# Cloud Computing Security threats and Countermeasures

Hamza Ahmed

## Introduction

Within the last decade, there have been several advances in technology that have created more opportunities for people to communicate around the world. Technology trends have reached not only the enterprise environments, but also in ordinary people's homes. Cloud computing implementation has revolutionized the tech community, and spread throughout the business world. It is no longer just for the private sector, but has been widely adopted by the public sector, as more companies have turned to cloud services in collaboration and storage. Cloud computing is not a new innovation, but it is new in the aspects of constructing for advanced computation power, and improvement in storage capabilities. The change to cloud technology permits new mechanisms of technology that offer users abilities in storing, and sending information over the internet. Cloud computing is dependent on the framework of the internet, and suffers from the same vulnerabilities and security threats. While there are several advantages to adopting and moving to this new technology that makes it a formative option for consumers and companies, the security threats and vulnerabilities have the potential to seriously challenge its longevity. Within this paper, it will provide information backed by research and data that define cloud computing and its benefits, while also outlining the threats and countermeasures available.

While cloud is not anything new to the technology community, within the last few years "cloud" has been the leading buzzword. Cloud computing is relativity new in virtualization that allows the user to rent bandwidth, operate virtual machines, and process power. It provides a scalable service delivery platform for enterprise users and individuals. Cloud computing implementation provides a faster, flexible, and cost effective amalgam of technologies which involves various tools for its achievement. The three delivery models that are used in cloud computer include Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Software as a Service (SaaS). The main objective of utilizing cloud computing is used as extraneous hardware connected to support downtime on each device within the network. In principle, users have the capabilities of hosting software, storing, and processing data from a remotely accessed server. In the technological aspects, cloud computing is referred to as a transformed model of computing where computation and operations are carried out over data in the cloud.

The cloud is usually a data center that is collected by a third party. Cloud computing has proven to be useful in several aspects that encompass service offerings that permit options for collaboration. More importantly, cloud computing has provided small companies the ability to compete on a level playing field with leading companies. This has made the options for implementing cloud computing so popular. In cutting through the veil of cloud computing, the ubiquitous global network offers service providers mechanisms for economically delivering network-based computing services. As cloud computing is advantageous to several different users, cloud computing cannot control the established responsibility for privacy and security threats that can undermine the integrity of the business. The problems lie in the lack of control or location of the remotely accessed servers, as well as problems with access, and potential of cybercrime. The risks associated with the cloud environment create a substantial threat to information security.

## Cloud Technology

In order to understand the security threats and vulnerabilities of cloud computing, the reader must understand what cloud computing is. Cloud computing is generally referred to as a metaphor, utilized by the internet of interconnected computers over the internet through the intranet. Cloud computing is stored over the servers as they host files and construct a cloud by providing information available for numerous computers and servers. Cloud computing allows for data to be accessible. The formation of the cloud hosted on remote servers, permits users accessibility of information for any location and on any computer with internet access. Collaborative options are a main advantage of cloud computing where programs and documents are available to group members' without barriers to location. Enterprises and businesses look to balance the reward and the risk of implementing cloud computing. Information security is utilized as a method of protecting information systems. However, the longevity of the amount of variability given to cloud computing is not carefully monitored. This opens the door for a need to protect the infrastructure from risks, vulnerabilities, and potential threats. Cloud computing is regarded as a better means of providing secure technology, however, it has yet to measure the extent of the impact of security risks.

According to research, "Cloud Computing appears as a computational paradigm as well as distribution architecture and its main objective is to provide secure, quick, convenient data storage and net computing service, with all computing resources visualized as services and delivered over the Internet" (Zhao, Liu, Tang, Sun, Zhang, Ye, Tang, 2009). Cloud computing is essentially described by any goal-oriented action in respects to developing and advancing computers. Cloud computing incorporates designing and building hardware and software systems for several purposes that processes various types of structuring and managing information. The range in actions from discovering and assembling critical information, those are creating smart performing computer systems, generating media, and other possibilities. Cloud computing has an open platform that provides users variability of services. Were site specific hardware and software connections are not a requirement. According to NIST,

Cloud computing is merely a model for enabling convenient, on-demand network access to shared data pools) of configurable computing resources (e.g.,, Networks, servers, storage, application, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Scholz, 2013, pg.145).

