# A Review on Risks Analysis towards the Correctness of the Data in the Cloud

[1]S. Annapoorani, [2]G. A. Mylavathi, [3]Dr.B. Srinivasan
[1]Assistant Professor, [2]Assistant Professor, [3]Associate Professor
Department of Computer Science
Gobi Arts & Science College, Gobichettipalayam, Tamil Nadu, India

---

***Abstract* — In recent years, cloud computing has been an emerging technology computing model in the IT industry. Machines involved in cloud computing deliver services in a scalable manner. It provides efficient computing by centralizing storage, memory processing and bandwidth. Adopting cloud computing can result in both positive and negative effects on data security. This paper presents a study about the security risk issues involved in cloud computing. It highlights the different types of risks and how their existence can affect the cloud users. It also discusses the different circumstances in which the risks occur and the measures to be taken to avoid them. The paper also attempts to lay out measures to be taken while using cloud computing to reduce negative effects on the outcome and maintain data integrity.** *(Abstract)*

***IndexTerms*— Computing Model, IT Industry, Security Risk Issues.** *(keywords)*

---

## I. INTRODUCTION

Cloud computing has served the ever growing storage and data processing needs, however it has also given rise to a number of risks. The risks arise due to the various factors such as the location of the data centres, data segregation, data integrity, infrastructure and lack of knowledge about the governing policies. In a cloud computing environment, the resources are used when required and this is expected to translate into reduced costs of maintenance and elastic scalability. For example, in order to process a user request, the service provider decides upon the resources to be utilised for the particular task and when these resources needs to be released. Since the entire process is carried out by the service provider and not by the user, the security and integrity of the user's data becomes a significant concern.

This paper analyses three major risks associated with cloud computing namely, 1) Security risks 2) Privacy risks 3) Consumer risks. In section 2 cloud computing is explored as a process along with its pros and cons. Section 3 focuses on the risks involved and the need for risk analysis. It further dwells on specific risks involved in the arena of biomedical information sharing. Further, the privacy risks involved in the two main cloud structures and risks associated with the consumers are also discussed. These risks are put into perspective by considering Google Docs as a background. A conclusion is established in Section 4 after reviewing through preceding sections covering the current cloud computing practices and risk mitigation measures being factored in the process.

## II. WHAT IS CLOUD COMPUTING

Cloud computing is an internet-based model of computing, where the shared information, software and resources are provided to computers and other devices upon demand. This enables the end user to access the cloud computing resources anytime from any platform such as a cell phone, mobile computing platform or the desktop. The data and the software applications required by the users are not stored on their own computers; instead they are stored on remote servers which are under the control of other hosts. The users are not necessarily aware about which server running on which host is providing the service. The current major cloud service providers are Microsoft, Hewlett Packard, IBM, Salesforce, Amazon and Google.

The two most significant components of the cloud computing architecture are the front end and the back end. The front end includes the client's computer and the application required to access the cloud computing system. All the cloud computing systems do not provide the same user interface. Web services like electronic mail programs control some existing web browsers such as Firefox, Microsoft's internet explorer or safari. Other type of systems has some unique application which provides the network access to its clients. The back end of the cloud computing architecture consists of the various servers, computers and the data storage devices, in other terms this network of interconnected devices constitute 'the cloud'.

Cloud computing components can be further typified as the cloud infrastructure, cloud platform and cloud application. Cloud infrastructure consists of various cloud services such as computational resources (Virtual Machines), data storage and communication networks such as Amazon's Elastic Compute Cloud. The cloud platform provides well-defined APIs for interaction with the cloud application such as the Google's App Engine or Salesforce.com. Finally the cloud application being the web service that runs on top of the cloud platform or the infrastructure. These are the commonly used public interface applications such as the Google's GoogleDocs. The Figure 1 represents the three cloud computing components.

