American Research Journal of Business and Management
ISSN 2379-1047

Original Article
Volume 1, Issue 3, 2015

Controlling & Analyzing Risks in Cloud Computing Security

Faisal Alsalamah[1]

Graduate Student, College of Business, Organization Change Department
Hawaii Pacific University, Honolulu, Hawaii - United States

Abstract: Computer programs and services are delivered online through the ever-present Internet from mega data centers are collectively referred to as 'cloud computing'. The emergence of this form of computing has important implications for commercial and government organizations with security and data privacy being major concerns.

Despite, one important caveat is that many of the attractive features of cloud computing can be at variance with the traditional models of security and control systems associated with conventional 'desktop computing'. In this paper, a brief overview of cloud services is provided together with an analysis and discussion of the inherent security risks associated with this form of computing. In particular, six of the main potential threats to cloud computing have been considered, namely data breaches, data loss, insecure interfaces and Application Programming Interfaces (APIs), denial of service, account hijacking, and potential abuse of cloud services. These threats, the role that technology can play in combating them, and the safeguards implemented to prevent violation of cloud computing systems are highlighted. In addition, the methods available to control these risks are discussed together with the measures that organizations can implement to prepare for cloud outages.

I. INTRODUCTION

Many believe that George Favaloro, a technology executive of Compaq Computers, first invented the term "cloud computing" in 1996. However, its first use in a modern context has been attributed to the Google CEO Eric Schmidt. The reason for the recent upsurge in interest in cloud computing is because of its ability to provide flexible availability of computing power at much lower cost to large corporations. The term is a metaphor reflecting a paradigm

shift as more computer memory, processing power and applications hosted are in remote data centers, or the "cloud" (Regalado, 2011). Cloud computing simplifies the concept of the many networked computers and systems acting in unison to provide online services through the Internet.

The National Institute of Standards and Technology (NIST) has recognized the importance of cloud computing. NIST developed standards and guidelines for providing adequate security information for all cloud computing operations. Interestingly, the specified standards and guidelines do not apply to national security systems (Jansen & Grance, 2011). The development of devices such as mobile phones, tablet computers, laptop computers together with the vast array of desktop computers, has created an insatiable demand for easy to use Application Programming Interfaces (APIs) to act as conduits between these computers and Internet services. Examples of APIs specifically written to access Web-based services include Safari (web browsers) and programs to allow users to interact with popular services such as email, online banking, e-commerce, social networking (including Twitter and Facebook), and personal data services such as Apple's MobileMe. Mirroring of websites, redundant servers, and Internet-based clusters are examples of hardware-based cloud computing services. Because APIs are used to access cloud computing services, there is an inherent security danger.

In principle, any computer literate individual with an Internet connection can access data in the cloud with the inevitable security risks. Six of the main potential threats to cloud computing will be analyzed and discussed, namely data breaches, data loss, insecure interfaces and Application Programming Interfaces (APIs), denial of service, account hijacking, and potential abuse of cloud services. It is important to realize that these are by no means the only risks. Malicious insiders shared technology issues, and insufficient due diligence may also pose serious threats to data security (Simmonds et al, 2001).

[1] *Corresponding Author: fofo420@hotmail.com*

II. CHARACTERISTICS OF CLOUD COMPUTING SERVICES

Before discussing the six most important security risks of cloud data, it is perhaps useful to describe the main characteristics of cloud computing architecture and its functionality. One of the main functions is to permit on-demand self-service. Most of the users can automatically alter their computing capabilities (e.g. Network storage, server time). In other words, there is no requirement for human interaction with the service provider. A Broad network access is another important capability provided by the network and accessible through the aspect of standard mechanisms aiming at promoting usage via mobile phones, tablets, laptops, desktop computers and other devices. Resource pooling is another feature of cloud computing when the provider pools their computing facilities to serve many users through the multi-tenant model.

The users required resources are assigned and reassigned dynamically in relation to demand. The user does not usually have any control or knowledge of the precise location of resources such as processing power, memory requirements, amount of storage, or the bandwidth of the network. However, permission may be granted to specify the resource location according to the country, state or even a specific data entry, especially when there may be security issues implications. An important feature is that there should be a rapid elasticity capability meaning that computing requirements can be provisioned and released, often automatically according to demand. Thus, there is virtually no limit to the capabilities that can be provided to the user. Measured service is when cloud computer systems controls and optimizes the resource usage automatically including bandwidth, processing power, storage and the number of active user accounts. It is relatively easy to monitor and control resource utilization, and produces a detailed, transparent report for the provider and the corresponding users.

