Cloud computing, Reliability and Security Issue

Alireza Ghobadi*, Roozbeh Karimi**, Farnaz Heidari**, Masoud Samadi*

**University Technology Malaysia (UTM), Jalan Semarak, Kuala Lumpur, Malayisa

**Sharif University(Pardis Kish branch), Kish, Iran

ghobadi@soha.com.my, karimi@soha.com.my, farnazheidari@yahoo.com, solariseir@IEEE.org

***Abstract*—Cloud computing with its utilities is one of the realities that the most of the industrial and educational has a dream. However, the cloud computing has the potential to solve a lot of problems (such as easy sharing, transform a large part of the IT industry) but still the performance, reliability, and the security is the most issues that still need to test and measured. This paper is the survey paper, which focuses on these three issues to identify them and discuss about the solutions, which proposed until today.**

***Keywords*— Cloud Computing; reliability; Security; Availability**

I. INTRODUCTION

With globalization, organizations are spread across the globe and their operations will involve data transfers between their global offices. This will lead to the need for the services, which can use anywhere with an economical way [1]. Developers introduce a new idea based on the internet, which no need to use large outlay of hardware and can have the most of the services that required. These widely popular services supported by 1000 servers without cost and implementation time consideration [1].

This solution can be solved the huge problems for those companies which has the wide office or wide users [2]. However, at the same time there are few questions rising up which asking about performance, reliability and security in cloud computing systems. The most of the industrial company wants to know can be trusted to these systems or how can be sure the services always available to the client [3].

Although the cloud computing is a new topic in the research area there are a lot of researchers try to explore the cloud computing definition, services and issues [2][3][4][5][6].

This paper introduces a cloud computing based on several research then focusing on services which defined based on cloud computing. The article following the issues based on services and the end focuses on reliability and security. Finally, conclude the paper in section VII.

II. RELATED WORK

Cloud Computing is one of the major technologies predicted to revolutionize the future of computing. The model of delivering IT as a service has several advantages. It enables current businesses to dynamically adapt their computing infrastructure to meet the rapidly changing requirements of the environment [7]. Perhaps more importantly, it greatly reduces the complexities of IT management, enabling more pervasive use of IT. Further, it is an attractive option for small and medium enterprises to reduce up-front investments, enabling them to use sophisticated business intelligence applications that only large enterprises could previously afford. Cloud-hosted services also offer interesting reuse opportunities and design challenges for application developers and platform providers. Cloud computing has, therefore, created considerable excitement among technologists in general.

This section provides a general overview of Cloud Computing, the technological and issue factors that have given rise to its evolution.

III. CLOUD COMPUTING DEFINITION

According to the several researches [8][9][10]11], several definitions can be found. One of the researchers defines cloud computing as delivering computing at the Internet scale. Compute, storage, networking infrastructure as well as development and deployment platforms, which provide available on-demand within several minutes.

However, the US National Institute of Standards (NIST) does the formal definition. It provides a list of accepted definitions of cloud computing terminologies and documented it in the NIST technical draft [11]. NIST is describing, cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., Networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

To further clarify, NIST specifies the following five essential characteristics that a cloud-computing infrastructure must have [12]. The cloud computing characteristics are defined in Table 1.

Table 1: Cloud computing charactrestics

No.	Characteristic	Definition
1	On demand self-service	The compute, storage or platform resources needed by the user of a cloud platform are self-provisioned or auto-provisioned with minimal configuration. This is in contrast to traditional in-house IT systems and processes, which typically require interaction with an IT administrator, a long approval workflow and usually result in a long time interval to provision any new resource.
2	Broad network access	Ubiquitous access to cloud applications from desktops, laptops to mobile devices is critical to the success of a Cloud platform. When computing moves to the cloud, the client

		applications can be very light weight, to the extent of just being a web browser that sends an HTTP request and receives the result.
3	Resource pooling	Cloud services can support millions of concurrent users; for example, Skype supports 27 million concurrent users [12]. Clearly, it is impossible to support this number of users if each user needs dedicated hardware. Therefore, cloud services need to share resources between users and clients in order to reduce costs.
4	Rapid elasticity	A cloud platform should be able to increase or decrease computing resources when it is needed. In a cloud platform, it is possible to specify The actual number of virtual servers will vary depending upon the load. Further, the time taken to provide a new server is very small, approximately minutes. This also increases the speed with which a new infrastructure can be deployed.
5	Measured service	One of the compelling business use cases for cloud computing is the ability to "pay as you go," where the consumer pays only for the resources that are actually used by his applications.

