UNIT IV RESOURCE MANAGEMENT AND SECURITY IN CLOUD 10

Inter Cloud Resource Management – Resource Provisioning and Resource Provisioning Methods – Global Exchange of Cloud Resources – Security Overview – Cloud Security Challenges – Software-as-a-Service Security – Security Governance – Virtual Machine Security
– IAM – Security Standards.

Inter Cloud Resource Management

Cloud computing is on-demand service provided by various organisations and companies. The main motive of the cloud computing is to give high speed internet facility, Low cost usage, Best cloud gaming, High specs PC usage to users. Organisations first established their computer and servers in Server farm in different locations , and they made it available to all users.

In short, Cloud computing is a term that provides the use of data centers to users. This organisations established their various servers and cloud storage services; This helps them to run the cloud computing very smoothly. As Cloud computing provides us High speed internet, Integrated and High PC specs, Low cost usage, Cloud gaming, Storage devices and hardware visualization, Cloud computing has achieved their best place all over the world.

We can compute to our account created in Cloud computing organization. This organization has established their difference services for different uses. Like Cloud computing for online browsing and gaming at high speed and low cost, Online data storage; This provides users online data storage to store their data digitally. Various Tech Giants companies stores their data in the services like this. This is helpful to various users, If our data is deleted from our PC or server, then we can recover it through this service which is very addition point.

What is Visualization in cloud computing ?

Visualization is a creation of Virtual Hologram anything. Like Server, Desktop, Computing, Internet Facility. In short, Virtualization is a technique, which allows organizations share a single physical instance.

Types of Virtualization:
Hardware Virtualization.
Operating system Virtualization.
Server Virtualization.
Storage Virtualization.
Visualization plays very important role in cloud computing, As it provides most important thing, Connection between Clients and users. If any company releases the next version of their application, then by the process of Visualization, Cloud computing provides us the latest version to use. In addition, This cloud services have their 2 different server points. Means, If their any server location is damaged or any technical error is occurred, then they use other server. This servers are programmed in Linux operating system, as it is very fast and efficient, various cloud services uses Linux OS. There are two types of Cloud computing; Public and private
Public - Data is made available to all users from their official homepage. Private - Data is private; No one can read and steal it.
How cloud computing works ?
To understand it in better way, I am classifying cloud computing in 2 different types. - Front end and back end. Back end of the computer is connected to the network physically and Back end is connected to users or clients. The back end is everything in the term "Cloud". Back end consists of Data storage servers, Internet, Network, Database, Computing, monitoring, Content, Block storage, Collaboration, Run-time and everything database. And later, This data is provided to users and clients by their High speed internet facilities.
What is Cloud Gaming ?
Cloud gaming is a similar service like cloud computing announced by Google in their I/O event 2018. Cloud gaming services provides us high speed cloud internet, Highly advanced PC specs and Best monitoring to run and play Games. This service has been officially started to roll-out all over the world by 2019, Google firstly launched this service, It aims to give the best gaming performance to Users and Clients on their smartphones, TVs and old laptops. And, According to a survey, Cloud gaming is going to be future of the Gaming consoles. Most of the gaming consoles like XBOX, PS4, Google are struggling on making Cloud Gaming more smoother and more reliable.

Online cloud computing services:
AWS - Amazon Web Services Google Cloud - By Google Azure – Microsoft Mega Service - By mega
RESOURCE PROVISIONING
RESOURCE PROVISIONING In cloud computing, a resource provisioning mechanism is required to supply cloud consumers a set of computing resources for processing the jobs and storing the data. Cloud providers can offer cloud consumers two resource provisioning plans, namely short-term on- demand and long-term reservation plans. Efficient resource provision which can guarantee the satisfactory cloud computing services to the end user, lays the foundation for the success of commercial competition [9].Resource provisioning is the allocation of a cloud provider's resources to a customer. When a cloud provider accepts a request from a customer, it must create the appropriate number of virtual machines (VMs) and allocate resources to support them. The process is conducted in several different ways: Advance provisioning : With advance provisioning, the customer contracts with the provider for services□ and the provider prepares the appropriate resources in advance of start of service. The customer is charged a flat fee or is billed on a monthly basis.
Dynamic provisioning : With dynamic provisioning, the provider allocates more resources as they are□ needed and removes them when they are not. The customer is billed on a pay-per-use basis. When dynamic provisioning is used to create a hybrid cloud, it is sometimes referred to as cloud bursting.
User self-provisioning :With user self-provisioning (also known as cloud self-service), the customer□ purchases resources from the cloud provider through a web form, creating a customer account and paying for resources with a credit card. The provider's resources are available for customer use within hours, if not minutes .

