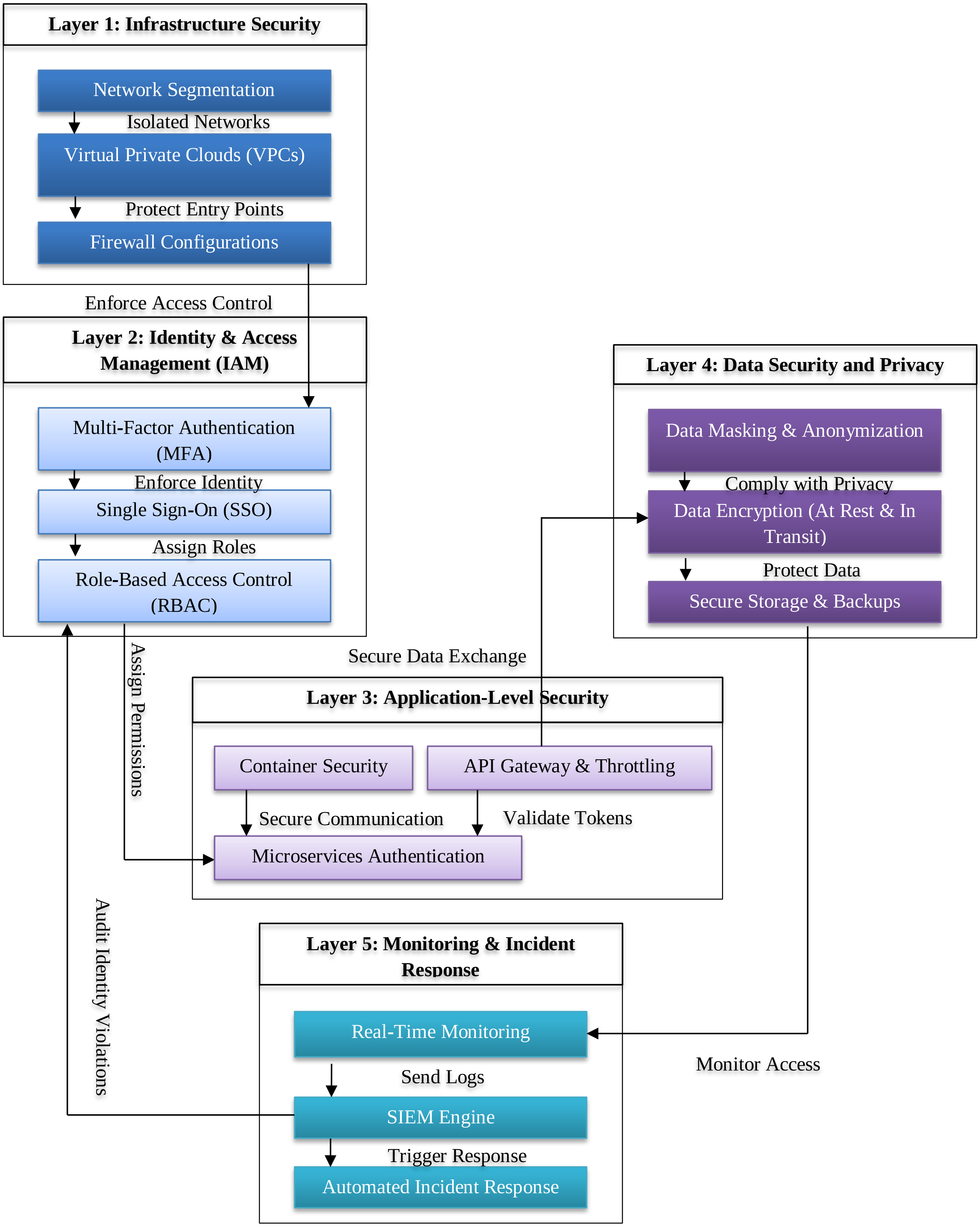
Layer 1: Infrastructure Security
Network Segmentation
Isolated Networks
Virtual Private Clouds (VPCs)
Protect Entry Points
Firewall Configurations
Enforce Access Control
Layer 2: Identity & Access Management (IAM)
Multi-Factor Authentication (MFA)
Enforce Identity
Single Sign-On (SSO)
Assign Roles
Role-Based Access Control (RBAC)
Assign Permissions
Layer 4: Data Security and Privacy
Data Masking & Anonymization
Comply with Privacy
Data Encryption (At Rest & In Transit)
Protect Data
Secure Storage & Backups
Secure Data Exchange
Layer 3: Application-Level Security
Container Security
API Gateway & Throttling
Secure Communication
Validate Tokens
Microservices Authentication
Audit Identity Violations
Layer 5: Monitoring & Incident Response
Real-Time Monitoring
Send Logs
SIEM Engine
Trigger Response
Automated Incident Response
Monitor Access

**Figure 1. Multi-Layered Security Framework**

#### *4.2.2. Single Sign-On (SSO) and Multi-Factor Authentication (MFA)*

Ensuring that Single Sign-On (SSO) and Multi-Factor Authentication (MFA) are in use can help organisations strengthen their identity management system. It is easier and safer for users because they only need to log in once to access several services. It handles your credentials automatically and cuts down on the danger of forgetting passwords and using the same ones too often. MFA makes it harder to access your account by requesting a second way to confirm your identity, like your phone, fingerprint or hardware device, together with your password. This makes it very hard for attackers to access the data, even if someone's login credentials are found. When using hybrid environments, combining SSO and MFA with directories (such as Active Directory) and cloud identity providers (for instance, Azure AD, Okta) allows easy and safe access to all platforms at the same time.

### *4.3. Layer 3: Application-Level Security*

In a hybrid cloud environment, application-level security is especially important for cloud-native applications built using micro services, containers and APIs. Since the application layer is now distributed and flexible, it opens up new chances for attackers who might miss any vulnerability found in the infrastructure level. Any effective application security plan should include safe coding methods, defenses during operation and ways to verify and authorize communication between different services.

#### *4.3.1. Container Security*

Container technology is crucial to cloud-native development, but its temporary and shared usage leads to special security issues. Ensuring the security of containerized applications requires checking the integrity of containers, inspecting for any vulnerability upfront and setting restrictions on what containers can do. Signing container images and using secure registries stop harmful or changed code from being used. During program execution, tools like container firewalls, seccomp profiles and AppArmor or SELinux policies can prevent a container from doing certain actions. Kubernetes and similar platforms come with extra security features such as pod security rules, network policies and RBAC, which should be set up to limit how containers can communicate and reduce overall risks.

#### *4.3.2. Micro services Authentication*

With micro services, services talk to each other using APIs, so having proper authentication and authorization between services is essential. Problems can arise if service-to-service authentication is not used properly, as it makes it possible for attackers to attack exposed APIs or inject malicious services. As a result, both the client and the server need to authenticate each other before being able to communicate. Security and observable service connections are provided by service meshes such as Istio, which include Mutual Transport Layer Security (mTLS), policy management and monitoring. Token-based authentication methods such as JSON Web Tokens (JWT) help pass user identity and authorization details around micro services safely.

#### *4.3.3. API Gateways and Throttling*

API gateways are responsible for managing, keeping an eye on and securing access to micro services. They allow important things like routing requests, limiting the number of requests, converting different protocols and ensuring authentication. The purpose of throttling is to stop Denial-of-Service (DoS) attacks by setting limits on how many requests a client can make during a given time period, which helps the system manage request traffic. Gateways are able to block requests by IP address, use Web Application Firewall (WAF) rules and examine requests for any malicious signs. Through API gateway logging and monitoring, it is possible to see how and when the API is used, helping to catch threats and change policies in advance.

### *4.4. Layer 4: Data Security and Privacy*

In hybrid cloud systems, where information can reside in several areas and is moved between different networks, protecting data becomes especially important. To ensure confidentiality, integrity and availability throughout the whole lifetime of data, as well as complying with privacy regulations and governance, you should have a fully developed data security strategy.

#### *4.4.1. Data Encryption (at Rest and in Transit)*

Encryption ensures that data is secure even when your systems are attacked. The data you keep at rest should be encrypted with strong algorithms such as AES-256, and you should also follow best practices for keys by using Hardware Security Modules (HSMs) and rotating keys on a regular schedule. Block storage, databases and object stores in the cloud are typically protected by native encryption and include key management services. To secure communication between different parts of the hybrid cloud, data in transport should be protected using TLS 1.2 or higher. Turning on encryption by default allows protection to be uniform.

#### *4.4.2. Secure Storage and Backups*

Ensuring secure storage is about the use of encryption as well as restricting access, constant supervision and robustness. IAM and audit logging should be set up to keep unauthorised people from accessing information or taking it out of the system. Backing up your data often is important in case of losing your data to ransomware or by accident. Backups must be securely encrypted, often tested for consistency and stored in different locations in case a disaster affects just one area. Having backups that cannot be modified or erased for a while protects against both ransomware and insider threats.

#### *4.4.3. Data Masking and Anonymisation*

Organisations can improve security in development, testing and analytics by using data masking and anonymisation. Sensitive information is hidden in the data by replacing it with realistic but made-up information that keeps the data useful. Conversely, anonymisation covers up all information that would link a record to a person. These methods are key to meeting privacy laws, including GDPR, HIPAA and CCPA. Privacy should be maintained in all data processing by stopping unapproved parties from accessing sensitive information.

### *4.5. Layer 5: Monitoring and Incident Response*

Monitoring and incident response are just as vital as the other layers to a thorough hybrid cloud security framework. The active and shared structure of hybrid clouds makes it necessary to keep an eye on their actions and respond quickly in case of danger. It is responsible for ongoing monitoring, intelligent linking of events and a quick response to prevent or control security breaches. When monitoring and response actions are done automatically, businesses enjoy greater security and the ability to handle rising security threats.

#### *4.5.1. Real-Time Security Monitoring*

Real-time monitoring in security means regularly checking the network, application and data to catch suspicious behavior as soon as it appears. It requires obtaining telemetry data from cloud servers, containers, APIs, network communication and individual devices. Real-time tools access log data, metrics and traces to help monitor and ensure the safety and well-being of cloud-native applications. Hybrid cloud monitoring should be able to track both local and cloud resources, so it needs consistent tools and dashboards by analyzing events, behavioral analytics that spot out-of-the-ordinary actions so that any unauthorised access, data leaks or increase of privileges can be detected.

#### *4.5.2. Security Information and Event Management (SIEM)*

SIEM systems merge and analyse information from various parts of the hybrid environment to spot and rank possible threats. These platforms gather logs, events and alerts from several sources, including software and hardware for security, access controls and application logs and combine them to find advanced patterns of attack. By using threat intelligence, they increase the accuracy of threat detection using known Indicators of Compromise (IOCs).

Machine learning is used by advanced SIEM solutions to improve the way threats are found and decrease the possibility of false positives. In hybrid cloud systems, SIEM tools need to be able to collect data from all types of sources, so no part of the network goes unnoticed. Tuning the system and updating its rules regularly maintains SIEM performance.

#### *4.5.3. Automated Incident Response*

As incident response can take a lot of time and may have errors, automation is now crucial for effective security management. Automated incident response means following set processes and plans to deal with usual security occurrences without someone manually handling them. If there are suspicious login attempts on an account, an automatic process can isolate it, request multi-factor authentication and send alerts to security.

SOAR platforms streamline the process by working with SIEMs, firewalls, IAM and cloud services. Automation speeds up responses, helps security teams work more efficiently and makes sure all incidents are handled the same way. When using a hybrid cloud, you should set up automation to act the same on your in-house systems and in the cloud, ensuring incidents are dealt with consistently.

## 5. Hybrid Cloud Security Architecture

The design uses security solutions in both local and cloud systems to ensure that every aspect of the system is defended through different security layers. According to the model, identity, data, application and network security all help ensure that confidentiality, integrity and availability are upheld in any distributed environment. Local security relies on firewalls, IDS, application container clusters and encrypted databases when the infrastructure is on-premises.

Security events and policy checks from these parts are transferred to a SIEM, which is connected to a DLP engine that correlates them. [18-20] IAMP is managed through a local gateway that ensures users and applications are identified and that access is set up according to roles. Also, systems that use machine learning scan for behavior that seems odd or suspicious to prevent possible infiltrations.

The public cloud also supports this by providing sophisticated cloud-native security. API gateways, web application firewalls, and Multi-Factor Authentication (MFA) provide safe access and verify user sessions for employees. IAM gateways manage access to cloud-native apps and confidential data in the cloud, while logging and monitoring tools collect telemetry for central processing. All data rests in storage using the same encryption, regardless of where it is saved, whether on a local computer or in the cloud. By using this dual approach, data can travel and be stored safely in the hybrid environment. Security at the application level is improved through the use of DevSecOps tools.

Using CI/CD, source code is always checked by SAST tools to ensure vulnerabilities are spotted in the first stage of development. When a build is verified, it is automatically deployed through the pipeline, following the shift-left principle. Connecting code scanning, vulnerability review and deployment ensures that safe and secure applications are released in the hybrid environment. This design ensures that RBAC is applied the same way in every layer, taking advantage of both local and cloud IAM policies. Analyzing patterns, confirming sessions and detecting anomalies allow the system to constantly watch over the network and respond quickly to incidents. A hybrid cloud deployment uses a mix of infrastructure, application and operational monitoring to secure data at each stage.

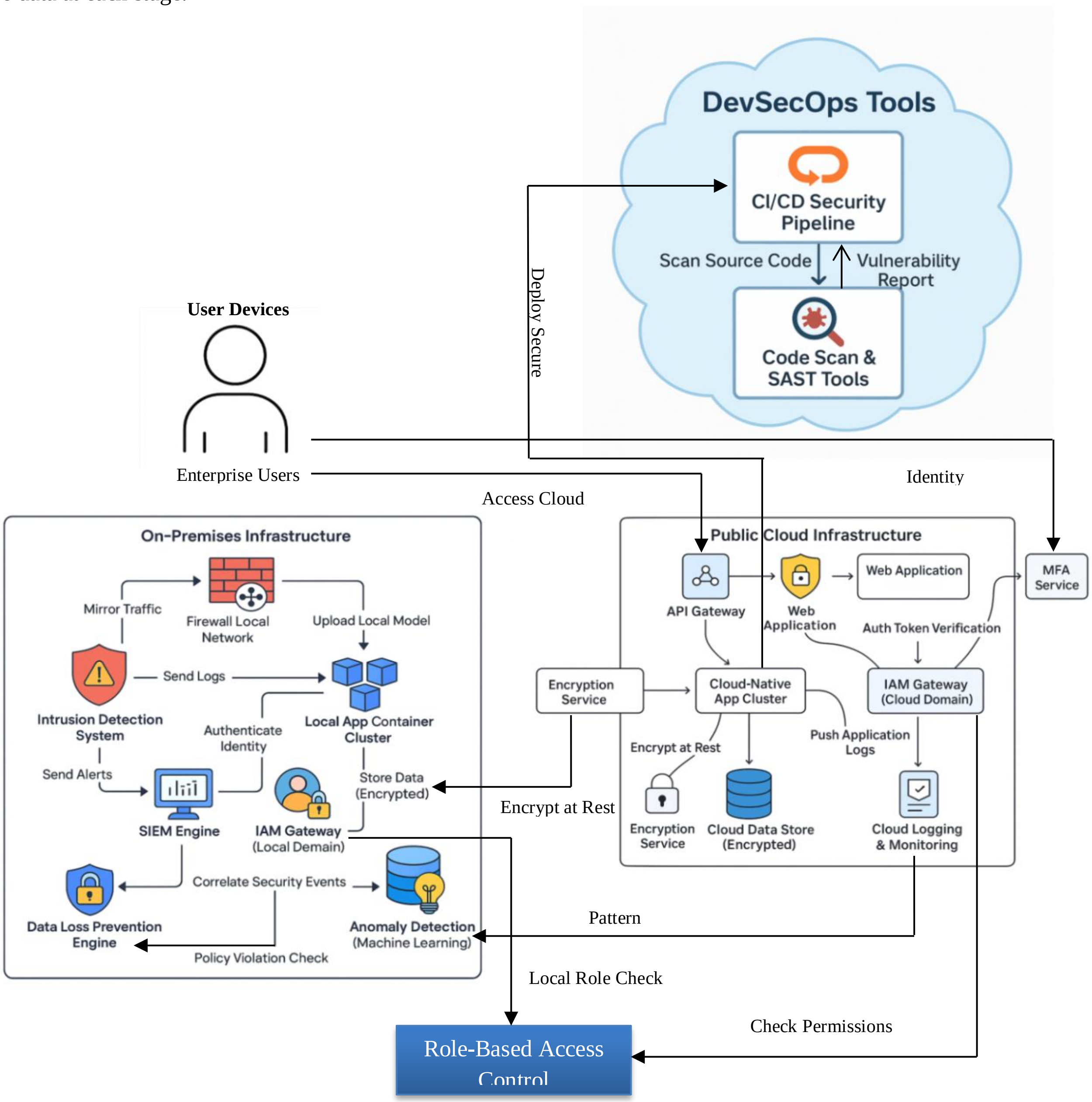

**Figure 2. Multi-Layered Security Architecture for Hybrid Cloud Environments**

## 6. Case Study or Experimental Evaluation

### *6.1. Deployment in a Hybrid Cloud Environment*

Rabbi Interactive, a digital agency, serves customers by developing applications that need a stable and secure cloud environment. By opting for hybrid cloud, the company combined the cloud expansion offered by AWS with the rules and security of its in-house facilities. This option made it possible for Rabbi Interactive to comply with regulations and still move workloads around as needed, based on sensitivity, security rules and how they function.

The decision to utilize a hybrid model made it possible for the company to place scalable services, client systems and analytics in the public cloud, while storing the most sensitive data and databases locally. Because of this strategy, the company now faces less risk and responds faster to possible threats, using the cloud as an elastic resource.

### *6.2. Tools and Technologies Used*

To ensure the strategy was successful, Rabbi Interactive combined the use of cutting-edge DevSecOps tools with security best practices. Internet Protocol Security (IPsec), Destination NAT (DNAT) and WAYS AWS used services to secure public cloud components. At the same time, using Docker and Kubernetes helped build and deploy identical microservices across both environments, supporting the same level of security policies.

By using AWS Cloud Watch and Data dog, we could observe and track the application in real-time and manage all alerts from one place. The use of the Zero Trust Security Model supports constant identification of users and makes sure that they receive only the required access to all applications. Due to this method, a breach led to far less movement sideways within the network.

### *6.3. Security Outcomes and Performance Metrics*

In the hybrid cloud setting, a security model that uses many layers made it possible to enhance security and still adapt quickly to changes. Detecting security problems used to take four hours, but thanks to the new system, this was brought down to only one hour. The deployment succeeded in lowering the number of unsuccessful detections of threats, from 20% to 5%, through the monitoring of all cloud and on-prem systems. Companies also made progress in becoming compliant. Automated security measures and continuous audits confirmed that all the company's data remained secure by adhering to rules and laws. Implementing AI technology helped improve the speed of resolving issues and reduced the risks from incidents.

### *6.4. Comparative Evaluation*

The information in the table compares a hybrid cloud deployment from Rabbi Interactive to a traditional single-purpose architecture.