The other definition from NIST is the deployment models for clouds. These models, namely (1) Private Cloud, (2) Public Cloud, (3) Community Cloud and 94) Hybrid Cloud. Table 2 has shown the cloud-computing model based on NIST definition [13].

Table 2: Cloud computing models

No.	Model	Definition
1	Private	This model infrastructure is built for a single enterprise. It is the next step in the evolution of a corporate data center of today where the infrastructure is shared within the enterprise.
2	Public	This model infrastructure is owned by a cloud service provider that provides cloud services to the public for commercial purposes.
3	Community	This model infrastructure is shared by a community of multiple organizations that generally have a common purpose. An example of a community cloud is OpenCirrus, which is a cloud computing research testbed intended to be used by universities and research institutions.
4	Hybrid	These model infrastructures are mixtures of these different deployments.

At the last part of define to learning about cloud technologies is to understanding the three cloud service models or service types for any cloud platform[12][13]. These are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These three focus on a specific layer in a computer's runtime stack the hardware, the system software (or platform) and the application, respectively. Figure 1 shows the three cloud service models and their relationships [14].

The lowest layer is the hardware. The cloud platform that enables this infrastructure to deliver is the IaaS architecture. In the IaaS service model, the physical hardware (servers, disks, and networks) is abstracted into virtual servers and virtual storage. These virtual resources can be allocated on demand by the cloud users, and configured into virtual systems on which any desired software can be installed [15].

Some researcher has been defined advantages. These advantages can be classified as Figure 1 [16][17][18].

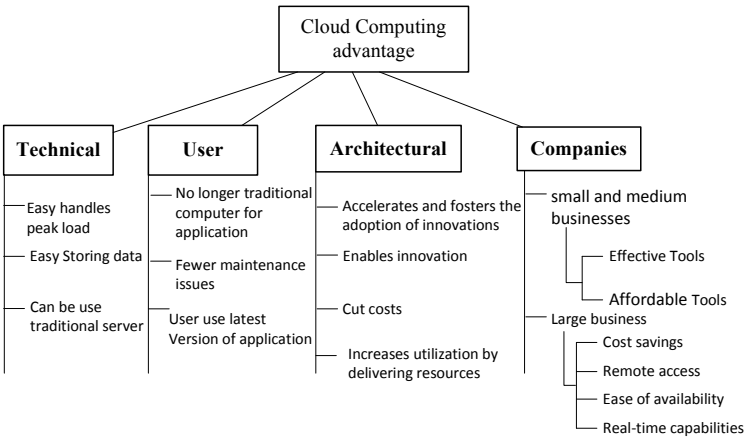

Figure 1: Cloud computing advantages [16][17][18]

V. ISSUES ON CLOUD COMPUTING

In this section, we summarize several issues, which mentioned by other researchers and categorized them. Even though "*Cloud Computing*" has offers with several benefits, but there are numerous issues and challenges for organizations embracing this new offer's technology.

Zhen [19] lists a number of major challenges with respect to (1) Data management and governance, (2) Service management and governance, (3) Product and process control and monitoring, (4) Infrastructure and system reliability and availability, and (5) Information and visualization security. To the technological aspects, the issues listed as below:

(1) Scale and elastic scalability: It is not only currently restricted to horizontal scale out, but also inefficient as it tends to resource over usage due to limited scale down capabilities and full replicate than only of essential segments [19].

(2) Trust, security and privacy: It is issues in any internet provided service. The specific clouds nature adds more aspects related (For example multi-tenancy arise and control over data location) [19].

(3) Handling data: Clouds is still complicated. As data size and variety grows, pure replication is no longer approach to consistency and efficiency issues. Lacking control over data location and missing provenance poses security and legalistic issues [19].

(4) Programming models: Clouds need to have highly scalable applications. To avoid of exploit clouds capabilities, the programing models should supported by simplify development [19].

