SURVEY ON CLOUD COMPUTING VULNERABILITY AND CYBER ATTACKS: A DEFENSIVE APPROACH

YUCEL TUREL

Polish Japanese Institute of Information Technology,
Koszykowa 86, 02-008 Warsaw, Poland
yturel@pjwstk.edu.pl, tyucel1@hotmail.com

(Received 5 January 2013; revised manuscript received 20 February 2013)

Abstract: Cyber attacks against cloud computing discourage users to migrate to cloud computing. Cloud computing currently has weaknesses in terms of securing data. Unprotected data and weak storage security are potential threats to cloud computing. There are security risks and they should be considered carefully before enterprises migrate to cloud computing. Specifying cloud computing vulnerabilities and defining cyber attacks against infrastructure of the Cloud are the targets of this research. Mitigation of the non-technical problems may decrease the security problems. However, cryptographics, distributed denial of service and flooding attacks damage the servers and services. In this research, my aim is to demonstrate cloud computing vulnerability and the threats against data and storage. Once the cloud security problems are defined, the next step is to look for a solution. Using forensic methods to inspect intrusion attempts, implementing an online forensic workstation monitoring the login details of cloud authentication server, providing evidence of cyber crime are recommended.

Keywords: cloud computing, security, IaaS, PaaS, SaaS, forensic, encryption

1. Introduction

Cloud computing describes the use of a collection of services, applications, information, and infrastructure comprising of pools of computer, network, information, and storage resources.

Cloud computing provides many advantages for businesses such as elasticity of resources, decrease in need for large upfront investments (on infrastructure) and reduction in cost of ownership (at least in theory).

Nowadays, it is very common for enterprises to migrate to cloud from their in-house server farms. The main reason for this is that cloud computing offers virtual platforms based on pay-per-use to provide scalable access to data and applications. Thus, there is no physical infrastructure that users can reach but virtual environment that they can access via internet. Scalability and elasticity of the services are the major advantages for end-users. Using cloud computing, the users cut their costs in terms of upgrading hardware and software, allocating space for the server farm, employing administrators and IT technicians. Cloud computing provides Infrastructure as a service **IaaS**, Platform as a service **PaaS** and Applications as a service **SaaS**.

One of the main challenges of cloud computing is security and trust. Security is a big issue for the cloud clients as they have to ensure that their confidential data are secure and only accessible by them. Cloud computing has security weaknesses. Security issues in cloud computing depend on various factors such as jurisdictions, service level agreement, authentication, data and storage security. Single security design cannot solve the cloud computing security problem; traditional and new technologies must be merged for protecting the total cloud computing integrity. There are severe threats like Ddos attacks against cloud computing. Insider attacks should also be considered and necessary steps should be taken, to prevent and stop this type of attacks. Some questions arise on the customer side: How could customers ensure that the cloud providers serving them have taken necessary action with regard to regulatory compliance, security? How could the confidentiality of the business critical data be maintained by the service provider? Basic tasks, such as applying patches and configuring firewalls, can become the responsibility of the cloud service provider, not the user. Who is liable for any possible errors? How can customer's loss be compensated? In addition, there is the risk of vendor lock. How feasible is it to bring the solution back in-house if things go wrong on the Cloud?

As a result of globalisation, the free movement of individuals and the widespread use of ICT (information and communication technology), there are a wide number of scenarios on the intersection between cybercrime jurisdiction and the ubiquity of cloud computing services that raise confronting legal and policy issues.

Data travelling in different jurisdiction and geographical distribution of cloud services always need more research and investigation on legal complications. The concept of jurisdiction varies from one country to another, and its scope relies very much upon the tradition of a legal system and its approach by local courts and tribunals. Cross border data travelling has possible advantages and some disadvantages. Customers can choose the location of data to be stored from the provider's options. This can cut costs but brings some disadvantage such as slowing routing capabilities. This results in lack of performance especially when making distinctions between the traffic on multiple routes. Security, confidentiality and trust are the main key elements from the user's point of view. Thus, I will check some of the recent attacks and identify weaknesses of the systems, evaluate the threats against Cloud platform and provide a subjective ranking of the threats.