Platforms used in cloud computing such as PaaS, SaaS, and IaaS, are utilized by hosts such as, Terremark, Savvis, and Rackspace. Cloud computing incorporates a model of indispensable features that includes four deployment models, and three service models. The features considered indispensable include; on-demand self-service that the user can deliver competency in computing as necessary without the need of a human interface of the service provider.

Broadband network access provides competency over the network through tools that endorse the use of various platforms. The increased versatility of the platform that requires a scalable system, which is augmented and mechanically controlled by leveling a metered service (NIST, 2011). The position of the cloud on four separate backgrounds which takes into account of a private cloud that is specifically owned by entities in the business sector, public cloud, community cloud, and hybrid cloud (NIST, 2011). The technological environment presently has empowered each user to get involved in cloud computing, in both the domestic and commercial sectors. There are several programs that have been used over the internet without arrangement which uses cloud computing, which includes the popular search engine, Google, and every email provider. The development of cloud computing has given way for numerous applications, businesses, and websites to launch cloud services. There is no necessary advanced knowledge or expertise in the technology infrastructure of cloud technology that restricts users from using them. The popularity of cloud computing brings into focus a need that provides an elevation of capacity, in regards to the capabilities of investing in new licensing, infrastructures, jobs, and software creation. The infrastructures of cloud computing are available on a subscription or pay per use based services, that provide dependable services through data centers, and virtualization of various technologies.

## Benefits of Cloud Computing

Cloud technology is not owned independently by one entity, instead offers users the methods of having free access or renting for more capabilities of the cloud where they do not have worry about ingest resources and capital expenses. The increase in IT companies has made the surge in traffic incapable of being handled with just a few servers that carry volumes of data and customer needs. Essentially, "Cloud Computing enables ubiquitous, 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" (Hashizume, Rosado, Fernandez-Medina, Fernandez, 2013). Cloud computing implementation supports the advanced needs of IT without the need to invest in large data centers. Business units are capable of being more efficient in processing, centralized storage, bandwidth, and memory. Dynamic provisioning permits for services that are critically based on the increased demand of more data. Cloud computing offers automatic provisioning offered through software automation that allows the development and reduction of service capabilities. Access to networks is provided through several arrays of services that are incorporated in mobile devices that can be calibrated from laptops, API, and other internet capable devices.

Cloud computing systems that consist of infrastructures and applications provide users the capabilities of using the system any place, at any time. Cloud computing systems provide its users with unlimited access from virtually anywhere. Two components such as redundancy and hardening are used in enhancing the availability of the hosted applications and the cloud system. Vendors that provide cloud platforms and cloud infrastructures utilize virtual machines that are the basic component of cloud computing systems, such as Amazon Web Services, VMware, Microsoft Hyper, and others. It offers the services of providing on demand services that fit the individuals' resource requirements, and offers geographic redundancy that enable high availability from a single host. EBay and Amazon, some of the biggest e-commerce websites, use cloud computing because they can control peak problems through the recompense or interchanging of their internal computation with cloud technology.

Other benefits include decreasing the cost to the infrastructure, self-maintenance, the overall lowering of client hardware, and software costs (Sosinky, 2010). Cloud computing offers unlimited storage capabilities, and the ability for individuals and companies to acquire software applications through the cloud at no additional charge. Collaboration of sharing of files and data is essential in providing open accessibility in different geographical locations. Overall, cloud computing offers users reduced IT expenditures, accessibility to mobile devices, agile IT services, and more scalability. Although Cloud computing has supplied numerous opportunities that provide accessible and scalable services to users, it has also elevated risks. These risks expose the vulnerabilities that can prevent users from trusting cloud computing that include, control, confidentiality, privacy, compliance, and other several threats to security.