A number of service models have been developed to facilitate user interactions with cloud computing systems. One such model is the Software as a Service (SaaS) in which the consumer uses the applications of the providers running on the cloud computing infrastructure. The applications can be accessed from various client computers through the client interface as the web, or a specially developed program interface. The management and control of the underlying cloud infrastructure are transparent to the user. A second model is a Platform as a Service (PaaS). It has the permission to run their own software applications on the cloud infrastructure. The Infrastructure uses the Service (IaaS) model enables its user to configure storage, processing, network characteristics, as well as allowing them to deploy and run their own software, including operating systems and APIs. Once again, the user does not have control over the primary cloud infrastructure with a degree of control. This is over the storage, operating systems, and their own applications.

A private cloud is a computing infrastructure developed exclusively for the use of a single organization spread over several different departments to permit multiple users to access the data (Jansen & Grance, 2011). A private cloud is usually under the supervision and operation of the corresponding owner or sometimes by a third party, with its physical infrastructure present in the house or at a remote data center. In contrast, a community cloud is configured for the exclusive use of a specific group of users, often in business organizations that have concerns about data security and user conformity matters. It is self-evident that a public cloud is implemented for the use of the general public. Typically, it is managed and run by an academic, business or government organization, and hosted by the cloud provider at a remote data center. Finally, the infrastructure of a hybrid cloud is comprised of two or more discrete infrastructures such as private, community or the public that remains distinct entities, but is integrated together using standard or proprietary technology. This system facilitates the portability of both data and programs including the cloud bursting for the relative load balancing amid the clouds.

The cloud infrastructure comprises both a physical layer (the hardware) and an abstraction layer (the complex software which runs on the physical layer). The cloud infrastructure comprises the hardware and software executed to enable the cloud computing to be enacted. The nature of the physical and abstraction layer characterizes the embodiment of cloud computing. Crucially, the user has no permission in managing and controlling the primary infrastructure of the cloud but may have some limited control over their deployed applications and configuration settings for the API hosting environment (Gruschka et al, 2009).

III. DATA BREACHES

There can be no doubt that one of the major cloud computing threats is the risk of data breaches. In principle, the vast network of diverse computer systems that comprises the Internet can potentially be accessed by any computer-literate skilled hacker with malicious intent from any country in the world. Thus, cloud computing service providers and their customers can be exposed to a serious computer security threat. In 2012, more than 200 incidents of server breaches were reported that led to the loss of roughly 9 million data records (Radware, 2013).

In 2011, an attack against Sony's PlayStation Network affected the user data of more than 100 million customers. The PlayStation Network was hosted on a cloud service based on Amazon's Web Services. Sony's cloud-networks were breached because of “a SQL Injection coding error” which introduced a security weakness. It was reported that the breach seriously compromised the data of an estimated 77 million users, including personal contact details, financial information, Sony passwords, security questions and answers, and so on; truly a cloud security breach of massive proportions. The implications for the company were worldwide adverse publicity and ultimately costs of $24 billion made up mainly of lost sales. The control solution was to employ expensive specialist forensic software experts to track down the cause and eliminate it by removing the software security flaw in the network code, a very expensive undertaking.

A second major breach occurred when the cloud service provider CloudFlare was maliciously attacked in May 2012. Entry to the network was obtained by utilizing Google Gmail vulnerability. The approach of the hackers was to use a multi-layered crack-attack, which targeted specific four security flaws. CloudFlare quickly gave a detailed account of the breach for the benefit of the wider programming community. Briefly, AT&T was duped into redirecting a voicemail to a falsified voicemail box. Then, Google's software procedure for account recovery was exploited by using the fraudulent voicemail box. This exploitation enabling the hackers to obtain the Gmail account recovery personal identity number (PIN), and obtain permission to hack the account. Next, a flaw in Google's Enterprise Application recovery process enabled the hackers to bypass the two-stage authentication requirements of the CloudFlare.com user universal resource locator (Jansen & Grance, 2011).

