ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.6

Security Aspects of Cloud Migration

Ruchi Tyagi
M.Tech Student
Department of Computer Science & Engineering
Dr. A.P.J. Abdul Kalam Technical University, Uttar Pradesh, India

Abstract:
While the cloud is always present in the technology wordbook, over half of the IT pros responded to the survey of May, 2012 from Wisegate aforesaid it's "too risky for prime time" and only apt for applications like CRM and email services. Security continues to be a serious concern, the poll found. Certainly, security cannot go unnoticed; however it's not insuperable also. It's not completely different from securing on-premises systems, consultants say; it's simply that the perimeter has modified. Additionally, several organizations notice that their cloud service provider done a laborious job of managing security than what they can do as an individual. As cloud computing is being swiftly adopted by every sector, migration of existing applications and data into a cloud is not negligible and involves multiple phases. While the functional requirements are to be handled by the IT pros, the non-functional aspects like security, privacy, authentication, etc. ought to be addressed by the apt stakeholders. The stakeholders ought to be out-and-out in their research and planning so as to guarantee a sleek and successful migration. This research paper takes a glance at the safety issue of predominant cloud architectures as well as covers all important and vulnerable endpoints, and it also offers guidance for queries that can be raise from cloud providers and the ways to counter client issues. It additionally reviews the highest threats and governance areas as known by the Cloud Security Alliance.

I. INTRODUCTION

Cloud Computing has become one of the most talked about technologies in recent times and has got lots of attention from media as well as analysts because of the opportunities it is offering. It has been estimated that the cost advantages of Cloud Computing to be three to five times for business applications and more than five times for consumer applications [28].Cloud Computing is a term used to portray both a platform and type of application. As a platform it supplies, designs and reconfigures servers, while the servers can be physical machines or virtual machines. Then again, Cloud Computing depicts applications that are out to be accessible through the web and for this purpose expansive data centers and effective servers are utilized to host the web applications and web services [9].The cloud is a metaphor for the web and is an abstraction for the complex framework it covers. There are some critical points in the definition to be discussed on the subject of Cloud Computing. Cloud computing contrasts from conventional computing paradigms as it is versatile, can be encapsulated as a theoretical element which gives diverse level of services to the customers, driven by economies of scale and the services are dynamically configurable [22].

1. CLOUD MIGRATION

Cloud could be better comprehended as a framework in which information is put away halfway and can be gotten to anyplace through the web. Cloud computing accentuates on shared assets by numerous clients which can be powerfully reallocated according to request. This boosts figuring power and diminishes the general cost of assets. Distributed computing has now a tremendously demanded carrier because of the benefits of high computing strength, scalability, reasonably-priced cost of offerings, accessibility, excessive overall performance and availability. Cloud migration is the relocation of process far from one location storage space which prompts critical decrease in operational expenses and regularly makes numerous arrangements more versatile to an assortment of various estimated organizations The processing and useful resource sharing work is carried out by means of the cloud provider, cloud arrangements take into account the improvement of inward assets and brings down general organization of the IT assets in an association like general hardware upkeep, reinforcement procedures and calamity recuperation. After migration to the cloud, a company transfers the risks related to these objects to the cloud service provider. It's far pretty hard to sincerely choose the safety of your records and information as it is relied upon what cloud model is selected and which service company an enterprise chooses. There may be risk concerned in migrating to the cloud and as a end result there will be loss statistics and may lose control of your important resources and data records often termed as 'crown jewels' of an enterprise. Essentially, whilst migrating to a cloud solution, an enterprise loses a sizeable degree of manage over its records and information and is relied on the cloud service providers.

2. CLOUD DEPLOYMENT MODELS

There are usually three cloud deployment models used: private, public, and hybrid. A further version is the network cloud or community that is less-commonly used.

2.1 PRIVATE CLOUD

A private cloud is constructed and overseen inside a solitary association and provide the clients with their own physical servers because of which there would be no resource sharing and data is completely isolated. But, isolation comes at a cost as it is the most expensive cloud solution. It can either be hosted by any trustworthy third-part or by a self hosted private cloud (Figure

2). Associations utilize programming that empowers cloud usefulness, for example, VMware, vCloud Director, vCloud connectors or OpenStack.

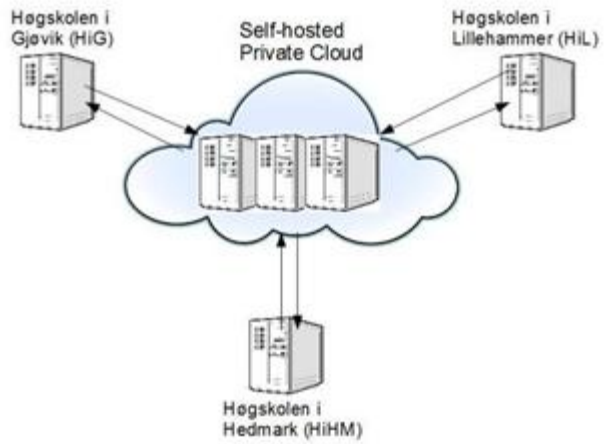

Figure.2. Self-Hosted Private Network

2.2 PUBLIC CLOUD

A public cloud (Figure 3) is an arrangement of figuring assets given by outsider associations i.e. third-party organizations. In this client doesn't have to own any server and in the view of the fact the client doesn't needs any framework, there is no need of any costly investment. The most prominent public cloud incorporates Amazon Web Services, Google AppEngine, and Microsoft Azure.

Figure.3. Public Cloud

2.3 HYBRID CLOUD

A hybrid cloud is a cross breed cloud and is a blend of computing assets supplied by both private and public cloud. It provided its clients with an opportunity to separate their data on private cloud while scaling their use on public cloud .If the workload on private cloud increases client can balance their resource needs on public cloud.

2.4 NETWORK CLOUD

A network cloud offers figuring assets over a few associations, and can be overseen by either hierarchical IT assets or outsider suppliers i.e. third-party providers. It is based on the trust between organizations. In a community model various organizations with the same resources can come together but data will still be separated and will not be shared with a non-trust worthy organization. The cloud based model security is adaptable, proficient and financially savvy to an association utilizing its offerings when contrasted with the conventional data centers security or information center's security. Contrast between the two is depicted by Table I.

Table .I. Contrast between the Cloud and Conventional Security. [6]

Cloud Security	Traditional IT Security
3rd Party Data Centers	In-House Data Centers
Low Infrastructure Investments	High Costs
Quickly Scalable	Slow Scalable
Efficient Resource Utilization	Lower Efficiency
Reduced Time to Market	Longer Time to Market
Usage-Based Cost	Higher Operational Cost

3. CLOUD COMPUTING SERVICE MODELS

A cloud computing service model shows the cloud services or offerings relation with the customers or its clients. Basic service models accessible within the industry embody a mix of Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). These service models may work autonomously or could be utilized cooperatively with each other – for instance, PaaS is reliant on IaaS since application stages require physical foundation. Figure 5 shows the resources or data managed at each level of service.