### Areas Where Security Is an Issue

Confidentiality is crucial to cloud computing infrastructure. The aim is to keep the user's data from the eyes of others. Cloud computing can be available on public networks, and has made this component an overall attractive option for increasingly more users. Data on a traditional network is kept confidential through cryptography and physical isolation at local data centers. However, the open platform allows for users to access files and data that can be available to other unauthorized users. The risks of external data storage, and the dependency on the public internet, the overall lack of control, and the integration and multi-tenancy with internal security. Unlike traditional technology, the cloud provides particular features that offer scalability and resources. They are distributed from cloud providers, virtualization, and heterogeneous service. Meager security measures that include authentication, authorization, and identity are not enough, which are not different from in any other IT environment. One of the biggest concerns by the businesses is the moving of sensitive data and critical applications to a public cloud network, that takes the control out of the users' hands. Security issues within cloud computing are a concern on the platforms used such as, PaaS, SaaS, and IaaS. Specifically, "A threat is a potential attack that may lead to a misuse of information or resources, and the term vulnerability refers to the flaws in a system that allows an attack to be successful" (Hashizume, Rosado, Fernandez-Medina, Fernandez, 2013).

### Service Models

The service models and the deployment models are how cloud computing operates, and they are the most vulnerable to security threats to users. Software as a Service (SaaS) is primarily used as an online application, where the providers provide, manage, and maintain each service that consist of the infrastructure, software, and platform. This service model, the users cannot manage their own services, but they are to use applications from the service providers through web browsers or thin client. These models include Google platform and services, and other similar services. Platform as a Service (PaaS) is an advanced model, which allows users the ability to customize their own features and configurations used in developing their own applications. The service model can be divided into three categories, add-on, open, and stand-alone application platform. Stand-alone application platforms allow the user to create their own applications. Add-on allows users to modify and customize their added features and configurations with the use of the provided environment. While open platform is similar to stand-alone, users can create their own environment.

According to Tech Target, PaaS is the most popular model where users can rent operating systems, hardware, network and storage capacity over the internet. (TechTarget, n.d) It is an advantageous model where features are consistently upgraded. The collaborative effort of developing programming without global barriers, makes it also the most vulnerable. Infrastructure as a Service (IaaS) provides a cost effective and pragmatic layer of data replication, consolidation, and transformation that allows for information to information users (Raggert, 2010, pg. 3). IaaS allows users applications, and data to clash without affecting data from the user. Providers maintain and manage their own equipment, and the capabilities of scalability as the infrastructure changes, and demands of the user. Users can purchase the hardware and administrative system, where they setup application and platforms for their own use. They have to manage and maintain the operating systems, databases, platforms, and applications on their own. IaaS, however, keeps data and information present in the systems for user's access.

Cloud computing offers consistency, in regards to the overlapping of information sources that can authenticate contradictory information, which ensures a constant access of information for the users. Each point of entry where data flows from systems to IaaS, it validates and provides quality checks. The service model is based on a consistent flow of data that is categorized as a pull and pull information model, used primarily in search engine services such as Google, Yahoo!, and others. However, SaaS carries security burden on the cloud provider, although it offers a higher degree of integrated functionality, PaaS offers greater customer control and extensibility (Mather, Kumaraswamy, Latif, 2009). The relationship between the service models characterizes their dependencies and needs for security. "PaaS, as well as SaaS, are hosted on top of IaaS; thus, any breach in IaaS will impact the security of both PaaS and SaaS services, but also it may be true on the other way around" (Hashizume, Rosado, Fernandez-Medina, Fernandez, 2013). The relationship between the service models increases the dependency of security, where any attack on the cloud service layer can compromise the other layers. Each can rent from each other which provides an inconsistent mixture of security models and measures, which creates confusion over responsibility when an attack occurs.

### The Deployment Models

The deployment models that are available to users are private, public, and hybrid clouds. Private clouds can only be accessed through the internet on a private network. They must attain authorized access to join on the same network, and use the same services. The infrastructure is maintained and deployed through a third party, or organization. This access is available to telecommuters that work remotely, and have access to applications on multiple devices such as smartphones, computers, and tablets from anywhere. Private cloud provides higher security measures, better performance, and greater user experiences. Users in remote locations can modify settings, access desktop files, run computer applications, and access data from any geographical location.