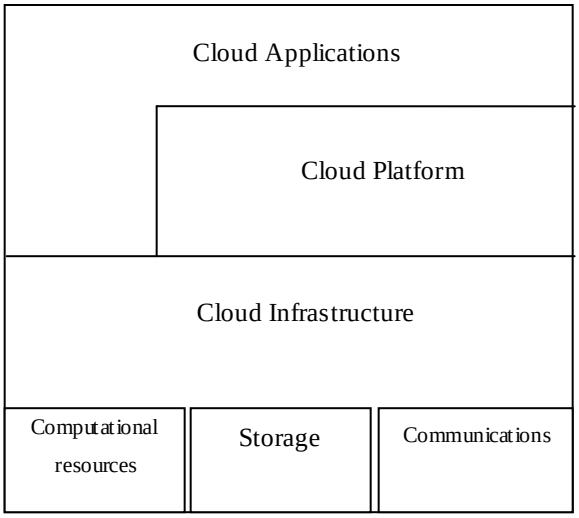


Figure 1. The different cloud computing components. The layered figure represents the inter-dependency between the different layers in the cloud.

**Advantages in Cloud Computing**

- Reduced setup costs can be considered as a major advantage for cloud computing, since the costs involved in setting up a data centre are not very high.
- In addition to the IT industry, even small scale businesses can adopt this environment (model).
- Considering cloud computing from the aspect of power management, it serves as a virtual server which is easier to implement in comparison to physical servers.
- Hardware management failure can also be localized and rectified with relative ease.
- Various data centres are spread throughout the country and thus it makes easy for the businesses to use preferred sites.
- The assessment of data can be done any time and is highly beneficial for the IT industry in reducing workloads.
- The cloud computing environments are easily scalable.
- Backup recovery is very easy in Infrastructure as a Service (IaaS) Providers, hence there is efficient incident response whenever data needs to be recovered.

**Disadvantages in Cloud Computing**

- A major disadvantage in cloud computing is that it is under the maintenance and supervision of a third party. Hence the confidentiality and security measures are less secured.
- In cloud environments the data is not specifically segregated. It is distributed throughout the cloud network and causes problems when specific data needs to be segregated.
- Another major drawback is the dependence on network connectivity. Network failures can result in loss to the company by causing extensive time delays.
- The Service Lease Agreements (SLA) are the agreements made with the service providers controlling varied equipment in the cloud network. These agreements should be carefully verified before entering into a contract of service.
- The quality of service is a key determining factor in the efficiency of a cloud network. A reliable service provider providing desired quality of service may be difficult to source and the process set-up could turn out to be time consuming.

## III. RISK ANALYSIS

In order to create awareness among the users of cloud computing regarding the serious threats and vulnerabilities involved in cloud computing environments, a study on various risks is imperative. In the sections below, we discuss the different risks.

### Security Risks

The state of preventing a system from vulnerable attacks is considered as the system's security. Security risks involved with the governmental use of cloud computing have various risk factors. Seven important identity factors for risk in a cloud computing model are: Access, Availability, Network load, Integrity, Data Security, Data Location and Data Segregation.

### Access

The data in a private organization allows only the authenticated users to access the data. The access privilege must be provided only to the concerned customers and auditors in order to minimize such risks. When there is an access from an internal to external source, the possibility of risk is more in case of sensitive data. Segregation of the data is very important in cloud computing as the data is distributed over a network of physical devices. Data corruption arises if appropriate segregation is not maintained. Currently, there are no federal policies addressing how government information is accessed.

**Availability**

Availability plays a major role in cloud computing since the needs of the customers should be attended on time. A research from the University of California had tracked the availability and outages of four major cloud vendors. It was found that overload on the system caused programming errors resulting in system crashes and failures. Due to the lack of backup recovery Apple, Mobile, Google Gmail, Citrix and Amazon s3 reported periods of unavailability ranging from 2 to 14hrs in a span of just 60 days. This resulted in a loss of confidence among the customers and the vendors.

Natural disasters can also present significant risks. A lightening strike at one of Amazon.com's facilities caused the service to go offline for approximately 4 hours. This component of the cloud was difficult to replace immediately and resulted in delays.

**Network Load**

Cloud network load can also prove to be detrimental to performance of the cloud computing system. If the capacity of the cloud is greater than 80%, then the computers can become unresponsive due to high volumes .The computers and the servers crash due to high volume motion of data between the disk and the computer memory. The percentage of capacity threshold also poses a risk to the cloud users. When the threshold exceeds 80%, the vendors protect their services and pass the degradation on to customers. It has been indicated that in certain cases the outage of the system to the users are still not accessed.

Flexibility and scalability should be considered pivotal when designing and implementing a cloud infrastructure. Money and time also plays an important role in the design of the infrastructure. Customers will always have expectations on the durability and the efficiency of the system. Going forward the customers will also demand the need of interoperability, ability to switch providers and migration options. Another risk factor of cloud computing is the implementation of the application programming interfaces (API).

**Integrity**

Data integrity affects the accuracy of information maintained in the system. In a cloud computing model data validity, quality and security affect's the system's operations and desired outcomes. The program efficiency and performance are addressed by the integrity. An apt example for this would be that of a mobile phone service provider who stored all the customer's data including messages, contact lists etc in a Microsoft subsidiary. The Provider lost the data and the cloud was unavailable. The customers had to wait until they got the necessary information from the cloud and the data was restored.

**Data Security**

Another key criterion in a cloud is the data security. Data has to be appropriately secured from the outside world. This is necessary to ensure that data is protected and is less prone to corruption. With cloud computing becoming an upcoming trend, a number of vulnerabilities could arise when the data is being indiscriminately shared among the varied systems in cloud computing. Trust is an important factor which is missing in the present models as the service providers use diversified mechanisms which do not have proper security measures.

**Data Location**

Data Location is another aspect in cloud computing where service providers are not concentrated in a single location but are distributed throughout the globe. It creates unawareness among the customers about the exact location of the cloud. This could hinder investigations within the cloud and is difficult to access the activity of the cloud, where the data is not stored in a particular data centre but in a distributed format. The users may not be familiar with the underlying environments of the varied components in the cloud.

**Data Segregation**

Data Segregation is not easily facilitated in all cloud environments as all the data cannot be segregated according to the user needs. Some customers do not encrypt the data as there are chances for the encryption itself to destroy the data. In short, cloud computing is not an environment which works in a toolkit. The compromised servers are shut down whenever a data is needed to be recovered. The available data is not correctly sent to the customer at all times of need. When recovering the data there could be instances of replication of data in multiple sites. The restoration of data must be quick and complete to avoid further risks.

We examine how cloud computing is assessed in a biomedical laboratory which experiences risks due to hackers. In a biomedical laboratory, data is always exposed to threats both internal and external. Less separation is provided by the cloud in case of a separate server in a laboratory. The risks include the hacking of the hypervisor, where a shared CPU can be easily attacked. The data can be manipulated, deleted or destroyed as a result of the attack. Such attacks on biomedical data can have serious implications to the end users. Thus the Data Base Manage System (DBMS) and web servers face vulnerability if the infrastructure of the cloud is not properly designed. There are certain non technical risks which arise due to outsourcing of information. Encrypting the data from the technical aspect is important to ensure that the data is not hacked or attacked. Strong encryption is needed for sensitive data and this would mean increased costs.

**Privacy Risks**

Several complex privacy and confidentiality issues are associated with cloud computing. In this section, we dwell on some of these different privacy risks involved in cloud computing environments. There are no laws that block a user from disclosing the information to the cloud providers. This disclosure of information sometimes leads to serious consequences. Some business users may not be interested in sharing their information, but such information is sometimes placed in the cloud and this may lead to adverse impacts on their business. For example, recently when Facebook changed it's terms of service, the customers were not informed about it. This made it possible to broadcast the information of the Facebook customers to others if the privacy options were not set accordingly. This amplifies the importance of reading and understanding the Terms of Service and the Privacy Policy of the cloud providers before placing any information in the cloud. If it is not possible to understand the policy or it doesn't satisfy the needs of a user, the user can and must always opt for a different cloud provider. Several organisations have analysed the issues of privacy and confidentiality in the cloud computing environment. These analyses have been published by a Privacy Commissioner, an industry association and a commercial publisher.

Domestic clouds and trans-border clouds are two distinct cloud structures. Certain privacy issues are specific to each cloud structure. In a domestic cloud structure, the complete cloud is physically located within the same territory. This gives rise to fewer privacy issues such as whether the data is collected, used and stored in an appropriate manner and whether the data is disclosed to authorised recipients only. Another privacy issue in the domestic cloud structure is related to the rights possessed by the data owners to access their data. The circumstances under which the data owner can access and correct the data should be defined clearly. The above privacy issues can also be extended to all other cloud computing environments in general.

Trans-border cloud structures have their cloud transferred across the borders. This gives rise to more privacy issues. The best example for a trans-border cloud operator is the Google Docs. People from different parts of the world store data in Google Docs. When data is transferred between different organisations located at different countries, serious privacy issues could occur.