Once the hackers had gained access to an administrative email account, CloudFlare's BCCing flaws enabled the hackers to reset the customer password. A devastatingly simple attack, which reveals the lengths that cyber criminal, will go to breach a cloud-computing network. The implications are that potential users of cloud computing networks lack faith in the safety of their data. The question remains how these breaches can be controlled and ideally eliminated. Clearly, rigorous and strict testing of the program interfaces must be implemented to control network security breaches. Personally, if anyone ran a company providing cloud services, he should employ well paid skilled hackers and use their undoubted skills to test the integrity of that company’s security systems and advertise this fact to customers. It is better to have the enemy within the company than without trying to break in.

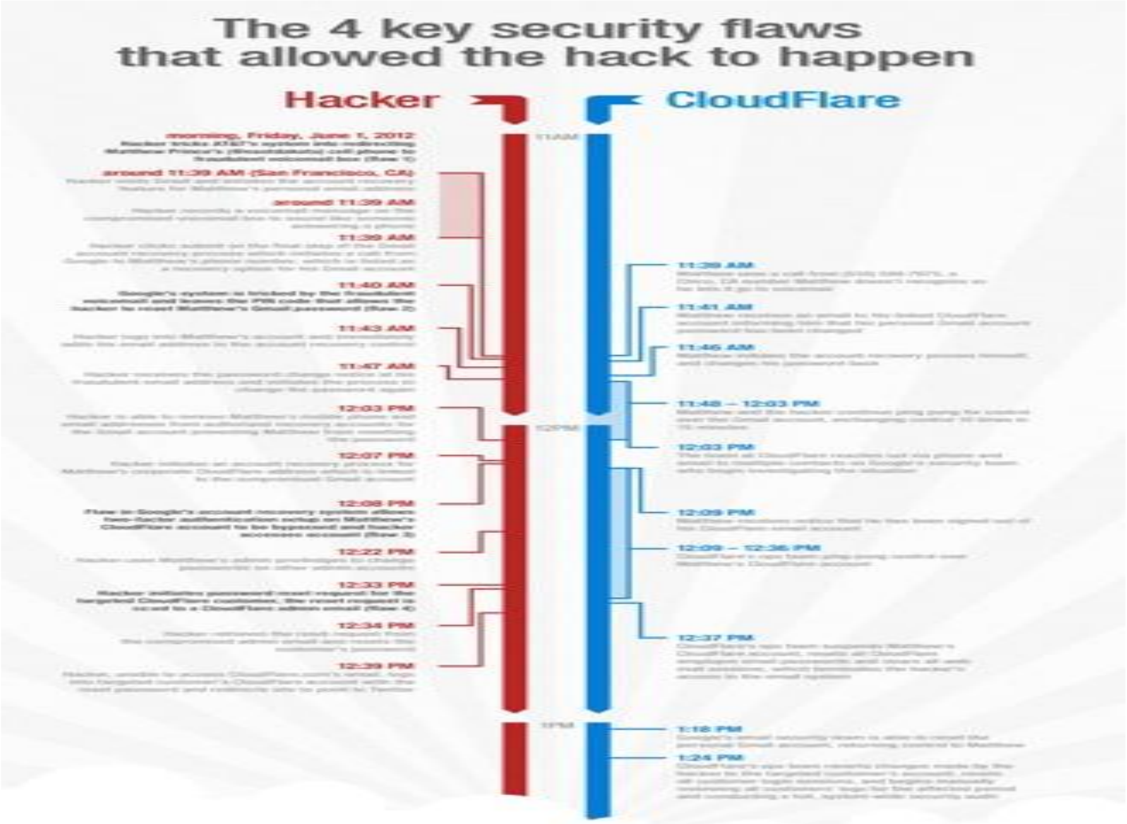

Figure1. *The four key security flaws and the sequence of events that led to the security breach of CloudFlare.*

A perhaps surprising finding is that around 40% of the reported data breaches during 2013 under the elaborate HIPAA Act, which involved the aspect of security, privacy, and breach warning regulations were shown to have been perpetrated by business associates (Sugang, 2012).

Clearly, it is very difficult to control breaches initiated by business colleagues. The United States Department of Health and Human Services is addressing this issue through the broadening of the HIPAA fine net to take account for the business associates. Interestingly, the legislation aims to hold contractors/subcontractors employed by a business associate liable for security breaches. For example, a business associate linked to an organization that holds protected health information is required to go through a strict analysis of their security measures. For HIPAA hosting providers, three tiers of security are demanded namely administrative, physical and technical security.

