How Secure you are in a Cloud

Kriti Arora

***Abstract* – Cloud Computing is one of the hottest trend setting technology these days. It is a process and method by which organizations big and small can increase their IT infrastructure and computational capabilities without actually doing much investment. The concept of cloud computing can open a new plethora of avenues and opportunities for the small and middle level organizations. But as the popularity of Cloud computing increased, new security concerns and risks are being identified daily related to data stored in cloud. Due to this, many new customers are reluctant to move to cloud or adopt cloud computing in a major way. Security of customer data is a big concern for almost every organization and when your sensitive data resides in a shared space like the cloud customers are all the more apprehensive about the security of their data. This paper deals with major Security risks and concerns related to cloud computing, how they can be handled and what considerations customers opting for cloud computing should keep in mind for handling each security risk.**

***Index Terms* – Cloud computing, security issues in cloud, data security, network security, authentication, authorization, virtualization, denial of service**

I. INTRODUCTION

Cloud computing is the latest and hottest trend for middle and small size organizations today aiming to achieve greater power of IT infrastructure capabilities without incurring huge costs. Gartner defines Cloud Computing as ‘‘a style of computing where massively scalable IT-enabled capabilities are delivered ‘as a service’ to external customers using Internet technologies’’. As per the definition provided by the National Institute for Standards and Technology (NIST), “cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”. Cloud computing transforms the way information technology (IT) is consumed and managed, promising improved cost efficiencies, accelerated innovation, faster time-to-market, and the ability to scale applications on demand. Among the various advantages and benefits offered by Cloud computing most important are fast deployment, pay-for- use, lower costs, scalability, rapid provisioning, rapid elasticity, ubiquitous network access, greater resiliency, hypervisor protection against network attacks, low-cost disaster recovery and data storage solutions, on-demand security controls, real time detection of system tampering and rapid re-constitution of services. While the cloud offers these advantages, it also poses the data stored in the Cloud to a whole new plethora of security hazards and risks. Until some of the risks are better understood and handled, many of the major organizations, new companies are holding back their plans on adopting Cloud computing in a big way. Hence while the customers are excited by the opportunities to reduce the capital costs, and the chance to divest themselves of infrastructure management and focus on core competencies, and above all the agility offered by the on-demand provisioning of computing, they are concerned about the security issues and challenges which need to be addressed before they adopt cloud computing in a major way. This paper deals with the various Security issues and concerns faced by Cloud computing users. Section 2 gives a brief overview of the architecture and benefits of Cloud and the various technologies employed in it. Section 3 gives a detailed account of various Security threats and risks faced by data residing in cloud computing environments. For each Security risk and concern it discusses the type of security attacks, methods and solutions to address that security concern and some generic considerations and guidelines for customers to keep in mind.

II. CLOUD COMPUTING ARCHITECTURE AND MODELS

Cloud Computing provides environments to enable resource sharing in terms of scalable infrastructures, middleware and application development platforms, and value-added business applications. Cloud computing involves deploying groups of remote servers and software networks that allow different kinds of data sources to be uploaded for real time processing to generate computing results without the need to store processed data on the cloud.

A. CLOUD DEPLOYMENT MODELS

Depending on who is providing the cloud services and how they are provided, there are four deployment models of cloud computing: (i) **Private cloud** in which cloud services are provided solely for an organization

ISSN: 2278 – 1323

and are managed by the organization itself or a third party. It is mainly implemented on private networks within an organization's internal datacenter. Since it is accessed and used mainly by employees within the organization and certain designated stakeholders, security is not a major concern. (ii) **Public cloud** in which cloud services are available to anyone interested in availing them. Resources and services are dynamically provisioned on on-demand basis to customers via web applications or web services. It is based on pay-per-use model and shares resources and services among the customers. It is less secure than Private cloud since many different types of users are sharing resources, services, web applications for different purposes simultaneously. (iii) **Hybrid cloud** is a combination of private and public clouds. It is basically a private cloud linked and made available to one or more external public clouds. It provides virtual IT solutions to a number of customers through a mix of private and public clouds but managed and controlled centrally as a single unit. (iv) **Community cloud** shares cloud service among several organizations that form a community with shared concerns. The cloud services in this case may be managed by the organizations themselves or a third party agency may be hired to manage the cloud services from an offsite location. A special case of community cloud is the Government or the G-cloud that provides services to all government agencies.

B. SPI MODEL – SAAS, PAAS and IAAS

Based on the type and range of services provided in a Cloud environment, three delivery models are defined for clouds - SAAS or Software as a Service, PAAS of Platform as a Service and IAAS or Infrastructure as a Service. These delivery models are popularly known as the SPI (Software, Platform and Infrastructure) delivery model are described below.