In this paper cloud computing security weaknesses, threats and proposed solution to analyse virtual disks are investigated. Monitoring cloud traffic using forensic methods is the main focus. Digital Forensics methods help to collect evidence after malicious intruders penetrate into the systems. The system can be hold idle for a long time, or the data can be stolen, changed or deleted. In section 5.1 I summarise the new methodology briefly.

2. Cloud configuration

IaaS, PaaS and SaaS are the services mainly provided by cloud computing (see Figure 1), and are described below:

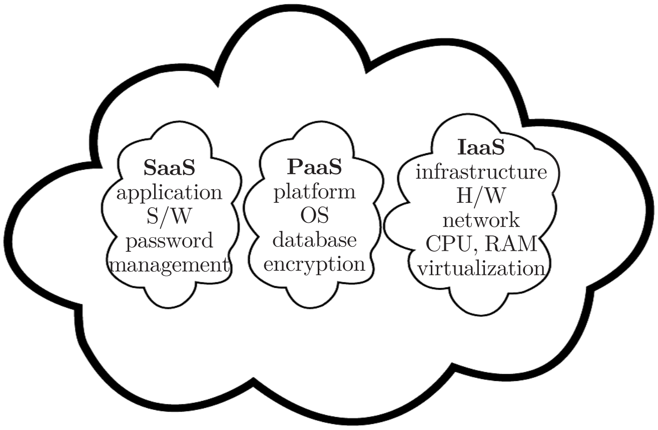

Figure 1. Cloud configuration basics

IaaS (Infrastructure as a Service): it is the delivery of computer infrastructure (typically a platform virtualization environment) as a service. Rather than purchasing servers, software, data center space or network equipment, clients buy those resources as a fully outsourced service.

It focuses on managing virtual machines, and the risks are little different than with other cloud types, the main risk is malicious user or forgery of services. IaaS requires governance and usage monitoring.

PaaS (Platform as a Service): it is the delivery of a computing platform and solution stack as a service. It facilitates the deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers. At this level data encryption takes place and PaaS can be inherently secure, but the risk is the slow system performance. Still, any solution implemented should manage the connection to the cloud service and automatically encrypt 'confidential user' data such as home addresses, social security numbers or even medical records.

SaaS (Software as a Service): it is a model of software deployment whereby a provider licenses an application to customers for use as a service on demand. It delivers applications to the end users. At this level, authentication and password management take place. The main risk is likely to stem from multiple passwords accessing applications [1].

Cloud computing consist of different layers which are accessible by users. Cloud layers as seen in Figure 2, start with network layer at the bottom and go up to the top layer 7 entitled as application software. These layers interact with each other to provide next layer service.

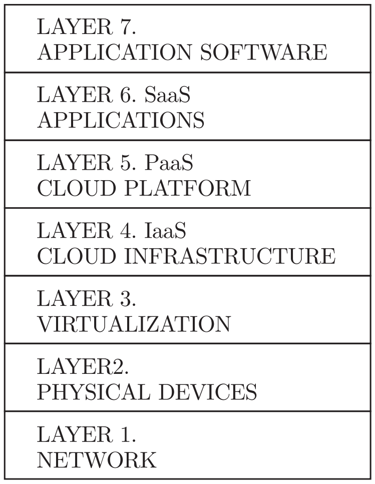

Figure 2. Cloud layers

1. **Network layer:** Network protocols such as TCP/IP and domain name server, including switching and routing principles are provided. Mainly, ISP (Internet service provider) connections are observed at this level.
2. **Physical devices:** Hardware, router, firewall, *etc.*
3. **Virtualisation layer:** It enables user request for computing resources by accessing virtual machines.
4. **Cloud Infrastructure:** Servers, workstations, memory provided to end users.
5. **PaaS layer:** It provides operating system and system settings for applications.
6. **Application layer:** It is the most important for users to access and operate smootly software and applications.
7. **Application software:** Computer software used by customers.