III. VARIOUS RESOURCE PROVISIONING TECHNIQUES
A. Particle Swarm Optimization(PSO) algorithm and Simulated Annealing(SA) algorithm Marwah Hashim Eawna et al., 2015 propose dynamic resources provisioning in multi-tier application by using meta- heuristic technique such as Particle Swarm Optimization (PSO) algorithm, Simulated Annealing (SA) algorithm and hybrid algorithm that combine Particle Swarm Optimization (PSO)

.
nd Simulated Annealing (SA). In PSO algorithm, there is calculated average computation cost of all tasks on all the compute resources. There is used PSO as a local searching select local best position (Lbest) and global searching to select global best position (Gbest).

The Global Cloud Exchange

Back in 2005 Sun Microsystems announced the company planned to build the world's first online compute exchange. More then three years later there has been no other mention of this supposed compute exchange. In the original press released they described the offering as a plan to introduce a new electronic trading environment that will allow customers to bid on CPU usage cycles. They went on to say that being able to dynamically bid for open compute cycles will provide companies across the globe with unprecedented flexibility in planning for the purchase and use of compute power. This is a new paradigm in computing where companies can access an unlimited number of CPUs as they need them. Today as cloud computing begins to take off and regional cloud utilities start to come online the idea of a cloud exchange is again beginning to be discussed. Back in April at the Interop conference several attendees mentioned they wanted to see the creation of such an exchange platform. The reasoning was that as new regional clouds come online having a uniform point of entry to a world wide cloud ecosystem will make this type of transition more efficient.

Right now most clouds have there own set of APIs, interfaces and unique technologies. An open compute exchange may provide a centralized point where cloud consumers and providers would be able to make decisions based upon which cloud resources they may want to utilize as well as a clearing house for providers with excess capacity. Variables may include metering based on actual use of the resources in CPU hours, gigabits (Gbs) consumed, load, network I/o, peak vs off peak time frames, geographical location, SLA's, and quality of service rules could be just some of the metrics that determine the price of a cloud providers resources. One usage example might be in terms of a green or eco-centric point of view. Let's say Cloud A uses cheaper coal based energy source and Cloud B uses a more expensive Hydro source. Although more expensive, choosing Cloud B may help offset an enterprises carbon credits and therefore actually be a bit cheaper from a carbon point of view. Another example may be based on geographical cloud computing. Let's say a UK cloud and a North

American cloud. Rather scaling based on system load, a cloud user may want to monitor application response times based on geographical location and scale according to an end users experience. By have the option to access compute capacity through an exchange, cloud consumers who are running global network services would no longer have to signup for several cloud services. This would also effectively render edge based CDN services like Akamai irrelevant.

Cloud Security Challenges

Data Breaches

Consequences of a data breach may include:
Impact to reputation and trust of customers or partners
Loss of intellectual property (IP) to competitors, which may impact products release
Regulatory implications that may result in monetary loss

1. Brand impact which may cause a market value decrease due to previously listed reasons
2. Legal and contractual liabilities
3. Financial expenses incurred due to incident response and forensics

2. *Misconfiguration and Inadequate Change Control*

This is one of the most common challenges of the cloud. In 2017, a misconfigured AWS Simple Storage Service (S3) cloud storage bucket exposed detailed and private data of 123 million American households. The data set belonged to Experian, a credit bureau, which sold the data to an online marketing and data analytics company called Alteryx. It was Alteryx that exposed the file. Such instances can be disastrous.

3. *Lack of Cloud Security Architecture and Strategy*

Worldwide, organizations are migrating portions of their IT infrastructure to public clouds. One of the biggest challenges during this transition is the implementation of appropriate security architecture to withstand cyberattacks. Unfortunately, this process is still a mystery for many organizations. Data are exposed to different threats when organizations assume that cloud migration is a ―lift-and-shift‖ endeavor of simply porting their existing IT stack and security controls to a cloud environment. A lack of understanding of the shared security responsibility model is also another contributing factor.

4. Insufficient Identity, Credential, Access and Key Management

Cloud computing introduces multiple changes to traditional internal system management practices related to identity and access management (IAM). It isn't that these are necessarily new issues. Rather, they are more significant issues when dealing with the cloud because cloud computing profoundly impacts identity, credential and access management. In both public and private cloud settings, CSPs and cloud consumers are required to manage IAM without compromising security.

5. Account Hijacking

Account hijacking is a threat in which malicious attackers gain access to and abuse accounts that are highly privileged or sensitive. In cloud environments, the accounts with the highest risks are cloud service accounts or subscriptions. Phishing attacks, exploitation of cloud- based systems, or stolen credentials can compromise these accounts.

6. Insider Threat

The Netwrix 2018 Cloud Security Report indicates that 58 percent of companies attribute security breaches to insiders. Insider negligence is the cause of most security incidents. Employee or contractor negligence was the root cause of 64 percent of the reported insider incidents, whereas 23 percent were related to criminal insiders and 13 percent to credential theft, according to the Ponemon Institute's 2018 Cost of Insider Threats study. Some common scenarios cited include: misconfigured cloud servers, employees storing sensitive company data on their own insecure personal devices and systems, and employees or other insiders falling prey to phishing emails that led to malicious attacks on company assets.