(5) Systems development and management: All providers, developers, and users should be able to control and restrict distribution and scaling behaves. Currently executed mostly manually, thus contributing to substantial efficiency and bottleneck issues. On the other hand, non-technological issues play a major role in realizing these technological aspects and in ensuring viability of the infrastructures in the

first instance [19]. To these belong in particular (1) economic aspects, (2) legalistic issues and (3) aspects related to green IT need to elaborated as the cloud offers principally "green capabilities" by reducing unnecessary power consumption. Based on above information, several researchers can be listed some issues on cloud computing [18][19][20]. These issues are based on the cloud architected and services, which already defined previously. These issues classified in Table 3.

Table 3: classification of Cloud Computing issue

No	Issue	Sub-Issue
1	Fault tolerance	Disruption on Application
		Disruption on Back-up
		Outage of services
2	Security	*Confidentiality* (Focal concern in terms of data)
		Availability (Focal concern in term of infrastructure and visualization)
		Policy and Privacy (Concern of information of customers, consumers and employees)
3	Load balancing	Monitoring of continually of services
4	Interoperability	To allow applications to be ported between clouds
		User accessibility
5	Scalable Data Storage	Cloud provides through load balancing and application delivery solution(Horizontal)
		Resources likes to use old mainframe model (Vertical)
6	Service	Software as a Service (SaaS)
		Platform as a Service (PaaS)
		Hardware as a Service (HaaS)
		Infrastructure as a Service (IaaS)

The Expert Group Report [21] mentions a number of issues including (1) Concerns over security with respect to knowledge, information and data residing on an external service device, (2) Concerns over services' and resources' availability and business continuity, and (3) Concerns over data transmission across anticipated broadband speeds.

This paper, focus on the just Fault Tolerance (FT) and Security issues. These two issues will be discussing in the next section.

VI. Fault tolerance Issue

Fault Tolerance issue is one of consideration issue on the programing model in cloud computing [22]. Although the programing is the same fundamental concept from traditional parallel and distributed environments, but there is several issues (such as large variations in resource heterogeneity, stability and performance; exception handling in highly dynamic in that resources can join and leave pretty much at any time environments, etc.) [23].

Generally, Cloud computing is classified into private Clouds, public Clouds, and hybrid Clouds. Public Clouds provide shared services through large-scale data centers that host a very large number of servers and storage systems. The purpose of a public Cloud is to sell IT capacity based on open market offerings. Anyone can deploy applications from anywhere on the public Cloud and pay only for the services used. The examples of public Clouds are Amazon's EC2 [23] and GoGrid [24] are. In contrast, the purpose of private Clouds is to provide local users with a flexible and agile private infrastructure to run workloads within their own administrative domain. In other words, private Clouds are small-scale systems compared to public Clouds and usually managed by a single organization. Examples of private Clouds include NASA's Nebula [25][26].

VII. Security Issue

Based on previous definition of Cloud computing, Cloud computing is a paradigm shift of technology that have emerged and has been adopted by many IT organizations in the recent year. This shift in technology has changed the overall architecture and system requirements, compared to traditional server-based systems. Cloud-based system architecture provides Internet-based services, computing and storage in all fields including health care, finance, government etc with the reduced price[27].

While there is a serious concern for an organization to move towards the cloud based service, security risk associated within the platform are one of the urgent concern for an organization to make this move. Different cloud based deployment models have brought the wide range of security risks and concerns that have to be evaluated and mitigated [28]. Traditional defense in depth security model which include physical security, perimeter security, firewall, antivirus software, etc. are not directly applicable to cloud-based systems. This means that various organizations must adopt the best security practices and standards that are somehow incompatible to traditional defense in depth security models. However, the same principle of multi-layered security is still applicable.

Because of above explanation, the security issues for cloud computing platforms classified by several non-profit organizations that consist of industry representatives - Cloud Security Alliance (CSA) followed by two esteemed government organization, named National Institute of Standard and Technology (NIST) and European Network and Information Security Agency (ENISA)[29][30][31].

CSA is a non-profit organization, initiated by industry representatives in November 2008. It supported by large number of IT companies, including Google, VMware, Microsoft, IBM, Ericsson, etc [32]. The main motive of this organization is to provide security assurance and education in the field of cloud computing [33]. CSA published its first draft "Security Guidance for Critical Area Focus in Cloud Computing" on April 2009 which provides information about security issue in cloud computing platforms. The guidance is divided into fourteen domains. The first domain named "Architectural Framework" gives brief information about cloud computing platform and its reference model from the security perspective. The rest of the domains are divided into top two categories named governance and operation. The governance category discusses "strategic and policy issues of cloud computing platforms" and operation category focuses "on more tactical security concern and their implementation within the architecture" [34].