Public cloud is the most common cloud deployment that provides access to internet application, and accessibility from wherever there is an internet connection. The users will be able to share information and files efficiently through the cloud. This cloud is provided by a cloud service provider through commercial services. Users are able to develop and produce components on an affordable basis, unlike traditional internet services. They are established by various organizations that include shared communities, workstations, and other places where storage can be exploited, utilized, and accessed through the cloud. They are several advantages to public cloud services, where users are able to configure, install, and store data. Public cloud is inexpensive, reliable, easily connected, and, irrespective to the geographical location. The hybrid cloud is the third deployment model that combines public and private cloud platforms that divide applications into separate categories. Where there is a greater demand for security, applications are only accessible through private clouds. Applications that demand a lower level of security are available to the public cloud. The different cloud infrastructures provide a constant flow of applications and data moved throughout each deployment model. The hybrid cloud is necessary in maintaining a level of security for the organization, and allows users to access services in the cloud. Organizations can take advantage of the cost affectivities and scalability that exists in the public cloud computing environment, while also not exposing the application to third-party vulnerabilities (Tech Target, nd). The users and organizations can obtain inexpensive services, while managing services in both clouds. However, each deployment offers vulnerabilities and security threats that can compromise entire networks and organizations.

## Security Threats

Cloud computing provides a paradigm shift which will affect various subcategories within the computer networks such as software and hardware companies, and service providers. Treats to cloud computing are detrimental to the political, social, and ethical landscape of the internet. Geopolitical issues tangled into security threats are a serious concern that cloud service providers must appease to the regulatory environment to appeal to the global market. The legal aspects of cloud computing stem from trademarks, copyrights, and the probable infringement on user's privacy and personal information. There are several threats that include risks to service and network that have yet to be calculated. According to the Cloud Security Alliance (CSA), they have discovered several threats to cloud computing, that includes abuse and nefarious use of cloud computing. The top threat is the ability for bots to spread malware and spam. Cyber-attacks can infiltrate the public cloud and upload large amounts of malware to computers connected, and use the cloud to attack other machines. Attacks range from Man in the Middle attacks (MITM) that can inject false information into transferred data, sniffer attacks, reuse of IP addresses, cross site scripting, SQL injection attacks, Denial of Service (DoS) attacks, and cookie poisoning (Ashktorab, Taghizahdeh 2012). Many cloud service providers allow users to try out service on a trial basis, giving hackers the ability to access cloud systems. Hackers can upload malicious codes and make way for cybercriminals to conduct activities with detrimental consequences. Hackers will usually wipe data, and can cause data to be wiped out entirely, leading to legal and security issues. Cybercriminals will target cloud service providers with weak registration systems, and weak fraud detection.

The threats to cloud computing places considerable emphasis on the ability for cybercriminals and attacks that can use flash, and other applications to hide their malicious codes, that can spread rapidly to compromise the cloud (Pacella, 2011). Attacks to cloud systems have been reported by Salesforce.com, SunTrust Bank, and others that were victims of scammers that were able to infiltrate the system and steal personal data, as well as phishing scam to compromise the system. The next threats are insecure interfaces, APIs, and Virtual Machines. Users of the cloud used the APIs and software interfaces that provide access and manage cloud services. APIs is most critical because they provide management, provisioning, and monitoring of the cloud service processing. Applications are a central component of cloud service, and have to be secure in access controls, authentication, activity monitoring, and encryption. Applications are available via the internet, and flaws create vulnerabilities to applications created on the SaaS service model. According to research, "Attackers have been using the web to compromise user's computers and perform malicious activities such as steal sensitive data" (Owens, 2010).

The cloud is probable to threats that impact the entire infrastructure. Security and data breaches are mainly connected to the lack of training of cloud policies, and unauthorized access (CSA, 2013). Easy accessibility over the internet from multiple devices in the workplace makes cloud computing advantageous to employees, however, it also exposes a serious security risk. "The Cloud Security Alliance 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 (Wi-Fi), vulnerabilities found in the device OS and official applications, insecure marketplaces, and proximity-based hacking" (Hashizume, Rosado, Fernandez-Medina, Fernandez, 2013). These security risks make the infrastructure vulnerable to inside attacks that can be carried out by malicious employees that create a destructive pathway for criminals to steal private information from other employees in the cloud.