SAAS or Software as a Service – In this delivery model, software applications are hosted remotely by the cloud service provider on the cloud and made available to customers as a service through the Internet. A single instance of the software application runs on the cloud and is used and shared by multiple cloud users. Rather than purchasing servers, software, licenses, data center space or network equipment, clients instead buy access to software applications as a fully outsourced service. SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support web services and service-oriented architecture (SOA) mature and new developmental approaches become popular. SaaS is also often associated with a pay-as-you-go subscription licensing model. Software as a service applications are accessed using web browsers over the Internet therefore web browser security is vitally important. Information security officers will need to consider various methods of securing SaaS applications. Web Services (WS) security, Extendable Markup Language (XML) encryption, Secure Socket Layer (SSL) and available options which are used in enforcing data protection transmitted over the Internet. [2] [4]

PAAS or Platform as a Service – PAAS provides an integrated software development environment as an encapsulated service for customers. The customer can use the PAAS Cloud provided development environment to develop their applications without having to purchase, deploy, and manage the development platforms. PAAS abstracts everything upto the OS and Middleware so that a developer can tap to build their applications without having any clue about what is going on underneath the service. It offers developers a service that provides a complete software development lifecycle management, from planning to design to building applications to deployment to testing to maintenance. Everything else is abstracted away from the ''view'' of the developers. The use of virtual machines act as a catalyst in the PaaS layer in Cloud computing. Virtual machines must be protected against malicious attacks such as cloud malware. Therefore maintaining the integrity of applications and well enforcing accurate authentication checks during the transfer of data across the entire networking channels becomes important.

IAAS of Infrastructure as a Service – This delivery model has a single tenant cloud layer and provides basic computing and storage services to customers on a pay per use basis. Resources such as Servers, storage systems, networking equipment, data center space etc. are pooled by the cloud provider and made available to customers. This greatly
minimizes the need for huge initial investment in computing hardware such as servers, networking devices and processing power. IaaS and other associated services have enabled startups and other businesses focus on their core competencies without worrying much about the provisioning and management of infrastructure. IaaS completely abstracted the hardware beneath it and allowed users to consume infrastructure as a service without bothering anything about the underlying complexities. The customer does not manage or control the underlying cloud infrastructure but has the control over operating systems, storage, deployed applications, and possibly select networking components.

ISSN: 2278 – 1323

III. SECURITY CONCERNS IN CLOUDS

In traditional application implementations, the sensitive data of each organization resides within the enterprise boundary and is subject to its physical, logical, system and personnel security and access control policies. However, in most of the Cloud models, the enterprise data is stored outside the enterprise boundary, at the Cloud vendor/provider end. Consequently, the Cloud vendor must adopt additional security checks to ensure data security and prevent breaches due to security vulnerabilities in the application or through malicious employees, customers or outsiders. Cloud computing employs many new technologies such as networks, distributed and shared databases, operating systems, scheduling mechanisms, virtualization, transaction management, load balancing, concurrency control, access control and memory management. Hence the security threats and issues of each of these technologies become applicable to Clouds and they are vulnerable to attack though any of these components. Moving customer's critical and sensitive data to such a network accessible shared environment introduces new security threats and concerns. When those network resources are built on systems, platforms and applications shared with others, another set of threat vectors is introduced. The control mechanisms itself can be attacked, breaking down isolation between users, potentially allowing another user to access data or resources.

Some threat vectors are not new to cloud, but have somewhat different dynamics. In classic IT Architecture, PCs inside the organization may be at risk of compromise through a host of attack vectors exploiting local applications such as browses or documents viewers. If less data is stored locally, less is immediately at risk, but now the attacker could compromise credentials to gain access to the user's cloud privileges. When relying on a cloud service to handle data, appropriate care must be made to arrange for appropriate security management practices, such as encryption and appropriate deletion. Similarly, all organizations are vulnerable to an insider attack from a trusted insider, but moving things to the cloud can raise the costs of misplaced trust. A cloud system with a well-thought out identity interface and a clear access control system can restrict access and foster accountability. Thus proper handling of security threats, taking adequate counter measures and employing effective security solutions becomes very important in a cloud environment. Security in the cloud is achieved, in part, through third party controls and assurance much like in traditional outsourcing arrangements. But since there is no common cloud computing security standard, there are additional challenges associated with this. [5]

In the following section, we examine the various security challenges and threats that organizations adopting cloud technology will need to consider, types off attacks that can happen and various risk mitigation measures, security control solutions and strategies that can ensure that these threats are taken care of in a cloud environment. In particular, we examine the following points for each identified security threat:

- Details of security threats and risks against information assets residing in cloud computing environments.
- The types of attackers and their capability of attacking the cloud.
- Counter measures and solutions for handling each security threat
- The relevant considerations or points to ponder for customers for each threat