Administrative security includes auditing, policy implementation, careful selection of staff (after strict background checks) and their training, and, notably for HIPAA-specific requirements, associate business training. Thus, it is ironic that business associates are trained to have an intimate knowledge of the computer systems with the security consequences outlined above. Rigorous selection and monitoring of business associate computer activity seems to be the only control mechanism available because one is dealing with an 'insider'. It is self-evident that the role of physical security is to prevent unauthorized personnel from having the opportunity to access cloud servers. The aims of technical security are to provide a secure environment for data hosting. To protect cloud computer systems from unauthorized access, it is essential to implement file integrity monitoring to firewalls that oversee web-computing applications (Sugang, 2012).

It is perhaps instructive to give one example of a security breach attributed to a business associate who disregarded HIPAA regulations in 2013. The case affected the web design company ClearPoint Design. The security breach perpetrated by the business associate compromised the data of about 15,000 individuals in three different healthcare organizations. The breach came about after ClearPoint Design had leased one of the dedicated servers from the Hosting.com for hosting and monitoring online intake form for patient request services. Unfortunately, the server was breached by a hacker who cleverly altered the website code to enable a diversion of the unencrypted disbursement data to an unauthorized Gmail account and gained an administrative right to the main server containing the protected health information (PHI). In another breach, approximately 4 million confidential patient records, including clinical, diagnostic and health insurance information, were stolen from Advocate Health Care second rated as the largest HIPAA ever data breach reported following the breach notice rule implementation during 2009.

It is noteworthy that the data was stolen from the hard drives on four unencrypted computers. This was a serious security oversight as the patient data should have been stored on a secure network. To remedy this security flaw, Advocate Health Care retrospectively implemented mapping of its software systems and computer framework to identify accurately where patient data was stored on their system, and additional security measures implemented. This approach should be the first step in the data encryption process and includes identifying and classifying sensitive data followed by the deployment of a secure encryption algorithm. An important control, which should be implemented to safeguard data on a secure network, is the utilization of disk-level encryption and storage space spot network. This system automatically encrypts the data virtually simultaneously as it is written to a hard disk. Encryption of the stored data or data routed through the network should be obligatory to meet the set standards of the HIPAA for relative encryption of the ePHI (Sugang, 2012). This procedure should be carried out under all circumstances when data is being stored or archived into backup files.

Ideally, when dealing with sensitive PHI data, an enterprise-class private cloud should be used this is exclusively dedicated to the particular organization processing the data. Under no circumstances should sharing of resources be permitted with an outside agency. Such a system is an ultra-secure system because the data are captive within the organization but do not overlook the security risk of rogue business associates. All HIPAA clouds-hosting providers should offer an encryption service that includes encrypted off-site backup for additional data security. That is to safeguard against catastrophic damage to the cloud hosting data center such as fire, cyber criminal activity or indeed terrorist activity. Without encryption, unauthorized personnel may potentially access sensitive data with potentially disastrous consequences.

It is important to realize that there is now a legal requirement under the infringe notice rule of HIPAA publicly to notify any breach affecting the sensitive data of more than 500 people. Nevertheless, remember that encryption alone cannot provide total protection of data. Ideally, a multi-layered layered security approach should be implemented with other data security tools deployed including daily or hourly log reviews, file integrity monitoring, a web application firewall, along with other optional technical security measures. At the administrative level, further measures can be adopted at the outset. The HIPAA host's audit reports should be inspected to determine that they have undergone additions to the modern OCR HIPAA audit program protocol. Ensure that IT services meet the compliant security values of HIPAA and that employees are suitably trained and aware of the importance of security issues. Finally, if a hosting service will not permit the review of the business associate agreement then under no circumstances use this cloud host. (Radware, 2013).

Unfortunately, it is highly probable that more and more breaches will occur as the ever-increasing number of dissident hacking communities carry out sophisticated attacks against vulnerable cloud-computing networks. Though, organizations serious about data security should deploy the appropriate measures.

IV. DATA LOSS

A serious threat posed to cloud computing service networks is the potential to lose vital data. The majority of computer users will have lost a small amount of vital data at some time, whether it was an essay due to be handed into a tutor, irreplaceable sentimental photographs or that great novel you had started. No doubt some busybody informed a computer user in hindsight that he should always back up your data – not very helpful! However, consider the incredible volume of data handled by cloud computing service providers to understand the potential for data loss. When data stored on cloud servers is of a sensitive personal nature or commercially important, then the owner is naturally being wary of this threat having entrusted the integrity of their data to the care of the service provider. Inevitably, there are many ways in which data transmitted to cloud computing hosts can be lost including corruption in the network, accidental deletions or as a result of malicious intent.

