International Journal of Information Technology and Knowledge Management (ISSN: 0973-4414)
July-December 2012, Volume 5, No. 2, pp. 496-501

Cloud computing security and privacy concerns

Ashish Saravg, Dr. Chander Kant
Research Scholar, School of Computer Science & IT, Singhania University, Jhunjhunu, Rajasthan
Assistant professor, Deptt. of Comp. Sc. & Appl., K.U. Kurukshetra, Haryana (India)
ashish.saravag@gmail.com, ckverma@rediffmail.com

Abstract: In last few years, cloud computing concept has groomed a lot which result that it has become the fastest growing business for the IT industry. Because it has became a promising business concept with win-win situation for the clients to shift. Now, recession-hit companies have acknowledged that simply by shifting into the cloud they will gain the fast access to best breed of business applications or appreciably enhance their productivity, all at negligible cost.

But as the concept grows up, a lot of Security issues have also raised up in cloud computing. Nowadays it is becoming challenging task for the IT professionals to secure the digital infrastructure of any organization. In today's scenario, each and every organization is totally dependent on the latest technologies those are updating & growing on daily basis. So that now it is becoming more challenging to secure the digital assets of a company in accordance with the changing demand & growing technologies which were almost fixed earlier.

Cloud computing is a latest emerging business concept. As more and more data and information of individuals and companies is placed in the cloud, their concern about data and environment safety, security issues, requirements and challenges has also grown.

Keywords: Cloud Security, Cloud Service Provider, Cloud Computing**.**

1. INTRODUCTION

Cloud computing acceptance is growing very quickly. Mostly IT departments are forced to spend a lot of time, money and energy on its IT infrastructure implementation, maintenance, and up gradation. So that now gradually more, IT giants as well as middle size organizations are moving to cloud computing technology which minimizes their set up cost & time required to install all digital infrastructure. Now just by adopting cloud computing IT professional are required only to focus on strategies not on technologies which will boost up their revenues.

Cloud service providers (CSPs) (e.g. Microsoft, Google, Amazon, Salesforce.com, Go Grid) are using the concept of virtualization for computing assets through the Internet. For these service providers, virtual machines from different organizations have to be placed on the same physical server to maximize the efficiencies of virtualization. This figure (see Figure 1) shows the result of the survey conducted by International Data Corporation (IDC) conducted a survey [1] of 263 IT giants and their line-of-business colleagues to collect their opinions and understand their views on services offered by cloud computing vendors.

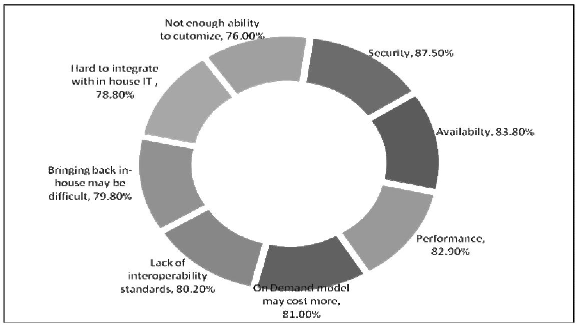

Figure 1. Results of IDC ranking security challenges (n=263)

In the study the main concern of the organizations is security which stood first among all the concerns of corporate giants about cloud computing. The organizations & the IT professionals are mainly worried about how security, privacy &

reliability can be taken cared in Cloud Computing. Storing vital applications and important data to a shared cloud instead of saving it in own place is a major concern for organizations those are adopting the new environment. So now it is the responsibility of a cloud service provider that he must guarantee that customers will continue to have the same reliability, privacy and secure control on their applications as they have at their own place.

1.1 Cloud Computing Evolution

The History begins from the following technologies:

1.1.1 Cluster Computing:

This is basically clustering of the coupled computers, to work in a group to accomplish a single computing task by working closely equivalent of forming a single computer. The cluster components are not necessarily, connected to each other through fast local area networks. This grouping of computers improves the performance, speed and availability as well as reduces the overall cost, instead of working over a single computer.

1.1.2 Grid Computing:

Grid computing links various geographically distributed individual computers to build a single large infrastructure. It combines the various computer assets from multiple administrative domains to accomplish a single computing task. The main differences between the grids computing from cluster computing are

(a). More loosely coupled

(b). Heterogeneous

(c). Geographically distributed.

