International Journal of Academic Research in Computer Engineering
Print ISSN: 2476-7638 and Online ISSN: 2538-2411
Vol. 2, No. 1, Pages. 24-33, May 2018

International Journal of Academic Research in Computer Engineering

Volume 2, Number 1, Pages 24-33, May 2018
www.ijarce.org

IJARCE

Analysis of Scalability and Risks in Cloud Computing

Uranus Kazemi[1*], Reza Boostani [2]

1. Department of Computer Engineering, University of Apadana, Shiraz, Iran.
2. Assistant Professor, University of Shiraz, Iran.

Receive Date 2017.02.21; Accepted Date: 2017.10.09, Published Date: 2018.05.15

*Corresponding Author: U. Kazemi (uranuskazemi@yahoo.com)

Abstract
Cloud computing means relations of many computers are performed by a contact channels like internet. In this way, we will have ability to send, receive, and save data in the internet. Also, cloud computing gives a chance to compute or have parallel processing with using many virtual machines. Nowadays, efficiency, scalability, availability and security may express great risk in cloud computing. At the moment, our industry is change to the cloud computing. Because, this technique is very reliable and economical. In many companies, there are obstacles in relation to the security with using cloud computing service. One of the most important security issues is a lock of audit for various security aspects in cloud computing environment. This descriptive analytic study examines matter in connection to availability, the subject of scalability , the risks of cloud computing, the security of the information and infrastructure audit and also we will pay attention to identify how infrastructure based on cloud computing are safer and more accessible.
Keywords: Cloud Computing, Scalability, Risk, Availability, Security.

1. Introduction

Cloud computing is a new technology that can share available sources with other user for example; a company may require a powerful server for doing operations with heavy workload twice a year. This company expends the high costs and purchases proper hardware servers for this purpose and uses them at the time of need and after this time, It expends to maintain them whole year, while they are not used. Now, this company can use the available hardware sources in cloud when it needs to hardware source with a much lower cost and solve its problem in certain timeframe and doesn't need to expend for purchasing and maintaining hardware requirements. The share of source in the cloud environment is the same concept. Now you suppose that many companies and organization need to have the resources, in addition, their demands are different. Cloud environment must be able to be responsibility to the requests of the user in using the resources, So that resources stand dynamically and based on user demand with the increased workload. The system should cover well the demands of user. This is where the concept of reliable, flexible, and scalable system will be understood. The system should be scalable enough to be maintained with the increased workload performance in this case we can say that the system is reliable and flexible. Strengths of the study compared to similar papers: In this paper, in addition to the issues and challenges related to risk and scalability, security, and accessibility has been analyzed, as well as ways to solve problems and control each of them as much as possible is expressed.

2. Cloud Computing

Cloud computing means the computation that is taking by many groups of remote servers that are networked together, which leads to the centralized storage of data and to be accessible on time to the services and computer resources. Simply, cloud

computing is to access computing resources via the internet and in practice rather than on you keep information on your hard drive or update continuously the required application program, you use a service on the internet to provide similar needs as mentioned. cloud computing is a computational model where a large number of systems connects each other for private or public network to provide dynamic infrastructure and scalability for application programs, data storage and files. With the advent of this technology, It is dropped significantly the price computation, hosted applications, storing content, delivery services originally, the idea of cloud computing is based on reusing IT capabilities.

3. Scalability in Cloud Computing

Cloud computing is a new model based on Internet that sets IT services as tool in the hands of users. The access to hardware resources and software in cloud computing is based on user's demand and happens to be quite flexible.

Scalability is one of the most main important characteristics and challenges in the cloud environment, so that it is considered in each of the proposed architecture. In general sense, scalability means the ability to expand the system and to maintain its performance. If it is considered unlimited the number of users simultaneously use from system, likely the amount of traffic and workload at a particular service, which necessitate to expanding the system and add to the new items to the system, the concept of scalability is more important. Thus, scalability is one of most important features and advantage of computing environment of cloud computing and is defined as the capability of system in order to meet the growing needs of the workload (increase the number of users and etc.) accurate management of hardware, software and virtual resources. Not only scalability is associated with the reliability, but also gives the possibility to the system that maintains its performance at an acceptable level. In fact, when the system increase its capacity and maintain its effectiveness at the high level, is a scalable system. To achieve this in cloud environment is not easy and involves a lot of complexity. A system is scalable that can adapt itself based on user's requests. So, the scalability is the ability of the system to manage and supply resources when the system is faced with a heavy workload. Of course, it should be added after reducing the workload, the management of the system is also linked to its scalability. In fact, when a user requires more needs with special features, scalability arises and it requires new policies in the design of the system.