Data loss is considered to be one of the most important security threats to cloud computing. Verizon has reports that corporations lost approximately 1.1 billion records during the last four years and lost circa 44 million records so far in 2013. An important distinction needs to be made between a data breach and data loss. In a data breach, a hacker is deliberately trying to gain access to confidential data with malicious intent. However, data loss, as mentioned briefly above, can be caused by accidental deletions or unexpected corruption. A security risk that is very difficult to guard against is when a rogue employee downloads confidential information directly from a corresponding cloud to one of the unsecured devices, such as a USB stick, and literally 'walks out the door' of the data center (Grueter, 2013).

Grueter (2013) recommends some of the vital strategies of protection against unintentional or malicious data loss by employees. With significance is the need to educate employees concerning the risks attached to data loss with the duty to safeguard it? The use of docTrackr will give a excellent company control of data security even if the data has been stolen. Furthermore, if the data surfaces in the wrong hands, a company should determine the source of the leak retrospectively.

V. INSECURE INTERFACES AND APIS

Software developers are given strict specifications when they write APIs that will communicate directly with cloud computing services. Poorly coded APIs can provide an entry for hackers into a cloud computer system, which may lead to serious data breaches that are damaging to the service provider systems and client data, and can ultimately be very costly. Thus, API coding should be taken very seriously from the outset, as an API can be a critical weakness in web cloud security services. An API can act like a 'Trojan Horse' to provide a gateway for cyber criminals to gain illicit access to computer systems and confidential data. It is good practice to ensure that APIs are open only to users with an authorized key. Hackers use a number of mechanisms to infiltrate a provider's service using the APA. Insecure APIs can be vulnerable to persistent attack from a distributed denial of service (DDOS) attacks (infra video), blocking the gateway through which data from a Web service is routed. SQL script injections may be used to re-route or copy user data to off-site servers operated by cybercriminals (Aboukhadijeh, 2013).

In 2008, a poorly coded API was responsible for a security breach to MySpace-Yahoo services when the hacker was able to peruse private celebrity photographs. It has been reported that the HTML5 Fullscreen API has been used to mimic a legitimate Bank of America financial transactions site, and other APIs can mimic an entire website luring in unsuspecting user to give personal and financial details. These two examples illustrate the obvious malicious outcomes of insecure APIs. Another outcome of poorly crafted APIs is the perception of poor quality, insecure service provided by the service host, which comes about because of the rapid dissemination of adverse publicity, which in turn undermines customer confidence in a site. Because API interfaces afford ways for different systems programs to communicate, it is vital that their security is 100% guaranteed with security loopholes eliminated (Aboukhadijeh, 2013).

There are three stages involved in developing a secure API namely planning, testing, and checking the API after it has deployed. When constructing an API flow chart, the most important questions to ask are what are the important factors involved in deciding the nature of access controls to data and the architecture for functional security. These questions have been considered in detail by government agencies and are reproduced below

- Who should be allowed to access the API and, therefore, the data?
- What information should the API grant access?
- Should the access be read–only, read/write, or write–only?

To answer all of these questions, many opinions have to be carefully considered, and appropriate safeguards implemented to safeguard computer systems and networks. If the API is deployed for the exclusive use of internal personnel, then the methods used to establish the intranet (firewall, gateway, network settings) can be used. When the general public will use the API, network controllers must ensure that the API can only access the designated services. Authentication can serve roles quite distinct from security, but its main function is to allow the API developer to regulate API users. If only a limited number of public users are permitted to access the API, then authentication procedures such as OAuth and API keys can be deployed to regulate access. Even if general public access to use the API is granted, the authentication protocols allow the API manager to regulate usage so that they can rapidly detach malicious users from the network. It is imperative that API developers implement the permissions needed for each particular use. Security is at its strongest when read-only permission levels are set for data access, with permission levels locked. In other circumstances, an API may be deployed to collect submissions when write-only or read-write permission may be necessary. In this case, the API should be custom written so that users can submit and edit only their data (Gruschka et al, 2009).

