Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 8 (2013) pp. 279-289
© MIR Labs, www.mirlabs.net/jias/index.html

Modeling Security Risk Factors in a Cloud Computing Environment

Nada Ahmed[1], Ajith Abraham[2]

[1]Faculty of Computer Science & Information Technology, Sudan University of Science Technology, Khartoum, Sudan
nessa@pnu.edu.sa

[2]Machine Intelligence Research Labs (MIR Labs), Scientific Network for Innovation and Research Excellence, WA, USA
ajith.abraham@ieee.org

Abstract: With the rapid developments in information technologies and the success of Internet, computing resources have become cheaper, more powerful, and more available than before. This technological development has enabled the realization of long held dream called “computing as utility”, in which resources are provided as a general utility that can be leased and released by users through the Internet in an on-demand fashion. It emerged in to the market with a huge potential to fulfill this dream and many attractive promises that are inviting to many con summers around the world. As such, it offers many advantage, in terms of reduced cost, relief from managing complex IT infrastructure, flexibility, and scalability. However, cloud computing is a risky paradigm. For instance, the use of cloud services, which are external assets to their consumers, implies unprecedented risks that must be taken in account. |This paper highlights and categorizes risk factors associated with security involved in cloud computing and list some remediation to avoid these risks and help promote the benefits and mitigate the risks associated with cloud computing.

1. Introduction

Cloud computing raised as the most significant developments in modern computing, where computing resources such as: processing and storage are being offered as on demand services to individuals, companies, and government agencies, with users employing cloud computing for database management and mining, sharing and storing information, and deploying web services [9, 30, 31]. On an operational level, cloud computing free up the resources and refocusing them on core business activities, thereby, the potential for innovation is increased. A recent Gartner research report predicts that the global cloud market is expected to burst in the coming years [6]. The emergence of cloud computing represent a fundamental change in the way information technology service is invented, deployed, developed, maintained, scaled, updated, and paid [33]. Consumers in cloud computing use services as needed, shared resources as a service that can rapidly and elastically scale up and down as needed, and pay only for what is used, all these things is characterized the cloud computing [27].

Cloud computing aims to provide users with more flexible, scalable computing application, storage, and platforms in a transparent manner [32]. It provides a level of abstraction between the physical infrastructure and the owner of the information being stored and processed, because it stores the application software and databases in large data centers, where the management of the data and services are not trustworthy [5, 10]. In recent years there is obvious migration to cloud computing with end users, quietly handling a growing number of personal data, such as photographs, music files, book marks, and much more, on remote servers accessible via a network [16].

The use of cloud computing services can cause risks to consumers. Before consumers start using cloud computing services they must confirm whether the product satisfies their needs and understand the risks involved in using this service [11].

One of the largest disadvantages of cloud computing revolves around security and confidentiality [45]. The focus of this paper is to identify the risk factors that is associated with cloud computing, thereby they slowdown the adoption to cloud computing. Section 2 provides a brief description and makes a comparison between risk and the difference terminologies used to represent the same concepts. Section 3 details an overview of cloud computing its definition, service, and deployed models. Section 4 provides a detailed survey of the risk factors involved, and gives some recommendations to prevent or reduce its occurrence followed by Conclusions in Section 5.

2. The Nature of Risk

There are several words often used to represent the similar concepts even though they have different meanings and relationships to each other, Some examples are: Vulnerability, Threat, Risk, and exposure. It is important to know and understand the definition of each word.

Vulnerability refers to any weakness in software, hardware, or procedural that may provide an attacker an unauthorized access to a computer, network, or any resource within the environment. This vulnerability may be a service running on a server, unpatched applications or operating system software, or an unsecured physical entrance.

A threat is any potential danger to information or systems. The threat is someone, or something, that will identify a specific vulnerability and use it against the asset of the organization or an individual. Threat exploits vulnerability to cause damage or destruct a resource. A threat agent is the entity that takes advantage of vulnerability. A threat agent could be an intruder, a process, or an employee making an unintentional mistake that could expose confidential information or destroy asset.

An exposure is an instance to being exposed to losses from a threat agent. Vulnerability exposes an organization to possible damages. A risk is likelihood of a threat agent taking advantage of vulnerability. Risk ties the vulnerability, threat, and likelihood of exploitation to the resulting business impact (See Figure 1) [5, 17]. Risk is a choice individuals make depending on many factors, and the environment in which we live, it is not a fate [9]. There are many research works trying to make a definition of risk. ISO 31000:2009 with ISO/IEC Guide 73 defines risk as the “ effect of uncertainty on objectives” [15]. Others define risk as: “any context, whether in the technical context or otherwise is rarely zero” [28]. Third definition for risk as confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability, likelihood of occurrence and potential impact are the mean factor to rate the criticality of risk [29]. Risk is the possible impact or result of an event on assets of an organization, or when a threat is trigged by vulnerability [9, 26].

Risk is associated with the idea of reward. The organization can force challenge when there is not a well understand or fail to manage risk [15]. A control is generally put in to place to mitigate the potential risk. A control may be a policy, procedure, a software configuration, or a hardware device that eliminates the vulnerability or reduce risk. As risk cannot be completely eliminated, there is a need to reduce it.

Risk management is “the process of understanding, costing, and efficiently managing unexpected levels of variability in the financial outcomes for business” It includes all activities involved to bring risk to an acceptable level with acceptable cost [9]. Many research fields, e.g statistics, biology, engineering, and system analysis, have been considered about risk and its management. The risk management goal is to rank and prioritize risks in order to identify where the improvement is happen and, thus, focus all efforts on minimizing the effects of risk events [15].