A. Data Security - Encryption, Insider attacks

THREAT: Data security refers to how secure is your data that is stored inside the Cloud environment. When data is stored in a Network enabled Cloud environment which is shared by many users it is vulnerable to attacks from insiders as well as outsiders. Malicious users among cloud providers or other customers can access and attack the data stored in cloud by accessing critical data that they are not authorized to access. These malicious attackers may be customers, providers, users or some third party hackers trying to break into the customer data. These attackers can employ various attack mechanisms like eavesdropping, data hacking, man in the middle attack and may use cloud hardware, software or infrastructure, social engineering and supply chain mechanism for attacking the cloud data. The threat from external attackers may be perceived to apply more to public Internet facing clouds, however all types of cloud delivery models are affected by internal attackers. Cloud providers with large data stores holding sensitive data such as credit card details, personal information and sensitive government or intellectual property, are at risk to attacks from groups, with significant resources, attempting to retrieve data for unscrupulous financial gains. All cloud models - SaaS, PasS and IaaS face the data security threat as data storage in cloud is an intrinsic service provided by most of the Cloud vendors. A strong or substantial attacker could exploit weak encryption policies, and privileged cloud provider management access, to recover customer data using a complex software or hardware attack on user endpoint devices, or cloud infrastructure devices. This attack may involve account or access hijacking using provider supply chain, social engineering or stealing someone's credentials. [3]

ISSN: 2278 – 1323

SOLUTION: Most of the approaches to handle Data security threat involve the use of strong encryption techniques for data security and fine-grained authorization to control access to data. Strong encryption techniques such as Transport Layer Security protocols (SSL/TLS) and encryption mechanisms like Internet Protocol Security (IPsec) are employed to safeguard the data stored in the shared Cloud environment. These encryption mechanisms often involve the use of an authorization key to decrypt the encrypted data and this key is provided only to authorized users and customers. This ensures that any unauthorized person cannot read, interpret or share the data stored in the Cloud. The access to Encryption keys is also of paramount importance while using an encryption system to safeguard data security. Lost, misplaced or hacked keys can wreak havoc with the data security. Alternately, the authentication mechanisms for accessing data on the cloud need to be very secure and foolproof so that any unauthorized person cannot access other user's data intentionally or otherwise. The cloud provider can control the access to data and needs to employ strong identity and access management services. All customers and users must be properly verified and their access rights defined and documented before providing them access to Cloud services. Cloud Security Alliance (CSA) is a non-profit organization that promotes the use of best practices in order to provide security in cloud environments. CSA has issued an Identity and Access Management Guidance[8] which provides a list of recommended best practices to assure identities and secure access management. This report includes centralized directory, access management, identity management, role-based access control, user access certifications, privileged user and access management, separation of duties, and identity and access reporting.

CUSTOMER CONSIDERATION: The first step is to ensure that a secure fool proof Encryption mechanism is being employed by your Cloud provider. SSL/TLS and 256-bit SSL encryption algorithms are generally used for encryption and provide quite strong encryption security. For encryption of data to be effective means of maintaining data confidentiality, decryption keys must be segregated securely from the cloud environment to ensure that only an authorized party can decrypt data. The access to Encryption keys is very important and all keys need to be secured and safeguarded closely to effectively implement security of cloud data. The encryption keys should not be shared between different customers and the access should be governed directly by the customer. Remember that lost, misplaced, shared or hacked keys can become major lacunae in the data security. An additional challenge around encryption in the cloud is to prevent manipulations of encrypted data such that plain text, or any other meaningful data, can be recovered and be used to break the cipher.

Additionally some security checks and tests can be conducted periodically by the customer or asked to be conducted by the Cloud vendor to ensure and validate data security. The following assessments can be used to test and validate the security of the enterprise data stored at the Cloud vendor. Any vulnerability detected during these tests can be exploited to gain access to sensitive enterprise data and lead to a financial loss. [1]

_ Cross-site scripting[XSS]
_ Access control weaknesses
_ OS and SQL injection flaws
_ Cross-site request forgery[CSRF]
_ Cookie manipulation
_ Hidden field manipulation
_ Insecure storage
_ Insecure configuration.

The proper disposal of obsolete data or data that is no longer required is also important. Such unnecessary data must be properly deleted. All encryption keys and backups must be destroyed so as to ensure that sensitive data does not fall into malicious hands by mistake or by intention.

B. Network Security -Traffic Hijacking

THREAT: Since Cloud data and services are made available to customers through the Internet it can be easily hacked or compromised while it is in transit through the computer networks. In fact entire cloud network could be hacked or attacked by malicious attackers and hence it becomes very important to secure cloud networks. Data in transit is vulnerable to various network security threats which include various types of attacks such as MITM (Man-In-The-Middle) attacks, IP spoofing, port scanning, packet sniffing, etc. Malicious users can exploit weaknesses in network security configuration to sniff network packets. Hence, the cloud user must also protect the infrastructure used to connect and interact with the cloud. This task is further complicated since the cloud lies outside the firewall in many cases.