Government agencies employ a designated cyber security team to oversee security and thus protect important cloud servers holding data of national importance. It is interesting to note that API and Web security can be implemented using the virtually identical methodology to secure servers and the websites they host. The same technology is often utilized to empower websites and APIs (APIs and URLS being used in a similar fashion), with information being requested, an action performed, and the appropriate data returned as per the request. It should be remembered that web pages are designed for ease of human interpretation whereas APIs are designed for computer program interactions; however, the underlying security focus to protect data is for all intents and purposes identical. Thus, commonly used network security checks are also applicable in monitoring APIs (Gruschka et al, 2009).

Security controllers will endeavor to make sure that well-established, secure protocols are deployed on the network. They will also carry out secure code reviews from time to time, in particular by checking the API code for vulnerabilities that may have ‘slipped through’ the network of controls. Another standard practice to ensure that the security of a network is to check regularly by conducting automatic vulnerability scans and closely scrutinizes the results. In particular, a new API on the network should ring alarm bells and similarly scrutinized with great diligence (Gruschka et al, 2009).

VI. DENIAL OF SERVICE

Although at first sight denial of services (DoS) seems to be a inconvenient temporary inability to access data, it is a major threat to cloud computing networks in its most insidious guise. Although the integrity of data stored on the cloud computing host’s servers is maintained, DoS can temporarily deny legitimate users access to vital data, which can have under certain circumstances grave consequences. DoS is perhaps the malicious hackers favorite means to disrupt cloud server functions and is a common form of attack. The basis of a DoS usually results from a hacker overloading the network with many spurious, invalid requests to the host servers. As a result, the host channels all of its resources in a futile attempt to respond to the invalid requests at the expense of valid requests from legitimate users. The consequences of DoS can involve system crashes, serious data loss, and many angry telephone calls from frustrated users demanding to know when the integrity of the network will be restored as they cannot carry out for example, important time dependent online banking transactions, which may lead to them incurring bank charges (Sugang, 2012).

The hacker can target an individual computer or an entire commercial network with a DoS attack using a number of well-known strategies. One favorite method is a SYN flood where the intention is to overwhelm the host by sending TCP connection requests a faster rate than the computer can process them, called TCP SYN packets. The attacker aims to create a random source address for each of the packets with the SYN flag set in each packet to open a new connection to the server from the false IP address. The code demands that the server responds to the request and waits for confirmation that never arrives. With repeated requests, the server connection table is rapidly filled at which point all new connections, including legitimate requests, are ignored. When the attack ceases, the server resumes its normal activity as SYN attacks rarely crash its operating system. Newer server operating systems are designed to negate such table attacks, but they can still be vulnerable (Radware, 2013). Defensive measures available to control these attacks include the use of micro blocks, SYN cookies, RS cookies, and stack tweaking.

Another favoured method of attack is known in programming parlance as the ‘Ping of Death.' The approach of the hacker is to transmit IP packets that are designed to crush the TCP/IP stack of the operating systems running on many computer systems, by exceeding the maximum permissible length of 64 Kbytes. On older Windows 95 and Windows NT computers, WinNuke attacks can disable the network. It is fair to say that a distributed Dos (DDoS) attack has the greatest impact on computer systems made ‘famous’ by the DDoS attack against Facebook, Twitter, and other social media sites; all users of these sites were equally affected. Effectively, hundreds of millions of users were prevented from online communications by a single targeted DDoS attack (Radware, 2013). This clearly highlights the risks of a DDoS attack on government agencies and business corporations computer systems. To control against such attacks, various software tools are available to test the network IPS and firewalls for DoS weaknesses. Programs have been developed, such as idappcom’s Traffic IQ Professional that allows the abused user to respond to the controlled attacks of their own.

DoS testing is perhaps one of the most difficult security checks to instigate. A search for DoS vulnerabilities can be implemented using vulnerability scanners such as QualysGuard and webInspect. These programs can help identify configuration weaknesses that DoS programs can exploit. While it is difficult to predict when a DoS attack will occur, a number of processes can be deployed as countermeasures against such malicious attacks. It is very important to test and apply security patches (including service packs and firmware updates) as soon as they become available for network hosts, such as routers and firewalls, as well as for the operating systems of servers and workstations. It would also be prudent to use an Intrusion Prevention System (IPS) to monitor regularly for all forms of potential DoS attacks. IPSs were originally developed for resolving the ambiguities present in the passive network monitoring through the placement of a detection system in-line. IPSs are a great improvement upon firewall security technology, which determines computer access based solely on IP or port addresses because they analyze the actual content of the application program for malicious code. DefensePro IPS NBA offers advanced intrusion detection and prevention capabilities against DoS, providing maximum protection for applications, hosts, and network components. In addition, it contains several different applications-level protection features that prevent attempts by other malicious code to disrupt computer systems. A network analyzer should also be deployed in continuous capture mode to monitor for DoS attacks (Radware, 2013).

In the future, it is highly probable that skilled cyber criminals will develop new and ingenious methods of DoS attack of increasing complexity. These attacks will become more and more difficult to detect early, and sophisticated measures will need to be developed to prevent damage to the integrity of the cloud network. The implications for all cloud-hosting providers are the requirement to protect their network and its user's data from hackers with malicious or criminal intent effectively. Control prevention systems to prevent network intrusion by these cyber criminals should always try and anticipate the next threat. An effective prevention system, based on adaptive behavioural-based and signature based technologies, is the IPS and network security solutions developed by. It provides corporations and government agencies with effective network intrusion prevention and DoS protection systems. It is self-evident that network controllers should take great pains to identify all traffic that is necessary for approved network usage and deny access to all other activity (Radware, 2013).

VII. Account Hijacking

Another serious threat to cloud computing hosts is the hijacking of user accounts and data. In part, this threat arises because authorized company personnel are routinely permitted to access remote data on the cloud using a variety of mobile devices or remote computers when working from home, for example. The potential for hijacking exists because most remote computers, mobile phones, tablets, etc., will not have comparable security mechanisms enacted compared to those present on the workstation computers in their place of employment (Sugang, 2012).

Previously, hackers required considerable computing skills to hijack accounts and sensitive information stored on a cloud computer network. Unfortunately, a number of specialist hijacking programs freely available on the Internet that provide specifically designed tools to allow less able cyber criminals to hijack computer networks. Firesheep is one such hijacking program which requires only a modicum of technical knowledge to access illegally account information on cloud computing systems including very confidential financial and medical data. So, what controls can a provider put in place to ensure that strict secure browsing and cloud data protection is enabled on its network?

One approach is to deploy Blacksheep, which is a Firefox plugin designed to detect the hijacking of account information by Firesheep. BlackSheep was programmed to send ‘fake’ ID information throughout a network and then to monitor subsequent activity to determine whether it had been hijacked. Firesheep remains largely passive until it identifies targeted domain session information. When this data is received, Firesheep then sends a request to the similar domain through the session information hijacked to access the name/address of the hijacked user together with the profile of the individual, if possible. It is the perspective of the request that BlackSheep identifies to enable the detection of the Firesheep presence on the network. If Firesheep code is detected, the vulnerable user will be receiving a terse warning message (Sugang, 2012).

Nonetheless, the implication for the host provider is that hijacking has been a ‘honey pot’ target for hackers simply to exercise their skills for as long as networks have existed. The implication for companies hosting remote computer services is security, security and more security. Web sites consider the application of SSL connections in the preliminary login pages with a reverse to the non-encrypted traffic for the succeeding communication. In that perspective involving the user’s accessibility password and the username under protection, once there is an authentication, the users on the similar network can successfully access the network traffic. This also involves obtaining of the session ID of the user and hijacking their session on the specified website. With the situation always treated as one of the stern risks, especially specified on some of the insecure networks including public WIFI hotspots. At some point, a relative degree of technical understanding was necessary for accomplishing the specified attack (Sugang, 2012).

Firesheep accesses the specified attacks to the corresponding masses as it turns the session of hijacking into the click and point exercise. Unless the website’s commands the SSL for traffic on the site, the hijacking process will constantly remain as the relative threat. The BlackSheep is applicable in determining whether someone has activated and running Firesheep on a similar network. Security approaches to take are to manage login credentials with a single password and apply two-factor authentication for sensitive accounts (Sugang, 2012). The application of the specified solutions enables the prevention of the susceptible account information with a corresponding protection of cloud data deemed to accessibility by the wrong people.

