# Cloud Security Threats

**Author: Mr. Sibu Thomas**
Astt. Professor, Dept. of Computer Science,
St. Thomas College,
Ruabandha, Bhilai,
Chhattisgarh, India.
thomas_shibu@rediffmail.com

**Author: Mrs. K. Manju**
Astt.Professor, Dept of Computer Science
St. Thomas College,
Ruabandha, Bhilai
Chhattisgarh, India.
manjukaran17@rediffmail.com

***Abstract:*** **Cloud is a fundamental shift in the IT architecture, which is why there's a lot fear amongst enterprise to move towards it. Knowing the types of security risks involved can help reduce that fear and increase its adoption. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. Implementing a Cloud computing solution requires many parameters to be preconceived, including the premise of security.**

**The aim of this paper is to highlight the security challenges currently faced in the Cloud computing. The importance of security requirements is discussed by illustrating the**

**Cloud trade of like identifying the right cloud service provider, vulnerabilities of shared technologies, data aggregation programs. Security in Cloud computing is dependent on the capabilities and constraints of the Cloud. The extension of virtualization in the cloud affects and increases organisations' security perimeter to a newer level. As a result the traditional protocols around enterprise information security are diminished .The importance of securing the cloud cannot be underestimated.**

**The outcome of the paper highlights the security concerns and challenges currently experienced within Cloud computing.**

***Keywords*: Virtualization, Cloud service providers, Data aggregation, Premise-based vulnerability, and Cloud based vulnerability**

## I. Introduction

**CLOUD (Common Location independent Online Utility on Demand)** in its broadest usage refers to the delivery of scalable IT resource over the Internet. It implies a service oriented architecture, reduced information technology overhead for the end-user, great flexibility, reduced total cost of ownership on demand services etc.

Cloud service is just like "putting all your eggs in one basket". This paper discusses some cloud security threats, which are over hyped in the last two years. Almost every software or services company announcing their own cloud based offerings. But there's still a lot of FUD (fear, uncertainty and doubt) in the minds of enterprise user of about moving towards its adoption. The advantages the clouds are supposed to deliver become dissipated in the mist of confusion, deception, deceit and disillusionment. All of a sudden, an enterprise applications move from the confines of its own data center in to public cloud, which is shared by multiple users. There have been publicized attacks on cloud computing providers and this paper discusses recommended steps to handle cloud security issues to clarify before adopting clouds computing.

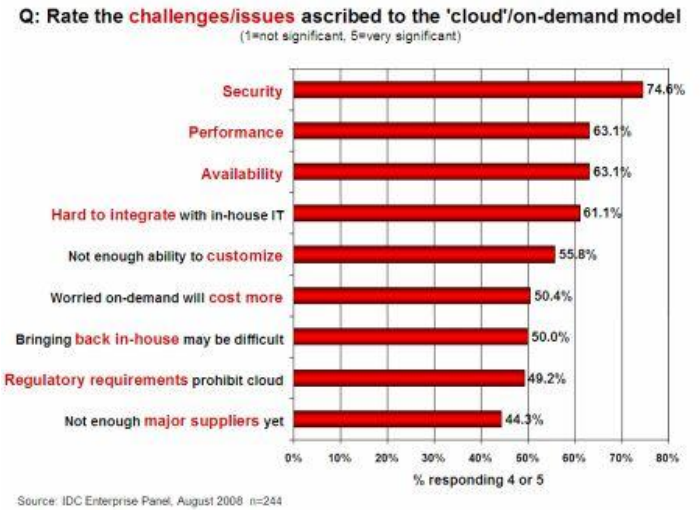
## II. Cloud computation Implementation Guidelines.

1. Understand the cloud by realizing how the cloud's uniquely loose structure affects the security of data sent into it. This can be done by having an in dept understanding of cloud computing transmit and handles data.
2. Demand transparency making sure that the cloud provider can supply detailed information on its security architecture and is willing to accept regular security audit. The regular security audit should be from an independent body or federal agency.
3. Reinforce Internal security by making sure that cloud provider's internal security technologies and practices including firewalls and user access controls

are very strong and can mesh very well with the cloud security measures.

4. Consider the Legal Implications by knowing how the laws and regulations will affect what you send into the cloud.

5. Pay attention by constantly monitoring any development or changes in the cloud technologies and practices that may impact data' security.