CSA (Cloud Security Alliance) describe Logical construction of security issues identified based on 13 items in two main categories called "Strategic and Policy Issues" and "Tactical Issues" in Table 4.

Table 4 : Security Issues defined by CSA.

	Issue	Description
Strategic and Policy Issues	Governance and Enterprise Risk Management	Focuses on agility of an organization to govern and measure risks associated with cloud computing platforms and recommends that security department should be included during Service Level Agreement and contractual obligations
	Legal Issues: Contracts and Electronic Discovery	Deals with legal issues associated include the strategy and policy that is needed to be applied in a cloud in order to protect the information and computer systems, regulatory requirements, privacy requirements and international law to be followed by cloud providers.
	Compliance and Audit	Focuses on compliance requirements for cloud computing platforms, such as regulatory, legislative etc., and its impact on internal security policy.
	Information Management and Data Security	Focuses on data manipulation, such as creation, usage, sharing, storage, deletion, and archiving, and identifies who is responsible for data confidentiality, integrity and availability.
	Portability and Interoperability	Focuses on interoperability standards required between different cloud providers and provides some recommendation to be followed by both deployment and delivery models of cloud computing platforms.
Tactical Issues	Identity and Access Management	Focuses on importance of identity and access management in cloud environments. Further, also focus on federated identity and the problem faced by organization while extending its identity to cloud.
	Virtualization	Discusses security issues related to system hardware and virtualization technology. Some of the items covered in this domain are hypervisor vulnerability, risk associated with multi-tenancy, VM isolation and VM co-residence.
	Security as a Service	Focuses on open issues identified by CSA which include participation of trusted third parties for security assurance, incident management, compliance attestation, and identity and access management.
	Traditional Security, Business Continuity and Disaster	focuses establishing traditional security functions, business continuity process, i.e. continuity of components of a cloud platform by assuring CIA (confidentiality, integrity, availability) and backup, disaster recovery process for cloud storage.
	Data Center Operations	Provides information on how we can evaluate the provider's data center operation in order to select the best one for long term stability.
	Incident Response, Notification and Remediation	Helps to understand complexities, brought by cloud in current incident handling program. Further, it also addresses the necessary environment that is needed to be set up between both user and provider for proper incident handling and forensic.
	Application Security	Delivers the information on modern software development cycle that is needed to be utilized by cloud computing platform. Further, it also gives us information on security threats and vulnerabilities pertaining to cloud based delivery models (IaaS, PaaS and SaaS).
	Encryption and Key Management	Gives information on protecting access to data and resources. Further, it also recommends us to use OASIS Key Management and Interoperability Protocol for key management functions.

The other organization, which works on standards, is NIST (National Institute of Standards and Technology). The US government, assisting cloud computing platform users by identifying security-related vulnerabilities in the platform. Security issues discussed by NIST are specifically focused to public cloud vendors, as it states that organizations have more control of each layer of security when private cloud deployment model is used. Logical construction of security issues identified by NIST is described by Table 5.

Table 5: Security Issues defined by NIST.

No	Issue	Description
1	Governance	Focuses on policies and procedures needed to be followed by organizational units. It also raises an issue of information security risks. Enterprise risk is due to lack of control of services offered by cloud and it recommended using auditing tools and risking management program.
2	Compliance	Focuses on policies and procedures needed to be followed by organizational units. It also raises an issue of information security risks. Enterprise risk is due to lack of control of services offered by cloud and it recommended using auditing tools and risking management program.
3	Trust	Discusses various topic and issues of internal threats caused by multi-tenancy, maintaining data ownership and intellectual property rights, risk management, gaining visibility and security control offered by CSP.
4	Architectural	Section discusses the issues pertaining to software systems utilized by cloud platform. Most of the issues discussed in this section are due to unique characteristics of cloud computing platforms which are completely different compared to traditional data centers. The issues covered in this section are hypervisor security, virtual network protection, virtual machine images and client side protection.
5	Identity and Access Management	The researchers from NIST focus on identity verification, authentication and access control mechanism and also recommend using SAML for authentication and XACML for access control
6	Software Isolation	Warns about the threats associated with multi-tenancy such as the attack vector.
7	Data Protection	Focuses on the need of data privacy and isolation, as data from different customers resides on common data center in cloud computing platforms.
8	Availability	Discusses about the threats that have a negative impact on organizational resources.
9	Incident Response	Focus on reactive countermeasure for the attacks and threats in a cloud environment.