2.1. Virtualisation

Cloud computing is defined as a pool of virtualized computer resources. Virtualisation provide more efficient use of the hardware resources as it is shown in Figure 3. It helps to install operating system and software directly on physical hardware via vmware. Vmware can be easily moved, copied between host servers to optimize hardware resource utilization. Virtualization provides possibility to add new services without investing in new infrastructures, training new personnel or licensing new software. Virtual storage is also offered to end users [2].

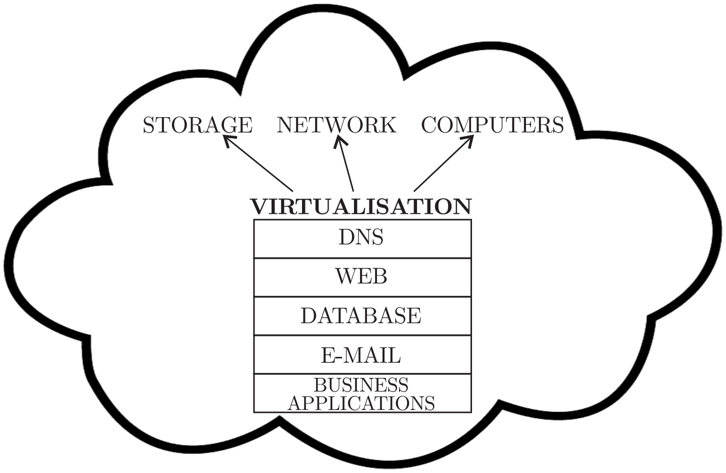

Figure 3. Cloud virtualisation

In cloud, virtual machine is created by a hypervisor or virtual machine monitor (VMM) which is a piece of computer software or hardware. Thus, cloud computing uses hypervisor to manage virtual devices. A computer on which a hypervisor is running one or more virtual machines is defined as a *host machine*. Each virtual machine is called a guest machine. The hypervisor presents the guest operating systems with a virtual operating platform and manages the execution of the guest operating systems. Multiple instances of a variety of operating systems may share the virtualized hardware resources [3].

The hypervisor lets us show the same application on lots of systems without having physically copy that application onto each system. Because of the hypervisor architecture, it can load any (or many) different operating system as though it were just another application. Therefore, the hypervisor is a very practical way of getting things virtualised quickly and efficiently [3].

3. Data protection in the cloud

Storage management is extremely important in cloud computing. To avoid losses, the cloud system must provide data protection. If loss does occur, the environment must be able to recover the data quickly in order to restore access to the cloud services.

Data protection is vital whether the cloud environment is private, public or hybrid. When outsourcing applications, a company should never assume that the cloud service provider includes storage management, data protection or disaster recovery among its services. It is therefore important to ensure from the very beginning that the provider delivers the necessary data storage and protection services, and is familiar with the technologies and products used for storage management in the cloud.

3.1. What is cloud storage?

Cloud storage offers uploading data, applications, documents, photos, videos, games and so on to a shared pool. These documents can then be accessed from any location over the internet or any type of device (desktop, laptop, mobile phone, tablet, *etc.*) regardless of the actual physical location of data. For example, Amazon 'Dropbox' is the virtual storage of Amazon cloud.

3.2. What types of the encryption methodology does cloud storage provider offer?

A cloud storage provider might store the data in an encrypted form and keep the key in a safe and secure location. When a user introduces username and password to log into the service storage provider will decrypt files so that user can access them. This means that user can invite other people to log in and view his files because the storage provider manages the encryption.

Data can be encrypted by user via web browser, so it is being sent between user and the cloud storage provider, it cannot be read or modified along the way. If users are using a web browser they will see a padlock symbol and the URL will start with '`https://`'. Once the files are received by the cloud provider they will be decrypted so if user want their files stored in an encrypted form they should encrypt them before user send them or use a cloud storage provider who encrypts them on your behalf. But what if the user forgets about the encryption key?