7. Insecure Interfaces and APIs

Cloud computing providers expose a set of software user interfaces (UIs) and APIs to allow customers to manage and interact with cloud services. The security and availability of general cloud services are dependent on the security of these APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent the security policy. Poorly designed APIs could lead to misuse or—even worse—a data breach. Broken, exposed, or hacked APIs have caused some major data breaches. Organizations must understand the security requirements around

designing and presenting these interfaces on the internet.

8. *Weak Control Plane*

Moving from the data center to the cloud poses some challenges for creating a sufficient data storage and protection program. The user must now develop new processes for data duplication, migration and storage and—if using multi-cloud—it gets even more complicated. A control plane should be the solution for these problems, as it enables the security and integrity that would complement the data plane that provides stability and runtime of the data. A weak control plane means the person in charge—either a system architect or a DevOps engineer—is not in full control of the data infrastructure's logic, security and verification. In this scenario, controlling stakeholders don't know the security configuration, how data flows and where architectural blind spots and weak points exist. These limitations could result in data corruption, unavailability, or leakage.

9. *Metastructure and Applistructure Failures*

Cloud service providers routinely reveal operations and security protections that are necessary to implement and protect their systems successfully. Typically, API calls disclose this information and the protections are incorporated in the metastructure layer for the CSP. The metastructure is considered the CSP/customer line of demarcation—also known as the waterline. Failure possibilities exist at multiple levels in this model. For example, poor API implementation by the CSP offers attackers an opportunity to disrupt cloud customers by interrupting confidentiality, integrity, or availability of the service.

10. *Limited Cloud Usage Visibility*

Limited cloud usage visibility occurs when an organization does not possess the ability to visualize and analyze whether cloud service use within the organization is safe or malicious. This concept is broken down into two key challenges. Un-sanctioned app use: This occurs when employees are using cloud applications and resources without the specific permission and support of corporate IT and security. This scenario results in a self-support model called Shadow IT. When insecure cloud services activity does not meet corporate guidelines, this behavior is risky— especially when paired with sensitive corporate data. Gartner predicts that by 2020, one-third of all successful security attacks on companies will come through shadow IT systems and resources.

Sanctioned app misuse: Organizations are often unable to analyze how their approved applications are being leveraged by insiders who use a sanctioned app. Frequently, this use occurs without the explicit permission of the company, or by external threat actors who target the service using methods such as credential theft, Structured Query Language (SQL) injection, Domain Name System (DNS) attacks and more.

11. Abuse and Nefarious Use of Cloud Services

Malicious actors may leverage cloud computing resources to target users, organizations or other cloud providers. Malicious attackers can also host malware on cloud services. Cloud services that host malware can seem more legitimate because the malware uses the CSP's domain. Furthermore, cloud-hosted malware can use cloud-sharing tools as an attack vector to further propagate itself.

SaaS security

SaaS providers handle much of the security for a cloud application. The SaaS provider is responsible for securing the platform, network, applications, operating system, and physical infrastructure. However, providers are not responsible for securing customer data or user access to it. Some providers offer a bare minimum of security, while others offer a wide range of SaaS security options. By 2022, Gartner projects that 95% of cloud security failures will be the customer's fault. To avoid security breaches, customers can implement improved security practices and technologies. Below are SaaS security practices that organizations can adopt to protect data in their SaaS applications.

- **Detect rogue services and compromised accounts.** The average organization uses 1,935 unique cloud services. Unfortunately, the IT departments believe they use only 30 cloud services, according to the 2019 McAfee Cloud Adoption and Risk Report. Moreover, nearly 9% of those cloud services were rated as high-risk services. Organizations can use tools, such as cloud access security brokers (CASB) to audit their networks for unauthorized cloud services and compromised accounts.
- **Apply identity and access management (IAM).** A role-based identity and access management solution can ensure that end users do not gain access to more resources than they require for their jobs. IAM solutions use processes and user access policies to determine what files and applications a particular user can access. An organization can

apply role-based permissions to data so that end users will see only the data they're authorized to view.