The widespread use of smart phones these days and their connectivity to cloud has added another risk factor for cloud data security. Attacks are now emerging that are targeted for mobile devices and rely on features traditionally associated with laptops and desktops, including: (i) rich application programming interfaces (APIs) that support network communications and background services, (ii) always on wireless Internet

ISSN: 2278 – 1323

access, and (iii) large local data storage capabilities. When these attacks employ state of the art software and hardware they really can pose a major threat to the data being transmitted through the cloud networks. The Cloud Security Alliance [7] has released a document that describes the current state of mobile computing and the top threats in this area such as information stealing mobile malware, insecure networks (WiFi), vulnerabilities found in the device OS and official applications, insecure marketplaces, and proximity-based hacking [3].

SOLUTION: Encryption is the best solution for securing data in transit through the various networks. Encryption ensures that even if the data is tapped or sniffed during transmission it is unreadable and difficult to understand by the attacker thus losing its significance. In addition, authentication and integrity protection mechanisms ensure that data only goes where the customer wants it to go and it is not modified in transit i.e. integrity of data is maintained during transmission. Encryption involves the use of strong network traffic encryption techniques such as Secure Socket Layer (SSL) and the Transport Layer Security (TLS) for security. In case of Amazon Web Services (AWS), the network layer provides significant protection against traditional network security issues, such as MITM (Man-In-The-Middle) attacks, IP spoofing, port scanning, packet sniffing, etc by employing encryption mechanisms. For maximum security, Amazon S3 is accessible via SSL encrypted endpoints. The encrypted endpoints are accessible from both the Internet and from within Amazon EC2, ensuring that data is transferred securely both within AWS and to and from sources outside of AWS. [5][3]

CUSTOMER CONSIDERATION: Customers should ensure that strong and proven encryption mechanisms like TLS and SSL must be used for encrypting data being transferred through networks. While using Encryption for data security, providers need robust key management processes in place so as to assure the customers of the security of their data. Stringent authority checks for new and existing users and strong authentication mechanisms can help minimize data security risks due to social networking and social engineering. Also the access to data must be made available to users on as and when required basis and the access should be revoked when the need cease to exist.

Time to time checking and auditing of network security can help identify probable risks and handle them timely. The following assessments test and validate the network security of the SaaS vendor:

_ Network penetration and packet analysis
_ Session management weaknesses
_ Insecure SSL trust configuration.

Any vulnerability detected during these tests can be exploited to hijack active sessions, gain access to user credentials and sensitive data and thus should be addressed through encryption mechanisms.

C. Data Locality and Segregation

THREAT: The cloud environment by nature adopts a distributed model for computing and storage whereby the complete computing power and storage capacity of cloud is distributed between various machines that may be stored at different geographical locations. In such environment it is very essential for the cloud provider to be able to exactly know the physical location of each customer's data. If the customer does not know about the exact location of his data it can create issues. Due to compliance and data privacy laws in various countries, locality of data is of utmost importance in many enterprise architecture. For example, in many EU and South America countries, certain types of data cannot leave the country because of potentially sensitive information. In addition to the issue of local laws, there's also the question of whose jurisdiction the data falls under, when an investigation occurs. A secure SaaS model must be capable of providing exact location information of customer's data on the cloud and the security measures provided therein.

As a result of multi-tenancy, multiple users can store their data using the applications provided by cloud in SaaS. In such a situation, data of multiple customers can reside at a common cloud location. Intrusion of one customer's data by another customer becomes an obvious threat in such a multiuser shared environment. This intrusion can be done either by hacking through the loop holes in the application or by injecting client code into the SaaS system or it can be through mistaken unintentional access to other's data. Thus providing separation between a cloud provider's users' (who may be competing companies or even hackers) to avoid inadvertent or intentional access to one customer's sensitive information by other customers becomes important. A client can write a masked code and inject into the application. If the application executes this code without verification, then there is a high potential of intrusion into other's data. A cloud model should therefore ensure a clear boundary for each user's data. The boundary must be ensured not only at the physical level but also at the application level. The service should be intelligent enough to segregate the data of different users and allow only the authentic owners of data to access their data. The introduction of a faulty or

ISSN: 2278 – 1323

misconfigured component required by another cloud user could potentially impact the integrity of data for other cloud users sharing infrastructure and storage space.[1]

SOLUTION: Cloud providers need to provide exact location information of customer's data stored on cloud. The need to maintain a detailed log of which customer's data is stored in which geographical location under which server so that this information can be readily made available to the customer as and when required. Also the customer data must be maintained, safeguarded and backed up frequently at various locations to provide against any data loss due to failed servers or other device failures. Virtualization is one of the key paradigms of a cloud environment. A Cloud provider typically uses VMware or Virtual Machine software and a hypervisor to provide an isolated operating environment to each customer where each customer gets an illusion as if he is working as a standalone user in the available hardware environment. The hypervisor or virtual machine monitor is an additional layer of software between an operating system and hardware platform that is used to operate multi-tenant virtual machines. This helps to avoid inadvertent or intentional access to any customer's sensitive data or work by other customers or users. Technologies are currently available that can provide significant security improvements for VMs and virtual network separation. In addition, the trusted platform module (TPM) can provide hardware-based verification of hypervisor and VM integrity and thereby ensure strong network separation and security. [3]