3.3. Security weaknesses in cloud computing

Security experts at the Fraunhofer Institute for Secure Information Technology (SIT) in Darmstadt, Germany have discovered that numerous cloud storage service providers do not check the e-mail addresses provided during the registration process. This fact in combination with functions provided by these service providers, such as file sharing or integrated notifications, result in various possibilities for attacks [4]. For example, attackers can bring malware into circulation or spy out confidential data from cloud environment [5].

Fraunhofer SIT informed the affected service providers many months ago. Although these weaknesses can be removed with very simple and well-known methods, such as sending an e-mail with an activation link, not all of them are convinced that there is a need for action [4]. Consumers who use the affected services should be careful. Those who receive a request to download data from the cloud or upload data to it should send an e-mail to the supposed requestor to verify whether the request was really sent by them [4].

3.4. What makes the cloud so vulnerable

Vulnerability is an important risk factor. The success rate of threats against cloud computing depends on the system's strength to resist the attack. Networks aren't isolated anymore. Once the Internet is there, customer networks become connected with public infrastructure, and cloud providers are given services.

Cloud computing's core technologies, web applications, databases, virtualisation and cryptography have vulnerabilities such as virtual machine escape, session hijacking and insecure cryptographic algorithms.

The biggest weaknesses of the cloud, however, are basic issues that are often easily resolved. Weak authentication protocols, an open management port, or the need to manage cloud resources remotely are all reasons why the cloud can become vulnerable. Hackers are recognizing all of these open ports, and starting to use them.

4. Cloud computing threats

4.1. Non-technical cyber security threats

To study non-technical threats to cloud computing, it is needed to provide risk factors for the enterprises. This list of threats will provide wider knowledge and educate users on the reality of cyber threats [6]. We identify the following threats:

- **Poor Passwords:** implementing a policy on strong user passwords is critical to data protection. It is especially important for users with access to the most sensitive information. Modern password-cracking programs can easily break weak passwords, such as those containing common words or word groups found in a dictionary.
- **Physical Security:** physical security is essential to preventing unauthorized access to sensitive data as well as protecting an organization's personnel and resources. An effective physical security system is an integral part of a comprehensive security program. Physical safety measures include securing access to dedicated computers, server rooms, routers, printers, and any areas that process or store sensitive data.
- **Insufficient Backup and Recovery:** lack of a robust data backup and recovery solution puts an organization's data at risk and undermines the effectiveness of its IT operations. Data and system recovery capabilities allow an organization to reduce the risk of damage associated with a data breach. It is essential to conduct routine backups of critical data and store backup media in a safe and secure manner.
- **Improper Destruction:** paper documents, such as reports and catalogs, may contain sensitive data. Unless these documents are destroyed properly (for example, by shredding or incinerating), they may be salvaged and misused. Discarded electronic devices, such as computers or portable drives, that have been used in processing and storing sensitive data, remain vulnerable unless the data are erased properly. A data breach can occur if recovery tools are used to extract improperly erased or overwritten data [6].

To identify cloud computing top threats for 2013, Cloud Security Alliance (CSA) conducted a survey of industry experts to compile professional opinion on the greatest vulnarebilities within cloud computing. Experts identified the following critical threats to cloud security [7].

4.2. Insecure interfaces and APIs

Cloud computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. The security and availability of general cloud services is dependent upon the security of these APIs. These interface must protect against both accidental and malicious attempts, otherwise data breaches and data losses are inevitable.

4.3. Cryptographic attacks

There are three common cryptanalytic attacks. Each of them assumes that the cryptanalyst has complete knowledge of the encryption algorithm used.

4.3.1. Ciphertext-only attack

The cryptanalyst has the ciphertext of several messages, all of which have been encrypted using the same encryption algorithm. The cryptanalyst's job is to recover the plaintext of as many messages as possible, or better yet to deduce the key (or keys) used to encrypt the messages, in order to decrypt other messages encrypted with the same keys.

Given: $C_1 = E_k(P_1)$, $C_2 = E_k(P_2)$, …, $C_i = E_k(P_i)$
Deduce: Either P_1, P_2, …, P_i; k; *or an algorithm to infer* $P_i + 1$
from $C_i + 1 = E_k(P_i + 1)$

4.3.2. Known-plaintext attack

The cryptanalyst has access not only to the ciphertext of several messages, but also to the plaintext of those messages. His job is to deduce the key (or keys) used to encrypt the messages or an algorithm to decrypt any new messages encrypted with the same key (or keys).