Insiders can potentially acquire cryptographic keys, passwords, and files that can be harmful to the organization. These attacks and threats overall compromise files that lead to fraud, theft, and other damages. CSA says, "If an attacker gains access to your credentials, he or she can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites" (CSA, 2013). The increase in this threat is due to lack of transparency that the provider's procedures and processes. The vagueness of this threat is raised when the provider does not make clear the authentication, nor the methods used in granting authorized access, and legal compliances. Providers are not thoroughly screened and can potentially be hackers or scammers masquerading to steal confidential information without little to no detection. The threat of malicious insider attacks weighs heavily on the organization that can damage the reputation, and have a financial impact, as well. The threat of inside attacks also raises the risks of privacy controls. Privacy issues stem from data collection, storage, disclosure, access, and retention (Svantession, Clarke 2010). Legal compliance has become a cardinal issue, where there has not been a definite policy in place to protect users' privacy and personal information. Their information can be shared without their consent, giving way to identity theft, and other issues. Data leakage and data loss are perceptible when it comes to accessing threats and risks in cloud computing. Data leakage and loss are substantial risks that can affect confidential data used by government and large corporations. The threat can occur by operational or natural failures. They can result from undependable data storage or the use of encryption keys infiltrated. Within the infrastructure, operational failures are risks where deletion and modification of records and files without intentional or unintentional secured backup in place (CSA, 2013). Data storage that is unpredictable makes data and files unrecoverable if information is lost or deleted. Encryption keys can be used to provide unauthorized access, and will ultimately affect data that are lost to the user or the organization. Confidential and high level files run the risks of being corrupted, copied, or other problems. Examples of this problem happening include several large corporations being hacked and infiltrated where millions of user's data were lost from social media, email, and other secure accounts.

### Vulnerability

While it is difficult to see the extent of the external threats and risks to cloud computing, it is impossible to know the extent of internal threats of the vulnerability of the infrastructure. Cloud computing creates challenges that place the enterprise in a risky situation with lack of traditional layouts. This can lead to several safety concerns and threats listed above, as well as vulnerabilities within the virtual machine. What makes the infrastructure vulnerable is a combination of weak anti-virus software, encryptions, and flaws in clients' application that can lead to attacks of acquiring sensitive and personal data from users and corporations (CSA, 2013). Cybercriminals can gain access to credentials by malicious or unaware employees that are not complying with company policies for network devices. As discussed, employees can leave out sensitive information, and provide access unknowingly for unauthorized users to see. This lack of security exposes vulnerabilities that can lead to service or account traffic hijacking. This can leverage the power of corporations' reputations to launch attacks on other enterprises. The vulnerabilities in malicious attacks are visible when the hiring of unknown third party cloud providers is given access to unlimited amounts of information from organizations. Granted access to third party providers, can ensure intruders, adversaries, and attackers the ability to gather and collect confidential data.

The vulnerabilities in the virtualized technology are due to the cloud virtualization where the information of users' applications are on virtual machines (VMs) that are on a shared infrastructure. "Virtualization allows users to create, copy, share, migrate, and roll back virtual machines, which may allow them to run a variety of applications" (Hashizume, Rosado, Fernandez-Medina, Fernandez, 2013). Hackers are able to encroach into Virtual Machines, due to their hardware, which is maintained under the same third party provider. These vulnerabilities expose the lack of security, where systems can be easily compromised, as cybercriminals work to get computer, server, and cloud memory. The vulnerabilities related with session hijacking and traffic hijackings are predominant for gaining unauthorized access to cloud systems and services. According to published research, "Virtualized environments are vulnerable to all types of attacks for normal infrastructures; however, security is a greater challenge as virtualization adds more points of entry and more interconnection complexity" (Hashizume, Rosado, Fernandez-Medina, Fernandez, 2013). Once sessions in cloud computing are compromised cybercriminals have the attainability to progress with numerous attacks and activities, and send commands on behalf of the original user. As cybercriminals penetrate cloud computing, the session rider deletes user data, executes online actions, and distributes spam to intranets from the internet. Virtual machines share resources which create problems with security. As attackers gain access to one server, they can also gain access to CPUs, I/O, memory, and other sources. A cybercriminal can compromise the migration module in the virtual machine, and turn it into a malicious server. This can compromise the confidentiality and integrity of the network. VM create vulnerabilities where an attacker can create images containing viruses such as a Trojan horse and infect other machines, this can lead to unintentional data leakage and VM replication (Grobauer, Walloschek, Stocker 2011).