## III. Combating the Cloud Security Threats

Cloud computing requires to keep all the data in the cloud. Knowing Basic cloud security threats and risks involved can help to reduce the fear and FUD of adoption. Some of the key security threats are as follows:

### 1. Identifying the right cloud service provider:

One does not need a crystal ball to deduce that cloud computing will be the next big thing and because of this there needs to be some re-thinking of a company's security strategy in order to safeguard the company data.

The first big question is: should you trust the providers themselves? Just because you're buying a service, there is no guarantee that the seller is not going to abuse his power. But it's not just about abuse Cloud service providers are also likely to be a big target for hackers, as a successful intrusion will likely give an attacker access to valuable data of a large number of businesses. And as cloud services become popular it is nearly certain that they will become the focus of a wider range of attacks and not just intrusions. A cloud service provider's main concern is to ensure uptime for clients; the whole business depends on it therefore malicious hackers could try to blackmail or extort money from them to avoid Distributed Denial of Service attacks (DDOS) on their infrastructure, so it is important that one has the means to deal with such an event.

Another important consideration is the service provider integrity. Here one needs to ask a number of questions:

- Can you be sure that in the event of an intrusion the service provider will notify you?
- Will your business get access to the server logs?
- If not, do you have the certainty that the service provider is effectively monitoring the logs and has the proper know-how to both identify issues as well as fix them?
- Does the service provider have an effective backup strategy?
- Does it include offsite backup?
- How long will it take in case of a catastrophic failure for your business to be up and running again? (Is that an estimate or guaranteed time frame?)
- How robust is your internet connection?
- In the event of internet failure how will your business cope?
- What happens in the event that your cloud service provider ceases operations (goes bankrupt, legal disputes, natural disaster)?
- If your cloud service provider were to stop offering their service abruptly do you have a strategy in place to get your business operating again?
- How long will your downtime be and how much will that cost?

Cloud computing can save an organization both time and money; however, it will still require some security considerations. Above are some tips on what to look for and what questions to ask before deciding on which service to go for. Cloud computing can be a great asset as long as it is used properly and the necessary plans are in place to deal with unforeseen circumstances.

Because cloud computing is becoming more prevalent, it is important for businesses to learn how to choose the right cloud provider that will allow them to make the most out of this efficient and innovative computing technology.

Navigating through the cloud providers can seem like a confusing task. The key to finding the right cloud provider is to focus on the cloud services they provide and the quality of the services. The following are a few tips on choosing the right cloud provider:

- **Performance Measurements:** It is important to have reasonable expectations when it comes to the performance of the cloud. Cloud providers, like any server provider, cannot always achieve 100%

performance. Cloud providers that offer 99.9% performance benchmarks understand how the performance of the cloud works.

- **Talk to Vendors and IT Webmasters:** When choosing a cloud provider, you can often get a quality assessment regarding cloud providers from other vendors as well as IT webmasters that have been involved with cloud providers. Researching cloud providers through you computing networks will help you get a sense of the best cloud providers.

- **Test Cloud Provider:** If you want to make sure the cloud provider you are considering is right for you, you can start out by giving them a non-critical part of your business to see how they handle it. If things go well, you can then give them more business or if things don't work out, you can move to another provider.

- **Security and Data Storage:** It is vital that you learn all about how the cloud provider handles securing the cloud. You should find out about their security infrastructures and how they handle data backup. A quality cloud provider should have high priority security measures in place.

- **Service Agreement:** You should make sure you have a service agreement from the cloud provider that outlines the metrics that they will meet and the penalties that will result if they fail to meet the metrics. Not every cloud provider will provide the services they promise so it is important that you do your homework and make sure you have a written outline of how the provider will manage essential aspects of the cloud.

- **Ensure cloud providers make functions available using multiple network paths** The internet is under multiple ownership. This is fortunate, as it offers a multi-path network capability such that, if any one part of the internet goes down, availability tends to remain due to the capability for alternative paths to be taken. But it is also unfortunate, as it means root-cause analysis for network issues can be, at best, painful. Most good cloud function providers will use multiple networks to ensure high availability – but some may only have a single provider, and even if the internet itself is OK, a break in service from that single provider can lead to the lack of availability of a core function for the composite application. Look for providers who have multiple network providers and, where possible, multiple datacentre facilities to ensure functional availability. Also, ensure you have multiple network providers yourself – a break in your connection will mean no access to any functionality.