Given: P_1, $C_1 = E_k(P_1)$, P_2, $C_2 = E_k(P_2)$, …, P_i, $C_i = E_k(P_i)$
Deduce: Either k, *or an algorithm to infer* $P_i + 1$ *from* $C_i + 1 = E_k(P_i + 1)$

4.3.3. Chosen-plaintext attack

The cryptanalyst not only has access to the ciphertext and associated plaintext for several messages, but he also chooses the plaintext that gets encrypted. This is more powerful than a known-plaintext attack, because the cryptanalyst can choose specific plaintext blocks to encrypt, ones that might yield more information about the key. His job is to deduce the key (or keys) used to encrypt the messages or an algorithm to decrypt any new messages encrypted with the same key (or keys).

Given: P_1, $C_1 = E_k(P_1)$, P_2, $C_2 = E_k(P_2)$, …, P_i, $C_i = E_k(P_i)$,
where the cryptanalyst gets to choose P_1, P_2, …, P_i
Deduce: Either k, *or an algorithm to infer* $P_i + 1$ *from* $C_i + 1 = E_k(P_i + 1)$. [8]

4.4. DoS/DDoS attack

The rapid development of the Internet over the past decade appeared to have facilitated an increase in the incidents of online attacks. A DoS (Denial of

Service) attack is a type of attack focusing on cutting availability. Such an attack can take many shapes, ranging from an attack on the physical IT environment to the overloading of network connection capacity, or through exploiting application's weaknesses. A DoS attack involves using one computer or internet connection to flood a server with packets (TCP/UDP). The objective of this attack is to 'overload' the server's bandwidth, and other resources, so that anyone who may be trying to gain access to the server is not served, hence the term 'denial of service' is used. A DDoS (Distributed Denial of Service) attack is almost the same as a DoS attack, but the results of the DDoS attacks are massively destructive. As the name suggests, the DDoS attack is executed using a distributed computing method often called a 'botnet army', the creation process of which involves infecting computers with a form of malware that gives the botnet owner access to the computer. This could be anything from simply using the computer's connection to attack on the service or all the way to gain complete control over the computer. One may aggregate the army together with hundreds or thousands or even more to attack the server so much that it has no choice but to shut down from the overload of bandwidth, RAM and CPU power. Therefore, it is much harder for a server to withstand a DDoS attack as opposed to the simpler DoS incursion [9].

The hackers target to cut the internet access of an organization for a long time. This is the basic idea behind DDoS attacks. Victims of DDoS attacks are online businesses, service providers, *etc.* DDoS attacks cost businesses revenue loss and more importantly, damage of their business reputation. Their server could be shut down for days.

4.5. Syn flood attack

A Syn flood occurs when a host sends a flood of TCP/SYN packets, often with a fake sender address. Each of these packets is handled like a connection request, causing the server to spawn a half-open connection, by sending back a TCP/SYN-ACK packet (Acknowledge), and waiting for a packet in response from the sender address (response to the ACK Packet). However, because the sender address is fake, the responses never come. These half-open connections saturate the number of available connections that the server is able to make, keeping it from responding to legitimate requests until after the attack ends [9].

4.6. Botnet attacks

A distributed DoS (DDoS) attack is launched by a mechanism called Botnet through a network of controlled computers. A software program controls the computers and for specific purposes, known as bots. Bots are small scripts that have been designed to perform specific, automated functions. Bots are utilized by agents for Web indexing or spidering, as well as to collect online product prices or to perform such duties as chatting. However, bots are negatively associated with remote access Trojan Horses (*e.g.*, Zeus bot) and zombie computers that are created for less favorable purposes. Bots in large quantities provide the power of a computer to create prime tools for such activities as the widespread delivery of spam email, click-fraud, spyware installation, virus and worm dissemination, and DDoS attacks (*e.g.*, black energy bot). DDoS attacks usually take advantage of the weaknesses of a network layer, particularly, SYN, UDP, and Internet control message protocol (ICMP) flooding. Such attacks encroach the network bandwidth and resources of the victim, thus facilitating the denial of legitimate access [9].