- **Encrypt cloud data.** Data encryption protects both data at rest (in storage) and data in transit between the end user and the cloud or between cloud applications. Government regulations usually require encryption of sensitive data. Sensitive data includes financial information, healthcare data, and personally identifiable information (PII). While a SaaS vendor may provide some type of encryption, an organization can enhance data security by applying its own encryption, such as by implementing a cloud access security broker (CASB).
- **Enforce data loss prevention (DLP).** DLP software monitors for sensitive data within SaaS applications or outgoing transmissions of sensitive data and blocks the transmission. DLP software detects and prevents sensitive data from being downloaded to personal devices and blocks malware or hackers from attempting to access and download data.
- **Monitor collaborative sharing of data.** Collaboration controls can detect granular permissions on files that are shared with other users, including users outside the organization who access the file through a web link. Employees may inadvertently or intentionally share confidential documents through email, team spaces, and cloud storage sites such as Dropbox.
- **Check provider's security.** The Cloud Adoption and Risk Report surveyed respondents on their trust of cloud providers' security. It found that nearly 70% of them trust their providers to secure their data. However, only 8% of cloud services actually meet the data security requirements defined in the CloudTrust Program. Only 1 in 10 providers encrypt data at rest, and just 18% support multifactor authentication. Clearly, not all of that customer trust is deserved. An audit of a SaaS provider can include checks on its compliance with data security and privacy regulations, data encryption policies, employee security practices, cybersecurity protection, and data segregation policies.

SaaS security solutions

Several types of security solutions can help organizations improve SaaS security. The solutions can be implemented separately or together as part of a CASB.

- **Data loss prevention (DLP)**) safeguards intellectual property and protects sensitive data in cloud applications, as well as at endpoints such as laptops. Organizations can define data access policies that DLP enforces.
- **Compliance solutions** provide controls and reporting capabilities to ensure compliance with government and industry regulations.
- **Advanced malware prevention** includes technologies such as behavioral analytics and real-time threat intelligence that can help detect and block zero-day attacks and malicious files that may be spread through cloud email and file sharing applications.
- **Cloud access security brokers (CASBs)** protect enterprise data and users across all cloud services, including SaaS, PaaS, and IaaS. According to Gartner's Magic Quadrant for Cloud Access Security Brokers, CASBs detect threats and provide IT departments with greater visibility into data usage and user behavior for cloud services, end users, and devices. CASBs also act immediately to remediate security threats by eliminating security misconfigurations and correcting high-risk user activities applications. CASBs provide a variety of security services, including:
    - Monitoring for unauthorized cloud services
    - Enforcing data security policies including encryption
    - Collecting details about users who access data in cloud services from any device or location
    - Restricting access to cloud services based on the user, device, and application
    - Providing compliance reporting

CASB solutions, which are typically SaaS applications, may provide additional capabilities. These may include:

- File encryption
- Pre-built policy templates to guide IT staff through the process of policy creation
- User entity behavior analytics (UEBA) backed by machine learning
- In-application coaching to help end users learn improved security practices

- Security configuration audits to suggest changes to security settings based on best practices

IT departments can learn to protect their cloud applications and data by following cloud security best practices and implementing effective SaaS security solutions. Cloud security solutions from McAfee enable organizations to accelerate their business growth by giving them visibility and control over their applications, devices, and data. Learn more about McAfee cloud security technology.

Cloud Security Governance - Optimizing the Business Benefits of Security in the Cloud

Why Cloud Security Governance Is Needed

Enterprises are increasingly pursuing the business advantages of migrating technology platforms and services into the cloud environment leveraging one or more of the three main cloud service areas – Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These advantages include but are not limited to rapid information system deployment, significantly reduced operating costs, massive economies of scale, processing speed, and agility. However, subscription to these services often imply security and compliance challenges for enterprises who are often unprepared to resolve them.

Data breaches, system vulnerabilities, insufficient identity, and credential and access management are some of the typical security challenges in the cloud environment that subscriber enterprises must address. In some situations, an enterprise may lack adequate operationalization and enforcement of policies, procedures, a formal operating model, or even a properly constituted organizational function to effectively manage security in the cloud. In other situations, the enterprise may also not sufficiently exercise its responsibility to protect data in the cloud or may lack the means for senior management visibility into cloud security performance and risks. These issues may prevail even when an enterprise stands to gain significant business benefits from transforming its service delivery model via the use of cloud computing platforms.

The underlying business problem leading to these challenges is the lack of effective governance of cloud security. In this blog, I explore cloud security governance, common challenges, and review key targets that can help enterprises optimize the business benefits of cloud security programs.

What Is Cloud Security Governance?

Cloud security governance refers to the management model that facilitates effective and efficient security management and operations in the cloud environment so that an enterprise's business targets are achieved. This model incorporates a hierarchy of executive mandates, performance expectations, operational practices, structures, and metrics that, when implemented, result in the optimization of business value for an enterprise. Cloud security governance helps answer leadership questions such as:

- Are our security investments yielding the desired returns?
- Do we know our security risks and their business impact?
- Are we progressively reducing security risks to acceptable levels?
- Have we established a security-conscious culture within the enterprise?

Strategic alignment, value delivery, risk mitigation, effective use of resources, and performance measurement are key objectives of any IT-related governance model, security included. To successfully pursue and achieve these objectives, it is important to understand the operational culture and business and customer profiles of an enterprise, so that an effective security governance model can be customized for the enterprise.

