Analyzing the risks involved in cloud computing environments

Chikram Sridhar[1], Ramesh Polisetti[2] , M.Rakesh Chowdary[3]
[1]Assistant Professor, Department of CSE
[2]Assistant Professor, Department of CSE
[3]Research Scholar at Satyasai University of Technological & Medical Sciences, Bhopal, M.P.
[1,2,3]Sree Datha Group of Institutions

Abstract: Cloud computing is the latest buzzword in the head of techies round the clock these days. The importance and the different applications of cloud computing are overwhelming and thus, it is a topic of huge significance. It provides several astounding features like Multitenancy, on demand service, pay per use etc. This paper presents a study about the 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

Keywords- Cloud computing, database as a service, cloud platforms

I. INTRODUCTION

The last few years, a new generation of technology has positively invaded our lives providing a number of capabilities that has made our digital behavior much easier than before. This technology is commonly known as “cloud computing”. Various well-known services such as email, instant messaging, and web content management, are among the many applications that can be offered via a cloud environment. Although many of these services and applications were offered, through the Internet, before the cloud era; cloud computing environments offer greater degree of scalability, flexibility, and resource pooling thus elevating its use, leading to its great expandability and applicability noted nowadays [1].

While the degree of Internet users that enroll and access cloud based services rises dramatically every day, recent surveys reveal the uncertainty and instability of cloud environments. In June 2009, a survey conducted by a document management software company revealed, that 41% of senior IT professionals don’t know what cloud computing really is [2]. From the remaining 59% of IT professionals, who stated that they know what cloud computing is, 17% of them understand cloud computing to be internet-based computing while 11% believe it is a combination of internet-based computing, software as a service (SaaS), software on demand, an outsourced or managed service and a hosted software service. The remaining respondents understand cloud computing to be a mixture of the above. One of the innovations that cloud computing introduced and played a key role in its rapid development is the use of virtualization as a way for providing three basic types of services: software, platform and infrastructure. However, most of the recent studies [3-7] have identified a number of security and privacy challenges uniquely to the cloud. Although, typical security and privacy concerns, such as data protection, unauthorized access, data handling and traceability, are the same as in traditional distributed systems, but the solutions required and the requirements introduced by those in a cloud context are very different than those used in traditional systems. When engineering software systems, it is necessary to identify and model respective security and privacy properties based on the system specific context so that appropriate security and privacy requirements can be identified and analyzed. The elicited security and privacy requirements should be implemented within the system, which should enclose all the necessary measures for dealing with possible security and privacy threats that will cause harm to its assets or users. A number of research efforts [8-11] have already contributed to the area of identifying and analyzing security and privacy requirements for the development of software systems. However, these works have not been developed for cloud-based systems. On the other hand, industry-led reports [1, 2, 12] have been published discussing security and privacy issues within the context of cloud computing. However, most of these reports provide a list of security and/or privacy issues without providing a clear linkage with relevant security and privacy properties and threats. Moreover, they do not explicitly discuss any set of requirements that are essential for analysis and design methodologies to incorporate, to support security and privacy analysis for cloud based systems.

II. RELATED WORK

A number of surveys have been conducted on cloud services. The survey conducted by International Data Corporation (IDC) where data security has been rated as a major concern [11] concludes that cloud services are still in their early stages. The key challenges faced by cloud computing is discussed in the survey conducted by Buyya [12]. Physical security is discussed in the white paper published by Amazon Web Services (AWS). Major cloud service providers such as Google, Microsoft [13] have now started focusing deeply on security issues in cloud computing. Some of the major risks faced by the customers while using the cloud computing infrastructure are also identified by Heiser and Nicolett [14]. In our paper, we have summarized major risks that must be addressed by the cloud service providers. We have discussed the risks related to data security, availability, storage, segregation, integrity and recovery. In addition, risks related to the cloud infrastructure were also explored

III. PROPOSED SYSTEM

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, and 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, MobileMe, 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 lightning 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 [16]. 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 [15]. 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 [17]. 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. The following sub section describes the risks factors in cloud environments.

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 center 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.

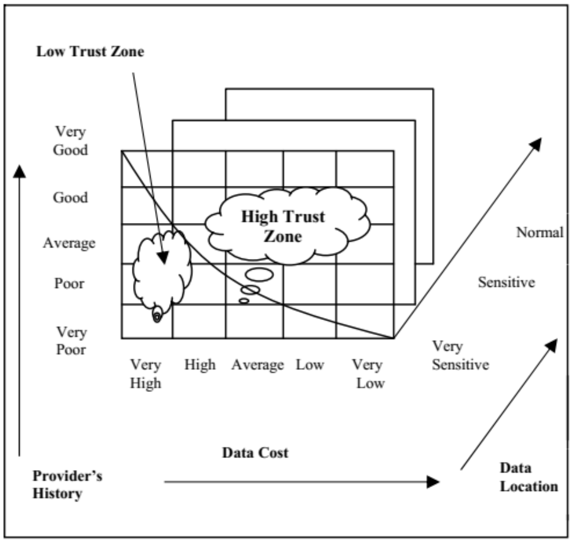
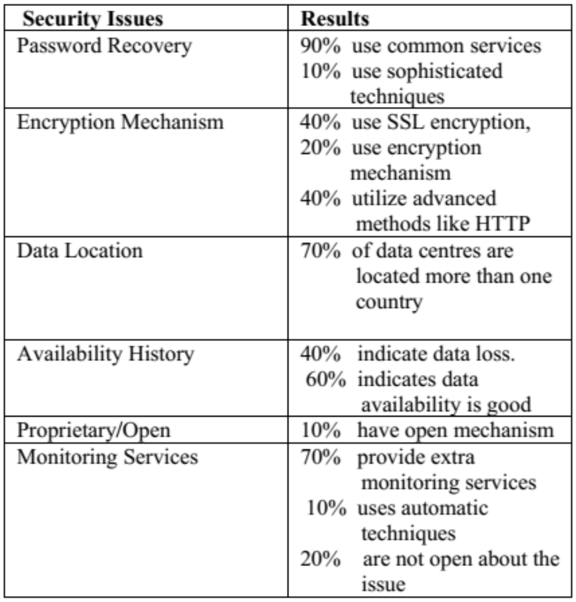