The other organization which tried to provide the list of security issues, is the European organization called ENISA (European Network and Information Security Agency).

ENISA published its first document "Cloud Computing Benefit, Risk and Recommendation for Information Security" in November 2009. The document began with highlighting key benefits of security for cloud computing platforms. The rest of the document discusses security issues, which are structured into three categories. All security issues discussed in each category are listed on the Table 6.

Table 6: All security issues in Cloud computing.

Issue	Sub-issue	Description
Policy and organizational	Lock-in	Discusses about data and service portability issue in terms of adoption of cloud service model.
	Loss of governance	Are challenges are remaining in this sub domains also discuss portability issues and its impacts on organization assets, risks and vulnerabilities.
	compliance challenges	
	Loss of business reputation due to tenant activities	
	Cloud service termination or failure	
	Cloud provider acquisition	
Technical	Resource exhaustion	Start with a list of threats present in a computing platform. Some of the threats discussed in this topic are availability due to resource exhaustion, VM monitor vulnerability, insider threats, denial of service, network related threats, and lack of sufficient effort from consumer to secure execution environment.
	Isolation failure	
	Cloud provider malicious insider	
	Management Interface compromise	
	Intercepting data on transit	
	Data leakage on up/download, intra cloud	
	Insecure or ineffective deletion of data	
	Distributed Denial of Service	
	Economic Denial of Service	
	Loss of encryption keys	
	Undertaking malicious probes or scan	
	Compromise service engine	
	Conflict between customer hardening procedure and cloud environment	
legal	Subpoena and e- discovery	Begin with subpoena and e-discovery issues, which provide information on how to respond subpoena and e-discovery issues. The rest of the legal issues discussed in this section are focused on data manipulation, data location compliance, data protection compliance and risk of losing intellectual property, when data is stored in a cloud.
	Risk from change of jurisdiction	
	Data Protection Risk	
	Licensing risk	

As a comparison between these definitions, unlike other government-funded organizations like, CSA and ENISA, NIST does not make any top-level classification of security issues like, organizational, policy or legal. However, each issue discussed by NIST can be linked with the sub-issue identified by other organizations.

VIII. Experimental Results and Analyses

According to above information, two examine the security defines an environment to test the security with and without Appling recommendation. The test environment has been shown in Figure 2.

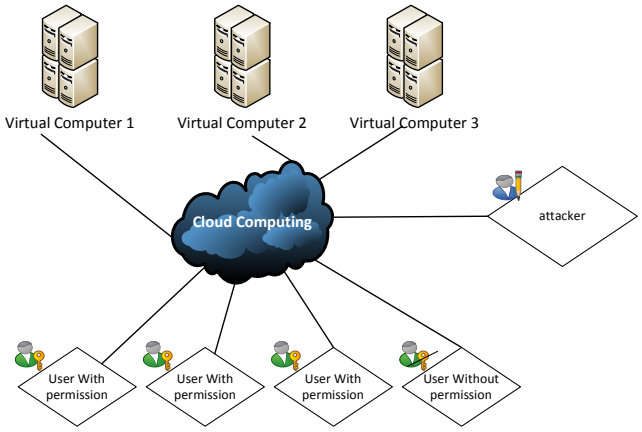

Figure 2: Testing environment

In this environment used the desktop with three Virtual Machines. Each Virtual machine has deferent OS, which defines in Table 7.

Also each one has five software's (Photoshop, word, PowerPoint, Notepad and eclipse) and one application provides as services software.

The VMs has hide connection to gather and can be shift the services from one to the other for several purposes. The users have to communicate to cloud by the Access Control List (ACL). ACL determine the access level of the users to the software's.

Table 7: Virtual Machines and descriptions.

No.	VM	OS	Install software List
1	VM1	Windows server 2012	Photoshop Word PowerPoint Notepad and Eclipse
2	VM2	IOS Snow	
3	VM3	Ubuntu 12.1	

There two kind of the attackers in this system defines one is the unauthorized user and attacker itself. First, assume the system do not have any policies on the VM (policy issue), no identify management system (Identity & Access Management issue) no software protection (Isolate software issue), no date protection on database and desktop (Data protection issue). Based on the system unauthorized users and attacker activities defines on Table 8.