Cloud Security Governance Challenges

Whether developing a governance model from the start or having to retrofit one on existing investments in cloud, these are some of the common challenges:

Lack of senior management participation and buy-in

The lack of a senior management influenced and endorsed security policy is one of the common challenges facing cloud customers. An enterprise security policy is intended to set the executive tone, principles and expectations for security management and operations in the cloud. However, many enterprises tend to author security policies that are often laden with tactical content, and lack executive input or influence. The result of this situation is the ineffective definition and communication of executive tone and expectations for security in the cloud. To resolve this challenge, it is essential to engage enterprise executives in the discussion and definition of tone and expectations for security that will feed a formal enterprise security policy. It is also essential for the executives to take full accountability for the policy, communicating inherent provisions to the enterprise, and subsequently enforcing compliance

Lack of embedded management operational controls

Another common cloud security governance challenge is lack of embedded management controls into cloud security operational processes and procedures. Controls are often interpreted as an auditor's checklist or repackaged as procedures, and as a result, are not effectively embedded into security operational processes and procedures as they should be, for purposes of optimizing value and reducing day-to-day operational risks. This lack of embedded controls may result in operational risks that may not be apparent to the enterprise. For example, the security configuration of a device may be modified (change event) by a staffer without proper analysis of the business impact (control) of the modification. The net result could be the introduction of exploitable security weaknesses that may not have been apparent with this modification. The enterprise would now have to live with an inherent operational risk that could have been avoided if the control had been embedded in the change execution process.

Lack of operating model, roles, and responsibilities

Many enterprises moving into the cloud environment tend to lack a formal operating model for security, or do not have strategic and tactical roles and responsibilities properly defined and operationalized. This situation stifles the effectiveness of a security management and operational function/organization to support security in the cloud. Simply, establishing a hierarchy that includes designating an accountable official at the top, supported by a stakeholder committee, management team, operational staff, and third-party provider support (in that order) can help an enterprise to better manage and control security in the cloud, and protect associated investments in accordance with enterprise business goals. This hierarchy can be employed in an in-sourced, out-sourced, or co-sourced model depending on the culture, norms, and risk tolerance of the enterprise.

Lack of metrics for measuring performance and risk

Another major challenge for cloud customers is the lack of defined metrics to measure security performance and risks – a problem that also stifles executive visibility into the real security risks in the cloud. This challenge is directly attributable to the combination of other challenges discussed above. For example, a metric that quantitatively measures the number of exploitable security vulnerabilities on host devices in the cloud over time can be leveraged as an indicator of risk in the host device environment. Similarly, a metric that measures the number of user- reported security incidents over a given period can be leveraged as a performance indicator of staff awareness and

training efforts. Metrics enable executive visibility into the extent to which security tone and expectations (per established policy) are being met within the enterprise and support prompt decision-making in reducing risks or rewarding performance as appropriate.

The challenges described above clearly highlight the need for cloud customers to establish a framework to effectively manage and support security in cloud management, so that the pursuit of business targets are not potentially compromised. Unless tone and expectations for cloud security are established (via an enterprise policy) to drive operational processes and procedures with embedded management controls, it is very difficult to determine or evaluate business value, performance, resource effectiveness, and risks regarding security operations in the cloud. Cloud security governance facilitates the institution of a model that helps enterprises explicitly address the challenges described above.

Key Objectives for Cloud Security Governance

Building a cloud security governance model for an enterprise requires strategic-level security management competencies in combination with the use of appropriate security standards and frameworks (e.g., NIST, ISO, CSA) and the adoption of a governance framework (e.g., COBIT). The first step is to visualize the overall governance structure, inherent components, and to direct its effective design and implementation. The use of appropriate security standards and frameworks allow for a minimum standard of security controls to be implemented in the cloud, while also meeting customer and regulatory compliance obligations where applicable. A governance framework provides referential guidance and best practices for establishing the governance model for security in the cloud. The following represents key objectives to pursue in establishing a governance model for security in the cloud. These objectives assume that appropriate security standards and a governance framework have been chosen based on the enterprise's business targets, customer profile, and obligations for protecting data and other information assets in the cloud environment.

1. **Strategic Alignment**

Enterprises should mandate that security investments, services, and projects in the cloud are executed to achieve established business goals (e.g., market competitiveness, financial, or operational performance).

2. **Value Delivery**

Enterprises should define, operationalize, and maintain an appropriate security function/organization with appropriate strategic and tactical representation, and charged with the responsibility to maximize the business value (Key Goal Indicators, ROI) from the pursuit of security initiatives in the cloud.

3. **Risk Mitigation**

Security initiatives in the cloud should be subject to measurements that gauge effectiveness in mitigating risk to the enterprise (Key Risk Indicators). These initiatives should also yield results that progressively demonstrate a reduction in these risks over time.

4. **Effective Use of Resources**

It is important for enterprises to establish a practical operating model for managing and performing security operations in the cloud, including the proper definition and operationalization of due processes, the institution of appropriate roles and responsibilities, and use of relevant tools for overall efficiency and effectiveness.