VIII. Abuse of Cloud Services

Cloud computing provides organizations with powerful data sharing capabilities and the ability for personnel to work together effectively on team projects. Unfortunately, the abuse of cloud computing services by sophisticated cyber criminals presents a significant threat to data security. The great advantage of cloud computing service companies for the hackers is that they give them access to powerful computing systems, which they can use for illicit gain or simply malicious intent. It is particularly useful to allow them to send malicious files to thousands or even hundreds of millions of unsuspecting users worldwide. By modifying and utilizing the network code, the hackers can hide their identity and physical location behind a subscriber account they covertly infiltrated (Gruschka et al, 2009).

A good example of this form of abuse of cloud services were documented recently. The hackers known as the Chinese Advanced Persistent Threat group enticed unsuspecting users of Dropbox and Wordpress into malware download from the specified Dropbox account that contained deliberately harmful information. The hackers used an email notification device programmed in the Wordpress and the Dropbox to target The New York Times and spread malicious emails to many individuals. The first phase of the attack was to upload malicious files to a free Dropbox account and then sent links to the binaries, using email, to the target users. The malicious content was delivered using a technique that was not detected by the security systems deployed. The malicious software when viewed by an unsuspecting user exploited vulnerabilities in the targeted computer system software and displayed a ‘legitimate’ file to allay suspicion. Once the malicious file infected the computer network, the next phase of the attack was initiated. The file then interrogated a WordPress blog and retrieved command and control information and then the world was their oyster (Gruschka et al, 2009).

IX. Implication and Control

This is a very difficult form of attack to protect users against because it involves well-known brand names where security is assumed to be locked tight by customers. The best advice is that great caution should be exercised before deciding to progress with the downloading of files from any of the specified cloud services, even those with a previously admirable security reputation such as Dropbox (Gruschka et al, 2009). Even today, security vigilance must be maintained as two of the great names in computing namely Apple and Google announced vulnerabilities in their systems despite having unlimited resources to recruit the best programmers. Apple has just released a supplemental update of OS X v10.8.5. The update addresses the vulnerability in the Directory Services, which could allow an attacker to bypass password validation and it is recommended to update the operating system as soon as possible. Similarly, a recent release of Google Chrome 30.0.1599.66 fixes 50 vulnerabilities, the most severe of which has been rated as high by Google and all users of Chrome are recommended to upgrade to this version as soon as possible (Gruschka et al, 2009).

X. CONCLUSION

In recent years, there has been a major growth in the uptake of cloud computing services, but users should be very wary of the risks associated with this technology before adopting it to store their precious data. If this form of computing is to become mainstream, it must seriously address the top 6 threats to cloud computer services highlighted in this paper.

There can be no doubt that sharing computer resources among different organizations will pose a risk to data security. Cloud computing represents a revolution in computing resource deployment compared to Web 1. It is important to maintain an acute awareness of the threats to the security of the data held by cloud service providers. It will be imperative to continue the development of strongly constructed responses to repel the efforts of the most persistent cyber criminals to encourage the further use of cloud computing by big business and government agencies.

REFERENCES

[1] Aboukhadijeh, F. (2012). Using the HTML5 Fullscreen API for Phishing Attacks. http://feross.org/html5-fullscreen-api-attack/

[2] Grueter, E. (2013). Share Files In The Cloud? Read The Year's Top 4 Cloud Threats.

http://www.doctrackr.com/blog/bid/321477/Share-Files-In-The-Cloud-Read-The-Year-s Top-4-Cloud-Threats.

[3] Gruschka, N., Iacono, L., Jensen, M., & Schwenk, J. (2009). On Technical Security Issues in Cloud Computing. IEEE International Conference on Cloud Computing. 109-116.

[4] Jansen, W., & Grance, T. (2011). National Institute of Standards and Technology (NIST), U.S.

[5] Department of Commerce. Guidelines on Security and Privacy in Public Cloud Computing. Special Publication 800-144, 1-70.

[6] Radware. (2013). Intrusion Prevention Systems. http://www.radware.com

[7] Regalado, A. (2011). Who coined the term "Cloud Computing"? Technology Review

http://www.thebusinesstechnologyforum.com/2011/10/who-coined-the-term-cloud-computing/

[8] Simmonds, P., Rezek, C, & Reed, A. (2001). Security Guidance for Critical Areas of Focus in Cloud Computing v3.0. http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[9] Sugang, M. (2012). A Review on Cloud Computing Development. Journal of Networks, 7(2), 305-310. doi:10.4304/jnw.7.2.305-310