The vulnerabilities in the interfaces and APIs are unsecured because they play a critical part in provisioning, management, orchestration, and monitoring of the activities that function in the cloud environment. The accessibility and the security of cloud computing are solely dependent on the security measures in the APIs. The weak vulnerabilities of features that are usually offered from APIs, create various security risks that undermine the integrity, confidentiality, accountability, and availability of unauthorized access, and malicious activities. The API dependencies provide a lack of monitoring, logging abilities, unauthorized access, and central loss of controls. The human interactions that lead to carelessness from untrained or unknowledgeable individuals provide further damage to the technology. The lack of employee screening and hiring practices challenges the infrastructure that will lead to users having unlimited access to data in the cloud. Third party service providers rarely conduct customer background checks, and anyone has the ability to open an account with an email, and a valid credit card. Apocryphal accounts allow for cybercriminals performing any malicious attacks under anonymity. People will continue to be a significant vulnerability in cloud infrastructure because they will not be educationally aware of suppliers, service providers, end-users, and organizational customers. Cloud computing technology depends on the outsourcing of information and providers that have the ability to store data not specific to direct jurisdiction. Customers will often not be aware of where the location of their data is, and data can be stored in a shared environment where a difference in diligence to encrypt data may not be substantial. The demand for technology to be available for users to modify and customize their network needs is popular. However, there are certain aspects to the cloud infrastructure that can compromise entire government entities if steps are not taken to set out guidelines and protection against the vulnerabilities in cloud computing.

Impact

The impact of cloud computing is justified through its many threats that are postured from security threats and weaknesses that expose the vulnerabilities placed on the APIs, IAs, and cloud computing infrastructure. Although the benefits of cloud computing offer a substantial amount of advantages to the public and private sectors, the impact of the disadvantages creates a critical impact to the infrastructure. The lists of issues range in their impact, but overall are a vital concern which includes, regulatory compliance, data segregation, recovery, data locations, long term viability, user access, and investigative support. These security threats and vulnerabilities create critical barriers to service providers and cloud users in creating sustainable technologies to reach underdeveloped countries and economies. The abundant factors of the infrastructure have generated weaknesses that have decreased the proposition value of the cloud, and critically discouraged investors. Cloud computing in international communities has serious inferences of the lack of transparency, potential political corruption, and weak legal system that can exacerbate security risks even further. State nations can differ on the matter of hacking, where officials in China view hacking as an ethical practice, and even sponsored a school of hacking that is a substantial threat to security officials in the United States. Foreign cybercriminals have spurred US officials to create new protocols for privacy and security in the cloud infrastructure. The lack of trust in the cloud infrastructure places serious impact on the extent of investigative powers of illegal activities, which may be outside their jurisdiction (Brodkin, 2008). The vulnerabilities and threats that are exposed in the cloud computing systems are mainly due to the unpredictability of reliance on the internet. The technical errors made by humans, and actions of parties involve recognizing the interface risks to organizations. More importantly, these concerns impact the user's ability to acquire the correct credentials for accreditation, applications, security management, and business continuity that can lead to data loss, leakages, attacks, and breaches (NSA, 2009).

### Countermeasures

Since cloud computing faces the same challenges as other networks and infrastructures that utilize the internet, there are several ways in which countermeasures can avert the risks and threats that are manageable against cloud security. The NSA, as well as the CSA, have established numerous countermeasures that can be implemented in the cloud infrastructure. These include, "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" (Hashizume, Rosado, Fernandez-Medina, Fernandez, 2013). Other countermeasures are established in order to prevent the use of attacks that include better methods of transforming sensitive data over public cloud deployments. More importantly cloud servers require better data portability and protection from external threats. This includes, creating identity and access management guidance. In protecting hard drives that are shared to be entirely removed, that are destruction strategies, as well as creating dynamic credentials, and signatures. Encryption needs to be more dynamic and secure to protect files and other user data. Better encryptions allow for better methods in storage, acquisition of data, provisions for security and information from service providers and vendors that help in regulations dimensions and opportunities in the cloud.