- **Use cloud providers with service priority for best performance** The very capabilities of general availability outlined above means performance across the internet is difficult to guarantee. As a packet of data can take any route it wants, it could take different amounts of time dependent on network conditions. Look for cloud providers who offer quality and priority of service using services such as multi-protocol labelling service (MPLS) and 802.1p/q. Also, look at the use of other tunneling or direct connecting services, such as leased or dedicated lines where core functions are concerned.

- **Cloud providers must be able to cope with function chain failover** Should there be a failure in the chain, what happens? A good cloud provider will have multiple instances of a function running, and should be able to failover gracefully to another instance. This will require the maintenance of certain network information; however, otherwise transactions may become confused.

- **Cloud providers' functions must be contextually identifiable** All functions must be fully cognizant of what they are doing, and make this information available, should any failure occur. Store and forward messaging is required in the cloud, so any break in service provides a known state, and that this is one which can automatically resume when the failure has been addressed. Look for a cloud provider who offers a fully audited store and forward capability as part of their service.

- **Mitigate the risk of malicious hackers hijacking the chain** A knock-on issue from providing failover capabilities can be that it becomes easier for a chain to be hijacked by a malicious user. If they can inject themselves into the chain when the failure happens (which may well have been initiated by the hacker), the process can continue blithely unaware that the whole chain has been compromised in this way. Ensuring no part of the chain can be hijacked this way, through the use of full contextuality, audit trails and cloud-based intrusion detection capabilities will mitigate this issue.

- **Take responsibility for data security with cloud providers offering data-leak prevention, content inspection and encryption** As well as ensuring that

the process chain itself is not hijacked through functional injection, you must ensure the information in the chain cannot be compromised. Data-leak prevention, content inspection and encryption will help here.

- **Only use cloud-providers who offer good performance, availability and security**

To meet the promise of a fully functional environment, the cloud needs a solid foundation, and this will be dictated by the network it is dependent on. Second-rate cloud providers will be the ones who give cloud a bad name through poor performance, availability and security. Through meeting the above criteria, cloud aggregators will be able to provide enterprise-class services through providing certain functions themselves and using functions from other in a fully managed and audited manner.

## 2. Vulnerabilities of shared technologies

Vulnerability management involves a lifecycle process that includes discovering assets and vulnerabilities, prioritizing assets, prioritizing the remediation activities for vulnerabilities associated with the assets, performing the remediation activities, and finally, measuring the process.

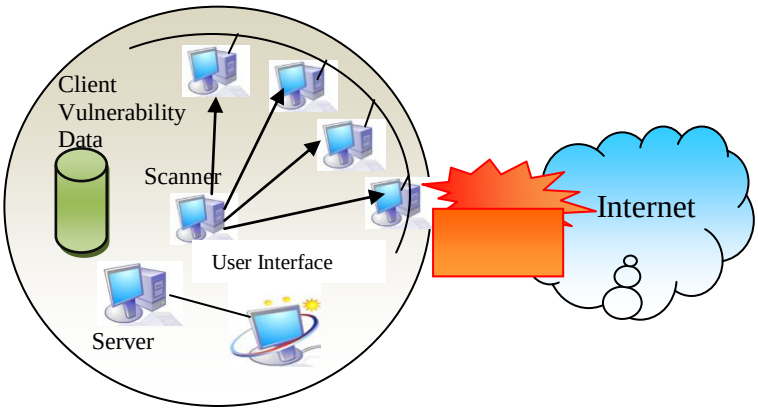
Security vulnerabilities are a fact of life. The problem will never go away. The goal of this lifecycle process is to assess and manage the risk associated with security vulnerabilities. Part of managing the risk is remediation and understanding what to resolve on pre-determined priorities.

### 2.1 Management approach

Several solution providers have introduced products and services that automate parts of the vulnerability management process.