3.1. The Variety of Scalability in Cloud Computing

Scalability is efficiently the allocation and management of resources and based on user's requirements as mentioned. Generally when the discussion about scalability arises, the purpose is that the virtual resources management based on user request to be allocated resources automatically to applications programs. In general the system should handle to increasing and reducing the resource efficiently and effectively. A highly scalable system can cover more number of users in order to use the application programs and therefore the efficient use of resources will boring.

- Horizontal scalability: It means to add new server.
- Vertical scalability: It is defined as increasing the capacity of system resources: such as enhance memory, cade memory, and processor during at the time of increase traffic and heavy workload. In fact, these methods mean increasing the size and capacity of the hardware server without software changes and modify the code. As it stands this method limited us to increase the capacity of the hardware which in turn increase costs.
- Dynamic scalability: This term is often said cloud scalability that allows the software to provide configurable infrastructure resources without any interaction Dynamic scalability can be either proactive a reactive.
- Proactive scalability: This includes a scheduler for changing infrastructure based on the forecast demand graph. This scalability can be configured the cloud management tools in such a way. To be able to answer requirement in the early morning hours with minimal existing infrastructure and then it is added to capacity again slightly reduced capacity until noon this strategy will not for the increased demand instead it works on the basis of a specific program.

Reactive scalability: In this strategy, the infrastructure reacts according to the changes in demand by adding or reducing capacity.

3.2. Scalability problems

The actions scalability are done by adding more restrictions in cloud computing for providing

better service to customers and checking out both systems will work correctly or not after the addition of new features.
There are many problems after adding new restrictions. Scalability problems only arise when an organization adds additional requirement to facilitate for customer. When the problems of scalability arises which many web application problem are cloud based cyber space. Scalability issues can be categorized into two types, the first type is horizontal scalability and the second type's vertical scalability. Horizontal scalability can be defined by adding virtual events or repeat virtual appearance, when there is a heavy load of web application program.
Today, the load balancing method is used to balance the load of application programs web, this method is a cost effective solution to distribute load for many cases and to increase performance. Usually scalability is done for giving benefit to the service provider and cloud service. So if you are faced with rising costs, the scalability should not be used any. Here it must be said that this system has a poor scalability.

3.2.1. Improvement Solutions of the Cloud Scalability

The scalability issues that is obvious when conversion scale is done for up scaling and downscaling. To address issues of scalability and its solutions in the beginning, the notification function is used, when it is done to add or remove a restriction, so it should be a notification or alarm management. The best way to solve issue related to scalability in the use of load balancing. The load balancing is to balance and manage all load and traffic application program. There are many sources of load balancing technique which are respectively assigned to each of the application program a particular source. It must also be considered that any of information in the cloud is divided equally. Thus the scalability is done according to the needs of users. This increase the scalability of cloud computing. For the benefit of downscaling, initially, the removed restrictions will be discussed whether or not their removal will affect. Sometimes some memories are deleted, but on the other hand, they are used by some users and will lead to big problems.
Therefore, when it is attempting to remove some memories, it should be noted that the memory is free; this is led to an increase in downscaling [1].

4. The availability of Cloud Computing

Availability usually means being prepared for something to use. Availability is synonymous with usability and accessibility. Both of them can be used elsewhere if it is used the term "availability" for PC, which means when the computer resources are available. Availability is directly proportional to reliability and maintainability.
The abundant availability requires locating the ineffective and futile application programs locating. There are many requirements for accessibility in the cloud. There must be balance between administrative costs and availability. There are several factors such as human mistake, software failure, hardware failure, transport machines from one server to another, and the software. Some of these factors affect the accessibility of cloud computing [1].