Risk Assessment is targeted to assess the threats, impacts, and vulnerability of information processing facilities and the likelihood of the in accordance with the external and internal relative technology standards. Risk assessment is deemed as an integral part of information management [40]. The main target of risk assessment is to define appropriate controls for reducing or eliminating those risks [41].

3. Cloud Computing - Fundamentals

Cloud computing is changing with the evolution of technology and its service. There is no standard definition has been yet agreed for cloud computing [5]. Many computing researches attempted to define cloud computing in various ways, here are some of these definitions: Some researches define cloud computing as a paradigm that refers to a service that satisfies all of the following conditions [7]:

- Users access or process data depending on service.
- Use network to deliver the service.
- Service depends on virtualization as it one of the resources, which means that the user has no need to be aware about which server is running and deliver the service.
- The data is under legitimate control of the user, and
- The service is obtained under flexible contractual arrangement.

Cloud computing is viewed as one of the most promising technology in computing today. A number of key characteristics of cloud computing are identified [5, 12, 13, 16, 18, 36, 37]:

On-demand self-service: consumers have the ability to use cloud resources as they need without human interaction with each service provider.

Broad (ubiquitous) network access: capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource sharing: using multi-tenant all resources are pooled together to serve multiple consumers. The customer has no knowledge about the exact location of the provided resource, resources are assigned or reassigned according to consumer demand.

Rapid elasticity: unlimited capabilities are available to customers for provisioning in any time. These capabilities can be elastically provisioned and released, to scale rapidly outward and inward proportional with demand.

Measured service (pay as you go): resources in cloud offered as utility which users pay for on a consumption basis. Cloud provider controls computing resource.

3.1. Cloud computing Service Models

The services which cloud computing promises to provided can be categorized in to three service models (Figure 2) [5, 12, 13, 16, 43]:

- **Software as a Service (SaaS):** Users can use provider’s applications running on a cloud infrastructure. users can access the application from various client devices through either a thin client interface, such as a web browser (e.g., web-based e-mail), or a program interface. The underlying cloud infrastructure including network, servers, operating systems, or storage are under the control of cloud provider not the consumer. SaaS commonly referred to the Application Service Provider (ASP) model, is heralded by many as the new wave in application software distribution [44, 45].

- **Platform as a Service (PaaS):** in this model consumer deploy on to the cloud infrastructure, by using the tools supported by the provider such as programming language, libraries, and services consumer can created or acquired their applications. The consumer has the control over deployed applications, but has not any control over the underlying cloud infrastructure including network, servers, operating systems, or storage.

- **Infrastructure as a Service (IaaS):** the users are given access to elements of the computing infrastructure itself. Cloud provider provision processing, storage, networks, and other fundamental computing resource where the consumer is able to deploy and run arbitrary software, which can include operating systems.

3.2. Cloud computing Deployment Models

Four deployment models have been have been identified for cloud [13, 12, 16, 43]:

- Private cloud: private organization comprising multiple consumers can operate the cloud infrastructure. it may managed and operate by the organization, third party, or some combination of them, and it may exist on or off premises.
- Community cloud: the cloud infrastructure is provisioned for several organizations and support specific community that has communal concerns. It may be owned, managed, and operated by one or more of the organizations in community, a third party, or some combination of them, and it may exist on or off premises.
- Public cloud: in this model the cloud infrastructure is made available to public. It may be owned, managed, and operated by the organization selling cloud services, academic, or government organization, or some combination of them.
- Hybrid cloud: the cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between cloud.

4. Risks factors in Cloud Computing

Information System Audit and Control Association made a survey (2010) of nearly 1800 US business and IT professionals, 45% consider the risks of cloud computing as overbalance the benefits [6]. The aim from finding, identifying, and classifying the risk factors that may slow down the adoption to cloud computing is to help the cloud provider as well as the potential customers of cloud computing to know the major risks, also to decide whether or not start moving to cloud computing, besides that to enable them to create and follow risk assessment strategy to proactively protect their asset from these risks. Risk in cloud systems must be considered at service, data and infrastructure layers [9].

1. Privileged user access [6, 25, 38], data access [10] Organization's private and sensitive data must be secure and only authenticated users can access it. When using cloud then, the data is processed outside the premise of an enterprise, which brings a level of risk because outsourced services bypass the "physical, logical, and personnel controls", that an in house IT department exerts. Therefore, any outside or unwanted access is denied. The concept of store data somewhere outside the enterprise brings with it the risk of malicious insider and the top threats in this category named account and credentials hijacking. If the provider stored data in multiple countries, then the access to data may be subjected to the privacy laws of host country.

Prevention [6, 25, 38]

- Get much information about the people who manage the data.
- Ask provider to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access.
- Make a policy such as strong authentication process, no shared accounts, and a proper understanding of the service level agreements (SLA).

2. Data loss [2, 14, 17, 39, 23]

Data loss means that the valuable data disappear into the ether without a trace, cloud customers need to make sure that this will never happen to their sensitive data. An example if some malicious hackers may delete or alter records without having backup, another example, customers could lose their data to a careless cloud service provider or a disaster, such as earthquake, flood, fire. Some customers may encrypt their data to prevent theft, but this can be backfire if they lose the encryption key, which can be very painful.

Prevention [17, 39]

- Implement strong API access control.
- Encrypted and protect integrity of data in transit.
- Analyzes data protection at both design and run time.
- Implement strong key generation, storage and management, and destruction practices.
- Contractually demand providers wipe persistent media before it is released into the pool.
- Contractually specify provider backup and retention strategies.