CUSTOMER CONSIDERATION: Lack of transparency about data handling and management is a big concern for most customers. Data owners or customers should know and audit where their data is stored, how their data is being handled at the cloud, and in particular, ensure that their data is not being abused or leaked. Specifically, customers should ask the cloud providers and ensure that they are using standard manual auditing procedures like SAS-70. A promising approach to address this problem is based on trusted computing. In a trusted computing environment, a trusted monitor is installed at the cloud server that can monitor or audit the operations of the cloud server. The trusted monitor can provide proof of compliance to the data owner, guaranteeing that certain access policies have not been violated. The monitor can enforce access control and data handling policies and perform monitoring/auditing tasks. To produce a proof of compliance, the code of the monitor is signed, as well as a statement of compliance produced by the monitor. When the data owner receives this proof of compliance, it can verify that the correct monitor code is run, and that the cloud server has complied with access control policies. [5]

NIST is a key organization in defining various standards for cloud computing. With regard to security and privacy aspects of cloud computing NIST has released standard guidelines for public clouds. The primary focus of the report issued by NIST is to provide an overview of public cloud computing and the security and privacy considerations involved. The NIST report recommends that it is important to understand the technologies the cloud provider uses to provision services and the implications of this technical control on security and privacy of the system. With such information, the underlying system architecture of a cloud can be decomposed and mapped to a framework of security and privacy controls that can be used to access and manage risk. Thus it is important for customers to ask the providers about the cloud architecture and understand the security risks. The NIST report recommends the providers to provide for additional security for virtualized cloud environments and the use of virtual firewalls to isolate groups of virtual machines from other hosted groups, such as production systems from development systems or development systems from other cloud-resident systems.[11]

D. Data Access, Authorization and Identity Management

THREAT: Data access control and authorization could be one of the big security determinants in a cloud environment. Data access issue is mainly related to security policies provided to the users while accessing the data. Implementation of poor access control procedures can create many threat opportunities for attackers. For example that disgruntled ex-employees of cloud provider organizations maintain remote access to administer customer cloud services, and can cause intentional damage to their data sources. Similarly an authorized customer having access, can use existing privileges to gain further access or support third parties in executing attacks against the confidentiality integrity and availability of information within the cloud service. Every organization will have its own security policies based on which each employee can have access to a particular set of data and services. But when this organization's data and services are stored in the cloud environment, authentication and access control are more important than ever since the cloud and all of its data are accessible to anyone over the Internet. [3] A cloud provider would need to imbibe and meld the customer organization's security policies and authorization framework to be able to provide consistent security.

ISSN: 2278 – 1323

There is a risk that insiders can deliberately be used to gain access to customer data and probe systems in order to assist any external attackers that require additional information in order to execute complex Internet-based attacks. Cloud customers should ensure that service providers are aware of this threat and have rigorous identity validation and security vetting procedures built into their recruitment process. Also there is a direct threat that a cloud provider can steal or misuse sensitive and proprietary company information and sell it to outsiders.

SOLUTION: Strong authentication is a mandatory requirement for any cloud deployment. User authentication is the primary basis for access control. All access information related to users – user name and company details, user ids, passwords, access rights and privileges, available cloud services should be documented in detail and stored in a secured database. Most companies, store their employee access information and their privilege rights in some type of Lightweight Directory Access Protocol (LDAP) servers. These access rights and privileges should then be implemented through detailed authentication and authorization mechanisms[1]. Identity management(IdM) or IDmanagement is a broad administrative area that deals with identifying individuals in a system (such as a country, a network or an organization) and controlling the access to the resources in that system by placing restrictions on the established identities. Cloud Security Alliance (CSA) is a non-profit organization that promotes the use of best practices in order to provide security in cloud environments. CSA has issued an Identity and Access Management Guidance [8] which provides a list of recommended best practiced to assure identities and secure access management. This report includes centralized directory, access management, identity management, role-based access control, user access certifications, privileged user and access management, separation of duties, and identity and access reporting.

The Cloud vendor can support identity management and sign on services using one of the following three models [6]:

3.4.1. *Independent IdM stack* – Here the Cloud vendor provides the complete stack of identity management and sign on services. All information related to user accounts, passwords, etc. is completely maintained at the Cloud provider end.

3.4.2. *Credential synchronization* – Here users do not need to remember multiple passwords and use their authentication details provided by their organization to sign-on to Cloud data and services. The user account information creation is done separately by each customer organization within their own enterprise boundary and the cloud vendor replicates the user account information and credentials from the enterprise database. The authentication happens at the Cloud vendor end using the replicated credentials and user information from the enterprise database. The cloud provider needs to ensure security of credentials during tranit and storage in this case to prevent leakage.