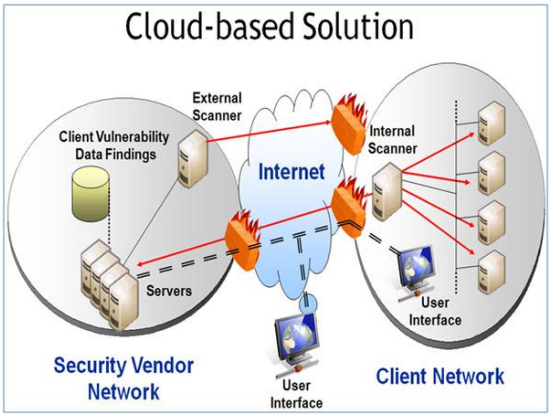
**In a premise-based deployment,** the solution includes hardware and software vulnerability scanners and associated components, which are entirely installed on the client premises. Client users typically login to a web portal accessible via the vulnerability management system within the organization's network. The scanners are located within the client premises and will typically assess vulnerabilities from outside or inside the organization's external firewall for the purpose of performing external and internal vulnerability assessments. All vulnerability findings are stored within the vulnerability management solution on the client premises.

**Figure 1 illustrates a premise-based vulnerability management approach.**




**In a cloud-based deployment**, vendors house a vulnerability management platform "in the cloud", typically in their own data centre. Organizations login to a common web portal over the Internet. They are able to view and manage their vulnerability assessment data within the portal. Vulnerability scanners for external vulnerability assessments are located at the solution provider's site. The solution typically includes one or more scanners that are deployed on the organization's premises for the purpose of performing internal vulnerability assessments. Vulnerability information for the assessments is stored at the solution provider's site (not at the client site) for both internal and external vulnerability assessments.

**Figure 2 illustrates a cloud-based vulnerability management approach.**



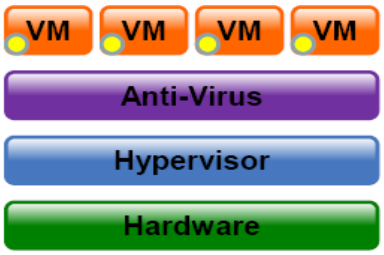

The main technology behind cloud computing is virtualization . Virtualization is mostly done with the

help of software and since any software is vulnerable to security threats, so is virtualization software. Some of the security threats to virtualizations are:

### 2.2 Security vulnerabilities

- **The security of the hypervisor**

We are taking one hardware server, placing a virtualization layer on top of it and then placing multiple guest operating systems and applications on the top of this layer. If a hacker manages to break –into the virtualization layer then he can have access to all applications hosted on it.




**Risk: A compromise of the virtualization layer could result in the compromise of all hosted workloads**

The virtualization layer represents another important IT platform in the infrastructure, and like any software written by human beings, this layer will inevitably contain embedded and yet-to-be-discovered vulnerabilities that may be exploitable. Given the privileged level that the hypervisor/VMM holds in the stack, hackers have already begun targeting this layer to potentially compromise all the workloads hosted above it. From an IT security and management perspective, this layer must be patched, and configuration guidelines must be established.

We recommend that organizations treat this layer as the most critical x86 platform in the enterprise data center and keep it as thin as possible, while hardening the configuration to unauthorized changes. Virtualization vendors should be required to support measurement of the hypervisor/VMM layer on boot-up to ensure it has not been compromised. The organizations should not rely on host-based security controls to detect a compromise or protect anything running below it.

**Risk: Adequate controls on administrative access to the Hypervisor/VMM layer and to administrative tools are lacking**

Because of the critical support the hypervisor/VMM layer provides, administrative access to this layer must be tightly controlled, but this is complicated by the fact that most virtualization platforms provide multiple paths of administration for this layer.

We recommend restricting access to the virtualization layer as with any sensitive OS and favoring virtualization platforms that support role-based access control of administrative responsibilities to further refine who can do what within the virtual environment. Where regulatory and/or compliance requirements dictate, organizations should evaluate the need for third-party tools to provide tight administrative control.

- **Patch management of virtualization software provider:** In virtualization multiple applications are lying on the same server, so one infection could easily spread across to other virtual machines. If vulnerability is found in the virtualization layer itself then these could be used to attack all the hosts sitting on that server. It is extremely important to keep track of all the vulnerability announcements coming from the virtualization software provider and patching them on time.

Typically, patch application involves system restart, and thus negatively affects service availability. Consider a service running inside a VM. Virtualization provides a way to remove faults and vulnerabilities at run-time without affecting system availability. For this purpose, a copy of the VM is instantiated, and the patch (be it OS level or service-level) is applied on the copy rather than on the original VM. Then, the copy is restarted for the patch to take effect after which the original VM is gracefully shut down and future service requests are directed to the copy VM. The patch is applied at the copy VM and the copy VM is restarted while the original VM still continues regular operation, thereby maintaining service availability. To ensure that there are no undesirable side effects due to the patch application, the copy VM may be placed in *quarantine* for a sufficiently long time while observing its post-patch behavior before shutting down the original VM. If the service running inside the VM is stateful, then additional techniques based on a combination of VM check pointing and VM live migration may be used to retain network connections of the original VM and to bring the copy up-to-date with the last correct checkpoint.