Table 8: Issues and attackers defination.

Issue	Unauthorized User	Attacker
Governance	No policy can be access on VM That user has access to other VM does not access	Cannot do action by low
	Can be access to the software which cannot access	Cannot protect system
	Can attack to ACL list	Can attack to ACL list
Compliance	Because no policies user can do any action without any law compliments	Because no policies user can do any action without any law compliments
Trust	No trust because of no policies defines	No trust because of no policies defines
Architecture	No structural architecture cannot be monitor cannot prevent or stop unauthorized user action	No structural architecture cannot be monitor cannot prevent or stop unauthorized user action
Identity & Access Management	If some authorized users' login with any way, cannot control any not right activities and changes.	No record from the attacker for managing any other attacks
	Can be install any unauthorized software or spy application.	
Software Isolation	Can be remove, delete, add or delete any software	Can be remove or delete any software
Data Protection	Can be Manipulate or remove some data	Can be Manipulate or remove some data
	Disturb system and other users	
Availability	Any access is open	Any access is open
Incident Response	Not activities if some incident happen because a lack of log or the same incident can be happen because of lack of policies and data backup	Can be destroyed the system

According to this environment can define several attack scenario or fault Torrance can be happened. However, generally, if the precaution has been applied on this system then system can monitor, control, respond and serve system. With this kind of the system, the user can be more trust and system is more trustable. In addition, the unauthorized user cannot do some action that is not defined from them because of the monitoring system and policy. If the user did some disturbing action, the system not only can be monitor but also can be response based on the damaging, which happened to the system. This action can be increased availability of system and trust as well.

In the other hand the attackers likes access to the cloud servers. With monitoring can be identify them and block ofvr if the attacker can be access to the system, it is hard for him to access data or software and disturb system or users.

VIIII. Conclusion and Future Work

Design and implementation of a generic and secure architecture for cloud computing platform is still an open issue in the field of security for IT organizations. Due to the varying nature of computing platform, in terms of delivery and deployment models, cloud still needs generic and secure architecture in term of its adoption. This paper focus on the fault tolerance and security issue on the cloud computing to identify based on the technical Mather. Also provides the table of the precaution based on these issues. Also for more understanding, defines a scenario and explains issues based on this scenario.

This research was focused on pre-definitions issue and for the future can be impalement a model that defined previously as scenario and test it to find other issues.

References

[1] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, *53*(4), 50-58.

[2] Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. (2008). A break in the clouds: towards a cloud definition. *ACM SIGCOMM Computer Communication Review*, *39*(1), 50-55.

[3] Mell, P., & Grance, T. (2009). Draft nist working definition of cloud computing. *Referenced on June. 3rd*.

[4] Wang, L., Von Laszewski, G., Younge, A., He, X., Kunze, M., Tao, J., & Fu, C. (2010). Cloud computing: a perspective study. *New Generation Computing*, *28*(2), 137-146.

[5] Foster, I., Zhao, Y., Raicu, I., & Lu, S. (2008, November). Cloud computing and grid computing 360-degree compared. In *Grid Computing Environments Workshop, 2008. GCE'08* (pp. 1-10). Ieee.

[6] Rochwerger, B., Breitgand, D., Levy, E., Galis, A., Nagin, K., Llorente, I. M., ... & Galán, F. (2009). The reservoir model and architecture for open federated cloud computing. *IBM Journal of Research and Development*, *53*(4), 4-1.

[7] Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision Support Systems*, *51*(1), 176-189.

[8] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing (draft). *NIST special publication*, *800*(145), 7.

[9] Wang, L., Tao, J., Kunze, M., Castellanos, A. C., Kramer, D., & Karl, W. (2008, September). Scientific cloud computing: Early definition and experience. In *High Performance Computing and Communications, 2008. HPCC'08. 10th IEEE International Conference on* (pp. 825-830). Ieee.

[10] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A& Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, *53*(4), 50-58.

[11] Mell, P., & Grance, T. (2009). Draft nist working definition of cloud computing. *Referenced on June. 3rd*.

[12] Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). NIST cloud computing reference architecture. *NIST special publication*, *500*, 292.

[13] Bhardwaj, S., Jain, L., & Jain, S. (2010). Cloud computing: A study of infrastructure as a service (IAAS). *International Journal of engineering and information Technology*, *2*(1), 60-63.