The separate grids can be dedicated to single application; but a single grid can also be accessed for a variety of different applications.

1.1.3 Utility Computing:

Utility computing works on pay per use basis i.e. paying for what you accessed and used from a shared pool of resources e.g. storage system, software and servers like public utilities e.g. water, electricity and gas etc. So utility computing is the wrapping up of computing resources as a metered service. This concept has the benefit of having negligible or no initial investment to access the various computing resources. Basically in this concept the computational resources are mainly rented as compared to the earlier scenario in which we required to purchase the products to avail the services.

This facility of being served as a utility became the basis of the "On Demand" computing. Cloud computing model further proposed the concept of delivering computing, application and network components as a service. IBM, HP and Microsoft were early giant leaders in the field of utility computing and they have invested a lot on the research work on working of the cloud architecture, payment system and development challenges. Google, Amazon and others started to take the lead in 2008, as they established their own utility services for computing, storage and applications.

1.2. Cloud Computing Models

Cloud computing offers both the software and hardware as a service over the internet (see Figure 2). These services are classified into three categories:

i. Software as a Service (SaaS)

ii. Platform as a Service (PaaS)

iii. Infrastructure as a Service (IaaS)

1.2.1 Software as a Service (SaaS)

Software as a Service is a software delivery model through which cloud computing make the availability of software's as a service to its clients [6]. These software services are delivered through a web browser to its user as a service on demand so that user will need to pay only for his usages. To use software as a service, users just need to request for particular software to its vendor and the vendor will provide the software within a short span of time. The end user need not to worry about the licensing and genuineness of demanded software.

1.2.2 Platform as a Service (PaaS)

It is similar to SaaS delivery concept which is designed to deliver platform as a service for computing over the internet and using it virtually to run the user's applications. It significantly changed the way of developing, deploying & running of the computing tasks of all applications required to run by any organization [6]. Now by using PaaS, IT professionals do not require evaluating, buying, organizing, and managing the hardware computing platform and software required for organization's applications, which in turn reduce the cost and complexity. All the services required during the life cycle of web applications will be provided by PaaS entirely through the internet. Users will only have to pay the subscription charges of the required software.

1.2.3 Infrastructure as a Service (IaaS)

In this model, the cloud service provider delivers the Infrastructure i.e. equipments those are required to support operations. The equipments may include storage devices, hardware, servers and various networking components. It is totally the responsibility of cloud service provider for housing, running and maintaining of these equipments. The client organizations need only to pay on per-use basis [6]. Cloud computing offers secure, scalable and robust Infrastructure-as-a-Service (IaaS). It is also known as Hardware as a Service (HaaS).

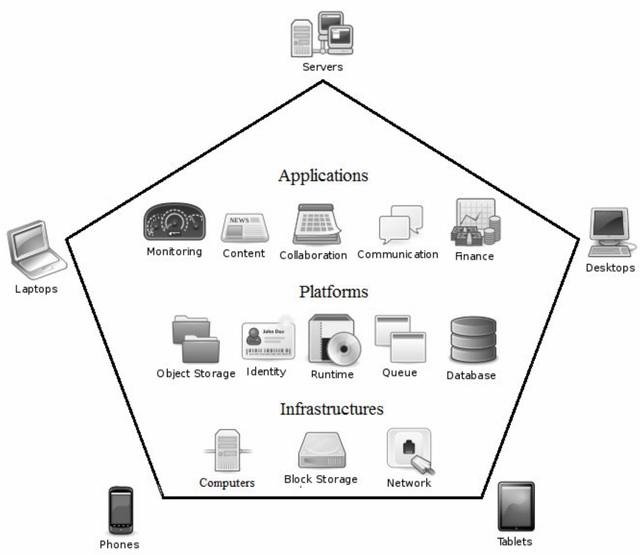

Figure: 2. Layers in Cloud Architecture

1.3 Characteristics of Cloud Computing

There are a lot of characteristics concerned to cloud computing. Some of them are [2]:

1.3.1 High level of Virtualization

The Cloud Computing implements the virtualization concept in its best way. All the cloud services are mainly scaled on the level of virtualization it offers. The various virtualizations are software and hardware resources virtualization management, scheduling and application. Users can access the network assets, database assets, computing assets, hardware assets and storage assets independently through the virtual platform.