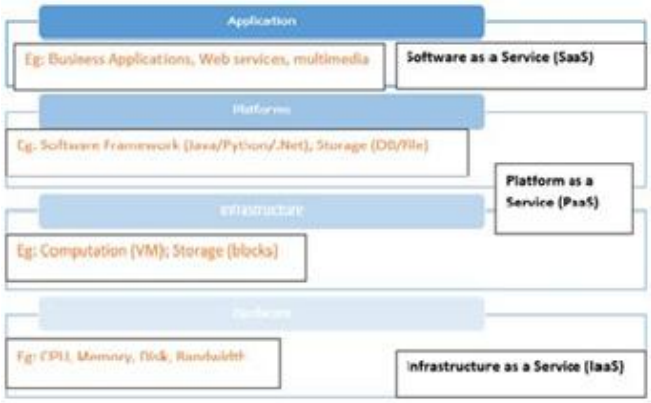

Figure.5. Resources managed at each level

3.1 IaaS MODEL

The IaaS service model of cloud focuses within the infrastructure segments of clients. These segments may incorporate virtual machines, storage, networks, firewalls, and routers, SANs, load balancers and different hardwares. IaaS composes guide access of the assets to the customer like working framework on virtual machines, or to the administration dashboard of a firewall, router or load balancer. Amazon Web Services is one of biggest IaaS provider. [6]

3.2 PaaS MODEL

The PaaS model gives an application stage to the customer with no reliance to the fundamental framework utilized by the cloud service providers for their applications package. PaaS routinely scales and provisions required framework components depending on utility necessities and scalability the usage of an APIs inclusive of features for less complicated programmatic platform control and solution development and improvement. Key

attributes that characterize PaaS is depicted in Figure 7. Google is a well known PaaS supplier [23], and Amazon Web Services conjointly provides some PaaS solutions additionally to the IaaS offerings [6].

Figure.7. PaaS Key Attributes [18]

3.3 SaaS MODEL

SaaS model gives online programming arrangements which completely manage the control over application software. SaaS application illustrations incorporate e-mail, project-management systems, CRMs, and social media platforms. Contrast amongst SaaS and PaaS is that SaaS gives online applications that are as of now created alongside the stage where the customer is not dependent on the platform the cloud service provider uses. [17]

Figure.8. SaaS Model [42]

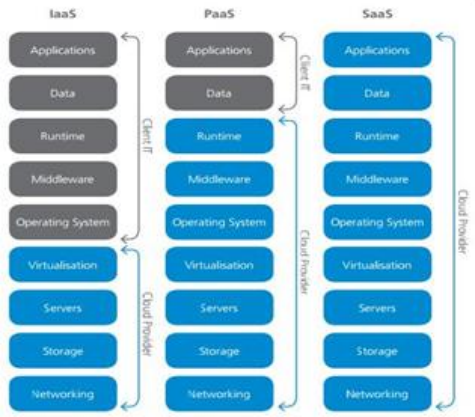

Figure.9. Who is responsible for what in each cloud computing model?

4. CLOUD COMPUTING EVOLUTION

There has always been a verbal confrontation about the evolution of Cloud Computing and the most critical point in that is Grid Computing. A few people call Cloud Computing and Grid Computing the similar phenomena while others call Cloud Computing an expansion of Grid computing. To find the reality we have to think about the Grid computing [40] Grid Computing is a complex phenomenon which has advanced through earlier improvements in parallel, disseminated and HPC (High Performance Computing) [44]. A standout amongst the most referred definitions of Grid computing at the beginning was from [20].

***"A computational grid is a hardware and software infrastructure that provides dependable, consistent, pervasive, and inexpensive access to high-end computational capabilities."*[38]**

The portrayal of Cloud Computing prior and of Grid computing here demonstrates that Cloud Computing and grid computing have numerous similarities. This prompts discourse Cloud Computing impact on organizations about the distinctions in these two advancements. The Table 2 underneath demonstrates the technical contrasts among Cloud Computing and Grid computing introduced by Katarina Stanoevska-Slabeva and Thomas Wozniak [40].

Table.2. Grid and Cloud Computing Technically Compared [40]

	Grid Computing	**Cloud Computing**
Means of utilization	Allocation of multiple servers onto a single task or job.	Virtualization of servers, one server to compute several tasks concurrently.
Typical usage	Typically used for job execution, i.e. the execution of a program for a limited time.	More frequently used to support long-running services.
Level of abstraction	Expose high level of detail.	Provide higher Level abstractions.

As specified above, there is a verbal confrontation in the innovation world that Cloud Computing has evolved from Grid Computing and that Grid Computing is the establishment for Cloud Computing. [22] For instance portray the relationship between the two as follows:

"We argue that Cloud Computing not only overlaps with Grid Computing, it is indeed evolved out of Grid Computing and relies on Grid Computing as its backbone and infrastructure support. The evolution has been a result of a shift in focus from an infrastructure that delivers storage and compute resources (such is the case in Grids) to one that is economy based aiming to deliver more abstract resources and services (such is the case in Clouds)."[22].

In this way we can abridge that Grid Computing is the beginning stage and basis for Cloud Computing. Cloud computing basically represents the expanding pattern towards the external

deployment of IT resources, for instance computational power, storage or business applications, and acquiring them as services [40].

5. SECURITY THREATS IN CLOUD MIGRATION

Threats and risk conditions should be broke down for advanced security and is instrumental while selecting and deploying appropriate security controls ideally. High risk factors or threats to the cloud computing environment incorporate Insecure Application Programming Interfaces, Malicious Insiders, Shared Technology Vulnerabilities, Data Loss/Leakage and Account Service and Traffic Hijacking. [24]

5.1. *Insecure Interfaces and APIs*

A cloud service provider uncovered a huge arrangement of programming interfaces or APIs that clients utilize, manipulate and connect with cloud services. These APIs have immense powers and benefits in the cloud framework including organization, scheduling and observing. The security and accessibility of cloud services is specifically corresponding and reliant on the respectability and security of these APIs. Different components and controls ought to be deliberate and designed like authentication, get admission to manipulate, encryption and activity monitoring for protecting towards unintended and malicious tries to breach the coverage or compromise the information or infrastructure. Absence of these controls expands the hazard and multifaceted nature of the new layered API and the cloud foundation as entirety. Overlooking these controls for APIs may open organizations to an assortment of security issues identified with secrecy, trustworthiness, accessibility and responsibility. This results in primary disruptions along with however not restricted to: anonymous access, reusable tokens, passwords, clean-textual content authentication, transmission of content, inflexible access controls or wrong authorizations and unknown service or API dependencies.

5.2. Malicious Insiders

Malicious insider threat is well-known to majority of agencies within the industry. This threat is enhanced for the customers who uses cloud services and for the cloud service providers due to many elements like single control area, lack of transparency of processes and load balancing of clustered customers. For instance, a provider may not uncover how it plays out the resource scheduling, virtual resources provisioning, and evaluation process and reporting on coverage compliance. These sorts of circumstances plainly makes an alluring open door for an assault which might be created or activated from different dangers including specialist programmer, organized crime, corporate undercover work or even state supported interruption. The level of access granted could empower such a foe to collect secret information or gain complete control over the cloud services.

5.3. Shared Technology Issues

Cloud service carriers and companies supply their offerings in a scalable manner through sharing infrastructure, platform or software. This mutual innovation threat is most regular in IaaS as the fundamental segments that make up this framework which incorporates physical equipment were not intended for strong isolation and does not bolster properties for a multi-tenure architecture. To handle this threat, typically a virtualization hypervisor intercedes or controls access between the guest operating systems and the physical infrastructure resources. There are situations where even hypervisors have shown imperfections that have empowered guest operating systems to gain inappropriate levels of control or impact on the underlying hidden physical infrastructure platform. Attacks may focus on the shared technology within the Cloud environment with prime concentration on the most proficient method to affect the operations of other cloud customers, and how to gain unauthorized access to information of others. A safeguard top to bottom defense intensive strategy is usually recommended which ought to consist of compute, storage, and network security enforcement and tracking. Strong compartmentalization ought to be utilized to guarantee that individual customer does not affect the operations of other tenants strolling on the same cloud provider. Customers must no longer have access to another tenant's actual or residual statistics, data, network traffic and so forth.