3.4.3. *Federated IdM or Integrated IDM* - The entire user account information including credentials is managed and stored independently by each customer enterprise. The user authentication occurs within the enterprise boundary. This involves setting up a centralized and integrated Access Management where a single login provides access to all cloud services. This approach ensures that all identity related functions such as authentication and authorization are consistently managed by the enterprises only. Many existing IDM solutions such as CloudMinder from CA technologies are based on this approach [10]. Proper trust relationships and validation mechanisms need to be established between the enterprise and the cloud applications to ensure unauthorized access and misuse of privileges doesn't happen.

CUSTOMER CONSIDERATION: Customers moving to cloud must ensure that the cloud provider has demonstrable security access control policies and authorization mechanisms in place that prevent privilege escalation by standard users, enable auditing of user actions, and support the segregation of duties provided for privileged users in order to prevent and detect malicious insider activity. In addition to customer access and rights, the Cloud provider access rights and privileges must be clearly documented and communicated to the customer. The Cloud provider should have as little direct access to customer data as possible. In cloud vendors such as Amazon, the Elastic Compute Cloud (EC2) administrators do not have access to customer instances and cannot log into the Guest OS. EC2 Administrators with a business need are required to use their individual cryptographically strong Secure Shell (SSH) keys to gain access to a host[1]. This minimizes the risk of unauthorized access. Proper Identity management policies and procedures must be defined and implemented for all users. Many a times user credentials are stored in the SaaS providers' databases and not as part of the corporate IT infrastructure. This means SaaS customers must

ISSN: 2278 – 1323

remember to remove/disable accounts as employees leave the company and create/enable accounts as come onboard. The trusted computing group's (TCG's) IF-MAP standard removes this dependency and allows for real-time communication between a cloud service provider and the customer about authorized users and their access rights [3]. There are several ways in which an identity federation can be accomplished such as the security assertion markup language (SAML) standard or the OpenID standard [11] and cryptographic mechanisms such as digital signatures. The cloud provider must us a combination of two or more of these technologies to ensure the access management policies are impenetrable and secure. Finally customers can use the following assessments to test and validate the security of the identity management and sign-on process of the cloud vendor [1]:

_ Authentication weakness analysis
_ Insecure trust configuration.

Any vulnerability detected during these tests can be exploited to take over user accounts and compromise sensitive data.

E. Virtualization Vulnerability -Shared Technology Vulnerability

THREAT: Virtualization is one of a number of enabling technologies of cloud computing that itself is a run-time method of segregation for processing data. A cloud provider commonly uses *virtual machines* (VMs) and a hypervisor to separate customer data and applications. The Virtual Machine Monitor (VMM) or hypervisor is low-level software that controls and monitors its virtual machines and is responsible for virtual machines isolation. As any other software a hypervisor or VMM can have its own security flaws. If the VMM is compromised, its virtual machines may potentially be compromised as well. Vulnerabilities have found in VMWare (Security Tracker: VMWare Shared Folder Bug), Xen (Xen Vulnerability), and Microsoft's Virtual PC and Virtual Server (Microsoft Security Bulletin MS07-049) [3]. Incorrectly defined security parameters and incorrect configuration of virtual machines and hypervisors can cause unauthorized access of one customer's sensitive data by another customer on the same cloud. In this case security of data depends on having adequate security controls in each of the layers of the virtualized environment. Virtual machine monitor should be 'root secure', meaning that no privilege within the virtualized guest environment permits interference with the host system. For example, the vulnerability of Microsoft Virtual PC and Microsoft Virtual Server could allow a guest operating system user to run code on the host or another guest operating system. Vulnerability in Virtual PC and Virtual Server could allow elevation of privilege. Another example would be the vulnerability in Xen caused due to an input validation error in tools/pygrub/src/GrubConf.py. This can be exploited by 'root' users of a guest domain to execute arbitrary commands in domain 0 via specially crafted entries in grub.conf when the guest system is booted [1].

An emerging concern for cloud delivery models using virtualization platforms is the risk of side channel attacks causing data leakage across co-resident virtual machine instances. A side channel attack is any attack based on information gained from the physical implementation of a system; e.g., timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information that can be exploited to access or damage the system [3]. Any authorized application running on a VMM can exploit the hypervisor in order to take control of the underlying infrastructure and cause irregular distribution of resources and computing power. Moreover, virtualization introduces the ability to migrate virtual machines between physical servers for fault tolerance, load balancing or maintenance [4]. This useful feature can also raise security problems. An attacker can compromise the migration module in the VMM and transfer a victim virtual machine to a malicious server. Also, it is clear that VM migration exposes the content of the VM to the network, which can compromise its data integrity and confidentiality. A malicious virtual machine can be migrated to another host (with another VMM) compromising it.