3. Account of service traffic hijacking [2, 14, 17, 24, 39, 23]

Account of service traffic hijacking attack can happen with stolen credentials, if an attacker gain access to someone's credentials then he or she can eavesdrop on its activities, transaction, manipulate data, and redirect the customer to illegitimate sites. There is four attack types of this kind of risk: man-in-the-middle attacks, phishing, spam campaigns, and DoS attack. Account of service traffic hijacking attack can cause more significant damage if the cloud provider provides single sign-on or ID management services.

Prevention [17, 39]

- Prohibit the sharing of account credentials between users and services.
- Leverage strong two-factor authentication techniques where possible.
- Employ proactive monitoring to detect unauthorized activity.
- Understand cloud provider security policies and SLAs.

4. Insecure Application Programming Interfaces [2, 14, 17, 24, 39]

APIs are software that provided by cloud service provider for customers to use to manage and interact with their services, APIs is an important and necessary part to security and availability of whole cloud services. To have secure API there are two barriers: inability to audit events associated with API use, and incomplete log data to enable reconstruction of management activity. Building interfaces, injecting services will increase risk there for some organization may in force to relinquish their credentials to third party in order to enable their agency. Different security issues may expose if the interfaces is comparatively weak, security control mechanisms may not be able to fend API hacks, this may lead to unauthorized access to even privileged user functions.

Prevention [17, 39]

- Analyze the security model of cloud provider interfaces.
- Ensuring strong authentication and access controls are implemented in concert with encrypted transmission.
- Understand the dependency chain associated with the API.

5. Denial of Service (DoS) [2]

The dependence of organization on 24/7 availability on some services increases the problems with DoS, which in original is Internet threat. DoS failure can cost service providers and customers. Botnet malware enable malicious software to be installed on machines and load themselves into the computers without the owner's knowledge for unacceptable purposes. When a machine infected by bot malware, it becomes a zombie and can be controlled by botnet controller, then it can be used as a remote attack tool waiting to activated by their command and control servers. Cloud services exploited by cyber criminals to make distributed denial-of-service (DDoS) attacks, resulting in flood a web server with repeated message causing hanging up the system and denying access for legitimate users.

Prevention [10, 17, 39]

- Achieved the perfection of properties like isolation, inspection, and interposition.
- Stricter initial registration and validation processes.
- Monitoring public blacklists for one's own network blocks.

6. Malicious insiders [2, 14, 17, 21,39]

Cloud provider usually uses to hide from its employees the policy and the level of access it provides to them. Only employees with higher level of access can gain access to private data and service. In some cases where only the cloud service provider is responsible about security, the risk of insiders become massive especially with the cloud provider's inability in monitoring its employees, and they can cause greater ruin, their impact appear on: the confidentiality, integrity, and availability of all data. Insiders malicious they can be current employee, a contractor, or business partner who can access the network or data for causing damage.

Prevention [17, 39]

- Enforce strict supply chain management and conduct a comprehensive supplier assessment.
- Specify human resource requirements as part of legal contracts.
- Require transparency into overall information security and management practices, as well as compliance reporting
- Determine security breach notification processes.

7. Abuse nefarious use of cloud computing [2, 14, 17, 39]

Some cloud service providers do not maintain enough control, which let hackers; spammers to take advantage of the opportunities such as free limited trial. The cloud providers face a challenge here because they have to determine what constitute abuse and set the best process to identify it. Abuse may take different shapes like if someone try to break an encrypted key, some malicious hacker use cloud server to launch DDoS attack, propagate malware or share thieved software. When there are some abuse and nefarious activities in progress, cloud-computing provider must become the first one to know.

Prevention [17, 39]

- Enhanced credit card fraud monitoring and coordination.
- Comprehensive introspection of customer network traffic.
- Stricter initial registration and validation processes.
- Monitoring public blacklists for one's own network blocks.

8. Insufficient due diligence [2]: To start using cloud, the organization needs to fully understand the cloud environment and its associated risk. An organization must be sure that they have appropriate resource and they have a team that are familiar with cloud technology to prevent the issues may arise from jumping to cloud computing such as operational and architectural issues.

Prevention [2]

Make sure that the sufficient resources is available and to perform extensive due diligence before jumping into the cloud.

9. Shared access [2, 17, 25, 39]

Multi-tenancy is key factor of cloud computing service. To achieve scalability cloud provider provide shared infrastructure, platform, and application to deliver their services, this shared nature enable multiple users to share same computer resources, which may lead to leaking data to other tenants, also one flaw could allow an attacker to see all other data. If the foundation of computing resources not offers strong isolation for a multitenant, the risk arises in all delivery models.

Prevention [17, 39]

- Implement security best practices for installation/ configuration.
- Monitor environment for unauthorized changes/ activity.
- Promote strong authentication and access control for administrative access and operations.
- Enforce service level agreements for patching and vulnerability remediation.
- Conduct vulnerability scanning and configuration audits.

10. Regulatory compliance [6, 19, 21, 25, 38]

Traditional service providers are subjected to external audits and security certification, and they give their customers some information about the security controls that have been evaluated. If the provider is unable or unwilling to undergo such audit should only be considered for most trivial functions. Many countries pass the laws that enacted data protection which European Economic Area (EEA) pass first, as CSA (2011) explains. Regardless of location, the custodian is ultimately responsible for ensuring the security, protection, and integrity of the data, especially when they are passed to a third party. Data location is a related issue and represents a big concern especially with regards to the privacy regulations in different jurisdictions or when data hosted in high-risk countries. In addition, CSA (2011) points out many governments restrict the transfer of data outside the country.