1.3.2 Flexibility to customize

Cloud computing facilitate its users the ability to customize the required services, applications and resources according to their own needs. Cloud computing platforms can be deployed in accordance with the needs of users. In cloud computing the users are always at priority, so that they are also able to unsubscribe or delete some services.

1.3.3 Cost-effective

Cloud computing offer various services as a utility, so the organizations need not to invest much in the starting of the business. Also the services provided through cloud computing require minimum hardware requirements. So the clients need not to purchase or upgrade the existing hardware to access the cloud services. So that cloud computing reduces the initial investment as well as running cost of the organizations.

1.3.4 Dynamic Scalability

The services through Cloud Computing can be scale up or down easily in a negligible span of time. The up gradation, signing in and signing off to the new services are quite easy. In Cloud, if a node fails, and then discard the node through the appropriate strategy and the cloud can be adjusted according the customer's need.

1.3.5 High reliability and security:

The whole cloud data and services are stored at many geographically distributed servers. If a certain server has a problem; then other servers on the cloud take over the control of the defected server immediately to ensure the normal working and calculation of the cloud. That's how the cloud provides the most reliable and secured data storage center with the world's most professional team in the management. So users need not to backup their data.

2.1. Common Concerns of Cloud Computing

The primary aim of both cloud vendors and clients is to ensure data security. Data security is mainly concerned to protect digital resources against risks, so the digital resources will remain meaningful and will never become obsolete to the concerned organizations. Security mainly aims to ensure the data privacy, reliability and accessibility, along with accuracy, liability and consistency.

We mainly divide the common security concerns about cloud computing in four categories [3]:

1) **Cloud platform:** The data security may suffer from the shortcomings of cloud hardware platform itself such as problems with virtualization, storage devices and networking components. The shortcomings can also be present in the cloud software, cloud platform and software code. Also the concerned are related to the security of physical data- center situated geographically.
2) **Data consistency:** This category primarily concerns about the data reliability, data lock in, data confidentiality and user details privacy.
3) **Access to the right user:** This category mainly concern about the right user's access in the clouds. A set of constraints must be set for proper authentication, authorization and level of accessibility of the user. This is mainly achieved by proper management of the user identity database and proper encryption.
4) **Compliance:** Because of its size and troublesome nature, the cloud should be taken cared by regulatory agencies to perform the routine security audit the geographically distributed data centers.

2.2. Security Issues and Challenges of Cloud Computing

Some security concerns are listed and discussed below [8]:

1. With this model the physical security has become a major because all the resources are shared among the various companies. So that any other company can easily violate the laws that may result into the loss of data.
2. Transition between the clouds platforms may result in loss of data due to incompatibility of one vendor's storage services with another vendor's services is a major issue in cloud computing e.g. Microsoft cloud storage services are incompatible with Google cloud storage services. [5]
3. The controlling of the encryption/decryption keys by unprofessional persons may result into failure of cloud set up.
4. Maintaining of consistency of the data is another main concern of the clients as well as of vendors. The data should be updated in all data copies in response to authorized user transactions.
5. The updated information about the cloud platform status usually not shared with the users.
6. Due to government regulations, they may apply strict limits on where data about its citizens can be stored and for how much time.
7. The changing nature of virtual machines will make it difficult to maintain so consistency will be difficult.

To deal with the security concerns listed above, the vendors will need to enhance and update the commonly used security practices. Some more challenges in implementing the cloud computing is listed below [8]:

2.2.1 Security Management

One of the most crucial jobs for an organization is to build up a formal team for the security management of organization assets. The team should be occupied with the strategic plans of the organization. The individual's role, their responsibility and organization expectations should be clearly stated among security team members. The confusion in above stated issues among the security team may lead to major loss to the organization.

2.2.2 Risk Estimation

Risk estimation is always important in every stage of business. It helps a lot to make better decisions which makes balance between both business motive and cloud assets of the vendors [10] [7]. Security risk's estimation should be planned and managed on periodic or as need basis. So the standard strategies should be followed for risk estimation.

2.2.3 Security Awareness among People

The cloud users are the weakest link for data security. