Cloud Security – The Challenges and Road Ahead

ATM APPLICATION TRANSFORMATION MANAGEMENT

Table of Contents

1. Abstract

Cloud computing has become an essential element of digital transformation these days with more and more organizations adopting cloud in the form of SaaS, PaaS or IaaS. Though this has given an edge to enterprises in the form of reduced TCO, improved business agility and increased resilience, it has popped up cloud security concerns of various forms and intensity. We understand the importance of detecting and addressing security concerns at the earliest to gain the optimum advantage of cloud adoption. Hence, this white paper aims to highlight various cloud security challenges and key preventive measures to ensure application and data security while leveraging optimum cloud capability.

2. Introduction

Cloud computing enables a consumer to easily gain on-demand network access to shared configurable computing resources (like servers, networks, storage, services, and applications) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Having said that, even though the enterprises migrating to cloud computing show rapid growth, security is still their major concern. Many enterprises are quite hesitant to move to cloud since they are not fully confident or do not have complete knowledge regarding the level of security provided by cloud vendors.

From recent industry surveys, it has been realized quite evidently that though enterprises are very much familiar with cloud computing as a concept, there are certain roadblocks hampering their cloud journey, with security being a major one. Some of the common security threats include identity theft, data breach and misconfiguration of policies. This restricts enterprises to using only limited features of cloud which can in-turn take away the bigger advantages of cloud migration or development.

Now, let's have a deep dive into what the roadblocks are and how to tackle them strategically.

.

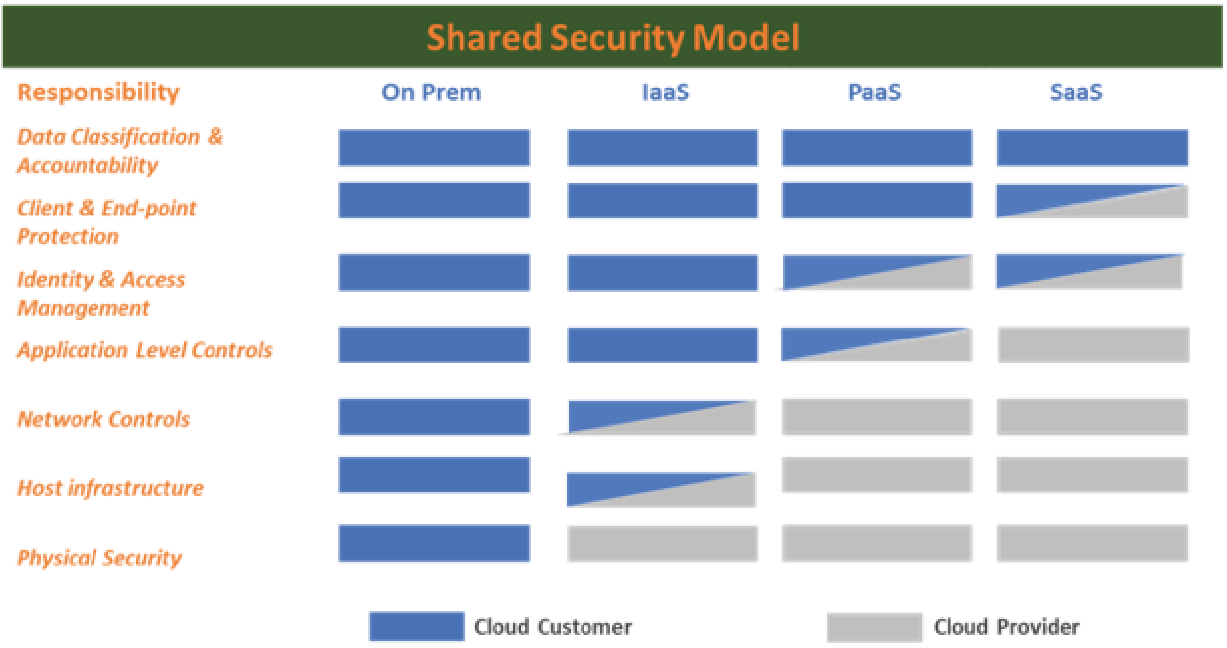
3. Cloud Security Challenges

3.1 Shared Security Model

Many enterprises are hesitant to adopt full-fledged cloud for one common concern – the shared operating model that cloud service works on. Cloud security is managed by the shared responsibility model between Cloud Service Provider (CSP) and cloud consumers. It defines various roles for CSP and cloud consumers to secure the cloud. Some of the security requirements are handled by CSP, some by consumers and some are handled jointly. At a high level, CSP is responsible for the security of the cloud and consumers are responsible for the security in the cloud.

In private clouds, enterprises are responsible for all aspects of security covering infrastructure, physical network, virtual network, firewalls, operating systems, identity access management, and service configuration. For public cloud, CSP owns the infrastructure, network and hypervisor while enterprises are responsible for workload OS, applications, virtual network, access to the environment and data.

Figure 1 below depicts model-wise sharing of responsibility between CSP and consumers.



Shared Security Model

Responsibility	On Prem	IaaS	PaaS	SaaS
Data Classification & Accountability	🟦	🟦	🟦	🟦
Client & End-point Protection	🟦	🟦	🟦	🟦⬜
Identity & Access Management	🟦	🟦	🟦⬜	🟦⬜
Application Level Controls	🟦	🟦	🟦⬜	⬜
Network Controls	🟦	🟦⬜	⬜	⬜
Host infrastructure	🟦	🟦⬜	⬜	⬜
Physical Security	🟦	⬜	⬜	⬜

🟦 Cloud Customer ⬜ Cloud Provider

Figure 1: Cloud model wise sharing of responsibility between CSP and consumer

3.2. Model-wise Threats

There are three main types of cloud service models – SaaS, PaaS and IaaS. Though the level of their capability has matured over the years, they are still prone to security threats, as mentioned below, if not implemented correctly and strategically.

3.2.1 Software as a Service (SaaS)

In the SaaS model, it is the cloud service provider and not the consumer who manages the underlying infrastructure, network, storage and, other capabilities for an application. The consumer accesses such application through a browser or API. Furthermore, as data is located at a shared location between tenants, the prime functions like data segregation, data confidentiality and data destruction become major areas of concern when sharing resources between vendors. Lack of full-proof authentication and authorization techniques can also endanger application security.

3.2.2 Platform as a Service (PaaS)

In the PaaS model, an application is deployed on a platform provided and controlled by cloud service provider. In such conditions, an improper configuration in the application or insecure or privileged permissions to data access can lead to data leak and data theft. Also, anonymous sign-up to the application can compromise security layers quite severely.

3.2.3 Infrastructure as a Service (IaaS)

In the IaaS model, it is the consumer who provisions processing, storage, network and other cloud services as well as deploys the application. Thus, the consumer has control over the operating system, network, firewall and storage and can allow direct access to privileged employees/ insiders. It does have a threat of hackers compromising such direct access and altering permissions to gain control over the infrastructure of other consumers.

3.3 Common Threats and Vulnerabilities

Here are some of the key threats and vulnerabilities that can impact cloud functioning quite deeply:

3.3.1 Insecure APIs

The services provided by different cloud service providers are exposed as Application Programming Interfaces (APIs). Customers use these APIs to interact, provision, manage and monitor the services. Poorly designed APIs carry a risk of threats like clear-text authentication, transmission of content and invalid authorization mechanism. If attackers gain access to customer's API tokens, they can easily misuse and manipulate customer data.

3.3.2 Malicious Insiders

It is quite possible that an insider, say for an instance an employee of either the cloud service provider or the consumer can attempt unauthorized access to the proprietary resources or sensitive information for vested interests. It is not very difficult for him/her to pass or bypass security measures as he/she will be thoroughly aware of the policies, procedures and vulnerabilities associated with the system.

3.3.3 Abusive Use of Cloud Computing

Some of the common forms of abusive use of cloud computing are poorly secured cloud service deployment, using free trials from cloud providers without verifying security compliance and fraudulent account sign-ups by hackers. Hackers can easily afford to rent a space from CSP and use the CPU power and network bandwidth to launch DDoS attacks, run malicious websites and control botnets. As PaaS platform allows customers to deploy their custom application on the platform supported by CSP, the attackers can exploit this as well to inject malicious code into hosting EC2 instance and infect the instance.

3.3.4 Shared Technology Issues/ Multi-tenancy Nature

As the infrastructure provided by CSPs is shared by multiple tenants, the underlying components like CPU Cache, and GPU, which comprise the infrastructure supporting cloud services does not offer strong isolation of properties in the environment. This makes it possible for an attacker to access another application running on the same virtual machine. Hackers can get unauthorized access to CPU, RAM, hypervisors and, applications. Furthermore, hypervisors can be exploited to gain access to other VMs on the same server.

3.3.5 Data Loss and Leakage

Cloud data may be lost/compromised due to many reasons like natural disasters/ catastrophic events, loss of encryption key to access the encrypted data or accidental deletion of data by CSP.

3.3.6 Service/Account Hijacking

Weak passwords, lenient identity and access management policies and lack of ongoing rotation of cryptographic keys help attackers to gain access to systems quite comfortably and without any suspicion. An attacker can steal cloud account information/credentials of an enterprise to perform malicious activities or to manipulate data. If unauthorized access to the infrastructure is successful, malicious software can be loaded on the host to crash servers of running applications.