SOLUTION: In a virtualized environment, the cloud provider needs to provide special security mechanisms and implement new technologies to handle the risk of attacks through all type of VM software(VMM, hypervisor or other VM interfaces). Technologies are currently available such as Hypersafe that can provide significant security improvements for VMs and virtual network separation. Hypersafe is a lightweight tool that ensures control-flow integrity in hypervisors using techniques using two techniques: non-bypassable memory lockdown which protects write protected memory pages from being modified, and restricted pointed indexing that converts control data into pointer indexes [3]. In addition, the Trusted Cloud Computing Platform (TCCP) can provide hardware-based verification of hypervisor and VM integrity and thereby ensure strong network separation and security. TCCP enables providers to offer closed box execution environments, and allows users to determine if the environment is secure before launching their VMs. The TCCP adds two fundamental elements: a trusted virtual machine monitor (TVMM) and a trusted coordinator (TC). The TC manages a set of trusted nodes that run TVMMs, and it is maintained but a trusted third party.

ISSN: 2278 – 1323

The TC participates in the process of launching or migrating a VM, which verifies that a VM is running in a trusted platform. Trusted Virtual Datacenters (TVDc) provides isolation between workloads by enforcing mandatory access control, hypervisor-based isolation, and protected communication channels such as VLANs [6]. Newer Virtual machine architecture models and VMware technologies are being designed and developed for combating the security risks due to virtualization. In their significant paper on Virtualization technologies, Mihai, Sailer and Schales from IBM suggest a secure version of virtual-machine introspection which combines discovery and integrity measurement of code and data starting from known hardware solutions. Their solution first detects the exact type and version of an operating system running inside a guest VM and then uses a rootkit-detection and recovery service to detect abnormal VM behavior and functions. Their solution built on the premises of Virtual Machine Introspection, Memory protection, Secure code execution and Secure control flows provides an effective architecture to handle all security risks arising out of virtualization [9].

CUSTOMER CONSIDERATION: In virtualized environment, security of data depends on having adequate security controls in each of the layers of the virtualized environment. In addition, secure deletion of memory and storage must be used to prevent data loss in a multi-tenant environment where systems are reused. The hypervisor layer between the hardware and virtual machine / guest OS has privileged access to layers above. It also has a great deal of control over hardware, and increasingly so, as hardware manufacturers implement hypervisor functions directly into chipsets and CPUs [3]. Cloud customers, therefore, need to know what virtualization technologies the cloud provider is using, understand what are its vulnerabilities and then must ensure that Cloud providers are employing proper tools and mechanisms to handle all security risks due to virtualization. The NIST report recommends that care should be taken to provision security for the virtualized environments in which the images of various applications run. It also recommends the use of virtual firewalls to isolate groups of virtual machines from other hosted groups, such as production systems from development systems or development systems from other cloud-resident systems [11]. A perfection of properties like isolation, inspection and interposition is yet to be completely achieved in VMMs.

F. Availability and Denial of Service

THREAT: Denial of service or non availability of cloud services could occur from multiple reasons ranging from network bandwidth issues to hardware issues such as failed servers to faulty application components. Well-publicized incidents of cloud outages include Gmail's one-day outage in mid-October 2008 (Extended Gmail Outage), Amazon S3's over seven-hour downtime on July 20, 2008 (Amazon S3 Availability Event, 2008), and Flexi Scale's 18-17 hour outage on October 31, 2008 (Flexiscale Outage) [3]. These outages can severely impact business operations of Cloud customers and could result in financial losses. Denial of service (DoS) is mostly associated with network layer distributed attacks, flooding infrastructure with excessive traffic in order to cause critical components to fail or to consume all available hardware resources. Within a multi-tenant cloud infrastructure, there are more specific threats associated with DoS. Some of these threats are: (a) Shared resource consumption – attacks that deprive other customers of system resources such as thread execution time, memory, storage requests and network interfaces can cause a targeted DoS, (b) Virtual machine and hypervisor exploitation – attacks that exploit vulnerabilities in the underlying hypervisor, or operating system hosting a virtual machine instance will allow attackers to cause targeted outages or instability. [3] It is also possible that in a shared virtualized environment, one malicious user by executing an errant program or an application having bugs(worms) that will consume all the possible resources like computing power and network bandwidth so as to deprive other users or applications of critical Cloud services. Thus, the system cannot satisfy any request from other legitimate users due to resources being unavailable.

SOLUTION: Resilience to hardware/software failures, as well as to denial of service attacks, needs to be built into the cloud architecture right from the ground level infrastructure and should be supported through all applications and services.