- **Monitoring the communication between VM's:**

When multiple virtual machines or host OSs sitting on the same hardware, then how should they communicate? Should the data from one VM travel first traverse the entire physical network, only to come back to another VM that's sitting right next to it? That's obviously not practical. In virtualization, the physical NICs on a host server are abstracted into a switching fabric. This way, all the inter-VM traffic on that host doesn't go out to the

main network, but remains within the same host. While this is good on one side, it can also be a security issue on the other, because your traditional network monitoring tools wouldn't really work. What's important therefore is to check whether a mirroring port can be setup on the virtual switching fabric, so that traffic going through it can be monitored.

**3. Data aggregation programs:**

The first step in protecting anything is to understand it. For aggregated data, this entails understanding what information exists, where it exists, and in what form. Determining an adequate level of protection also requires knowing the security requirements, owners and custodians, and potential risks and impacts. Once the basic information is known about large volumes of aggregated data, the data can be broken into smaller units and profiled. Profiling, or the process of describing, categorizing, and bounding information, is one way to understand the unique characteristics and protection requirements of information. In this case, a smaller and more manageable set of aggregated data is used for profiling. Owners use profiling techniques to explicitly and unambiguously define:

• Information descriptions and boundaries
• Designations of owners, custodians, and users
• Information security requirements, such as access and authentication requirements of users
• Logical and physical locations where the information is stored, transported and processed
• Information value and sensitivity.

If programs are used to aggregate data then you should be careful that those systems don't develop any vulnerability.

- **Privacy in the Cloud**

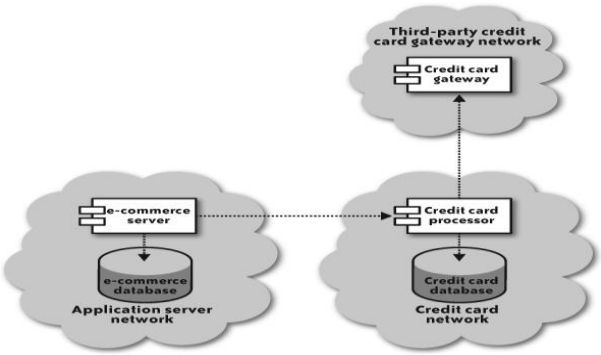
The key to privacy in the cloud—or any other environment—is the strict separation of sensitive data from no sensitive data followed by the encryption of sensitive elements. The simplest example is storing credit cards. You may have a complex e-commerce application storing many data relationships, but you need to separate out the credit card data from the rest of it to start building a secure e-commerce infrastructure.

***Note:*** When we say you need to separate the data, what we mean is that access to either of the two pieces of your data cannot compromise the privacy of the data. In the case of a credit card, you need to store the credit card number on a different virtual server in a different network segment and encrypt that number. Access to the first set of data provides only customer contact info; access to the credit card number provides only an encrypted credit card number.

It's a pretty simple design that is very hard to compromise as long as you take the following precautions:

- The application server and credit card server sit in two different security zones with only web services traffic from the application server being allowed into the credit card processor zone.
- Credit card numbers are encrypted using a customer-specific encryption key.
- The credit card processor has no access to the encryption key, except for a short period of time (in memory) while it is processing a transaction on that card.
- The application server never has the ability to read the credit card number from the credit card server.
- No person has administrative access to both servers.

Figure 3




provides an application architecture in which credit card data can be securely managed.

Under this architecture, a hacker has no use for the data on any individual server; he must hack both servers to gain access to credit card data. Of course, if your web application is poorly written, no amount of structure will protect you against that failing.

You therefore need to minimize the ability of a hacker to use one server to compromise the other.

- Make sure the two servers have different attack vectors. In other words, they should not be running the same software. By following this guideline, you guarantee that whatever exploit compromised the first server is not available to compromise the second server.
- Make sure that neither server contains credentials or other information that will make it possible to compromise the other server. In other words, don't use passwords for user logins and don't store any private SSH keys on either server.