4.1. Problems Availability of Cloud Computing

Availability means that a system is ready for using and is available to user; It is synonyms of cloud computing is a very important issue. When there is a burden of web application programs, and after that if any user wants to access the system it does not get, because all resources have been used by a person and the system not be available until that resource is free. If the system is not maintained properly, problems related to availability appear. To achieve access to the system, the system has to be reliable and also should be strong. So the system works properly in spite of maximum destruction and failure, and have maximum access. Other factors that affect the availability of cloud computing like hardware failure, human mistake or the server transfers from one place to another. Another server important factor that affects the availability is the grad of initiation software. In this way the software is upgraded, then the sequence of requests placed pending, at this time the grade of that work is starting. So the availability of cloud computing is reduced.

5. Risk analysis in the cloud computing

In order to implement cloud services, organizations need to ensure adequate security to not endanger their organization's information assets. Therefore the natures of cloud services are in such ways which are provided through a browser. So for there is a common threat about the browser, the cloud computing is targeted easily. Usually service providers claim to provide sufficient guarantee to fix the problems according to Service Level Agreement (SLA), but SLA are not enough alone. It is another matter to follow the SLA what guarantees exists. A sample of known threats regarding the application of could masses are in Table 1.

Table 1. Some of known threats regarding to the use of cloud computing.

Threats	Description
Service interruption	Loss of connection to the internet or communication with similar disorder.
Dos attacks	Disrupts or disable service provider.
XSS	Insert codes and distractive scripts in web pages.
CSRF	The combination of XSS attacks use of transformed URL.
Invalid service	Service offered by invalid service providers.
DNS poisoning exploit	Refereeing the user to a fraudulent website looks similar to the original site.

The most important concerns and challenges regarding to this technology is security and privacy. Giving confidential information to a company cause doubt in the movement to cloud computing. But in the end, the users have to outsource part of their information and maintain of others. As well as the hosted on a shared and outsourcing infrastructure in a place with the judicial system different from the place of the data owners requires guarantees in the jurisdiction area and privacy issues. Although the security after additional communication system is applicable, but the use of cloud computing is the initiator of new attacks. It may be necessary to change the authentication on software application and the necessary licensing in the commercial environment to cloud environments.

In cloud system, it is very difficult and a big issue to follow up and investigate the cause of attacks. Due to the lack of physical access and its complex structure, because if the cloud service is unavailable greater impact on customers than the traditional model. Another challenge is the security virtual machine. Virtual machine monitors are used by cloud providers may also be vulnerability such as the Xen.

5.1. Risk Detection

The applicable scenarios are shown in this section. There scenarios are analyzed for the diagnostic purpose, risk in cloud computing:

- A SME view of cloud computing.
- The impact of cloud computing on the elastically service.
- Cloud computing and a Government (for the use of Elfelt)

Here, they are not scenarios that will be checked for a cloud customer or a specific and real supplier, but the purpose is to provide the scenario that is in common for different organization.

5.2. The Definition of Risks

These points should be considered in the definition of risk:

- ✓ Always risk should be considered in connection with business opportunities and the desire to take risks. Sometimes risk arises in return for the opportunities.
- ✓ Cloud services are not only for easy access to storage of various means, but also include benefits such as easy communications between multiple point of cooperation, so the risk analysis should be considered in addition to the risks of strong data in multiple locations, the risks of sending data from a point to another point . There are the risk of using cloud computing should be compared with the risks of the use of traditional solutions.
- ✓ Cloud supplier may face to the risk by customers witch the risks should be considered due to the cost and profit in such as case. So all risks cannot be met, if a risk is leading the business to failure and causes serious damage to business reputation, there will be no possibility to pay indemnity against it for any business.
- ✓ Risk analysis in this report was conducted for the cloud technology and is not specific to any particular cloud computing provided by the company.

The level of risk is expressed through the view of customer. The point of cloud supplier is express where specifically mentioned; the probability distribution of risks and their effects are shown in figure 1.