**Table 1. Comparative Analysis of Traditional vs. Hybrid Cloud Security Approaches**

| Metric | Baseline (Traditional/Non-Hybrid) | Hybrid Cloud with Multi-Layered Security |
|---|---|---|
| Time to Detect Incidents | 4 hours | 1 hour |
| Threats Missed | 20% | 5% |
| Compliance Management | Manual, fragmented | Automated, unified |
| Scalability | Limited | Elastic (on-demand) |
| Security Posture | Siloed, inconsistent | Integrated, consistent |

## 7. Discussion

### *7.1. Benefits of the Multi-Layered Approach*

A multi-layered approach to security ensures comprehensive protection against the wide range of threats faced in hybrid cloud settings. Since security mechanisms are placed at different stages from infrastructure and managing identities to security at the application and data level, the system is less likely to experience a failure at any specific point. The different layers are arranged to help each other, allowing the system to respond to threats it is aware of or not. Regardless of breaking through the network firewall, it is still difficult for an attacker because they must bypass identity checks, encrypted space and real-time tracking.

The multiple layers in the design permit better monitoring and management of everything in the hybrid ecosystem. Such solutions make it easy for security teams to spot unusual occurrences and relate different security events. It helps respond to incidents faster and meets the requirements of the industry. Furthermore, by using Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA) and ensuring data is encrypted both while it's being moved and stored, security adapts well and is easy to scale up. In this way, no sensitive data is left unprotected, and workers can move securely from one cloud to another thanks to hybrid cloud models.

### *7.2. Challenges and Limitations*

Even though using multiple layers for security is helpful, it becomes difficult in a hybrid environment. The main thing that separates engineering from other fields is its complexity. Handling various security levels found in different platforms, vendor products, and settings is difficult and can create problems due to errors. Adding more tools or control layers to an organisation requires time and effort to connect them, look after them and ensure policies are in place. Infrastructure and services in your environment are not always easy to join with those available on the cloud. While cloud tools are strong, often, using them with older systems requires modifying them in major ways, making them less secure. It is difficult for organisations to regularly enforce certain policies among their teams, branch projects or while working with others, since these are often largely decentralised.

### *7.3. Cost-Performance Trade-offs*

A security framework with several layers will always impact the budget. While security threats are greatly minimised with this method, it often increases costs for both capital investments and daily activities. Using high-quality security tools, cloud monitoring, encryption, and skilled employees can reduce your business expenses swiftly. Moreover, using security approaches such as continuous monitoring or masking data can slow down or affect how quickly an application works.

Organisations ought to assess the risks, as well as what security measures fit the needs of the business, when evaluating the trade-off between security and cost. At times, spending too much on low-risk items may not provide sufficient benefit to the resources used. In contrast, not giving enough priority to important layers might open the company to breaches and break regulations. Hence, applying a risk-based strategy and always improving should be part of any security strategy to achieve optimal results and effective protection.

## 8. Future Work

Future research and development should pay attention to adding AI to security so that it is able to change its response to new kinds of threats as they appear. Despite strong security, most rules and configurations in use today cannot handle the continuous changes in threat types such as APTs and zero-day exploits. Using machine learning that learns from the network and people using applications will allow for automatic threat detection and faster action, requiring very few interventions. Creating a common process for handling security in all environments.

When organisations use several clouds, it becomes important to develop a unified system that allows for smooth policy management, identification of controls and reporting on compliance issues across all services and office technology. The adoption of confidential computing and secure enclaves is improving the way we safeguard data privacy when handling applications like medical analytics or any kind of financial transactions. Future studies should focus on light and fast encryption techniques as well as zero-trust models meant for edge computing and serverless services.

## 9. Conclusion

To secure cloud-native applications in a hybrid cloud, you should apply a combination of approaches handling security from infrastructure and identity through applications and continuous monitoring. Since cloud-native designs help organisations scale and remain flexible, they now face the challenge of managing security for both public and private environments. The study introduced an approach that integrates protecting infrastructure, IAM, containers, APIs, privacy and active monitoring to secure organisations deployed in hybrid environments.

The suggested architecture improves the view and control needed in many places, as well as makes the network more secure against various threats. Rabbi Interactive case study highlights that this method boosts the company's security and allows faster identification of incidents while remaining compliant. Despite the fact that combining and properly integrating security systems can be costly and tricky; the benefits are greater than the disadvantages. Since using both private and public clouds is becoming more popular, improvement in security strategies relying on automation and AI will become key to protecting cloud-native programs from the rising threat landscape.

## References

[1] Kratzke, N., & Quint, P. C. (2017). Understanding cloud-native applications after 10 years of cloud computing systematic mapping study. Journal of Systems and Software, 126, 1-16.

[2] Lackermair, G. (2011). Hybrid cloud architectures for online commerce. Procedia Computer Science, 3, 550-555.

[3] Aktas, M. S. (2018). Hybrid cloud computing monitoring software architecture. Concurrency and Computation: Practice and Experience, 30(21), e4694.

[4] Kuo, Y. H., Jeng, Y. L., & Chen, J. N. (2013, July). A hybrid cloud storage architecture for service operational high availability. In 2013 IEEE 37th Annual Computer Software and Applications Conference Workshops (pp. 487-492). IEEE.

[5] Hybrid Cloud Security, cloudsecurityalliance, online. https://cloudsecurityalliance.org/research/topics/hybrid-cloud-security#

[6] Fernandes, D. A., Soares, L. F., Gomes, J. V., Freire, M. M., & Inácio, P. R. (2014). Security issues in cloud environments: a survey. International journal of information security, 13, 113-170.

[7] Galibus, T., Krasnoproshin, V. V., de Oliveira Albuquerque, R., Pignaton de Freitas, E., Galibus, T., Krasnoproshin, V. V., ... & Pignaton de Freitas, E. (2016). Cloud Environment Security Landscape. Elements of Cloud Storage Security: Concepts, Designs and Optimised Practices, 1-18.

[8] Trisha Paine, Top Cloud Security Challenges in 2020, online. https://blog.checkpoint.com/securing-the-cloud/top-cloud-security-challenges-in-2020/

[9] Govindarajan, V., Sonani, R., & Patel, P. S. (2020). Secure Performance Optimisation in Multi-Tenant Cloud Environments. Annals of Applied Sciences, 1(1).

[10] Hybrid Cloud Architecture: How It Works and Top 4 Architecture Patterns, cloudian, online. https://cloudian.com/guides/hybrid-cloud/hybrid-cloud-architecture/

[11] Khan, S., Parkinson, S., & Crampton, A. (2017, December). A multi-layered cloud protection framework. In Companion Proceedings of the 10th International Conference on Utility and Cloud Computing (pp. 233-238).

[12] What is a hybrid cloud? VMware, online. https://www.vmware.com/topics/hybrid-cloud

[13] Shi, Y. (2018, December). Data security and privacy protection in public cloud. In 2018 IEEE International Conference on Big Data (Big Data) (pp. 4812-4819). IEEE.

[14] Check Point’s 2020 Cloud Security Report Highlights Enterprise Security Concerns and Challenges in Public Clouds, Check Point, online. https://www.checkpoint.com/press-releases/check-points-2020-cloud-security-report-highlights-enterprise-security-concerns-and-challenges-in-public-clouds/

[15] Cinque, M., Cotroneo, D., & Pecchia, A. (2018, October). Challenges and directions in security information and event management (SIEM). In 2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW) (pp. 95-99). IEEE.

[16] Hybrid cloud monitoring is crucial for maintaining performance, security, and cost-efficiency. Here are 8 key practices, with coherence, https://www.withcoherence.com/articles/8-best-practices-for-monitoring-hybrid-cloud-environments

[17] Gordon, A. (2016). The hybrid cloud security professional. IEEE Cloud Computing, 3(1), 82-86.

[18] Hybrid Cloud Case Studies, cloudzone, https://www.cloudzone.io/category/casestudies/case-study-hybrid/

[19] Venkateswaran, S., & Sarkar, S. (2018). Architectural partitioning and deployment modeling on hybrid clouds. Software: Practice and Experience, 48(2), 345-365.

[20] Zero Trust Security for Hybrid-Cloud Workloads, accuknox, online. https://accuknox.com/platform/hybrid-cloud-security.