5.4. Data Loss or Leakage

Deletion of the information or bargaining the honesty and accessibility of the information records without proper reinforcement framework set up is one of the numerous approaches to trade off organizations data in cloud environment. Situations like Unlinking a record from a bigger context may render it unrecoverable, Loss of an encoding key may result in effective obliteration of the information or the service itself. For this very reason, unauthorized parties must be averted from accessing delicate information. The risk and the probability of the information being traded off will increase inside the cloud infrastructure because of the high quantity of interactions and information exchanges amongst cloud and the customers, which can be demonstrated more perilous as a result of the compositional or operational qualities of the cloud environment. Data loss or leakage can devastatingly affect a business. Loss could essentially affect the employee, partner past the damage to one's brand and notoriety. Loss of core intellectual assets could have aggressive and financial implications. There may be consistence infringement and lawful consequences depending on the information that is lost or spilled.

5.5. Account or Service Hijacking

Attack strategies such as phishing, extortion, and exploitation of software vulnerabilities are utilized to figure Account or Service Hijacking in cloud framework setup too. Certifications and passwords are regularly reused which amplifies the impact of such attacks in the cloud. If an attacker gains access to the certifications, they can eavesdrop on the activities and the transactions in the cloud framework, control information and divert customers to ill-conceived locales. This service and infrastructure instances may turn into another base for the attacker and malicious activities which could leverage subsequent attacks as-well or be part of the bot-network.

6. SECURITY ISSUES IN DATA MIGRATION ACROSS CLOUDS

At the point when an organization relocates to the cloud, there could be potential outcomes of offering the information and data to another supplier of cloud services. This is usually visible in today's Global Hybrid Clouds. Security could be a basic part

which can be effortlessly dismissed and afterward abused by the digital lawbreakers compromising Confidentiality, Integrity and Availability of organization's information and services. Cloud service providers can provide a degree of protection in public clouds since they support multi-tenant architecture. However, an application can be tormented by the vulnerabilities or defects of your neighbor's code if resource scheduling is not emphatically compartmented and isolated. Tending to basic framework of the cloud and data center security is essential to control and relieve the service intrusions or vulnerabilities. Some of the big issues for Cloud services are around access control, authentication, user management and provisioning. Almost all Cloud providers utilize virtualization to offer economies of scale and optimal distributed framework, Virtualization has its own set of security issues. Cloud environments are shared and records are in a similar domain alongside statistics from other clients, Breaches can undoubtedly occur from one database to another. Cloud is also prone to a lot more Denial of Service attacks than any private physical data centers as they are accessible over the public network. If authentication and authorization parameters are applied poorly then data stored on the cloud can be accessed or hacked by exploiting the vulnerability.

7. CLOUD SERVICE PROVIDERS

There are numerous merchants for cloud hosting services and infrastructure. Below is the rundown of real players in the market with respect to the various cloud deployment models and service infrastructure. Rundown of top Cloud Providers [37]. List of top Cloud Providers:

- Amazon Web Services (AWS)
- Windows Azure
- Google Compute Engine
- IBM
- Rackspace hosting
- Hewlett-Packard (HP)
- Dimension Data
- QT Cloud Services
- Tsuru
- SalesForce
- WorkXpress
- Aruba Cloud

Table.3. Major Cloud Computing Vendors [37]

Vendor	IaaS	PaaS	SaaS	Storage
Amazon	EC2 (Elastic Cloud Compute)	Amazon Web Services*	Amazon Web Services*	S3 (Simple Storage Service)
Google	n/a	Google App Engine (Python, Java, Go)	Google Aps	Google Cloud Storage
HP	Enterprise Services Cloud – Compute	Cloud Application Delivery	HP Software as a Service	Enterprise Services Cloud – Compute
IBM	SmartCloud Enterprise	SmartCloud Application Services	SaaS products	SmartCloud Enterprise – object storage
Microsoft	Microsoft Private Cloud	Windows Azure (includes .NET, Node.js, Java, PHP)	MS Office 365	Microsoft Private Cloud
JoyentCloud	SmartMachines	Node.js	n/a	n/a
Rackspace	Cloud Servers	Cloud Sites	Email & Apps	Cloud Files
Salesforce.com	n/a	Force.com	Salesforce.com	n/a
VMware**	VMware vSphere, vCloud	VMware vFabric (Java Spring), vCloud API	n/a	n/a

8. SECURITY AND RELIABILITY FACTORS

There are many organizations providing cloud services and solutions within the industry, selecting an adept service relying upon the organizations necessity can be troublesome and tedious. While selecting the right service provider one must not sideline the security and unwavering quality element of the cloud services and dependably post for any escape clauses that could be abused if not gone to. The following are few tips and contemplations one must be watchful while choosing the cloud service provider [29] [15].

8.1 ENCRYPTION

Encryption is the most ideal way which can help and ensure the security of the organization's data. Ensure that an encryption facility is offered and bolstered by the service provider all through and after the migration process. Local encryption and decryption of the files in addition to storage and backup is always encouraged. Asking following intelligent inquiries would help in taking successful selection:

- How might we be harmed if the system or function had been manipulated by an outcast?
- How might we be harmed if the record or information has been modified unexpectedly?

8.2 CLIENT AGREEMENT

Always read the consumer agreement of the service you're planning to enroll in to discover how your cloud provider storage functions. This ought to be in-accordance with your organization's approaches and geological/nation's authoritative laws without unexpectedly encroaching the lawful limits.

- How could we be harmed if the method or process failed to offer expected outcomes?
- How would we be hurt if the resources or information were inaccessible for a timeframe?

8.3 STANDARD ACCESS MANAGEMENT

Identity and access control standards should be industry acknowledged and capable to incorporate with organization's internal access management and single-sign on architecture (SSO). Asking legitimate inquiries would help in taking successful and effective decision:

- How would we be harmed if the resources or data turned out to be extensively public and broadly dispersed?
- How would we be harmed if a worker of the cloud service providing organization got to the advantage and accessed the asset?

8.4 PHYSICAL SAFETY OF DATACENTER

Physical safety and geo-presence must be considered and insurance against cataclysmic events, also debacle recuperation arranging. Service provider's internal security policies must be comprehended to plan viable security model. Taking after consistent inquiries would help in taking a viable and powerful decision:

- How would we be hurt if the data were inaccessible for a timeframe?

8.5 SECURITY STANDARDS/CERTIFICATION

Security affirmation activities, certificates and standards reflect that service provider is serious with information security. Besides confirmations and these certifications, cloud providers must issue a commitment or authorization to conduct external third-party audits. Some of the applicable confirmations and standards are as follows [15]:

- AICPA 2014 Trust Services Criteria
- Canada PIPEDA (Personal Information Protection Electronic Documents Act)
- COBIT 5.0
- CSA Enterprise Architecture
- ENISA (European Network Information and Security Agency)
- Information Assurance Framework
- HIPAA/HITECH act and the Omnibus Rule
- ISO/IEC 27001:2013
- NIST SP800-53 Rev 3
- PCI DSS v3

8.6 AUTO-SCALING

Auto-scaling approach and service ought to be assessed as it specifically influences the execution when the request is in pinnacle. Auto-Scaling allows service to deliver better overall performance in response to heavier workloads and scales down whilst no longer required. Figure 11 shows the example of user authentication with various cloud- based services and client components.