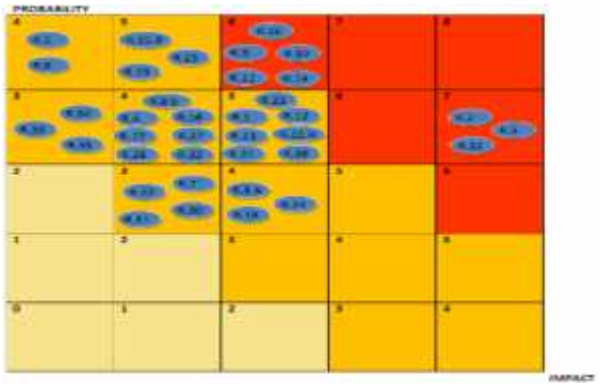

Figure 1. The risk probability distribution

The determinate risks in the risk detection period are identified in 3 classes [2]:

5. 2.1. Policy and Organization Risks

Some of items are following bellow:

- ➢ Look in: now there are a few tools, data strand, or service [3]. It is very difficult for a customer to switch from one supplier to another supplier or want to

displace data and service to the IT environment. On the other hand, cloud provider may have an incentive to prevent (directly or indirectly) portability service and data from their customer. There is independence in providing server in the cloud supplier, according to the obligations of supplier cloud, may be cause heavy losses in business and even the bankruptcy of cloud supplier. A vulnerability existing in look in includes:

- ✓ Lack of technologies and standard solution
- ✓ Choice of poor suppliers
- ✓ Lack of redundancy suppliers
- ✓ Lack of development and transparency of terms of use

Affected assets by the lock-in include:

- ✓ The celebrity company
- ✓ Sensitive personal data
- ✓ Personal data
- ✓ Personal vital data
- ✓ Real-time service delivery

So the risk is high in this case.

This risk include of other cases which is discussed below:

- SAAS look-in: customer data is designed in a database schema by the SaaS suppliers that are kept up. SaaS suppliers often use the API calls for reading data records. If a supplier does not provide this functionality to the customer. The customer will need to develop a program that extract data and enter it in the other supplier database.
- PASS look-in: This type of lock-in happens in the API layer and also in the component layer, for example, Pass supplier may offer a backup data center, In this case, the customer must use specific codes API provided by supplier and code the routine access to backup data center.
- IAAS look-in: These sections of the lock-in are related to the consumed infrastructure services.

➢ Lack of supervision: lack of supervision and control of the cloud may affect the organization's strategy the capacity of its supply goals loss of control and monitoring may cause to the failure to meet the security needs, reduce privacy the accuracy and availability of data and the deterioration of the performance and quality of service.

➢ Expiration and failure of the cloud service: like any emerging market in the field of IT, competitive pressures, a poor business strategy, lack of financial support and etc. can cause to exit some of suppliers or to force them to structure the proposed service. In other word we can say that it is possible to lose some cloud computing services in a short or average period. The impact of this risk is evident on cloud customers since it causes to waste and punish the service performance and their quality. On the other hand, the failure of services that have been outsourced to the cloud causes to increase the ability of the cloud customers for doing the performance of their duties and they give the responsibilities to their employees for provide their needs. In this case, the risk is moderate; Its vulnerabilities also contains:

- ✓ Choice of poor supplier
- ✓ Lack of redundancy supplier
- ✓ Lack of development and transparency of terms of use

Other risks of policy and organization include:

- ✓ Loss of business reputation due to ace tenant activities
- ✓ Cloud computing acquisition
- ✓ Failure of the supply chain
- ✓ Compliance challenge

5.2.2. Technical Risks

The Technical risks are as follows:

➢ Exhaustion of resources: cloud services are real-time service. So there is a level of calculated risk in the allocation of all services if cloud service, this is because the resources based on statistical result have been allocated. In this type, the amount of risk is average from the perspective of cloud supplier, the imprecise modeling use of resources or the inaccurate provision of source and lack of investment in infrastructure could be the following:

- ✓ Inaccessible to service: failure scenarios application that heavily use from a specific source. For example, heavy use of memory for simulating in applications such as to predict stock prices
- ✓ Agreement for access control: In some cases, it is possible to force the system to fail open in the event of exhaustion resource.