The following principles apply to protecting and securing aggregated data. These are briefly described in this section :

- Accountability
- Adequacy
- Awareness
- Compliance
- Measurement
- Response
- Risk Management

Each of the principles is stated using the present tense, conveying what actions, behaviours, and conditions demonstrate the presence of the principle in the organization's culture and conduct.

- **Accountability**: Organizational leaders are accountable for providing effective oversight of aggregated data security, including ensuring effective execution of the agreed to Protection strategies. Such accountability and responsibility are explicit, defined, acknowledged, and accompanied by the authority to act. Leadership accountability and responsibility for aggregated data security are visible to all stakeholders. Leaders possess the necessary knowledge, skills, and abilities to fulfil these responsibilities. Individual roles, responsibilities, authorities, and accountabilities are assigned. Leaders ensure that all users with access to aggregated data understand their responsibilities with respect to this access. Leaders conduct regular evaluations of their aggregated data security program, review the evaluation results, and report on performance to oversight authorities, including a plan for remedial action to rectify any deficiencies.

  For example, one area reviewed and reported on would be data retention policy and procedure. Leaders work with aggregated data owners and custodians to ensure processes are documented, implemented, and secure for purging data when the need or requirement to maintain the data has expired.

- **Adequacy**: Investment in aggregated data protection strategies (principles, policies, procedures, processes, controls) is commensurate with risk. Determination of risk is based on the value, sensitivity, and criticality of such data with respect to its vulnerability to loss, damage, disclosure, or denied/interrupted access. Probability, frequency, and severity of potential vulnerabilities are considered. Leaders ensure that sufficient resources (people, time, equipment, facilities, and dollars) are authorized and allocated to achieve and sustain an adequate level of aggregated data security.
  For example, leaders ensure data owners and custodians work together to understand the compartmentalization that sensitive aggregated data sets require. Leaders use policies to direct owners to declare value and identify security requirements integrity, and authentication) and direct custodians to implement sound and measurable security controls.

- **Awareness**: Leaders are aware of and understand the need to protect aggregated data. They understand what actions are necessary to protect stakeholder value with respect to such data. All users are aware of aggregated data security risks and protection strategies and understand their concomitant roles and responsibilities. Awareness is demonstrated by the motivation, training, and education provided to users who are given access to sensitive aggregated data and by attendance at periodic training as a requirement of continued access. Performance reviews include an evaluation of how well these responsibilities are fulfilled.

- **Compliance**: Aggregated data protection strategies are in compliance with legal and regulatory requirements, requirements of conducting business, and requirements established by external stakeholders. Actions necessary to evaluate compliance objectively (such as internal and external audits) are built into the security compliance program. This includes regular monitoring, review, and reporting of compliance findings to affected and interested parties. Leaders ensure that remedial and timely action is taken for any aggregated data security deficiencies.

- **Measurement**: Leaders identify and request periodic reports on measures and indicators that demonstrate the value and adequacy (or lack thereof) of aggregated data security protection strategies. "What gets measured gets done. Metrics are about transforming policy into action and measuring performance. Metrics indicate how well policies and processes are functioning and whether or not they are producing desired .performance outcomes.

- **Response**: All users (including leaders) act in a timely, coordinated manner to prevent or respond to threats to aggregated data security and compromises of it. Such response requires development and regular exercise of business continuity, disaster recovery, crisis management, and incident management plans so that the enterprise is adequately prepared in the face of an attack and is able to resume normal operations as quickly as possible.

- **Risk Management**: Leaders continually review, assess, and modify aggregated data security protection strategies in response to the dynamically changing risk environment in which they operate. Leader's articulate acceptable levels of risk to aggregated data assets based on their value, sensitivity, and criticality (see Adequacy). Such levels are examined during regular review and

assessment processes. Costs of compromise (loss, damage, disclosure, denied/interrupted access, costs to reconstitute) are quantified to the extent possible as part of ongoing risk management. Controls are selected to effectively mitigate risk and their performance is regularly measured and reviewed. Plans for remedial action to rectify risk mitigation deficiencies are developed and executed following each assessment.

- **Apply Good Security Practices**

As with management principles, a good set of commonly accepted security practices help an organization meet the protection requirements of aggregated data. Practice selection and adoption derive from the security strategy of an organization. Organizations use practices as they implement security policies, strategies, plans, and actions. To be effective and of greatest value, practices should guide control selection and address risk mitigation efforts necessary to adequately protect sensitive aggregated data.