5. **Sustained Performance**

Security initiatives in the cloud should be measurable in terms of performance, value and risk to the enterprise (Key Performance Indicators, Key Risk Indicators), and yield results that demonstrate attainment of desired targets (Key Goal Indicators) over time.

Virtualization Security in Cloud Computing

2011 ended with the popularization of an idea: Bringing VMs (virtual machines) onto the cloud. Recent years have seen great advancements in both cloud computing and virtualization On one hand there is the ability to pool various resources to provide software-as-a-service, infrastructure- as-a-service and platform-as-a-service. At its most basic, this is what describes cloud computing. On the other hand, we have virtual machines that provide agility, flexibility, and scalability to the cloud resources by allowing the vendors to copy, move, and manipulate their VMs at will. The term *virtual machine* essentially describes sharing the resources of one single physical computer into various computers within itself. *VMware* and *virtual box* are very commonly used virtual systems on desktops.

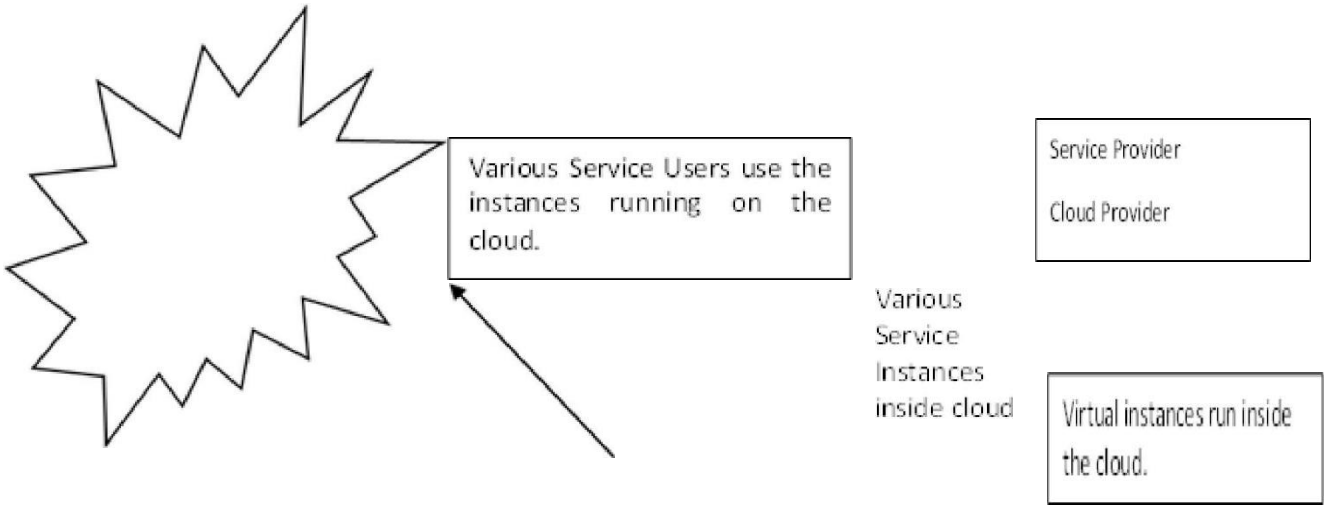
Cloud computing effectively stands for many computers pretending to be one computing environment. Obviously, cloud computing would have many virtualized systems to maximize resources.Keeping this information in mind, we can now look into the security issues that arise within a cloud-computing scenario. As more and more organizations follow the "Into the Cloud" concept, malicious hackers keep finding ways to get their hands on valuable information by manipulating safeguards and breaching the security layers (if any) of cloud environments. One issue is that the cloud- computing scenario is not as transparent as it claims to be. The service user has no clue about how his information is processed and stored. In addition, the service user cannot directly control the flow of data/information storage and processing. The service provider usually is not aware of the details of the service running on his or her environment. Thus, possible attacks on the cloud-computing environment can be classified in to:

1. Resource attacks:
   These kinds of attacks include manipulating the available resources into mounting a large-scale botnet attack. These kinds of attacks target either cloud providers or service providers.
2. Data attacks: These kinds of attacks include unauthorized modification of sensitive data at nodes, or performing configuration changes to enable a sniffing attack via a specific device etc. These attacks are focused on cloud providers, service providers, and also on service users.
3. Denial of Service attacks: The creation of a new virtual machine is not a difficult task, and thus, creating rogue VMs and allocating huge spaces for them can lead to a Denial of Service attack for service providers when they opt to create a new VM on the cloud. This kind of attack is generally called virtual machine sprawling.
4. Backdoor: Another threat on a virtual environment empowered by cloud computing is the use of backdoor VMs that leak sensitive information and can destroy data privacy.
5. Having virtual machines would indirectly allow anyone with access to the host disk files of the VM to take a snapshot or illegal copy of the whole System. This can lead to corporate espionage and piracy of legitimate products.