Figure.11. User Authentication Example [10]

9. CYBERCRIMES

9.1 CATEGORIES OF CYBER ATTACKS

Cybercrimes in cloud framework like all computer related attacks can be classified into two primary classes depending on the nature of attack: [35]

Technology-as-Target: Criminal offences focused on the computers and other data advancements and information technologies, along with those involving the unauthorized utilization of computers or insidiousness in connection to information.

Technology-as-Instrument: Criminal offences where the Internet, data advancements and information technologies are instrumental in the commission of a wrongdoing, including those extortion, fraud, identity theft, licensed innovation encroachments, illegal tax avoidance, tranquilize trafficking, human trafficking, sorted out wrongdoing exercises, tyke sexual misuse or digital tormenting.

Table.4. Categories of Cyber Attacks

Technology-as-Target	Technology-as-Instrument
Criminal botnet operations.	Money Laundering.
Malware Threats.	Identity Theft.
Distributed Denial of Service.	Cloud resources in Bot Network.
Hacking for criminal purposes.	Intellectual Data Infringements.

9.2 CLOUD SECURITY ATTACKS

MALWARE INJECTION ATTACK:

The applications and appliances using the cloud infrastructure to deliver services can be an email system, payroll system, web servers, etc. According to a report by Symantec, the number of web attacks spurred by 36% in 2011 [41] These attacks included information leakage, cross site scripting, injection flaws, improper error handling, broken authentication, improper data validation and malicious file execution.[41] In malware injection attack, hackers exploit vulnerabilities of a web application and embed malicious codes that goes undetected and that changes the course of its normal execution over the time. Cloud systems are susceptible to malware injection attacks. Hackers craft a malicious code, application, and virtual machine and inject them into target cloud infrastructure. Once the injection is completed, the malicious module is executed in stealth mode as a valid instance. Then, the hacker gains access to the cloud infrastructure and can perform various malicious activities such as eavesdropping, data manipulation, and data theft [16]. Hackers exploit the vulnerabilities of web servers and inject a malicious code in order to bypass login and gain unauthorized access to backend databases. If successful, hackers can manipulate the contents of the databases, retrieve confidential data, and take complete control of the web servers.

CROSS-SITE SCRIPTING (XSS):

Cross-site scripting (XSS) attacks are considered one of the dangerous attack types. It contributes 27% to the total web attacks in 2012 for cloud infrastructure web applications and databases [19]. In XSS, hackers inject malicious scripts, such as JavaScript, VBScript and Flash into a vulnerable dynamic web page to execute the scripts on victim's web browser which later can be compromised and could conduct illegal activities by tricking the victim into clicking a malicious link.

WRAPPING ATTACK:

When a customer demands services to a web server through an internet browser, the service is cooperated utilizing Simple Object Access Protocol (SOAP) messages which are transmitted through HTTP with an Extensive Markup Language (XML) layout (format). Wrapping attacks utilize XML signature wrapping to misuse a shortcoming when web servers approves marked solicitations [5]. The attack is done amid the interpretation of SOAP messages between a true blue client and the web server by copying the client's records and password in the login period, the hacker installs a false component (the wrapper) into the message structure and moves the original message body under the wrapper, replaces the content of the message with malevolent code, then afterward sends the message to the server. Since the original body is as yet substantial, the server will be deceived into approving the

message that has actually been altered. As a result, the hacker is able to gain unauthorized access to secured resources and process the proposed operations. Since cloud clients typically request services from cloud computing service providers through a web browser, wrapping attacks can cause same magnitude or more terrible harm to the cloud bases frameworks and services also.

10. SECURITY CONSIDERATIONS FOR CLOUD MIGRATION

Generally the security issues which emerge in Cloud Computing are the consequences of client's lack of control on the physical framework. organizations mostly don't know where their records are physically stored and which security systems are set up to protect data i.e. regardless of whether the information is encoded or not and if yes, which encryption strategy is applied likewise if the connection utilized for the travelling of data in the cloud is encrypted and how the encryption keys are overseen [45] Understanding the relationships and dependencies among Cloud Computing models is important for understanding the security risks of it. For all the cloud services IaaS is the establishment and PaaS is expand on it, while SaaS is expand on PaaS and IaaS as portrayed in the cloud reference model diagram Figure 12[12].

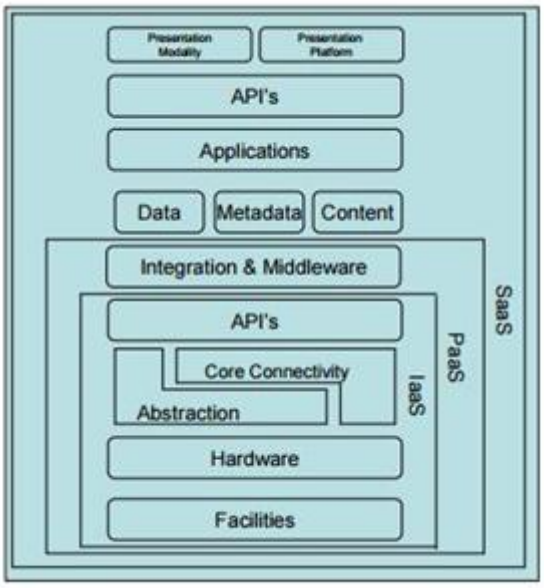

Figure.12. Cloud Reference Model [12]

Security controls in Cloud Computing are not quite the same as security controls in IT environment. Nonetheless, as Cloud Computing deploys distinctive service models, operation models and technologies, so it presents distinctive risks to an organization. The organizations security is actualized on at least one layer extending from the physical security, to the network security, to the system security, and the application security. The security obligations of provider and customer are subject to cloud models. For instance Amazon's AWS EC2, IaaS offering, has vendors obligation regarding physical, environmental and virtualization security. On the other hand customer is responsible for security at IT framework level i.e. operating system, applications and data. [13] We can outline this issue with the assistance of a Figure 13, which indicates how security structure responsibilities for distinct models vary [13]

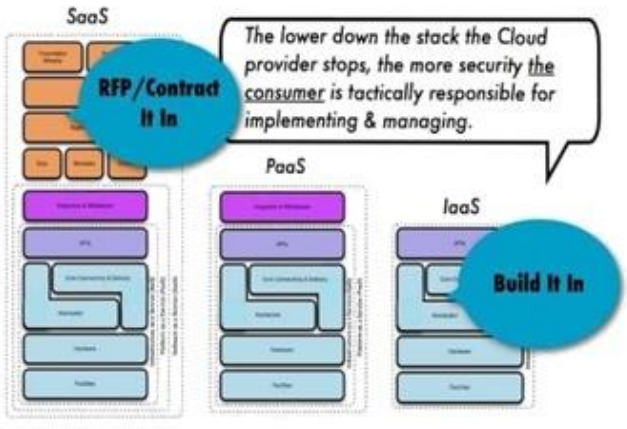

Figure.13. How Security Gets Integrated [13]

There should be certain issues and planning beforehand for the cloud migration which can give us better comprehension of Risks and vulnerabilities to mitigate risks in pre-migration phase [31].