- ✓ Economic losses and reputation: Due to failure of providing customer demand.
- ✓ Devise events due to poor estimates of resource needs.

- Failure in isolation: defined characteristics for cloud computing are multiple owner ship and resource sharing. It computational capacity, storage and network are shared among multiple users. These risks include the failure of the separation mechanisms between storage resources, memory failure, routing failure and even failure of reputation between different owners of common infrastructure (for example, it can be pointed to SQL interaction attack where data).
- malicious insider employee in the cloud supplier: The malicious acts of an insider employee can affect the confidentiality, the accuracy and availability of data type, IP, and all type of service and directly impact on the reputation of the organization, customer's confidence and customer's experience. This risk can be seen with more power an cloud computing because there are more people with risky role in the cloud architecture some of these role can be named such as the system administrator of cloud supplier, auditors, and the managers of security services who have a duty to report the intrusion detection and have responsibility for events. Since the use of cloud is expanding, employees cloud suppliers have become targets for criminal groups. In this type, the risk is also high [4, 5, 6].

5.2.3. Legal Risks

The legal risks are as follows:

- E-discovery and subpoena: the occurrence of arresting physical hardware resulting from the legal warrant of the responsible agencies and focus on cloud storage in one point can mean that customers are at the risk of exposing their data. The amount of risk is also high [7].

  The vulnerability of this risk includes:
  - The lack of source separation
  - Data storage in several areas and the lack of transparency in this regard
  - Lack of information about areas

  The affected assets include [8]:
  - The reputation of the company
  - Customer confidence
  - Sensitive personal data
  - Personal data
  - Vital personal data
  - Service delivery-real time service
  - Service delivery
- The risks of changes of jurisdiction: The customer's data may be stored in the multiple jurisdiction, some of these areas are associated with high risk (for example, data enter that are located in the risky countries). These area may be the lack of rules of prohibiting and limiting to provide the required fields for discover and data theft. It should be noted here that there is no risk posed to all areas, and only the areas are considered to be under the pressure of specific legal.

  In this type, the probability of risk is high.
- The risk of data support: The cloud computing has several risks of data support for cloud customers and their suppliers. For a customer cloud (in the role of data controller), it may be difficult to check the data processing done by supplier, and so it is difficult to ensure to do it through legal. It should be clear that the cloud customer is responsible for processing personal data, even when these processes are done by cloud supplier. The failure of law enforcement to protect data is used to different punishments that are various in difficult countries according to the rules.
  - ✓ There may be data security intrusion that the controller is not aware of them.
  - ✓ The cloud customer may lose the control of processed data by cloud supplier. This increases in the increase of data transfers.
  - ✓ The cloud supplier may receive data collecting by customer that required by law.
- Licensing risks: licensing conditions may not apply for a cloud environment. Like initial agreements and the checking of licensing line for instance, the customer bills may increase exponentially the machine in a cloud environment in the case of payment for each use of while he constantly uses of one case. Its vulnerability is the lack of development and transparency terms of use. The amount of risk is also moderate.