**The following practice areas** apply to protecting and securing all types of information, including aggregated data. These are briefly described in this section:
• Information Security Strategy
• Information Security Policy
• Security Architecture and Design
• Incident Management
• Partner Management
• Contingency Planning and Disaster Recovery
• Physical Security Management
• Information Technology
• Audit and Monitoring
• Vulnerability Management
Each of the practice areas is stated using the present tense, conveying what actions, behaviors, and conditions demonstrate the presence of the practice in the organization's culture and conduct.

- **Information Security Strategy**: The security strategy is part of the organization's overall strategic planning activity and serves as a systematic plan of action for implementing, maintaining, and improving the security posture of an organization. The strategy encompasses and describes the organization's information security program, including all of the activities and processes that are performed to ensure the mission's survivability. This includes the protection of aggregated data, considered in the context of all other security strategy actions. It considers the unique operating circumstances of the organization, as well as its culture, mission, and critical success factors. Effective security strategy aligns with, and supports, the business strategies and drivers of the organization.

- **Information Security Policy**: An information security policy is the compilation of guiding principles the organization defines to establish the limits and boundaries of behaviors for using information resources and assets, including aggregated data. The core of the information security policy defines the organization's risk tolerance, which is indicative of the range of security events the organization is prepared to withstand. For example, a higher risk tolerance may signify that the organization believes it would not suffer a significant or material impact if a security weakness or vulnerability is introduced and/or exploited. As the organization's risk tolerance narrows, a more extensive security strategy is necessary as well as well defined and prescribed guidelines for behaviour and action.

- **Security Architecture and Design**: Security architecture and design is the physical and logical implementation of the organization's security strategies, policies, and procedures. It is the organization's technical implementation of security structure throughout the various layers of the technical infrastructure. This includes physical devices, hardware, software, and the ways in which security is managed and administered in this infrastructure. Security architecture and design addresses the unique requirements reflected in the profile for each subset of aggregated data. This practice includes ensuring systems on which aggregated data is stored, processed, and transmitted are securely configured and that configurations are kept up to date using a well defined and enforced change management process.

- **Incident Management**: Incident management is the organization's process for identifying, reporting, and responding to suspected security incidents and violations, including those involving aggregated data. The organization is prepared for incidents involving the organization's network and technical infrastructure, physical facilities, and human resources, such as social engineering attempts. The organization's ability to address incidents as a part of the overall security strategy provides another tool for monitoring its environment, understanding what threat and vulnerabilities they are susceptible to, and to develop proactive mitigating and protective strategies. For aggregated data in particular, incident management includes the processes for required communication and notification of affected parties, such as customers. Incident management may also include remedial and corrective actions necessary to restore customer confidence.

- **Partner Management**: Partner management processes and activities require that vendors and service providers act in ways that support the survivability of the parent organization. Organizations communicate to these partners what is important to the organization, and how they are

expected to behave so that they do not expose the parent organization to further risk. Parent organizations recognize they ultimately retain responsibility for ensuring the tasks are completed and that the goals and objectives are achieved. It is essential that partner organizations understand their roles and responsibilities and are held contractually liable for adequately protecting aggregated data that is owned by the parent organization and for which the partner is a custodian or user.

- **Contingency Planning and Disaster Recovery**: Contingency planning and disaster recovery direct the approaches and actions taken by the organization to continue normal operational functions when confronted with significant or adverse disruption. Contingency planning involves the proactive and reactive steps to facilitate an effective and efficient recovery from any contingency that puts the organization's mission at risk. Managing the impacts involves and requires appropriate policies, plans, and procedures to be documented, communicated, tested, and evaluated before a contingency situation occurs. Contingency planning and disaster recovery practices include ensuring aggregated data backups are regularly made, transmitted securely (encrypted), reach their backup storage location, are stored securely, and that aggregated data can be restored to a known state from any given backup media.

- **Physical Security Management**: Physical security is a component of the comprehensive protection strategy, particularly for tangible aggregated data resources (such as hardware, software, and media). It complements the organization's network and system security by physically protecting and acknowledging the logical instantiation of systems and network security controls.