With so many obvious security issues (and a lot more can be added to the list), we need to enumerate some steps that can be used to secure virtualization in cloud computing.

The most neglected aspect of any organization is its physical security. An advanced social engineer can take advantage of weak physical-security policies an organization has put in place. Thus, it's important to have a consistent, context-aware security policy when it comes to controlling access to a data center. Traffic between the virtual machines needs to be monitored closely by using at least a few standard monitoring tools.

After thoroughly enhancing physical security, it's time to check security on the inside. A well-configured gateway should be able to enforce security when any virtual machine is reconfigured, migrated, or added. This will help prevent VM sprawls and rogue VMs. Another approach that might help enhance internal security is the use of third-party validation checks, preformed in accordance with security standards.



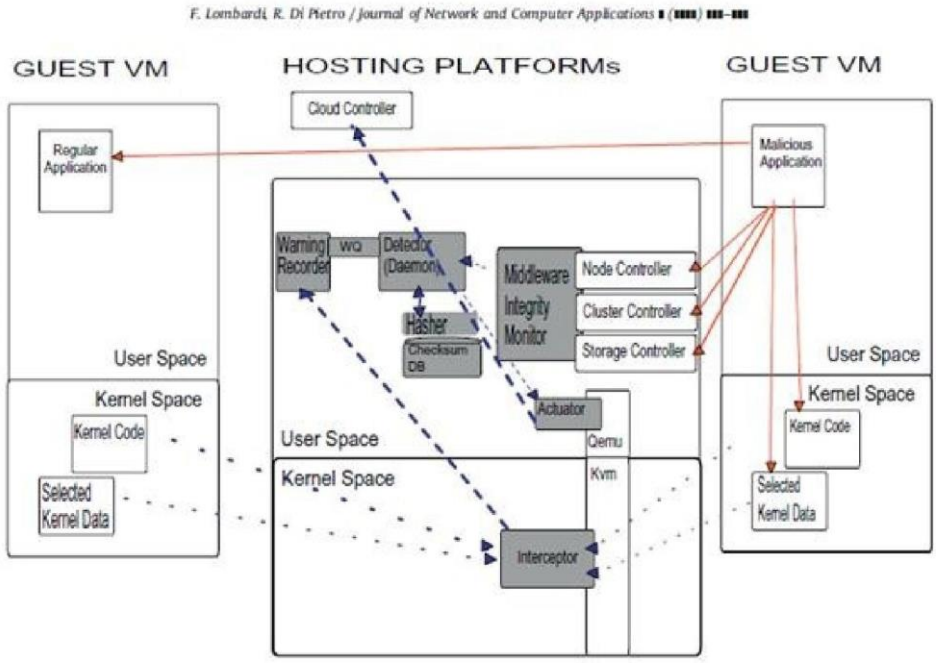
In the above figure, we see that the service provider and cloud provider work together and are bound by the *Service Level Agreement*. The cloud is used to run various instances, where as the service end users pay for each use instant the cloud is used. The following section tries to explain an approach that can be used to check the integrity of virtual systems running inside the cloud.

Checking virtual systems for integrity increases the capabilities for monitoring and securing environments. One of the primary focuses of this integrity check should the seamless integration of existing virtual systems like VMware and virtual box. This would lead to file integrity checking and increased protection against data losses within VMs. Involving agentless anti-malware intrusion detection and prevention in one single virtual appliance (unlike isolated point security solutions) would contribute greatly towards VM integrity checks. This will greatly reduce operational overhead while adding zero footprints.

A server on a cloud may be used to deploy web applications, and in this scenario an OWASP top-ten vulnerability check will have to be performed. Data on a cloud should be encrypted with suitable encryption and data-protection algorithms. Using these algorithms, we can check the integrity of the user profile or system profile trying to access disk files on the VMs. Profiles lacking in security protections can be considered infected by malwares. Working with a system ratio of one user to one machine would also greatly reduce risks in virtual computing platforms. To enhance the security aspect even more, after a particular environment is used, it's best to sanitize the system (reload) and destroy all the residual data. Using incoming IP addresses to determine scope on Windows-based machines, and using SSH configuration settings on Linux machines, will help maintain a secure one-to-one connection.

A Host-side Architecture for Securing Virtualization in Cloud Environment:

The security model prescribed here is purely host-side architecture that can be placed in a cloud system "as it is" without changing any aspect of the cloud. The system assumes the attacker is located in any form within the guest VM. This system is also asynchronous in nature and therefore is easier to hide from an attacker. Asynchronicity prevents timing analysis attacks from detect this system. The model believes that the host system is trustworthy. When a guest system is placed in the network, it's susceptible to various kinds of attacks like, viruses, code injections (in terms of web applications), and buffer overflows. Other lesser-known attacks on clouds include DoS, keystroke analysis, and estimating traffic rates. In addition, an exploitation framework like metasploit can easily attack a buffer overflow vulnerability and compromise the entire environment.