According to the NSA, employees as well as providers need to adhere to a clear policy and standards on safety in internet practices in order to discourage cybercriminals. A well-documented procedure and policy should enforce the laws that govern cloud computing. The policy should be reviewed and updated consistently according to the nature of information technology. Cloud service providers must also need to sign service agreements with organizations and users that clearly define the technical control, and safeguards taken to protect user's information, data, indemnity, and other concerns in the cloud environment. Service providers will also need to define management controls, which stipulate the potential risks, and how they will be managed, assessed, and mitigated. In organizations, the need for a defined incidence response and contingency plan is critical to protecting all users in the organization.

The use of the private cloud should be protected with firewalls, and antivirus software when dealing with the exchange of sensitive information (NSA, 2009). The CSA has set up several countermeasures that help in overall attacks that include implementing, architecture and data security. Dynamic cloud architecture has the potential to offer an unsurmountable amount of benefits that will satisfy the basic mandates of IT enterprise, and allow internal systems to meld with external systems. This will provide more constant and reusable methods for interconnecting the different implications of cloud providers (MacVittie Murphy, Silva, Salchow, 2010).

The CSA proposes that countermeasures should be taken in creating architecture and data security where challenges can be handled through appropriate security assessment. This includes implementing controls for APIs, the network, and the virtual machines. Data security provides the needs for privacy enhancement tools and method that comply with legal precedents, and protection of user data. As discussed previously, there are methods that can protect against security attacks, backdoor protection, guest operating system integrity, and VM specific attacks (Ashktorab, Taghizadeh, 2012). The use of Mirage Image Management Systems helps in the overall security of the cloud, since it helps in addressing the threats to virtual machine image security which are used throughout applications in the cloud infrastructure. Mirage Image Management Systems considers the four major components, image transformation by running filters, image maintenance, access control, and provenance tracking. Countermeasures are used in client based privacy manager that helps in reducing the risks and threats associated with data loss and leakage of private sensitive data. According to Ashktorab and Taghizadeh (2012) the main features of this countermeasure include obfuscation that automatically obfuscate the fields in data structure; preference setting; data access, that allows for users to access personal information and check accuracy; feedback that manages and displays feedback for the user; and personae that allow users to choose multiple personae when in the cloud (Ashktorab, Taghizadeh, 2012). Overall creating better security guidelines, policies, agreements with service providers, and protection of data is critical in operating confidently throughout the cloud infrastructure.

## Conclusion

There are several precautions and failsafe initiatives that can be taken in order to help lessen the impact of cloud computing. This includes providing a risk management plan to deal with risks (Ryan, Ryan 1995). Implementing a no-nonsense policy on devices and technology management helps inform employees on managing authentication and other external factors for cloud computing. Creating a disaster recovery plan is another critical solution for an organization that incorporates both onsite and offsite backup plans for storage availability. Cloud computing is the next phase in the evolution of internet capabilities. It is not a new innovation, but a new architectural model that offers a more scalable, flexible, and efficient way to employ many of the same components at the same time (MacVittle et al, 2010).

Cloud computing provides for easy collaboration and accessibility to files at any location at any time. It is a recent paradigm that allows individuals and organizations of every size to share services and resources in a cost effective and seamless manner (Krisna, Varma, 2012). While there are numerous security risks, threats, and vulnerabilities to cloud computing, reliance is on providers, organizations, and others to implement satisfactory countermeasures to keep cloud computing an optimal option. The proposed countermeasures will help to keep cloud computing an evolutionary mainstay, as new applications, services, and innovations will continue to place cloud computing as an indispensable source. As hackers and cybercriminals continue to get more sophisticated and educated in their methods of hacking, officials and experts must continue to find ways to protect the cloud infrastructure to address the growing concerns. As more methods are discovered, more solutions will be provided in creating security measures to strengthen cloud computing for the users.