5. Proposed solution

In this section, I am proposing a defensive solution in case of cyber attacks to cloud computing. It is not a complete solution to solve the security problem, it is only a 'proposal' that makes enterprises to think and consider in the future to implement forensics methods in their cloud servers.

5.1. Forensics methods

Cloud computing is scalable and advantegous in many aspects for the large and medium enterprises but no one knows where the actual physical servers are. The end-user can only access their data and application via internet on a virtual system. Hence, the data travels over the public network and it worries users about the security aspects of the systems.

According cyber attacks definitions in the previous parts, the security issues are becoming prime element and the preventative aspect of cloud security is an area of active research and development in the decision when enterprises to migrate from in-house server farms to cloud.

I examined digital forensics methods in order to provide solutions to cloud computing security. Forensics methods are being used by the Police forces, for example after a murder case a ballistic survey on a suspected gun is conducted and the bullet who killed the victim is revealed. The main goal here is to prove whether the bullet shot from the gun and the murderer's gun match.

Hence, digital forensics has the same goal as the traditional forensics science: to collect evidence for cyber crime. The history of cyber forensics is listed below in cronological order [10]:

1984

FBI Magnetic Media Program created... this later becomes the Computer Analysis and Response Team (CART);

1993

First International Conference on Computer Evidence held;

1995

International Organization on Computer Evidence (IOCE) formed;

1997

The G8 countries declared that ”Law enforcement personnel must be trained and equipped to address high-tech crimes” in the Moscow Communiqué of December;

1998

In March G8 appointed IICE to create international principles for the procedures relating to digital evidence;

1998
INTERPOL Forensic Science Symposium;

1999
FBI CART case load exceeds 2000 cases, examining 17 terabytes of data;

2000
First FBI Regional Computer Forensic Laboratory established;

2003
FBI CART case load exceeds 6500 cases, examining 782 terabytes of data.

Collecting evidence from virtual disks with traditional methods is very difficult and not feasible. With physically attached storage, it is easy to determine which storage device belongs to a given server. With the advent of storage networking and virtualization, mapping storage devices has become much more complex. Forensics science is a new way of tracking evidence in cloud environment and has recently gained significant popularity. It is mainly used against fraud and theft of data.

Even the hypervisor controls untrusted guest VM, virtual machine image taking is the first step of collecting evidence. Hypervisor produce every instance of the VM, but to check the previous instances that had been already executed from the the client's machine determime the validity of the new instance. Before producing an instance of the cloud, also it can be check who is requesting that instance type. Hypervisor could filter host base and guest base firewall entries using Iptable's.

Forensics science provides the recovery of deleted files, in part or whole. If a user deletes a file to the recycle bin and empties the recycle bin, those files may usually be recovered in whole for review. Due to the size of the virtual machines, they may not have been sent to the recycle bin as windows recycle bin has a file size limit. These files will be deleted directly by the system, but still may be recoverable for analysis.

A log server or in other words forensic workstation keeps track of connection details of cloud IaaS.It allows authenticatication of users but disconnects user with no valid user name and passwords; and keeps track of ip numbers and login details of users or intruders who want to log on to the authentication server of the cloud computing as it is shown in Figure 4. Centralisation of log files is also important, to keep logs together from different sources. Centralisation of log files could help analysers to view unauthorised loggings and what changes have been (deleted or updated) in the databases.

Potential evidence sources could be [11]:

a. Webserver logs;
b. Application server logs;
c. Database logs;
d. Guest operating system logs;
e. Host access logs;

f. Virtualization platform logs and SaaS portal logs;
g. Network captures;
h. Billing records.

Consequently, forensics science became a very important method for cloud computing virtual infrastructure in order to keep it safe and help recovery of the system after a malicious attack. It enables to collect evidence, it must either be collected or acquired, to present at the court in report form.