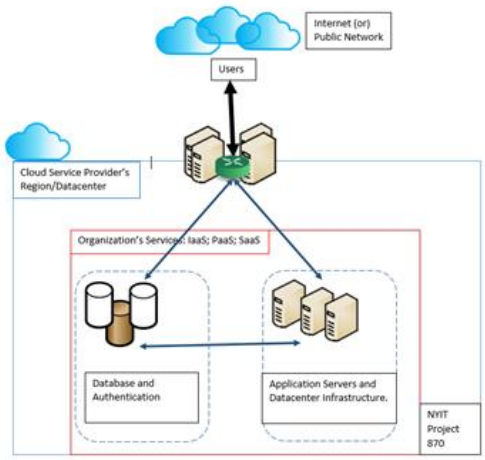

Figure.14. Cloud Network of New York Institute of Technology

Security Consideration 1:

Most of the cloud technology and infrastructure depends and rely on Open source technology like OpenStack which might have their own set of vulnerabilities. This means the basic building block vulnerabilities can be exploited.

Security Consideration 2:

Public models of the Cloud computing are of multi-tenant nature where the resources are shared amongst multiple users/clients. These shared resources may contain the proprietary knowledge and information which may be compromised and shared with the other organizations.

Security Consideration 3:

The cloud based applications needs to be updated regularly and it should be ensured that their security aspect is always prioritized.

Security Consideration 4:

Many countries has the legal obligation and security requirement that the personal and confidential data should reside within the geographical borders to avoid the infraction and charges.

Security Consideration 5:
Data Leakage and Data Loss are major threats to cloud computing. There should be proper steps and policies taken into consideration to mitigate them.

Security Consideration 6:
If not compartmented or isolated correctly, entire environment could be exposed to the malicious attacks by the hackers if even a single component is compromised. Components which may be affected could be hypervisor, Virtual machines, CPU, SAN storage, database, etc.

Security Consideration 7:
The data is available and transferred via public network and this traffic traverses through the public internet. If this data does not use secured channel like https protocols and authenticated as per industry standards then it could be easily compromised.

Security Consideration 8:
Insecure API: As we discussed this earlier in our paper, any malicious activity will expose all the applications to the security threats.

Security Consideration 9:
DOS (Denial of Service) attack is usually very expensive for the organization which depends on services. Security of the domain and cloud services should be of prime importance.

Security Consideration 10:
With strong encryption in place, data stored or hosted on the cloud can be is vulnerable to be hacked. Prime importance needs to be given to authentication and authorization parameters to enable only a set of users to access the data.

11. RISK FACTORS OF CLOUD MIGRATION

Effective analysis of the risks and factors causing risks can prevent from the disaster and plays a vital role in securing organization's data in the cloud by taking planned pro-active measures (or) by selecting appropriate cloud services and solutions to ensure the protection of the organization's information and assets. These risk factors are usually the link to actual threats and mitigating actions [26].

Multitenancy and isolation failure:
The cloud services use multi-tenant environment, where different entities share a pool of resources including storage, hardware and network components. All resources allocated to a particular tenant should be isolated and protected to avoid disclosure of information to other tenants.

Absence of DRP and backup:
Without proper DRP or backup procedures, it is a high risk for any organization. Such basic preventive measures should be aligned with the lieu with organization's requirement.

Lack of visibility of technical security:
Intrusion detection systems (IDS), intrusion prevention systems (IPS) and security incident and event management (SIEM) frameworks must be executed and effectively observed. This ensures that protection policy and governance are being complied to.

Physical security:
In an IaaS model, physical computer assets are shared with different entities in the cloud environment. If the physical access is granted, then there could be potential access theft and identity theft.

Off shoring infrastructure:
The data or the information within the cloud need to combine back to different clouds or internal datacenters through the border gateways which could be insecure and turn out to be uncovering both the cloud and internal framework and setup.

Virtual machine (VM) security:
An inactive VM could be easily ignored and critical security patches might be left unapplied. This outdated VM could progress toward becoming traded off when enacted.

Application mapping:
Applications not configured or designed effectively with reference to the correct model of the cloud computing could bring about extra undesirable elements and multiple vulnerabilities could be introduced.

Identity and access management (IAM):
This sort of solution may additionally bring about a database and rundown of access controls. If not secured and managed appropriately, one client could acquire access to another client's data.

Release management process:
Cloud service providers introduce security patches for their services and applications which are managed without the endorsement of the customers. There could be unexpected side effects and downtime.

Browser vulnerabilities:
Applications and services offered by SaaS providers are accessible to customers via secure communication through a web browser which are a common target for malware and attacks. It is quite possible that the browser becomes infected and the session could be compromised.

Collateral damage:
If one user or tenant of a public cloud is compromised and attacked then there could be an impact to the other tenants of the same Cloud service provider, even if they are not the intended target like in Distributed Denial of Service.

12. LEGAL ISSUES IN CLOUD MIGRATION

Cloud Computing created complex relationship among the data and organization which includes the presence of cloud service provider. In this worldwide circumstance it is a challenge understanding how laws apply to a wide assortment of combinational scenarios. Examining of Cloud Computing and related lawful issues requires consideration of the functional, jurisdictional, and legally binding measurements of an agreement/law. The following are the most widely recognized and well-suited cases of the legitimate issues that may arise while migrating the data on the cloud [15]:

Cross Border Transfers:
There are many countries which prohibit or restrict the transfer of information outside the geographic borders and bounds.

Usually the data transaction is allowed if the other country implements adequate protection of personal information and privacy rights. It is important for a cloud user to know where the personal data of its employees, clients, and others will be located to analyze and take prompt measures where restrictions and foreign data protection laws may impose and take effect.

U.S. Federal Laws:
Multiple federal laws such as GLBA, HIPAA, Children's Online Privacy Protection Act COPPA, which were orders issued by the FTC seeks organizations to adopt and implement privacy and security measures while processing or migrating the data and ensure the precautions during the contracts with other service provider.

U.S. State Laws:
In addition, there are many other local state laws superseding the obligation on organizations to provide effective and adequate security of personal data.

International Regulations:
OECD model or the APEC model are accepted and enforces by multiple countries in-favor of data protection. These laws dictate the hierarchy between the controller of the data and service provider is compatible and the service provider is the primary responsible unit for the collection and processing of personal data. The data controller is required to ensure the adequate technical and organizational security measures to safeguard the data.

Standards:
Industry standards like PCI DSS or ISO 27001 also plays a vital role and imposes effect which is similar to federal and state laws. Organizations dealing with PCI DSS or ISO 27001 must both comply with the respective standards and also make sure the legacy is passed and implemented even when passed to the subcontractors.

Contract Obligation:
Organizations may have their own contractual obligation to protect the personal information of their clients, contacts or employees. This obligation may be the core requirement of the organization and vital for its business operations. This may be understood from the privacy statement of the company in official disclosure section. This enforcement of the security should be continued task and the ability to meet the commitments and SLA of the contract should be stable. If the privacy notice allows individual data subjects to have access to their personal data and restrict to other users, then the same should be implemented by the cloud service provider.

Search and E-Discovery:
A client or organization may not be successful in applying e-discovery tools that it implements internally due to lack of administrative rights on hosted cloud infrastructure.

Possession, Custody, and Control:
Most of the jurisdictions partially obligate to produce the information limited to the documents and data while in the possession, custody or control in-order to reach to a rightful verdict. By hosting relevant data does not always mean that the service providers is liable and have to produce information as it may have a legal right to access or obtain the data, because not all hosted data may be in the control of a client/service provider.

Dynamic and Shared Storage:
The admin or the people with access are limited and aware of the importance and requirement of preserving the data. Preserving data in cloud may appropriate if the organization has extra space for hosting multiple back-ups and data blocks. After a client determines that such data is relevant and needs to be preserved, the client may need to work with the provider to determine a reasonable way to preserve such data.

Scope of Preservation:
Not all the data hosted in the cloud can be preserved or backed-up unless the client have the ability to preserve relevant information or data depending on the litigation or investigation.

Forensics:
For security reasons service providers refrain from allowing access to their hardware resources in multi-tenancy environment. In this scenario it is possible for a client to gain access of other client's data. In this case, the forensics process may be extremely complex. Generally the Virtual environment is implemented in a structured data hierarchy which doesn't lend to forensic analysis by default.

Response to Search Warrant:
The cloud service provider is likely to receive request to provide information via warrant or court order in which access to the client data is requested. This may be against the organization's policies and agreed SLA with the service provider. In this case to notify the service providing company should acknowledge the facts to the client which could be time consuming process.

Access and Bandwidth:
Access feature and bandwidth restrictions may limit the ability of the system to collect huge amount and volumes of data in fewer time frames in the case of forensic requirement.

13. ATTACK PATTERNS AND CLOUD SECURITY BREACHES

Cloud security is still major and constant concern for all the cloud service users/tenants because of multi-tenant architecture and shared infrastructure and there have been multiple instances where the cloud security was compromised causing serious consequences. Cloud customers need to clearly define and communicate any security related incidents to the cloud service providers to minimize these kinds of breaches. Below are few examples of the infamous security breaches of past three years [34]

13.1 WRAPPING ATTACK IN AMAZON EC2

The vulnerability in Amazon's store allowed the team to hijack an AWS session and access to all customer data. The data includes authentication data, tokens, and even plain text passwords. Amazon's EC2 was found to be defenseless against wrapping attacks in 2008. The examination indicated EC2 had a shortcoming in the SOAP message security approval component. A signed SOAP request of a legitimate user can be captured and modified. Subsequently, hackers could take unprivileged actions on victim's accounts in clouds. Utilizing XML signature wrapping approach, researchers also exhibited an

account hijacking attack that exploited defenselessness in the Amazon AWS [33]. By adjusting authorized digitally signed SOAP messages the assailant could acquire unauthorized access to a client's account, delete and create new images on the client's EC2 instance, and perform other regulatory undertakings.

13.2 SQL INJECTION ATTACK BY ASPROX

The Asprox botnet utilized thousand of bots that were equipped with an SQL injection kit to hearth an SQL injection attack [30]. The bots initially sent encoded SQL queries containing the endeavor payload to Google for seeking web servers that run ASP.net. At that point, the bots began an SQL injection attack against the web sites returned from those queries. Approximately 6 million URLs belonging to 153,000 distinctive web sites were causalities of SQL injection attack by the Asprox botnet. A scenario that demonstrates SQL injection attacking cloud systems was illustrated in [36]. An online retail SaaS application that allows multiple retailers to host their products and sell them through SaaS was used. The procedure of exploiting vulnerability and accessing to backend database was explained in details

13.3 US IRS TAX BREACH-2015

Hackers attacked the US IRS website and gained access to more than 100,000 accounts of citizens in May 2012. This attack was successful because of the vulnerability in an API service was exploited. The API was misconfigured and the "Get Transcript" service was exploited and hacked to gain the confidential and sensitive information of more than 100,000 citizens of US. Multiple authentications, encryption, monitoring and various additional security techniques could have been instrumental in preventing the attack.

13.4 SONY PICTURES DATA BREACH-2015

Hacking group named "Guardians of Peace" accessed the organizations data including employee information, financials, email addresses and further took extreme steps and destroyed thousands of Virtual Machines and hundreds of its servers following the attack. This was done by successful implantation of Malware which was the main reason for the wreaking havoc in Sony's network. Defense In Depth (DID) along with diligent network monitoring services could have been a life saver. Intelligent IDS and IPS along with strong network security precautions is vital for prevention of malware outbreak.

13.5 APPLE'S iCLOUD DATA BREACH

Hackers were successful in attacking and hacking celebrity cloud accounts and attaining access to the private information and photographs. This was successful due to lack of multiple authentications from Apple iCloud services. Social Engineering and dictionary attacks were huge contribution and played vital role in making this attack successful. Multi factor authentication and account block-out (or) threshold policy could have been vital in prevention of suck attack.

13.6 TARGET SECURITY BREACH-2013

70 million customer's credit card information during the holiday season of 2013 was compromised as the result of security breach at the famous retailing store 'Target'. This attack was due to stolen credentials via simple phishing emails. Further to agony it was later found that the IDS and IPS on site warned of the attack on multiple occasions, but those warnings were overlooked. This event also calls for the alarm on the PCI Data Security Standards since the compliance failed and resulted in infringement of the policies since the compromised data consisted of valuable information like customers' names, card numbers, expiration dates and card verification information.

14. CLOUD SECURITY GUIDELINES

Below are few guidelines and suggestions to mitigate the security vulnerabilities and threats in cloud computing and cloud migration process. This guideline plays vital role in preparation of successful cloud migration and secured cloud computing platform.

- Governance and guiding processes between customers and service providers should be termed as necessary in the design phase and in development of service. Service assessment and risk management protocols should be agreed upon and drafted in SLA service level agreement.
- Cloud service customers and providers should agree and develop robust information security governance, regardless of the services offered and/or deployment models. Information security governance must be mutual collaboration and coordination between customers and providers to reach predefined goals supporting business operations and information security back-bone.
- Governance should include periodic review and continual improvement cycle.
- Security departments and teams should play major role during establishment of Service Level Agreements.
- Service provider's infrastructure documentation must be studied and understood as it plays vital role in risk management.
- Due to multi-tenancy aspects of cloud structure, computing, alternative assessment options which are specific to cloud architecture must be aligned with risk management plan.
- Risk assessment approach and process should be consistent with impact analysis.
- Asset inventories supporting cloud services should be maintained with consistent asset classification between user and service provider.
- Risk metrics must be defined and mutually accepted and agreed by both the parties: service providers and client organization.
- Cloud infrastructure aware auditors familiar with the assurance challenges of virtualization and cloud must be preferred.
- Cloud Service Provider's SSAE, SOC2 or ISAE Type 2 report must be requested and worked on it to mitigate the stated risks.
- A right to audit clause should be determined from service provider, as this enables customers with transparency in the ever-evolving cloud environments.
- Service providers should be core-responsible party for the review, update and security of information security documents, vulnerability analysis, internal processes and GRC processes.
- Both service provider and client organization must be in agreement towards using a common certification assurance framework for IT governance and security controls.
- The Information Management lifecycle (Figure 15) must be implemented which includes six phases from creation to

destruction. Once data is created it can move freely between the phases without restriction.

Figure.15. Information Management Lifecycle

a. **Create:** Creation of new digital content, or the alteration/updating/modifying of existing content.
b. **Store**: Storing is when there is commitment to the digital data of storage repository.
c. **Use**: Data is viewed, processed and contributes to other process or activity.
d. **Share:** Information accessible to users, to customers, processes and users.
e. **Archive:** Data leaves active use and enters long-term storage.
f. **Destroy:** Data is permanently destroyed using secures shredding tools.

- Cloud service provider's data search capabilities and limitations must be known to understand the dataset of data discovery.
- Data retention rate and data destruction schedule must be monitored and single point of ownership of this task must be of the data owner. Cloud service provider must be vigilant and responsible to destroy the data upon request in all locations including slack in data structures and on physical media.
- Regular Backup validation and recovery practice in Disaster Recovery site must be done to ensure the functional and validity of the backups.
- For IaaS in particular, it is very important to understand what practices are implemented to delete or de-provision the VMs, related images, disks and storage devices.
- For PaaS, it is important to be able to migrate to different service provider when needed; so many factors should be noted like: services, monitoring, logging and auditing. Open platform components with a standard syntax and open APIs must be encouraged. It should also be planned and known what tools are available for secure data transfer, backup, and restore.
- For SaaS, metadata must be preserved and portable for migration. Regular data extractions and backups must be performed without the involvement of SaaS provider. Also, provision for the new vendor to test and evaluate the applications before migration must be confirmed.

15. CLOUD SERVICE CONSUMER'S ROLE

Cloud service clients/customers need to play a significant role and strongly co-ordinate with the cloud service providers to enforce complete security and mitigate any underlying vulnerabilities. This approach and practice would prove to be vital in protection against the threats and attacks during and after the data migration over the cloud or between multiple cloud services. Below are few guidelines and roles that cloud service consumers must embrace and practice for secured cloud migration and cloud computing infrastructure.

- Cloud customers must be fully aware of documentation regarding the cloud service provider's internal, external security controls and their adherence/compliance with the industry approved standards.
- Cloud customers should be aware of their service provider's security patch management policies and procedures. They should also know how these policies may impact their environments.
- Cloud customers should inspect the physical dependencies in service provider's infrastructure and cloud provider's disaster recovery and continuity plans.
- User credentials, administrative access and control of virtualized operating systems must be managed confidentially. It should be complimented with logging systems and strong authentication which is integrated with enterprise identity management.
- Customers should avoid designing and implementing proprietary solutions and connectors unique to cloud providers. This will increase the complexity and cause major barrier during cloud migration process.
- Customer Recovery Time Objectives (RTOs) should be fully read, understood and agreed by both service provider and consumer.
- Cloud customer should always be prepared for expected and unexpected termination of the contract.
- Customer should adapt industry standards for their application development over the cloud infrastructure to ensure its portability. Software Development Life Cycle (SDLC) illustrates in Figure 16 best example for software application development practices which affects the aspects of application architecture, design, development, quality assurance, deployment and decommissioning. It drives the process of application development into 5 logical and sequential stages. [1]

Figure.16. Software Development Life Cycle

- Cloud customers must ensure that the key management process is segregated from the cloud provider by creating a chain of separation. This plays vital role in conflict resolving between the cloud provider and customer during legal conflicts.

- Deep understanding of Cloud service provider's infrastructure is required including: security architecture, configuration and controls for later use of internal audits and proof of concept for actual migration process.

- For IaaS, Consumer must be fully aware of how virtual machine images can be captured and transported to new cloud providers with different platform and technologies. Also, after the migration, decommissioning of disks and storage devices must be successful.

- For PaaS, Consumer must assess the available tool's security data migration, backup, and restore. Also, prioritize services like monitoring, logging, and auditing to be transferred or migrated to new vendor.

- For SaaS, Consumer should assure the consistency and effectiveness of data during the migration between the old and new cloud service providers. Also plan to redevelop the custom tools implemented according to the new cloud service platform.

16. CLOUD AND BIG DATA SECURITY

Big data creates an open platform and huge opportunity for various vendors and enterprises across different industries to collaborate by tapping and migration between various cloud platforms into new volumes and varieties of data delivering breakthrough innovations. This is a huge platform with humongous integrations and massive level of data and sensitive information. This data, Big-Data without appropriate security and encryption can proved to be devastation. Below are few areas of Big Data which needs to be addressed to establish comprehensive security. Figure 17 shows the areas of Big Data that are described below. [14][43]

Figure.17. Areas of Big Data

16.1 DATA SOURCES

Exploiting big data and various forms of data, including both structured data of application's databases and unstructured data of multiple file types may sound complex, but it is practical and a doable task. Organizations usually leverage data from various resources like: information systems, platforms like customer management, video files, social media feeds, and other various sources with more diversity demanding to accommodate. These big data sources can include personally identifiable information, payment card data, intellectual property, health records, and much more. Consequently, the data sources being compiled needs to be secured in order to address security policies and compliance mandates. [43]

16.2 BIG DATA FRAMEWORKS

Usually the backend of big data environment is supported and powered by systems like: Hadoop, MongoDB, NoSQL and Teradata. These frameworks deal with massive amount of sensitive data at any given time. This sensitive information may be valuable asset to most of the enterprise organization and it doesn't have to reside on big data nodes, rather they can be in the form of migrating data, system logs, configuration files and error logs. These assets need to be identified and preserved.

Figure.18. Big Data Framework of Vormetric [43]

16.3 ANALYTICS

The final resultant of big data initiative and processing is the valuable output, the analytics and knowledgeable data which helps the organization's business to optimize and innovate further. This output and information is generally presented on smart dashboards and report viewers, they are easy to generate and accessible via on-demand queries. Since big data analytics provides an organization with critical competitive information, it is considered as intelligence that is most sensitive asset to the businesses. If not the analytics are exposed to the wrong hands, impact would be dangerous. Thus, security of the output analytics should be of highest priority.

Factors affecting implementation and migration of Big Data setup in cloud infrastructures:

- In-built Security compliance and secured Cloud infrastructure during and after the migration processes.
- Low upfront cost of infrastructure.
- Elastic nature of the data and computing resource that grows and shrinks with demand.
- Mitigation of internal information governance, compliance and security requirements.
- Scalable processing resources to existing data sources.
- Building solutions faster prompt prototyping by eliminating procurement and setup processes.

II. CONCLUSION

We would like to conclude this paper by stressing on the fact that the cloud computing is the current trend and future of the IT businesses and IT industry in general. This platform needs to be studied well before the migration of the infrastructure, platform or software services into the cloud infrastructure. Security needs in particular must not be sidelined and must be studied in great detail with respect to the crown jewels (Valuable Assets) of an organization and respective measures must be undertaken to protect them and mitigate the vulnerabilities and involved threats. Cloud security and data security share some similarities with traditional datacenter's security concerns and requirements along with some platform specific security requirements for cloud infrastructure and technology. We have outlined the possible vulnerabilities and threats which give any organization/infrastructure architect the opportunity to be pro-active in deploying tailored security models for its organization. In addition, we have listed the basic and general guidelines which may prove vital role in decreasing or mitigation of threat and attacks in cloud infrastructure with different cloud models and different deployments like: PaaS, SaaS, and IaaS. The guidelines may act as governing policies of an organization to protect it from various threats and complex attacks. We have also touched the Big Data technology and its security concerns, we have identified its core components that need to be protected and secures even before deploying any security solutions on top of the platform. With Big Data technology and cloud infrastructure the nature of security approach remains the same as there are many common threats and security concerns as listed above. The data migration phase and post migration security measures may be addressed using the provided security guidelines in contrast with the tailored and customized security requirements of the service or infrastructure of an organization

III. REFERENCES

[1].AmbySoft.(2014).SLDC AmbySoft.com. Retrieved from AmbySoft.com:Available: http://www. ambysoft.com/ essays/ agileLifecycle.html

[2].Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. April 2010. A view of cloud computing. Commun. ACM, pp50-58.

[3].Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M. (2009). Above the Clouds: A Berkeley View of Cloud Computing. Technical Report pp6. University of California at Berkeley

[4].Amrhein, D. & Quint, S. APRIL 2009. Cloud computing for the enterprise: Part 1: Capturing the cloud Available:http://www.ibm.com/developerworks/websphere/techj ournal/0904_amrhein/0904_ amrhein.html. techjournal/ 0904_amrhein/0904_amrhein.html. Last visited: 13.06.12.

[5].Austel, M. M. (2005). XML Signature Element Wrapping Attacks and Countermeasures. workshop on Secure web services, ACM Press, New York, NY, 20–27.