[14] Dikaiakos, M. D., Katsaros, D., Mehra, P., Pallis, G., & Vakali, A. (2009). Cloud computing: Distributed Internet computing for IT and scientific research. *Internet Computing, IEEE*, *13*(5), 10-13.

[15] Lenk, A., Klems, M., Nimis, J., Tai, S., & Sandholm, T. (2009, May). What's inside the Cloud? An architectural map of the Cloud landscape. In *Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing* (pp. 23-31). IEEE Computer Society.

[16] Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision Support Systems*, *51*(1), 176-189.

[17] Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision Support Systems*, *51*(1), 176-189.

[18] Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision Support Systems*, *51*(1), 176-189.

[19] Feng, D. G., Zhang, M., Zhang, Y., & Xu, Z. (2011). Study on cloud computing security. *Journal of Software*, *22*(1), 71-83.

[20] Buyya, R., Yeo, C. S., & Venugopal, S. (2008, September). Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities. In *High Performance Computing and Communications, 2008. HPCC'08. 10th IEEE International Conference on* (pp. 5-13). Ieee.

[21] Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. (2008). A break in the clouds: towards a cloud definition. *ACM SIGCOMM Computer Communication Review*, *39*(1), 50-55.

[22] Foster, I., Zhao, Y., Raicu, I., & Lu, S. (2008, November). Cloud computing and grid computing 360-degree compared. In *Grid Computing Environments Workshop, 2008. GCE'08* (pp. 1-10). Ieee.

[23] Rimal, B. P., Choi, E., & Lumb, I. (2009, August). A taxonomy and survey of cloud computing systems. In *INC, IMS and IDC, 2009. NCM'09. Fifth International Joint Conference on* (pp. 44-51). Ieee.

[24] Lenk, A., Klems, M., Nimis, J., Tai, S., & Sandholm, T. (2009, May). What's inside the Cloud? An architectural map of the Cloud landscape. In *Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing* (pp. 23-31). IEEE Computer Society.

[25] J. McKendrick, NASA's Nebula: a stellar example of private clouds in government.] and GoFront's Cloud [C. Vecchiola, X. Chu, R. Buyya, Aneka: A Software Platform for.NET-Based Cloud Computing, IOS Press, Amsterdam, 2009, pp. 267–295.

[26] Rajkumar Buyyaa, Chee Shin Yeoa, , Srikumar Venugopala, James Broberga, and Ivona Brandicc, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility", Future Generation Computer Systems, Volume 25, Issue 6, June 2009, Pages 599-616

[27] Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision Support Systems*, *51*(1), 176-189.

[28] http://www.thencta.com/cloudsecurity.html (accessed October 10, 2012)

[29] Brunette, G., & Mogull, R. (2009). Security guidance for critical areas of focus in cloud computing v2. 1. *Cloud Security Alliance*, 1-76.

[30] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing (draft). *NIST special publication*, *800*(145), 7.

[31] Denning, D. E. R. (1999). *Information warfare and security* (Vol. 4). Reading MA: Addison-Wesley.

[32] https://cloudsecurityalliance.org/membership/corporate/

[33] https://cloudsecurityalliance.org/about/

[34] http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[35] Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009, September). On technical security issues in cloud computing. In *Cloud Computing, 2009. CLOUD'09. IEEE International Conference on* (pp. 109-116). IEEE.

[36] http://social.technet.microsoft.com/wiki/contents/articles/security-considerations-for-software-as-a-service.aspx(accessed October 13, 2012).

[37] Shankland, S.: Brace yourself for cloud computing. CNET News. http://news.cnet.com/8301–30685_3–10378782–264.html (2009). Accessed Oct 2009

[38] The NIST Definition of Cloud Computing (Draft), Peter Mell, Timothy Grance, NIST. http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

Alireza Ghobadi I completed my B.S of Mathematic with Computer Science at Khaje-Nasir-Toosi University, Tehran (Iran), in 1997. Then, I worked in a few companies at the industry level (in the field of IT and semiconductors). Recently, I completed Bachelor of Information Technology (major: Information Systems Engineering) in 2007, First master in Master Of Computer Science (Under fund of Intel Company in Malaysia) in Multimedia university, and Second Master in University Technology Malaysia. Currently, I am doing PHD Of Computer Science and also I am working under a funded project dealing with file management and transmission. I am IEEE member since 2012.