6. Information Security and Infrastructure Audit in Cloud Computing

One of the main challenges is cloud computing that some of organizations make uncertain for adopting cloud security solutions. Europe network and information security Agency examined the concerns in relation of the security of cloud computing among more than a dozen of its risk. Two of then predicted a similar vulnerability (losing control and risk acceptance). It means that auditing is not available for customers. So in the context of cloud computing, security audit, in fact is necessary to separate two issues; The first issues is to have a cloud provider to create on appropriate tool in ensuring the security of information or infrastructure (security), the second issue is whether there is the possibility for the customer to confirm the security control in place or not as had been promised (audit). It is possible that cloud service provider consider only the first issue (security without audit). Like cloud provider who intend to obtain the accuracy of information based on backup. Control takes place, but the user may have no way for easy verification or backup audit that the cloud provider is making it. Therefore the audit is a major concern, as a means through which a customer can confirm the way in which his IT resources are doing. Our discussions will be focused on the relation to security audit on the customer and third party auditing of security controls cloud provider and its methods and does not address issues surrounding cloud or IT audit. In this research, efforts will be made to the overall theme of the cloud security audit depending on the answers to following key questions: (1) what topics are addressed the subjects of special audit for the approval to ensure the broader- based adoption of cloud computing technology? (2) How is the current status of cloud audit? (3) And in despite of many issues related to the audit, how can they be solved with the use of existing research, and what does other research need to be done based on the demands made? In order to do this work, we consider the needs and requirements of the users for the security audit of the cloud along with some of solutions derived from studies to get on idea of what can realistically be integrated in the security audit is expected in the near future (In contrast there are other unresolved issues that require more solutions in the long term). These will be in conflict with what is currently offering cloud service provider (such as vendor solution for the security of cloud audit). In analytical discussions, we will have a special look at audit issues that can potentially arise in the different cloud providers, such as: software as a service, platform as a service, storage as a service, and infrastructure as service.

We have categorized these subjects and will pay attention to the infrastructure of the security audit and the security of data and information. The infrastructure security is important for all the different layers of cloud services. For example, a customer who is developing a program on the cloud service provider and massively its development, he may also have the same concern about how the images of virtual machines and the stored snapshots using the completed of virtual servers. However, issues related to data and information security is more crucial for those users who are above the level of infrastructure such as the users reply on cloud database, the operating systems developing software, the complete application programs. If a cloud customer has its own virtual cloud infrastructure, so in most cases he has the ability to implement his systems to ensure the auditability of information.

Because they are the completed of virtual servers, and will have direct access to the installation whatever the application programs want. This is when the user does not have access to all levels and therefore much of what is happening on the basis of his information and it is clear that this requires more planning to maintain auditability.

6.1. User's Requirement for Security Cloud Audit

A wide range of user's security requirement with regard to audit cloud computing can be classification into two categories: security infrastructure and information audit. The adaptation of infrastructure audit issues occur with the systems use for processing the data and the security control used to protect the system. These concerns become more prominent by being agnostic the true nature of the business or activity that is accomplished and merely implies that there is a safe environment for business. The concerns about the audit information must be removed automatically with the protection of its information such as confidentiality, integration, and availability. The data and information are highlighted with the emergence of the information that stored and processed in the infrastructure system and is inherently dependent on the nature of its business.

- Requirement of infrastructure audit: Since the overall security in the IT industry is often done by using the best standard approaches. So it seems that concerns of

the user about the security of cloud infrastructure will also be eliminated by the standards mentioned. Two of the most usable and must important standards for in the security of infrastructure information are ISO 27001, ISO and PCI DSS, PCI in 2010.

- Audit requirements: Four major challenges of information as the audit of security data and information are data integrity, confidentiality of information, the origin of data, the origin of the dump data and information. Data integrity is meant to protect data against unauthorized disclosure [9, 10]. In the area of cloud computing, the origin of data, beyond the concept, is the ability to track accurately data and information at any time. This especial and particular concern in the cloud computing structures is for a reason that these systems may be dynamically moving in virtual systems and some of this information is stored because of the performance and scalability and some of them stored according to the rules expressed in different centers.

6. 2. Security Data and Information Techniques

In the previous section, we present an overview of the concerns for the users of cloud service. In this section, we will present a summary of some recent techniques in the field of audit information. Particular attention has been to the dedicated methods to be used in cloud environments and those which are easily adaptable to the offered cloud environments.