## References

Ashktorab, Vahid, Taghizadeh, Seyed Reza. (2012). Security Threats and Countermeasures in Cloud Computing. International Journal of Application or Innovation in Engineering & Management (IJAIEM). Vol.1, Issue 2. Retrieved from http://www.ijaiem.org/volume1Issue2/IJAIEM-2012-11-3-076.pdf

Badger, L., Grance, T., Patt-Corner, R., Voas, J. (2011). Cloud Computing Synopsis and Recommendations: Recommendations of the National Institute of Standards and Technology. *National Institute of Standards and Technology*. Retrieved from http://webtycho.umuc.edu

Brodkin, J. (2008). Gartner: Seven Cloud-Computing Security Risks. *InfoWorld.* Retrieved from http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks

E., Mathisen. (2011). Security challenges and solutions in cloud computing. *Proceedings of the 5th IEEE International Conference*. pp. 208-212.

Grobauer B, Walloschek T, Stocker E. (2011). Understanding Cloud Computing vulnerabilities. *IEEE Security Privacy*. 9(2):50-57

Jhingran, A. (2010). *IBM business analytics and cloud computing: Best practices for deploying Cognos business intelligence to the IBM cloud*. Ketchum, ID: MC Press.

Krishna, P. Radha and Kishore Indukuri Varma. (2012). Cloud Analytics A Path towards Next Generation Affordable Bi. *Infosys*. Retrieved from http://www.infosys.com/infosys-labs/publications/Documents/cloud-analytics-next-generation.pdf

Kundra, Vivek. (2010). Federal Cloud Computing Strategy. *CIO*. Retrieved from https://cio.gov/building-a-21st-century-government/cloud/

Hashizume, Keiko, Rosado, David G., Fernandez-Medina, Eduardo, Fernandez, Eduardo B. (2013). An Analysis of Security Issues for Cloud Computing. *Journal of Internet Services and Applications 2013*. Retrieved from http://www.jisajournal.com/content/4/1/5

MacVittie, Lori, Murphy, Alan, Silva, Peter, Salchow, Ken. (2010). Controlling the Cloud: Requirements for Cloud Computing. *F5 Networks*. Retrieved from http://www.f5.com/pdf/white-papers/controlling-the-cloud-wp.pdf

Owens D. (2010). Securing elasticity in the Cloud. *Commun ACM 53(6):46-51.*

Pacella, R. (2011). HACKING THE CLOUD. *Popular Science*, 278(4), 68. Retrieved from http://ehis.ebscohost.com.ezproxy.umuc.edu/eds/pdfviewer?sid=a4ec9f01-73ed-4527-8494 1b2a7df62848%40sessionmgr12&vid= 8&hid=2

Svantesson, D., & Clarke, R. (2010). Privacy and consumer risks in cloud computing. *Computer law and security review*, 26(4), 391-397. Retrieved from http://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1346&context=law_pubs

Raggert, Tom. (2010). Information as a Service (IaaS) - Service Improvement and Cost Savings. *MpHasiS*. Retrieved from http://www.mphasis.com/pdfs/WhitePapers/Iaas_Service%20improvement%20and%20cost%20saving.pdf

Samson, Tom. (2013). 9 top threats to cloud computing security. *Info World*. Retrieved from http://www.infoworld.com/t/cloud-security/9-top-threats-cloud-computing-security-213428

Ryan, D. and Ryan, J. (1995). Risk Management and Information Security. *Presented at the 11th Computer Security Applications Conference.* New Orleans, Louisiana.

Scholz, James. (2013). *Enterprise Architecture and Information Assurance: Developing a Secure Foundation*. CRC Press.

Sosinsky, Barrie. (2011). Cloud computing offers significant cost savings. *Cloud Computing Bible* p.278.

The NIST Definition of Cloud Computing. (2011). *NIST.* Retrieved from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N. (2009). Cloud Computing: A Statistics Aspect of Users. *First International Conference on Cloud Computing (CloudCom),* Beijing, China. Heidelberg: Springer Berlin. pp 347-358