To protect against non availability of cloud services due to hardware failures such as failed servers or databases, alternate servers and other hardware should be employed that can provide cloud services in case of hardware failures. Similarly, to handle network congestion and network outages, buffer load capacity should be maintained at the network servers. The cloud provider must always plan and employ network capability to support more number of users than the actual number of users to avoid network congestion. For example, Amazon maintains internal bandwidth that exceeds its provider-supplied Internet bandwidth [3]. Other techniques to mitigate denial of service due to network outages, includes using synchronous cookies and limiting the number of network connections. To prevent malicious users from causing denial of service attacks by consuming huge amount of cloud resources, cloud providers can force policies to allocate limited resources

ISSN: 2278 – 1323

to any particular user. Such limits on resource allocation and network bandwidth can be implemented through the hypervisors or the Virtual Machine Monitors that govern and monitor resource allocation in the cloud environment. At the same time, an appropriate action plan for business continuity (BC) and disaster recovery (DR) needs to be considered for any unplanned emergencies. This is essential to ensure the safety of the enterprise data and minimal downtime for enterprises.

CUSTOMER CONSIDERATION: The Cloud providers especially the ones providing SaaS applications need to ensure that customer enterprises are provided with cloud services around the clock. This involves making architectural changes at the application and cloud infrastructural levels to add scalability and high availability of cloud services. A multi-tier architecture needs to be adopted, supported by a load-balanced form of application instances, running on a variable number of servers to maintain cloud availability. Many cloud providers provide SLAs or Service Level Agreements that define limits on Cloud services such as network downtime and outages. Some pre-assessment tests can be done by the customers to test and validate the availability of Cloud services such as Authentication weakness tests, Load management tests and Session management tests [1].

IV. CONCLUSION

Cloud computing is one of the most promising emerging technologies. Due to the cost efficiency and flexibility that it provides, it can prove to be a dynamic game changer for many small and middle level organizations and independent users. But as discussed in this paper, security poses a big roadblock in the way of organizations wishing to adopt cloud technology in a major way. Despite the many advantages offered by cloud computing, customers are wary of moving to a cloud environment and are afraid to put their sensitive data on the cloud due to the various security threats faced by cloud environment. There are many significant security risks and concerns attached with cloud computing. Though many of these risks and threats existed earlier too but their scale and impacts are magnified in a cloud environment since the control and governance of cloud environment is not under the enterprises but under the different cloud provider. Lack of controls and transparency is one of the biggest concerns of customers moving to clouds. In this paper we have discussed major threats to Cloud computing, solutions to handle them and what customers moving to cloud environment should know and do about these risks. Many small and big solutions exist to handle the various threats posed by cloud computing. Careful analysis and understanding of these risks and a proper designed and well-coordinated solution to handle them can go a long way in making the path of cloud computing less dubious and more acceptable to customers. As of today, there is no one single perfect all-inclusive solution to handle all risks of cloud computing. But it would be great if such a framework could be prepared that can guide the cloud providers and customers and make the cloud computing experience fully secure and pleasant for future customers.

V. REFERENCES

[1] S.Subashini and V.Kavitha, "A Survey on Security issues in service delivery models of cloud computing", *Elselvier-Journal of Network and Computer applications 34 (2011)1-11*

[2] Kuyoro S.O., Ibikunle F. and Awodele O., "Cloud Computing Security issues and Challenges", *International Journal of Computer Networks – Vol 3, Issue 5, 2011*

[3] Jaydip Sen, "Security and Privacy Issues in Cloud Computing", *Innovation Labs, Tata Consultancy Services Ltd., Kolkata*

[4] Cloud Security Alliance, "The Notorious Nine – Cloud computing threats in 2013", Feb 2013, Available at: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

[5] Cloud Security Alliance, "Security Guidance for Critical areas of Focus in cloud computing v3.0", 2011, Available at : https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[6] Keiko Hashizume1, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, "An Analysis of Security issues for Cloud Computing", *Springr - journal of Internet Services and applications 2013*

[7] Cloud Security Alliance - Security guidance for critical areas of Mobile Computing, 2012 Available at: https://downloads.cloudsecurityalliance.org/initiatives/mobile/Mobile_Guidance_v1.pdf

[8] Cloud Security Alliance - SecaaS implementation guidance, category 1: identity and Access managament. Available at: https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_1_IAM_Implementation_Guidance.pdf

[9] Mihai Christodorescu, Reiner Sailer, Douglas Lee Schales, Daniele Sgandurra, Diego Zamboni, "Cloud security is Not(Just) Virtualization Security", IBM

[10] CA Technolgies – "Identity and Access Management (IAM) across Cloud and On-premise Environments: Best Practices for Maintaining Security and control"

[11] Badger, L., Grance, T., Patt-Corner, R., & Voas, J., "Draft Cloud Computing Synopsis and Recommendations.- National Institute of Standards and Technology (NIST)" *Special Publication 800-146. US Department of Commerce. May 2011*. Available at: http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf (Accessed on: November 20, 2012).

Kriti Arora is working as Assistant Professor in Shyam Lal college, University of Delhi. She did B.Sc. Physics(H) from University of Delhi and then did MCA from Thapar University Patiala. Prior to shifting to academics, she had a rich experience of working in IT industry for 10 years in Mainframe technology domain. She is interested in Network and Cloud Security research and has written a couple of research papers on these topics earlier.

ISSN: 2278 – 1323