Prevention [6, 25, 38]

- Cloud computing provider does not adhere to do this is signaling that customers can only use them for the most trivial functions.
-

11. Data breaches [2, 10]

Virtual machine (VM) could use side-channel timing information to extract private cryptographic keys in use by other VMs on the same server. Cloud environment present a high value target to attackers, and therefore, the data from different users hosted in cloud environment. Breaching in to cloud environment will potentially attack all users data. Those attackers can exploit a single flaw in one client's application to get to all other client's data as well, if the cloud service databases are not designed properly. Besides that, there is a risk from insiders, although they don't have a direct access to databases, the insider breaches risk is still high and can be a massive impact on the security. Verizon business in their '2011 Data Breach Investigations Report (DBIR)' [22] reported that both hacking and male ware arise as the most effected categories that lead to data breaches, the report mention that data breaches can occur due to:

- Utilized some form of hacking - 50%
- Incorporated malware - 49%
- Involved physical attacks - 29%
- Resulted from privilege misuse -17%
- Employed social tactics - 11%

Prevention

SaaS providers must be compliant with PCI DSS (Payment Card Industry-Data Security Standards) (PCI DSS, 2009) in order to host merchants that must comply with PCI DSS.

12. Long term viability [6, 19, 21, 25, 38]: The nature of business environment, competitive pressure, and the changes happening in it leads to some events that may affect the cloud service provider, such as merger, go broke, bankruptcy, or it acquisition by another company. These things lead to loss or deterioration of service delivery performance, and quality of service. Customers must ensure data availability in these situations.

Prevention [19]

- Customers should examine their providers by performing checks on their revenues, profitability, and number of customers.
- Customer should regularly backup their data and application.
- Service provider must make sure data security in negative business conditions like prolonged outage etc.
- Service provider must ensure the data safety in changing business situation.
- Customers should have emergency plans for their data and application porting and enquire whether the provider offers technical support in such scenarios.

13. Data location [6, 10, 19, 25, 38]: Most cloud service providers have many data centers around the globe. When the customer start using the cloud platform, they are not aware about the place of the datacenter in which their data stored beside that they don't have any control over the physical access mechanisms to that data. When regards to privacy regulation in different jurisdiction, in different countries where the government restrict the access to data in their borders, or if the data stored in high-risk countries, all these things make data location big concern issue.

Prevention [25]

- The service provider must tell their consumers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers.
- Cloud model must be capable of providing reliability to the customer on the location of data of the consumer.

14. Data segregation [8, 10, 19, 21, 25, 38]

Multi tenancy and shared resource are major characteristics of cloud computing where multiple users can share same computing capacity, storage, and network. The risk arise here come from the failure of the mechanisms to separate data in storage, and memory, from multiple tenants in the shared infrastructure. To observe system and end user security behaviors, the existence or absence of technical issue such as encrypted communication and virtualization security, and fundamental architectural concerns such as a dependence on the Internet and missing choke points can be used. In this environment the intrusion of data of one user becomes possible, therefore, the probability of this scenario depend on cloud model the likely in private models is lower than public models.

Prevention [10, 25]

- The cloud model should ensure a clear boundary for each user's data, not only on physical level but also at the application level.
- Test and validate the data segregation by doing SQL injection flaws, data validation, and insecure storage.
- Encryption. The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists, because encryption accidents can make data totally unusable.

15. Recovery [6, 19, 25, 38], Backup [10]

ENISA (2009) finds that 52.8% of SME (Small and Medium Enterprise) vote disaster recovery capabilities as a reason for start using cloud computing. Cloud users do not know where their data is hosted. Some events such as man-made, or natural disaster may happen; in such events customers need to know what will their data and long the recovery process take.

Prevention [6, 10, 19, 25, 38]

The cloud provider should has the ability to do a complete and quick restoration, and the customer should know how long it take.

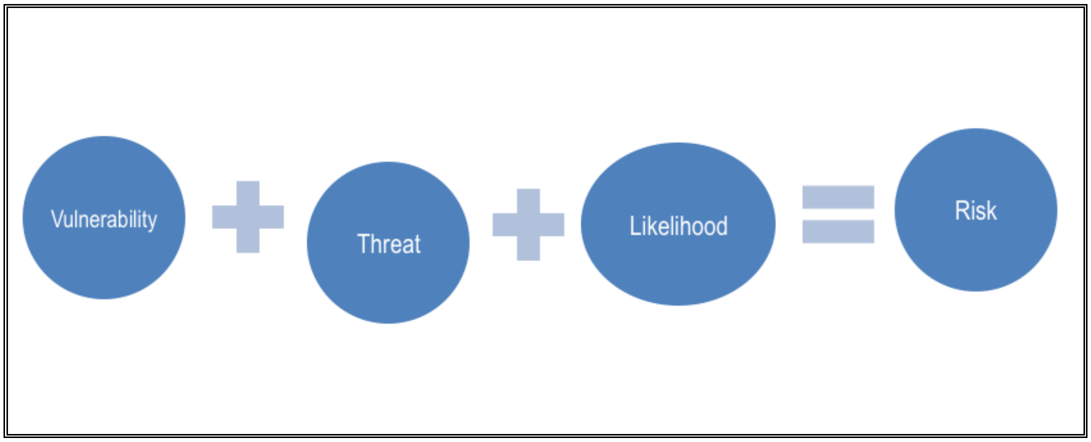

Figure 1: The relationship between Risk, Vulnerability, Threat, and Likelihood

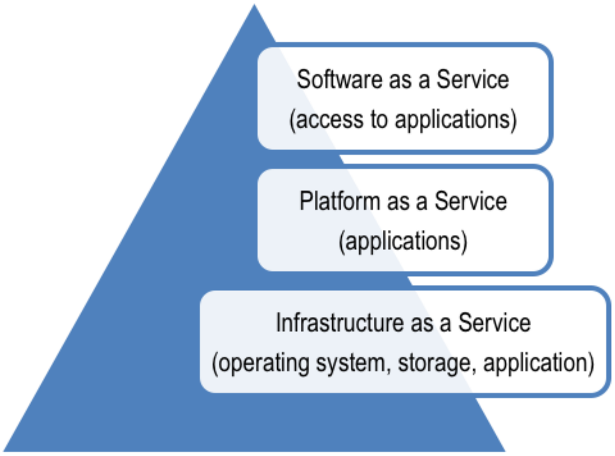

Figure 2. Cloud computing service models

16. Investigative support [6, 19, 25,38]

The investigation of an illegal activity may be impossible in cloud computing environment, because multiple customer's data can be a located in different data centers that are spread around the globe, which makes the investigation difficult, time consuming, and expensive. If the enterprise relies on the cloud service for the processing of business records then it must take into account the factor of inability or unwillingness of the provider to support it.

Prevention [6, 25, 38]

The contractual agreement should include the support of certain investigation activities.

17. Virtualization vulnerabilities [3, 4, 10, 19]

Virtualization is one of the fundamental components of the cloud service. However it introduces major risks as every cloud provider uses it. Beside its own risks it hold every risk posed by physical machines. There are two issues in using virtualization; first one is to ensure that different instances running on the same machine is separated from each other. Current virtual machines do not offer perfect isolation. The second is the control of administrator on host and guest operating systems. VMM (Virtual Machine Monitor) is a software layer that abstracts the physical resources used by multiple virtual machines. It provides a virtual processor, I/O devices, storage, memory and other virtualized system devices. Virtual machine should be "root secure" which mean to ensure no privilege with the virtualized guest environment permits interference with the host system. All virtualization software has vulnerability, which can be exploited by malicious, local users to bypass certain security restrictions or gain privileges. There are four types of virtual exploits risks: server host only, guest to guest, host to guest, and guest to host, which they are unknown and not mention in all people risk models. Still there is a need to achieved perfection of properties like isolation, inspection, and interposition in VMMs.

Prevention [10]

Achieved the perfection of properties like isolation, inspection, and interposition.

18. Availability [3, 4, 9, 10, 20]: The most important thing to the cloud-computing provider is that their customers must be provided with service around the clock, but outages do occur and can be unexpected and costly to customers. Cloud providers availability can be affected by many factors such as natural disaster, which can cause cloud services to become unavailable or lead to loss of Internet connectivity. Another factor that may affect availability is the priority of users on the cloud, how it determined, should the overcapacity threshold is reached. Every cloud provider aims to have good availability, which involves making architectural changes at application and infrastructure levels to add scalability and high availability.

Prevention [3, 6, 10]

- Considered an appropriate action plan for business continuity for any unplanned emergencies.
- The enterprise and cloud provider define, an SLA for the availability of service for critical business process.
- Consumers should always backup the data it's sharing with the cloud or at least insist on legalese that has the right amount of damages built in if that data is lost forever.

19. Third party management

There are many issues in cloud computing related to third party because the client organizations are not directly managed by the cloud service provider. Some old concerns in information security appear with outsourcing such as integrity control and sustainability of supplier and all risks that client may take if it rely on a third party. The new concern is the wish for cloud service to be much more of a utility in the way that it operates.

Prevention [8]

Have service relationship with many clients, which require a universally accepted audit certification reported into the client's Enterprise Risk Management and its Governance, Risk and Compliance Reporting.

20. Integration with existing enterprise security process [8]

Some organizations invested in access control and identity management system to provide a secure single sign-on to services and applications. These integration successes are challenged by cloud computing if they not have their own separately managed user identifier and access password. There are two areas where loss of integration can occur first. One where encryption keys come under the management of third party and not the client, second one if monitoring of user access is not available for behavioral monitoring.

Prevention [8]

- Cloud computing services should have their own separately managed user identifier and access password.
- Encryption key should come under the management of the client.
-

21. Ownership [3]

The data owner is sometimes not only the customers in the contract as some cloud provider include explicitly some terms state that the data stored is the provider's not the customer's. If the cloud vender is owing the data it gives them more legal protection in case if something goes wrong, beside that they can get additional revenue opportunities for themselves by searching and mining customer data. In few cases where cloud vendor went out of business, their customer private data sold as part of the asset to the next buyer.

Prevention [3]

The customer must make sure who owns the data and what can the cloud provider do with it.

22. Launch pad for brute force and other attacks [4]

Cloud services can be exploited as a launch pad for other attacks by performing strong force on line password guessing attacks. Although this kind of attacks is still expensive but it may affect systems using passwords-based authentication.

23. **Rogue clouds**

Cloud computing represents a new domain for exploit to crime groups. Rogue clouds are host confidential business data and provide all other cloud computing service for a high fee. Criminals groups can abuse this service to store and distribute criminal data; the risk of rogue clouds is to mining data for secondary uses such as marketing and reselling the mined data to other businesses.

24. Espionage risks [4]

In some cases the intelligence is needed to obtain information relevant to vital national or corporate interests. For this reason cloud service providers may be compelled to scan and search data that may relate to national security or some data transactions that may be liable to the laws of the jurisdiction of the country where the physical machine is located.

25. Governance [20], Regulation [4]

It is necessary for the organization that the cloud provider support the policies used with its data and application such as policies done for deploying, managing, archiving and deleting. As data is liable to laws and regulations, the cloud provider must keep the organization in compliance. Failure to comply with data protection legislation may lead to administrative, civil, and criminal sanctions. One of the (SLA) terms must be for responsibilities of cloud provider for enabling governance.

Prevention [4]

- Client can include clauses in their SLAs that indicate the law governing the SLA, the choice of the complete court in case of disputes arising from the interpretation and the execution of the contract.
- Ensure that SLAs and other legally binding contractual arrangements with cloud service providers comply with applicable regulatory obligations and industry standard.

26. Network security [10]

Sensitive customer's data is stored and processed by cloud provider. This data flow over the network needs to be secured to prevent leakage of sensitive information, because malicious users can exploit weaknesses in network security configuration to sniff network packets.

Prevention [10]

- Use strong network traffic encryption techniques such as Secure Socket Layer (SSL) and the Transport Layer Security (TLS) for security.
- Applying assessment such as Network penetration and packet analysis, session management weaknesses, and insecure SSL trust configuration to test and validate the network security.

27. Data confidentiality, privacy [1, 10, 20]

When dealing with sensitive data, privacy arises as an important issue, especially in a sharing environment like cloud computing, which involves sharing by users of their information on remote servers operated by other and they can access their data through internet or other connections. Many types of data undergo privacy laws, copyright protection or expert restrictions. Some of the feedback related to the confidentiality issues is as follows:

- The terms of service and privacy policy established by cloud provider vary significantly with user's privacy and confidentiality risks.
- The legal location of information in cloud computing may be more than one at the same time with differing legal consequences.
- Privacy and confidentiality protections of information and privacy obligations of those who process or store the information are significant effect by the location of information in the cloud.
- Both privacy of personal information and the confidentiality of business and governmental information, cloud computing has significant effects upon them.
- Remote storage may have inverse consequences for the legal status of protection for personal or business information.
- Cloud provider may be forced by laws to examine user data for proof of criminal activity and other cases.
- The assessment of information status in cloud as well as the privacy and confidentiality protections available to users is very difficult because of legal uncertainties.
- Privacy and confidentiality rights, obligations and status sometimes may change for some types of information and some categories of cloud computing users, when user exposes information to a cloud provider.

Prevention [20]

Cloud provider should deliver the added controls needed to protect sensitive data

Organization can audit cloud provider to prove that it followed the appropriate procedures.

28. Web application security [10]

Some vulnerability, which can create from security holes, can potentially have harmful impact on all cloud customers. Challenges that faced cloud SaaS application, is like the other web application come from traditional network security solutions such as network firewalls, network intrusion detection and prevention systems (IDS & IPS), do not treat the problem in a proper way. New risks arise with web applications that need application level defenses. In the report published by Verizon Business 'Verizon Business 2008 Data Breach Investigation Report' [23], 59% of data breach caused by hacking with the following breakdown:

○ Application/ service layer - 39%
○ OS/platform layer - 23%
○ Exploit known vulnerability - 18%
○ Exploit unknown vulnerability - 5%
○ Use of back door - 5%

If the application is vulnerable to attacks, the data behind the application is at risk.

29. Data Integrity [10]

One of the most critical elements in all systems is data integrity. It is easy to achieve in a standalone system with a single database and it can maintain via database constraints and transactions. Achieving data integrity is much complex in distributed systems where there are multiple databases and multiple applications. Cloud computing magnified the problem of data integrity, as there is mix of on-premise and SaaS applications exposed as service. SaaS applications are multi-tenant applications and they hosted by a third party. The biggest challenge, which endanger the data integrity is transaction management, at the protocol level, does not support transactions or guaranteed delivery. If data integrity is not guaranteed and there is lack in integrity controls, this may result in deep problems.

Prevention [10]

- Using the standard available for managing data integrity such as WS-Transaction and WS-reliability, although they are not yet mature.
- Making sure that the architects and developer do not compromise data integrity in their zeal to move to cloud computing.

30. Authentication and access control [3, 10]

The mechanisms that organization makes for Authentication, authorization, and access control depend on the process. The rules they follow to remove ancient accounts, the number of privilege accounts that can access their systems and thus customers data, if the cloud provider shared name spaces and authentication to create single-sign-on which is great for productivity, but it increase risks. Many companies increase their employee information in some type of Lightweight Directory Access Protocol (LDAP) server. In the SaaS model applications are stored outside the enterprise in SaaS providers databases, which require from customers to remember to remove account as employees leave the organization and create accounts as come onboard.

31. Identity management [10, 20]

In cloud computing the information that users need may come from different sources, that has its own access control mechanisms. Identity management (IDM) deals with identifying individuals in a system and operates constraint on the established identities to control access to the system resources. Identity management has three perspectives:

- The user access (log-on) paradigm: such as smart card
- The pure identity paradigm: the operations on identities such as creation, management, and deletion without regard to access.
- The service paradigm is a system that provides presence-based, on-demand, online, multimedia, personalized role-based services to users and their devices.

Prevention [10]

Support identity management and sign on services by using models such as Independent IDM stack, Credential synchronization, Federated IDM.

32. Interoperability and portability [20]

Interoperability means the ability of systems to communicate, in other words is the ability of the code to run with more than one cloud provider simultaneously. Portability is the ability to run systems written for one environment in another environment. Interoperability and portability become crucial because if the organization locks to a specific cloud provider, then the organization will be at the mercy of the service level and pricing policies of that provider and it hasn't the freedom to work with multiple cloud provider.

Prevention [20]

Consider Interoperability and portability before moving to cloud

33.Service level agreement (SLAs) [20]

The interaction between a cloud service provider and a cloud consumer is defined by an (SLA). In other words the (SLA) represents the foundation for the costumer to trust in the provider. The organization needs to ensure that the terms of (SLA) are being met. Besides other terms, an (SLA) may contain:

- The responsibilities of both provider and consumer
- A set of service the provider will deliver
- A set of metrics to determine whether those services are delivering as the provider promised**.**

Prevention [20]

- Organization needs to monitor the provider to ensure that the terms of SLA are being met.
- Cloud provider should have the transparency and notifying consumers of any outages or problems that occur.
- A provider might need to be certified for certain standard.