- **Information Technology**: Information technology security is the range of technical mechanisms that the organization deploys to enable and enforce policy, standards, and procedures. Technical practices and mechanisms are applied to counter known and anticipated threats and vulnerabilities to aggregated data, software, systems, and networks. In addition to threat avoidance, resistance, detection, and recovery, technology also supports security controls such as least privilege/separation of duties, access control, role based authentication, firewalls include use of policy segregated networks, change and patch management, aggregated database server configuration control, encryption, redundancy, adequate implementation of aggregated data profiles (including separating sensitive from nonsensitive data), etc.The security of aggregated data is governed by the information security strategy and plans, and spans physical, logical, and operational domains. The physical domain includes the networks and the directly connected systems. The logical domain includes the ways in which users access and authenticate to system and network resources related to aggregated data. This domain is typically governed by an information security department and by the immediate department where the systems reside. The operational domain, somewhat more fragmented, considers how and where certain mission related functions are performed, ultimately by the owners and users of aggregated data.

- **Audit and Monitoring**: Monitoring and auditing inspects and examines the degree to which the organization's policies are being implemented and followed. Monitoring activities are the means by which the organization systematically checks its security posture for weaknesses and vulnerabilities, and initiates appropriate responses where necessary. This includes observing system and network events, configurations, and processes under routine operation for suspicious or unauthorized events related to aggregated data security. The practices and technologies supporting monitoring require the expected or normal state of the system and network environment to be known and defined for aggregated data in processing, storage, and transmission. Where monitoring is the more continuous activity integrated into the organization's routine system administration and management, auditing inspects the security safeguards and controls to determine whether they comply with regulatory and legal requirements, policies, and standards.

- **Vulnerability Management:** Vulnerability management determines the state of technical and operational weaknesses in the technical infrastructure where data sides aggregated, and how to appropriately mitigate the weaknesses. Vulnerability assessment is a proactive or preventive monitoring activity where systems and networks are examined for known technical flaws or weaknesses. Results of a vulnerability assessment are analyzed, prioritized, and reported, with actions tracked to completion. Aggregated data is one form of information and benefits from the same organizational, process, technical, and human security controls that are well known and practiced in information security. Demonstrate that they are exercising due diligence through following commonly accepted good practice.

## Conclusion

The threats to cloud computing are at once serious, varied and broad. So if we think that by deploying virtualization technologies in data center, we will be safe from security threats, then think again. There are security threats to virtualization as well, which can be pretty serious. Customers must evaluate cloud infrastructure

vendors on more than price and top feature sets before deciding to move critical systems and applications.

The top security threats discussed in this paper can have catastrophic impacts to a customer, outweighing any perceived benefits derived from cloud computing. This paper identifies many of the threats and suggests solution that enables a safe transition to this exciting new technology paradigm.

**REFERENCES:**


[1] Cloud Computing. Wikipdia. Available at http://en.wikpedia.org/wiki/Cloud_computing.

[2] Liang-Jie Zhang, Qun Zhou, "CCOA: Cloud Computing Open Architecture," icws, pp.607-616, 2009 IEEE International Conference on Web Services, 2009.

[3] George Pallis, Dbworld IEEE Internet Computing special issue on Cloud Computing, 15 Sep 2008.

[4] Junes Varian, Evangelist, Amazon Web Services, "Cloud Architectures -New way to design architectures by building it in the cloud", 9th IEEE/NATEA.

[5] Peter Wayner, "Cloud versus cloud – A guided tour of Amazon, Google, AppNexus and GoGrid", InfoWorld, July 21, 2008.

[6] Frank E. Gillett, "Future View: The new technology \ ecosystems of cloud, cloud services and cloud computing.

[7] Hand E., Head in the clouds, Nature, Vol. 449, 24 October 2007, p.963.

[8] Amazon's terms of use http://aws.amazon.com/agreement.

[9] An information Centric Approach to Information Security. http://virtualization.sys.com/node171199.

[10]http://searchsecurity.techtarget.com/magazineFeature/0,296894 ,sid14_gci1349670,00.html

[11]http://chenxiwang.wordpress.com/2009/11/24/follow-up-cloudsecurity

[12] www.f5.com

[13] www.sentrigo.com

[14] www.sunmicrosystems.com

[15] www.microsoft.com

[16] www.cloudservices.microfocus.com

[17] Digital Defense Whitepaper 9000 Tesoro Drive, Suite 100 | San Antonio, Texas 78217 | www.ddifrontline.com ©2011