The above approach basically monitors key components. It takes into account the fact that the key attacks would be on kernel and middleware. Thus integrity checks are in place for these modules. Overall, the system checks for any malicious modifications in the kernel components. The design of the system takes into consideration attacks from outside the cloud and also from sibling virtual machines. In the above figure the dotted lines stand for monitoring data and red lines symbolize malicious data. This system is totally transparent to the guest VMs, as this is a totally host-integrated architecture.

The implementation of this system basically starts with attaching few modules onto the hosts. The following are the modules along with their functions:

Interceptor: The first module that all the host-traffic will encounter. The interceptor doesn't block any traffic and so the presence of a third-party security system shouldn't be detected by an attacker; thus, that the attacker's activities can be logged in more detail. This feature also allows the system to be made more intelligent. This module takes the responsibility of monitoring suspicious guest activities. This also plays a role in replacing/restoring the affected modules in the case of an attack.

Warning Recorder: The result of the interceptor's analysis is directly sent to this module. Here a warning pool is created for security checks. The warnings generated are prioritized for future reference.

Evaluator and hasher: This module performs security checks based on the priorities of the warning pool created by the warning recorder. Increased warning will lead to a security alert.

Actuator: The actuator actually makes the final decision whether to issue a security alert or not. This is done after receiving confirmation from Evaluator, hasher, and warning recorder.

This system performs an analysis on the memory footprints, and checks for both abnormal memory usages and connection attempts. This kind of detection of malicious activity is called an *anamoly based detection*. Once any system is compromised the devious malware tries to affect other systems in the network until the entire unit is owned by the hacker. Targets of this type of attack also include the command and control servers, as in case of Botnets. In either case, there is an increase in memory activity and connection attempts that occur from a single point in the environment.

Another key strategy used by atteckers is to utilize hidden processes as listed in the process list. An attacker performs a dynamic data attack/leveraging which hides the process he is using from the display on the system. The modules of this protection system performs periodic checks of the kernel schedulers. On scanning the kernel scheduler, it would detect hidden structures there by nullifying the attack.

Current Implementation:

This approach has been followed by two of the main open-source cloud distributions, namely Eucalyptus and OpenECP. In all implementation, this system remains transparent to the guest VM and the modules are generally attached to the key components of the architecture.

Performance Evaluation:

The system claims to be CPU-free in nature (as it's asynchronous)and has shown few complex behaviors on I/O operations. It's reasoned that this characteristic is due to constant file-integrity checks and analysis done by the warning recorder.

In this article, we have seen a novel architecture design that aims to secure virtualization on cloud environments. The architecture is purely host-integrated and remains transparent to the guest VMs.

This system also assumes trustworthiness of the host, and assumes attacks originate from the guests. As in security, the rule of thumb says: Anything and everything can be penetrated with time and patience. But an intelligent security consultant can make things difficult for an attacker by integrating transparent systems so that they remain invisible and that it takes time for hackers to detect these systems under normal scenarios.

Identity and Access Management Standards

Ensuring data confidentiality and integrity is critical in an era where many organizations rely on cloud services, Internet of Things (IoT) connectivity, Artificial Intelligence (AI) and machine learning. Users must be properly identified, authenticated and authorized to access data and applications without compromising the security of login credentials.

Identity and Access Management (IAM) protocols are designed specifically for the transfer of authentication information and consist of a series of messages in a preset sequence designed to protect data as it travels through networks or between servers. By using third-party authentication, identity management protocols eliminate the necessity of storing login credentials within the system for which they're used, providing a solution for organizations and institutions seeking to prevent the misuse or abuse of login credentials and reduce the risk of data breaches.

Breakdown of Identity and Access Management Protocols

Common identity management standards handle user requests for access to data or applications and deliver responses based on the information a user provides. If the format of the information, such as a password or biometric identifier, is correct, the protocol allows the level of access assigned to the user within the system.

Several protocols exist to support strong IAM policies by securing data and ensuring its integrity during transfer. Generally known as ‑Authentication, Authorization, Accounting,‖ or AAA, these identity management protocols provide standards for security to simplify access management, aid in compliance, and create a uniform system for handling interactions between users and systems.

Because each of these identity and access management standards has different applications, IAM professionals must work with organizations and institutions to implement appropriate protocols to ensure data security.

Standards have been updated in the past to address changes in technology and the new vulnerabilities presented by an increased influx of data. As the IoT, AI and machine learning all evolve, protocols will continue to change. Timely updates will keep systems secure and continue to provide the protection necessary for integrity of credentials and the security of sensitive data. Maintaining security standards ensures compliance with regulations and allows systems to continue operating without unauthorized interference.