Collection – "Process of gathering items that contain potential digital evidence [12]."
Acquisition – "Process of creating a copy of data within a defined set [12]."

For acquisition in current forensic practice regarding imaging memory, an active log file, or other dynamic process, the concept of 'snapshot forensics' is used. The analogy is that no two successive snapshots of a running child will capture exactly the same image (since the child is moving) but the snapshot accurately captures the appearance of the child and her background at a moment in time. Assurance of reliability for the snapshot then becomes assurance of its provenance and that it has not been modified since acquisition. Documentation can assure the identity, place and time of the snapshot while traditional techniques such as cryptographic hashes and chain-of-custody processes can provide integrity assurances [12].

There could be other methodologies to keep the cloud environment safe to build customer confidence but I believe forensics science introduces a new horizon in this field.

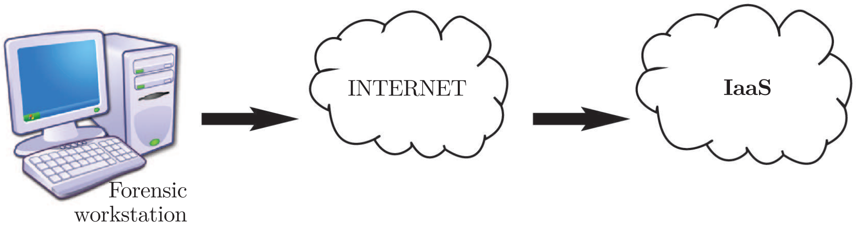

Figure 4. Cloud forensics

6. Conclusions

In order to keep cloud computing data safe, providers and users should take the necessary steps together. Accessing cloud services over the internet may not be secure. Encryption algorithms, passwords are not always the best solutions. DDoS attacks are serious attacks that make the cloud servers idle sending many sync requests from multiple hosts. Cryptographic attacks are also another threat to break the weak encryption algorithm to penetrate the system. Thus, identifying all those threats make CSP (cloud service providers) alert about covering weaknesses and build a secure robust Cloud system. Forensic methods keeping log of unauthorised users can help to keep track of crime evidence. To sum up, the total cloud security should be more secure thus becoming more defensive and hard to break up.

7. Future work

In this paper, I mainly identify cloud computer risks and cyber attacks. To protect cloud computing, a proposal for security methods are briefly mentioned. Further research work will be carried out in detail and solution to cloud computing security issues will be offered. A Forensic model will be applied to Cloud IaaS including a new architecture of security design.

References

[1] 2009 *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*, Cloud Security Alliance (CSA), http://www.diceitwise.com/what-is-iaas-paas-saas

[2] Asma A, Chaurasia M A and Mokhtar H 2012 *Int. J. Application or Innovation in Engineering & Management* **1** (2) 141

[3] https://en.wikipedia.org/wiki/Hypervisor

[4] Fraunhofer SIT 2012 *Cloud Computing: Same Weakness Found in Seven Cloud Storage Services*, *Science Daily*, http://www.sciencedaily.com/releases/2012/06/120629142416.htm **June29**

[5] Chen L, Liu B, Hu H and Zheng Q 2012 *Proc. 11th Int. Conf. on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom)*, Liverpool, England, pp. 1259–1264

[6] USA Government Report 2013 *Data Security: Top Threats to Data Protection*, Assistance Center: http://nces.ed.gov/ptac

[7] CSA Security Report 2013 *Top Nine Cloud Security Threats in 2013*, Cloud Security Alliance

[8] Sheider B 1996 *Applied Cryptography, Protocol, Algorithms and Source Code in C*, 2nd Ed., John Wiley & Sons

[9] Alomari E and Karuppayah S 2012 *Int. J. Comput. Appl.* **49** (7) 24

[10] http://www.pc-history.org/forensics.htm

[11] 2013 *Mapping the Forensics Standard ISO/IEC 27037 to Cloud Computing*, Cloud Security Alliance (CSA), **June**

[12] *ISO 27037, Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*, http://www.iso.org/iso/catalogue_detail?csnumber=44381