- Confidentiality and integrity of information: Encryption is a useful tool for ensuring the confidentiality of information, privacy and its integrity. Also, there are several approaches and techniques to search and investigate the existing information on the offered cloud servers [11, 12, and 13]. Wang and his cooperator Lee, in the recent research, mentioned the concepts in relation to the examination of the integrity of the data on the remote, which storage can be used (to verify the integrity of the stored data in a public cloud) to enable a customer. The authors proposed and approach and a solution for protecting the privacy of data from a non-authorized person that relies on protocol which search the different parts of a file before the encryption. This proposal also deals to the audit supports of all batches. Zhu and et al [14] offered a similar plan of mechanisms of data integrity, but it is assumed the third-party auditor (TPA) is a reliable representative from the owner of the original data. And thus it was not considered the controls to keep the contents of the original data evaluated by third person.
- Dates's and dump information: dump data is a very little attention compared to other security concerns for users. There are several ways to prove security. One of these ways is the devised devices to mobile phone. The use of these approaches created many assumptions. One of these assumptions is the storage device has a fixed memory with a known size, so it cannot protect the cloud scenario, so a lot of works still are needed about the data and dump information. Instead of such methods, it can be assumed that the cloud provider is a non-confidence factor, even if the erasure information is not proven and the customer does not have access to the source and storage medium, it is more important and significant. Thus it is more important for the beginning to encrypt data that are given to the service provider.

6.3. Security and Compatibility Due to Cloud Provider

We examined more than a dozen public cloud providers according to a recent study conducted by Gartner in determining a wide range of security provided by the cloud provider service [15, 16].

Cloud providers are Amazon web service, AT&T, Google, HP, IBM, Internap, Microsoft, Nirvanx, Rackspace, and Soft layer. All of them offer infra-structure as a service expects Microsoft (supports only the IaaS service by offering software to its seller agents) and Google (That IaaS is used in the beta testing at the time of writing).

- Infrastructure security: all the companies were surveyed that offered detailed information about their security controls and process as certifications in accordance with the standards such as PCI DSS, ISO 27001 and safe Harbor. All these companies also provided the surplus security services to its customers such as FirFox with public service. A few companies with larger technology (IBM, HP) include the custom developed operating systems that are available to customers. For instance, HP, with the use of technical white paper (a white paper is

a paper that an organization offers a very un precise technical description of the design, frame or production technology) of technology of IPS. This technology is primarily responsible for the security of its servers, hardware network and data center. The study also examined, the issues related to Armor strategy that is an adjustable user of IPS and firewall for the VMs that is performing in the cloud provider companies.

Other provider (such as Amozon, AT&T, Rackspace and Internop) only offers additional services such as firewall management, intrusion detection or prevention or identification and the access of management as modular that are independent security services. Another existing model to provide additional security services is the use of specialized partners for providing third-party security as a service. For example, soft layer offers customers a free application as "Accept PCI" that is the application of MCAfee secure (provider a service to do monitoring website and security certification). Only a company (Amazon) completed the security certification with detailed information about how customers use the public standards of cloud provider. It provides the description page of security controls and its own certification like many other cloud service providers. But it provides more detailed information about DSS PCI and ISO 27001 based on the questions asked by its customers (Amazon web services).

They also offer customers a set of documents that has helped them to give certification. These documents include the certification in accordance with PCI standards for AWS, documents at high levels like the description in field of environment. And more detailed documentation such as an accurate matrix of DSS PCI controls to describe someone who is responsible for individual controls. They offered a master key about the balance between the security responsibility of the cloud service provider and customers and stated that only a part of the environment that have PCI card based in AWS, QSA can rely on the status of credit service provider, but it still would be more services to meet all the standards in accordance with the PCI and other required tests such as how to manage card holder environment hosted by AWS (Amazon web service) [17].

AWS also states that numbers customer have received the PCI DSS certificate on, although parts of the Infrastructure hasted by AWS that are not entirely clear. AWS also offers numerous tips about the ISO 27001 standard. Although the requirements for more standards of high levels have no matching package and are unenviable where relevant details to some special controls lie.

To explain this issue, we analyze the PCI DSS that involves these cases: build and maintain a secure network, protect the data of cardholder. The implementation of strict proceeding of security and regular testing and network monitoring.

ISO27001 also requires the systematic assessment of information security risk, implementation of information security controls, the management of risk and adaption an overarching management process for security controls (ISO).