Figure 1. A Trust Matrix for Risk Analysis

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 [3].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. Table 1 provides a summary of the security mechanisms provided by major cloud service providers.



Security Issues	Results
Password Recovery	90% use common services 10% use sophisticated techniques
Encryption Mechanism	40% use SSL encryption, 20% use encryption mechanism 40% utilize advanced methods like HTTP
Data Location	70% of data centres are located more than one country
Availability History	40% indicate data loss. 60% indicates data availability is good
Proprietary/Open	10% have open mechanism
Monitoring Services	70% provide extra monitoring services 10% uses automatic techniques 20% are not open about the issue

Table 1. Security Mechanisms of Service Providers

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 its 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 organizations have analyzed the issues of privacy and confidentiality in the cloud computing environment. These analyses have been published by a Privacy Commissioner [4], an industry association [5] and a commercial publisher [6]. 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 authorize 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 organizations 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 [7]. 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 [8].

IV. CONCLUSION

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.

REFERENCES

[1] Microsoft Technical report: Privacy in the cloud computing era, a Microsoft perspective, November 2009, Microsoft Corp, Redmond, USA [Last access 12/08/2012]

[2] Version One Survey Results: Cloud Confusion amongst IT Professionals, 24 June 2009, http://www.versionone.co.uk/news /cloud-of-confusion-amongst-it-professionals.php [Last access 08/09/2012]

[3] Cloud Security Alliance “Top Threats to Cloud Computing V1.0”. https://cloudsecurityalliance.org /topthreats /csathreats.v1.0.pdf Retrieved 2012-09-22. [Last access 09/01/2013]

[4] S. Subashini, & V. Kavitha, “A survey on security issues in service delivery models of cloud computing”, Journal of Networks and Computer Applications, Vol 34, No.1, p.p. 1-11, 2011

[5] S. Islam, H. Mouratidis, & E. Weippl, “A Goal-driven Risk Management Approach to Support Security and Privacy Analysis of Cloud-based System”, Book chapter Security Engineering for Cloud Computing: Approaches and Tools, IGI global publication, 2012.

[6] S. Pearson, & A. Benameur, “Privacy, Security and Trust Issues Arising from Cloud Computing”, 2nd IEEE International Conference on Cloud Computing Technology and Science, pp 693 – 702, UK. IEEE Computer Society, 2010.

[7] C. Gong, J. Liu, Q. Zhang, H. Chen, & Z. Gong, “The Characteristics of Cloud Computing”, Proceedings of the 2010 39th International Conference on Parallel Processing Workshops, IEEE Computer Society Washington, DC, USA, 2010.

[8] H. Mouratidis, C. Kalloniatis, S. Islam, M. P. Huget, S. Gritzalis, "Aligning Security and Privacy to support the development of Secure Information Systems, Journal of Universal Computer Science, Vol. 18, No. 12, pp. 1608-1627, 2012

[9] C. Kalloniatis, E. Kavakli, S. Gritzalis, "Security Requirements Engineering for eGovernment Applications: Analysis of Current Frameworks", in proceedings of the 3rd International Conference on Electronic Government (EGOV'04), pp.66-71, 2004, Springer Lecture Notes in Computer Science.

[10] G. Sindre, & A. L. Opdahl, A. L., "Eliciting security requirements with misuse cases", Requirements Engineering Journal, Vol. 10, No.1, p.p. 34–44, 2005.

[11] S. Islam, H. Mouratidis, C. Kalloniatis, A. Hudic, & L. Zechner, "Model Based Process to Support Security and Privacy Requirements Engineering", International Journal of Secure Software Engineering (IJSSE), Vol. 3, No 3, September, IGI global publication, 2012.

[12] Cloud Computing. Academic Room. [Last access 16/06/2012]

Authors:

Chikram Sridhar working as Asst. professor with 2 years of experience at Sree Datha Group of Institutions.

Ramesh Polisetti working as Asst. professor with 2 years of experience at Sree Datha Group of Institutions.

M.Rakesh Chowdary Research Scholar at Satyasai University of Technological & Medical Sciences, Bhopal, with teaching experience of 5 years at Sree Datha Group of Institutions.