The privacy principles regulating trans-border dataflow defined by the different countries should be given importance by the cloud providers. For example Australia's National Privacy Principle 9 deals with trans-border data flows and is different from privacy regulations of other nations. Another example is where a health care provider uses a transborder cloud computing product to store and/or process patient data, they would have to ensure that the transfer is permitted under the relevant privacy law.

We examined the Google Docs' Privacy Policy, which must be read in conjunction with Google's general Privacy Policy. Several noteworthy provisions were observed in it.

**For example,**

*"When you access Google services via a browser, application or other client our servers automatically record certain information. These server logs may include information such as your web request, your interaction with a service, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser or your account."*

In the Privacy Policy, it is specified that 'our servers automatically record certain information'. While there are details provided for some types of data being collected, it refers to 'certain information' which is not clear whether the specified data are the only types of data collected.

If we consider Google Doc's Privacy Policy, it does not give a clear explanation about how a user's personal information will be used by Google and where it will be stored. A detailed analysis of Google's general Privacy Policy brings out this discrepancy.

**Consumer Risks**

The use of cloud computing services can cause risks to consumers. Before using a cloud computing product, the consumers should familiarize themselves with the product, confirm whether the product satisfies their needs and understand the risks involved in using the product. However, it is not possible for the consumers to understand about all the risks involved in using a cloud computing product. The supply of consumer cloud computing products is governed by contracts drafted by the providers with no input from the consumers. Sometimes the provider makes changes to the terms on which the product is provided and the consumers remain unaware about it. These sudden changes without informing the consumers can lead to major consumer risks.

In order to avoid both the privacy and consumer risks, the consumers need to familiarize with the cloud computing product they will be using. For example, when using Google Docs, one must read at least the following terms;

- Universal Terms of Service Additional Terms
- Program Policies Privacy Policy
- CopyRight Notices

By examining the above documents, several interesting features become apparent. First, to use any of Google's services, a consumer has to agree to be bound by a range of terms unilaterally decided by Google and those terms may be unilaterally changed by Google without specific notification. Google also states that they will treat a consumer's use of their services as an acceptance of the terms included in Google's contract. Further, it can be noted that, when Google disables access to a consumer's account, the consumer may be prevented from accessing content from their account. This is serious in relation to Google Docs services.

It can be concluded that the Google Docs users, knowingly or unknowingly agree to the terms which may have serious consequences. The legality of some of the terms is questionable.

## IV. CONCLUSIONS

With the increase in the growth of cloud computing, security needs to be analysed frequently. The Users should be aware of the risks and vulnerabilities present in the current cloud computing environment before being a part of the environment.

From this study of current cloud computing practices and inherent risks involved, it is clear that at present there is a lack of risk analysis approaches in the cloud computing environments. A proper risk analysis approach will be of great help to both the service providers and the customers. With such an approach, the customers can be guaranteed data security and the service providers can win the trust of their customers. Also the cloud users can perform the risk analysis before placing their critical data in a security sensitive cloud. Further additions to the matrix and inclusion of additional variables for assessment should be considered as cloud computing progresses to advanced levels where new risks could materialize. We have discussed mainly three major risks associated with cloud computing. With the rapid growth in this field of cloud computing, several other risks can occur.

In this world where everyone is becoming a part of cloud computing, we believe that awareness among the people regarding the existence of risk, security mechanisms provided by the different cloud service providers to eliminate such risks and the introduction of new risk analysis approaches has significant importance and scope.

## V. REFERENCES

[1] Amit Sangorya, Saurabh kumar, JaiDeep Dhok, and Vasudeva Varma. "Towards Analyzing Data Security Risks in Cloud Computing Environments", *International conference on Information systems, Technology, and Management*, Thailand, March, 2010.

[2] R Gellman. "Cloud Computing and Privacy". *Presented at the World Privacy Forum*, 2009.

[3] Scott Paquette, Paul T.Jaegar, Susan C.Wilson. Identifying the security risks associated with governmental use of cloud computing, *Journal of Government Information Quarterly 27*, pages 245-253, April, 2010.

[4] Sagar B Patil, Pooja A Vhatkar, "Towards Secure and dependable storage devices in Cloud Computing" *International Journal of Innovative Research in Advanced Engineering*, Volume 1 Issue 9, 2015

[5] Subra Kumaraswamy, Shahed Latif and Tim Mather. "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance". *Published by O'Reilly*, 1st edition, September, 2009.