[6].AWS, A. (2016, 01). Amazon Cloud Srv. Retrieved from Amazon: Available:https:/ aws.amazon.com/security /introducti on –to -cloud-security/]

[7].Azharuddin. NOVEMBER 2011. Difference between cloud computing and grid computing.

[8].Berry, M. (2016, 01). ITManagerDaily. Retrieved from ITManagerDaily: Available:http:/ /www.itmanagerdaily. com/cloud- computing-vendors/

[9].Boss, G., Malladi, P., Quan, D., Legregni, L., Hall, H. (2007), p2 Cloud Computing. Available: www.ibm. com/ developerworks/ websphere/zones/hipods/. Retrieved on 20th May, 2010.

[10].C.Chou, D. Authentification example.

[11].Cloud Security Alliance. (2009). Security Guidance for Critical Areas of Focus in Cloud Computing.p14

[12].Cloud Security Alliance. (2009). Security Guidance for Critical Areas of Focus in Cloud Computing.p18

[13].Cloud Security Alliance. (2009). Security Guidance for Critical Areas of Focus in Cloud Computing.p25, 26

[14].Cloud Standards Customer Council, C. (2013). Customer Cloud Architecture. Cloud Standards Customer Council,CSCC.

[15].CSA, C. C. (2009). Security Guidance. December.

[16].Dhore, A. S. (2012). CIDT: Detection of Malicious Code Injection Attacks on Web Application. International Journal of Computer Applications.

[17].DimensionData. (2016, 01). DimensionData. Retrieved from Cloud Modules: Available:http:// www.dimensiondata.com/ Global/Downloadable%20Documents/Cloud%20Security%20% 20Developing%20a%20Secure%20Cloud%20Approach%20Whi te%20Pape r.pdf#search=cloud%20security

[18].Discourse, S. D. Key characteristics of a PaaS offering. Available:http://www.siia.net/blog/index.php/2011/03/ siia-members-only-issue-brief-key-characteristics-of-a-paas-offering/. Last visited 16.06.12.

[19].Fire-Host. (2012, 05). FireHost. Retrieved from FireHost Report: Available:http://www.firehost .com/company/ news room/ web-application-attack-report-second-quarter-2012

[20].Foster I, Kesselman C (1998) Computational Grids. Available:http://citeseerx.ist.psu.edu/viewdoc/summary? doi=10. 1.1.36.4939

[21].Foster I, Kesselman, C, Tuecke S (2001) The Anatomy of the Grid: Enabling Scalable Virtual Organization. International Journal of High Performance Computing Applications 15(3):200-222 p2

[22].Foster I, Zhao Y, Raicu I, Lu S (2008) Cloud Computing and Grid Computing360-Degree Compared. In: Grid Computing Environments Workshop (GCE'08). doi:10.1109/ GCE.2008. 4738445 p1

[23].Google. (2016, 01). Google App Engine. Retrieved from App Engine: Available:https://cloud.google.com/appengine/

[24].Hewlett-Packard,C.a.(2016, 01).CSA.Retrieved from CSA: Available:https://cloudsecurityalliance.org/topthreats/csathreats.v 1.0.pdf

[25].Iacono, N. G. (2009). Vulnerable Cloud: SOAP Message Security Validation Revisited. IEEE International Conference on Web Services, Los Angeles.

[26].InfoSecurityEurope. (2014). InfoSecurityEurope. Retrieved from InfoSecurityEurope: Available:http:// www.infosecurity europe.com/__novadocuments/68600?v=635526169057470000

[27].Kourpas E (2006) Grid Computing: Past, Present and Future – An Innovation Perspective. IBM white paper.p13

[28].Lynch, M. (2008) The Cloud Wars: $100+ billion at stake. Merrill Lynch research note, May 2008. Retrieved May 15, 2010 Available:http://web2.sys-con.com/node/604936.

[29].Manciocchi, J. (2013, May 17). powersolution.com. Retrieved from powersolution.com: Available: http://www. powersolution. com/10-tips-to-ensure-data-security-in-the-cloud/

[30].N.Provos, M. A. (2009). Cybercrime 2.0: When the Cloud Turns Dark, Vol. 52. ACM Communications, 42–47. Retrieved from N. Provos, M. A. Rajab, and P. Mavrommatis, "Cybercrime 2.0: When the Cloud Turns Dark," ACM Communications, Vol. 52, No. 4, pp. 42–47, 2009.].

[31].OpenStack. (2016). OpenStack. Retrieved from OpenStack: Available:https://www.openstack.org/

[32].Papazoglou, M. & van den Heuvel, W. nov.-dec. 2011. Blueprinting the cloud. Internet Computing, IEEE, 15(6), 74 –79.

[33].PCworld. (2014, 05). PCworld. Retrieved from PCworld: Available:http://www.pcworld.idg.com.au/article/405419/researc hers_demo_cloud_security_iss ue_amazon_aw s_attack/

[34].Rando, N. (2016). searchcloudcomputing. Retrieved from search cloudcomputing: Available:http:// search cloud computing. techtarget.com/feature/Cloud-security-breaches-still-the-stuff-of-IT-nightmares

[35].RCMP-Canada, R. (2014, 01). RCMP Canada. Retrieved from RCMP Canada: http://www.rcmp-grc.gc.ca/pubs/cc-report-rapport-cc-eng.htm

[36].S.S.Rajan. (2010). Cloud Security Series | November 2010. SQL Injection and SaaS, Cloud Computing Journal,.

[37].SoftwareInsider. (2016, 01). Retrieved from Cloud-Computing: Available:http://cloud-computing. softwareinsider. com/

[38].Stanoevska-Slabeva, K., Wozniak, T. (2009). Grid Basics. In: Stanoevska-Slabeva, K., Wozniak, T., and Ristol, S., Grid and Cloud Computing A Business Perspective on Technology and Applications. Springer Berlin Heidelberg, 2009.p23

[39]. Stanoevska-Slabeva, K., Wozniak, T. (2009). Grid Basics. In: Stanoevska-Slabeva, K.,Wozniak, T., and Ristol, S., Grid and Cloud Computing A Business Perspective on Technology and Applications. Springer Berlin Heidelberg, 2009.p50

[40].Stanoevska-Slabeva, K., Wozniak, T. (2009). Grid Basics. In: Stanoevska-Slabeva, K., Wozniak, T., and Ristol, S., Grid and Cloud Computing A Business Perspective on Technology and Applications. Springer Berlin Heidelberg, 2009.p59, 61

[41].Symantec. (2012). Symantec Internet Security Threat Report. 2011 Trends, Vol. 17, April 2012. Retrieved from Symantec Internet Security Threat Report, 2011 Trends, Vol. 17, April 2012.].

[42].Vertisage. 2010. Saas and cloud computing enablement. Available: http://vertisage.com/ s-saas.html. Last visited: 13.06.12.

[43]. Vormetric Data Security, V. D. (2015). Vormetric Data Security. Retrieved from Vormetric Data Security: Available:http://www.vormetric.com/data-security-solutions/use-cases/big-data-security

[44]. Weishäupl T., Donno F., Schikuta E., Stockinger H., Wanek H. (2005). Business in the Grid: The BIG Project. In: Proceedings of the 2nd International Workshop on Grid Economics and Business Models (GECON2005). Available: http:// hst.home.cern.ch/hst/publications/gecon-2005-BIGproject. pdf. Accessed 5th May, 2010.

[45].Window Security, (2010), Available: http://www. window security .com/articles/Security-CloudTrustworthy-Enough-Your-Business.html. Retrieved on April 11, 2010.