- Data security: Now it is very limited the supports of cloud service provider for data security. In fact, the cloud service provider only supports the real time of any kind auditing that is related to cloud watch service of Amozon's API. (n.d. Amazon web service). As it is discussed previously, this API, In fact, just pays to the audit of performance to provide various statistics of AWS. The cloud audit is a wide industry that has been especially efforts to standardization of approaches to security compliance documentation, but it does not have much progress after sending a RFC to IETF in 2010. Also basic support of data security is very limited in software, platform, and storage level of cloud provider. Only an exception rule is that Amazon supports of data encryption through APIs of Java for S3 that is storage as a service provider some confidential issues have partly been resolved, but these are only the cases that data cannot be updated regularly.

7. Conclusion

In this study, we discussed issues about the cloud computing and its various feature. As a cloud is a shared system, so there will be many problems in its function. Heavy traffic is caused in cloud when

there are many requests for accessing to information. This problem can be remedied by using load balancing. Another important feature of cloud is scalability. Scalability is to add or remove samples according to customer requirements. Another important feature is security. There are many issues surrounding the issue of security such as risk. The identified risks in the risk detection process fall in 3 categories risk in policy and organization, technical risk and legal risk. Another important feature is availability. Availability problems occur due to human error, hardware failure and put the server from one location to another availability problem also arise because of the bad maintenance of the system. This problem can be remedial with the use of many hardware resources. Some of the problems can also be resolved by using the software update based on requirements. To achieve high availability it should be had a powerful system, and also the amount of availability can be increased and improved through providing new samples.

References

[1] Hassan, S. kamboh, A. Azam, F, Analysis of Cloud Computing Performance, Scalability, Availability, & Security, IEEE/IFIP International Conference on, 2013.

[2] Gartner, "Seven cloud-computing security risks," Network World, July 2008.

[3] Data Liberation Front, Google, http://www.dataliberation.org, Accessed at May 2013.

[4] Retailresearch.org: http://www.retailresearch.org/reports/fightinternalfraud.php.2012.

[5] Silva, F. Paulo, et al., Model for cloud computing risk analysis, ICN 2015: 152, 2015.

[6] Chou, C. David, Cloud computing risk and audit issues. Computer Standards & Interfaces 42, 137-142, 2015.

[7] Enterprise Storage Forum, ww.enterprisestorageforum .com/continuity/news/article.php/3800226.2012.

[8] Find Law http://technology.findlaw.com [Online], http://technology.findlaw.com/ articles/01059/011253.html

[9] Mather, T. Kumaraswamy, S. Latif, S. Cloud security and privacy: An enterprise perspective on risks and compliance. O'Reilly Media, Inc, 2012.

[10] Ali, Mazhar, Samee U. Khan, Athanasios V. Vasilakos. Security in cloud computing: Opportunities and challenges. Information Sciences 305: 357-383, 2015.

[11] Wang, Q. Wang, C. Ren, K. Lou, W. Li, J. Enabling public verifiability and data dynamics for storage security in cloud computing, IEEE Transactions on Parallel and Distributed Systems, 22(5), 847–859. 2011.

[12] de Carvalho, Carlos André Batista, et al, State of the art and challenges of security SLA for cloud computing, Computers and Electrical Engineering, 2017.

[13] Shahzad, Farru kh,State-of-the-art survey on cloud computing security Challenges, approaches and solutions, Procedia Computer Science 37: 357-362, 2014.

[14] Zhu, Y. Wang, H. Hu, Z. Ahn, G. J. Hu, H. Stephen, S., et al. "Dynamic auditservices for integrity verification of outsourced storages in clouds". In Proceedingsof the 2011 ACM symposium on applied computing, SAC'11 (pp. 1550–1557). NewYork, NY, USA: ACM.2011.

[15] Ruth, G. Chandrasekaran, A. Critical capabilities for public cloud storageservices, Stamford, CT: Gartner, Inc. Retrieved from: http://www.gartner.com/technology/reprints.do?id=1-1D9C6ZM&ct=121216&st=sg, 2012.

[16]Almorsy, Mohamed, John Grundy, Ingo Müller. An analysis of the cloud computing security problem, arXiv preprint arXiv: 1609.01107, 2016.

[17] Rasheed, H. Data and infrastructure security auditing in cloud computing environments, International Journal of Information Management (2013), http://dx.doi.org/10.1016/ j.ijinfomgt.2013.11.002.2013.