34. Performance [1, 20]

Before moving to cloud computing an organization need to be sure about adequate performance, because if moving to cloud will save money. However if the performance level is unacceptable then no need to this saving. Service Level Objectives (SLO) is used to define the performance that the cloud provider must deliver; it should be a part of (SLA).

Prevention [20]

Define the performance the cloud provider must deliver in Service Level Objectives (SLO), which should be part of the SLA

35. Testing [20]

Running the application in more than one virtual machine can do testing application in cloud and then start testing and when it finishes all virtual machines can be shutdown. There are some things in a cloud that tester must be aware about it such as: cloud service perform is much slower than local services, and many cloud services are massively redundant, meaning that the changes made to a cloud service must be replicated to other cloud provider's infrastructure.

36. Business Reputation Due to Co-Tenant Activities [21]

Due to the sharing resource nature of cloud computing, if one tenant carried malicious activities the reputation of other tenants may be affected. These activities may lead to:

- IP address getting blocked
- Confiscation of resources due to neighbor activities.

The impact can be appear as a problems for the organization's reputation in addition to service delivery, and data loss.

37. Supply chain failure [21]

In some situation, the level of security of the cloud provider may depend on the level of security of each one of the links and the level of dependency of the cloud provider on the third party. This situation can take place if cloud provider can outsource certain specialized tasks of its 'production' chain to third parties. Some issues can happen as a result of the lack of coordination of responsibilities between all the parties such as loss of data confidentiality, integrity and availability, unavailability of service, violation of SLA, economic and reputational losses due to failure to meet customer demand, cascading service failure, etc. Lack of transparency in the contract can be a problem for the whole system. Its impact can appear in decreasing the level of trust in the provider.

38. Resource Exhaustion [21]

Cloud provider allocates resource according to statistical projections. Inaccurate modeling of resources usage can lead to:

- Service unavailability: failure in certain application, which use a specific resource very intensively.
- Access control compromised: in the event of resource exhaustion, it may be possible to force system to 'fail open'.
- Economic and reputational losses: failure to meet customer demand
- The opposite consequences of inaccurate estimation of resource
- Infrastructure oversize: excessive provisioning leading to economic losses and loss of profitability.

39.Management Interface Compromise [21]

The risk increased in customer management interfaces of public cloud because they are Internet accessible and mediate access to larger sets of resources especially when combined with remote access and web browser vulnerabilities.

40. Conflicts between customer hardening procedures and cloud environment [21]

Cloud provider should articulate their isolation mechanisms and assist their customers to secure their resource by providing best guidelines. If the customers fail to properly secure their resources would place them at further risk.

41.Subpoena and e-discovery [21]

If the cloud provider's physical hardware is confiscated as a result of subpoena by law-enforcement agencies, the centralization of storage as well as shared tenancy of physical hardware means many more clients are at risk of the disclosure of their data unwanted parties.

42. Changes of jurisdiction [21]

The data center in which customer's data stored may be held in multiple jurisdictions, some of which may be high risk.

43. Licensing risks [21]

Licensing conditions may become unworkable in cloud environment. In the case of PaaS and IaaS, there is the possibility for creating original work in the cloud, but if not protected by the appropriate contractual clauses, this original work may be at risk.

5. Conclusions

Cloud computing represents a new computing paradigm, where computing resources are being offered to users as services. It comes with several benefits for both cloud providers and consumers. However, the need to understand the associated risks are imperative before deciding to make the shift towards cloud computing. Several risks need to be accounted and addressed. This paper is started with the definition of risk and provided a brief description about risk management, and risk assessment. Then we addressed risk factors related to cloud computing and give a description for each risk factor. The article is expected to help cloud providers, organizations, and individual users to understand and identify the various security related risks when using the cloud-computing environment.

References

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, M. Zaharia "A view of cloud computing," *Communications of the ACM*, vol. 53, pp. 50-58, 2010.

[2] 9 top threats to cloud computing security: http://www.infoworld.com/t/cloud-security/9-top-threats-cloud-computing-security-213428

[3] The 5 cloud risks you have to stop ignoring, March 19, 2013:http://www.infoworld.com/d/security/the-5-cloud-risks-you-have-stop-ignoring-214696

[4] K.-K. R. Choo, "Cloud computing: challenges and future directions," *Trends and Issues in Crime and Criminal Justice*, p. 1, 2010.

[5] K. M. Dahbur, Bassil Tarakji, Ahmad Bisher, "A survey of risks, threats and vulnerabilities in cloud computing," in *Proceedings of the 2011 International conference on intelligent semantic Web-services and applications*, 2011, p. 12.

[6] N. Brender and I. Markov, "Risk perception and risk management in cloud computing: Results from a case study of Swiss companies," *International Journal of Information Management*, vol. 33, pp. 726-733, 2013.

[7] D. C. Svantesson, Roger, "Privacy and consumer risks in cloud computing," *Computer Law & Security Review*, vol. 26, pp. 391-397, 2010.

[8] P. Dorey and A. Leite, "Commentary: Cloud computing–A security problem or solution?," *information security technical report*, vol. 16, pp. 89-96, 2011.

[9] S. Paquette, P.T. Jaeger, S. C. Wilson., "Identifying the security risks associated with governmental use of cloud computing," *Government Information Quarterly*, vol. 27, pp. 245-253, 2010.

[10] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, pp. 1-11, 2011.

[11] S. A. Chandran, Mridula" ,Cloud Computing: Analyzing the risks involved in cloud computing environments," *Proceedings of Natural Sciences and Engineering*, pp. 2-4, 2010.