In such a case, an attacker may restrict even the legitimate users from accessing online services. The attacker can disrupt the service in a virtualized cloud environment by consuming CPU, RAM, disk space and network bandwidth so that an application either stops responding or responds slowly to legitimate traffic.

3.3.7 Data Breaches

Data breach occurs mainly due to human error, vulnerabilities in the application like a bug either in code or in application or poor security practices like weak encryption key and lack of authentication/authorization control. An attacker tries to exploit bugs to steal information and disrupt services as well as to access underlying infrastructure. It can lead to serious theft or permanent loss of data and can cause an indelible impact to brand image.

3.3.8 Advanced Persistent Threats

If an attacker uses advanced exploitation techniques to gain access to an application or system, such an attack can remain undetected in the network for a long time. The usual intention of APT attackers is to steal high-value and intellectual information like defense and financial data.

4 Preventive Measures

4.1.1 Strong Password and Access Management Policies

Set strong passwords to access cloud services and change the passwords frequently to avoid misuse. CSP, as well as the consumer, should have strong access management policies in place and prepare a blacklist or white list for system access.

4.1.2 Data Encryption

Before moving data to cloud, encrypt it by using an encryption algorithm. Also, use cloud services for encrypting data in the cloud itself to prevent unauthorized access within cloud environment.

4.1.3 Compliance with Security Standards

Ensure the application deployed in cloud complies with the security standards and requirements at all layers right from design to implementation to deployment. Identify and eliminate vulnerabilities early.

4.1.4 Secure Cloud Networks and Connections

Cloud service provider should block traffic to known malware ports by screening at firewall itself. Additionally, CSP should provide options to consumer to block illegitimate traffic. Consumer should consider using provisions like VPN provided by CSP to isolate its environment from other consumers.

4.1.5 Detailed Cloud Service Agreement

Depending on the cloud service model opted for, the Cloud Service Agreement (CSA) should define security responsibilities of CSP and consumer. The agreement should clearly mention the clauses related to penalty or compensation in case of any breach.

4.1.6 Well-thought Exit Process

Once the service contract between CSP and consumer gets terminated and exit process is initiated, the consumer should ensure that there is no data left with the CSP or on the respective cloud platform. Also, the data transfer should be done in a secure pattern to avoid any leak or misuse.

4.1.7 Audit Cloud Environment

Conduct regular auditing by third-party or external groups to track activities of CSP employees and customers and to ensure compliance of IT host systems to meet customer's and regulatory requirements. Access the audit trail and ensure that the CSP logs and stores information like authentication, authorization and use of applications and data.

4.1.8 Establish Governance Model and Compliance Process

Customer should establish a governance framework to define the roles and responsibilities of users using cloud services. Specify the shared responsibilities between CSP and consumer. Create policies and procedures along with key aspects to be complied by all users to protect sensitive information. Create a risk management process to identify and document risks.

5. Hexaware Approach and Solution

Hexaware has extensive experience and expertise in providing cloud-based solutions. Our offering not just includes migration to cloud but also the development of cloud-native applications. Our neatly crafted the security framework ensures security of existing and new applications on all types of cloud platforms.

5.1 Identification of Security Requirements

We engage our state-of-the-art cloud security interaction model to perform gap analysis. The analysis helps to figure out which security controls are available and provided by consumer or CSP and which are unavailable or not provided. These gaps are then converted into security requirements, and a feasible solution is architected.

5.2 Security Solutions

5.2.1 Hexaware's Integrated CloudSecOps Platform

Hexaware's integrated CloudSecOps platform helps to secure operations like infrastructure provisioning, deployment and management of workloads and continuous integration and deployment. It is a centralized platform giving complete visibility of cloud environment and provides the following advantages:

- Assesses current security practices and recommends areas of improvement
- Manages security policy accounts, configures DLP principles and whitelists and blacklists traffic to virtual network
- Reviews network configuration and policies to identify the networks or applications susceptible to threats and vulnerabilities
- Monitors traffic continuously to detect anomalies
- Provides an integrated identity server to implement best-in-class authentication and access management solutions and extends on-premise security control/measures to cloud

5.2.2 Cloud Native Security Platform

Hexaware offers an end-to-end solution to secure workloads running on a cloud-native platform. Some of the standouts of this offering include:

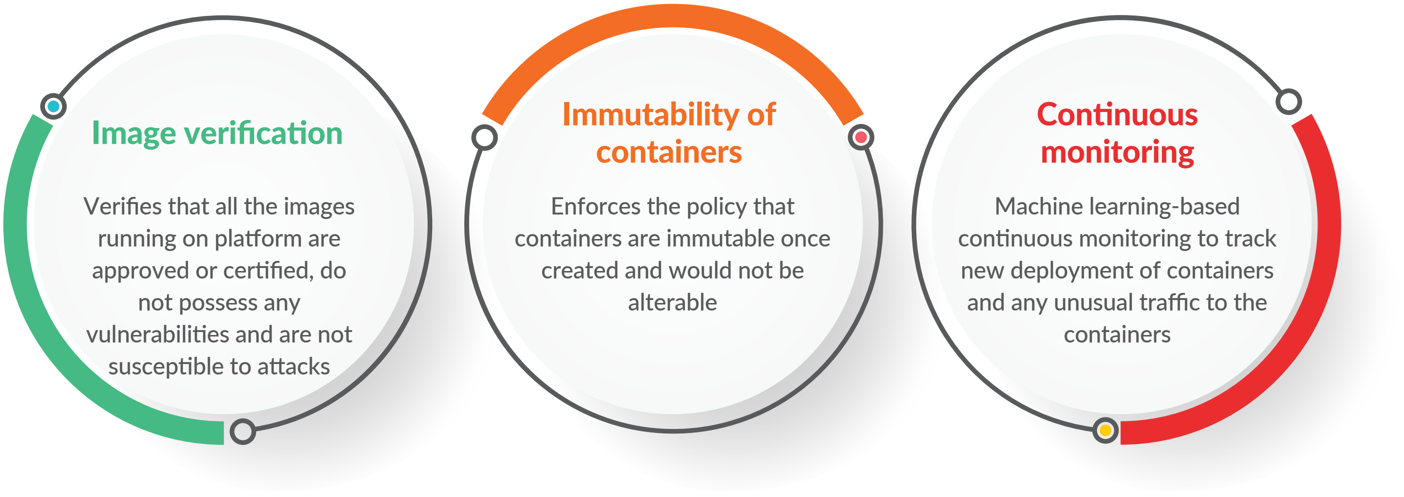


Image verification

Verifies that all the images running on platform are approved or certified, do not possess any vulnerabilities and are not susceptible to attacks

Immutability of containers

Enforces the policy that containers are immutable once created and would not be alterable

Continuous monitoring

Machine learning-based continuous monitoring to track new deployment of containers and any unusual traffic to the containers

6 Conclusion

Cloud adoption at an enterprise level can reap optimum benefits in long-run only when security issues are identified and addressed properly in a timely and systematic manner. Having thorough and updated knowledge of key threats and vulnerabilities can give an edge to cloud service providers as well as consumers in taking right steps at right time to keep data and application secure. Partnering with professional cloud service providers will ensure better cloud security and fast recovery from contingencies, both hardware and software.

7 Author Information

Rajarathinam is currently working as Principal Consultant and Enterprise Cloud Architect with ATM Practice at Hexaware. With over 18+ years of experience in the IT industry, he is involved in solution design and architecting enterprise applications on various Cloud Platforms.

8 References

https://csrc.nist.gov/projects/cloud-computing
https://security.web.cern.ch/security/home/en/index.shtml

NA Headquarters
Metro 101, Suite 600,101 Wood
Avenue South, Iselin,
New Jersey - 08830
Tel: +001-609-409-6950
Fax: +001-609-409-6910

India Headquarters
152, Sector – 3
Millennium Business Park
'A' Block, TTC Industrial Area
Mahape, Navi Mumbai – 400 710
Tel : +91-22-67919595
Fax : +91-22-67919500

EU Headquarters
Level 19, 40 Bank Street,
Canary Wharf,
London - E14 5NR
Tel: +44-020-77154100
Fax: +44-020-77154101

APAC Headquarters
180 Cecil Street,
#11-02, Bangkok Bank Building,
Singapore 069546
Tel : +65-63253020
Fax : +65-6222728

Safe Harbor Statement
Certain statements in this press release concerning our future growth prospects are forward-looking statements, which involve a number of risks, and uncertainties that could cause actual results to differ materially from those in such forward-looking statements. The risks and uncertainties relating to these statements include, but are not limited to, risks and uncertainties regarding fluctuations in earnings, our ability to manage growth, intense competition in IT services including those factors which may affect our cost advantage, wage increases in India, our ability to attract and retain highly skilled professionals, time and cost overruns on fixed-price, fixed-time frame contracts, client concentration, restrictions on immigration, our ability to manage our international operations, reduced demand for technology in our key focus areas, disruptions in telecommunication networks, our ability to successfully complete and integrate potential acquisitions, liability for damages on our service contracts, the success of the companies in which Hexaware has made strategic investments, withdrawal of governmental fiscal incentives, political instability, legal restrictions on raising capital or acquiring companies outside India, and unauthorized use of our intellectual property and general economic conditions affecting our industry.