[12] T. W. Dillon, Chen Chang, Elizabeth, "Cloud computing: issues and challenges," in *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*, 2010, pp. 27-33.

[13] P. Mell and T. Grance, "The NIST definition of cloud computing," *National Institute of Standards and Technology*, vol. 53, p. 50, 2009.

[14] M. T. A. Khorshed, ABM Wasimi, Saleh A, "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing," *Future Generation computer systems*, vol. 28, pp. 833-851, 2012.

[15] J. O. G. Fitó, Jordi, "Business-driven management of infrastructure-level risks in Cloud providers," *Future Generation computer systems*, vol. 32, pp. 41-53, 2014.

[16] D. L. Zissis, Dimitrios, "Addressing cloud computing security issues," *Future Generation computer systems*, vol. 28, pp. 583-592, 2012.

[17] M Potey, Manish, C. A Dhote, and Deepak H Sharma. "Cloud Computing Understanding Risk, Threats, Vulnerability and Controls: A Survey." *International Journal of Computer Applications* 67.3 (2013): 9-14.

[18] Cloud Computing use cases White Paper: http://opencloudmanifesto.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.pdf

[19] A. K. Sangroya, Saurabh Dhok, Jaideep Varma, Vasudeva, "Towards analyzing data security risks in cloud computing environments," in *Information Systems, Technology and Management*, ed: Springer, 2010, pp. 255-265.

[20] Moving to Cloud: http://cloudusecases.org/Moving_to_the_Cloud.pdf

[21] Cloud Computing: Benefits, Risks and Recommendations for Information Security (ENISA), European Network and Information Security Agency: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

[22] W. H. Baker, A Hylender, C David Pamula, J Porter, C Spitler, M, "2011 data breach investigations report," *Verizon RISK Team, Available: www. verizonbusiness. com/resources/reports/rp_databreach-investigations-report-2011_en_xg. pdf*, pp. 1-72, 2011.

[23] S. K. Shin, Kazukuni, "Towards secure cloud storage," *Demo for CloudCom2010*, 2010.

[24] S. L. Srinivasamurthy, David Q, "Survey on Cloud Computing Security," in *Proc. Conf. on Cloud Computing, CloudCom*, 2010.

[25] Brodkin, Jon. "Gartner: Seven cloud-computing security risks." (2008).

[26] L. B .A. J. Rabai, Mouna Aissa, Anis Ben Mili, Ali, "A cybersecurity model in cloud computing environments," *Journal of King Saud University-Computer and Information Sciences*, vol. 25, pp. 63-75, 2013.

[27] M. V. d. M. Carroll, A Kotze, P, "Secure cloud computing: Benefits, risks and controls," in *Information Security South Africa (ISSA), 2011*, 2011, pp. 1-9.

[28] P. F. Ryan, Sarah, "Trust in the clouds," *Computer Law & Security Review*, vol. 28, pp. 513-521, 2012.

[29] P. A. Shamala, Rabiah Yusoff, Mariana, "A conceptual framework of info structure for information security risk assessment (ISRA)," *Journal of Information Security and Applications*, vol. 18, pp. 45-52, 2013.

[30] W. H. Xiong, Hanping Xiong, Naixue Yang, Laurence T Peng, Wen-Chih Wang, Xiaofei Qu, Yanzhen, "Anomaly secure detection methods by analyzing dynamic characteristics of the network traffic in cloud communications," *Information Sciences*, vol. 258, pp. 403.2014 ,415-

[31] M. B. Mackay, T Al-Yasiri, A, "Security-oriented cloud computing platform for critical infrastructures," *Computer Law & Security Review*, vol. 28, pp. 679-686, 2012.

[32] D. C. Sun, Guiran Sun, Lina Wang, Xingwei, "Surveying and analyzing security ,privacy and trust issues in cloud computing environments," *Procedia Engineering*, vol. 15, pp. 2852-2856, 2011.

[33] M. Avram, "Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective," *Procedia Technology*, vol. 12, pp. 529-534, 201.4

[34] V. Choudhary, "Software as a service: Implications for investment in software development," in *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, 2007, pp. 209a-209a.

[35] Mackay, M., T. Baker, and A. Al-Yasiri. "Security-oriented cloud computing platform for critical infrastructures." *Computer Law & Security Review* 28.6 (2012): 679-686.

[36] G. Reese, *Cloud application architectures: building applications and infrastructure in the cloud*: " O'Reilly Media, Inc.", 2009.

[37] B. W. Grobauer, Tobias Stocker, Elmar, "Understanding cloud computing vulnerabilities," *Security & privacy, IEEE*, vol. 9, pp. 50-57, 2011.

[38] J. N. Heiser, Mark, "Assessing the security risks of cloud computing," *Gartner Report*, 2008.

[39] Hubbard, Dan, and Michael Sutton. "Top Threats to Cloud Computing V1. 0." Cloud Security Alliance (2010).

[40] L. D. Peiyu, LIU, "The new risk assessment model for information system in cloud computing environment," *Procedia Engineering*, vol. 15, pp. 3200-3204, 2011.

[41] S. H. Drissi, H Medromi, H, "Survey: Risk Assessment for Cloud Computing".

[42] B. P. C. Rimal, Eunmi Lumb, Ian, "A taxonomy and survey of cloud computing systems," in *INC, IMS and IDC, 2009. NCM'09. Fifth International Joint Conference on*, 2009, pp. 4.51-4

[43] F. K. Hoch, Michael Griffith, Anne, "Software as a service: Strategic backgrounder," *Software & Information Industry Association (SIIA)*, 2001.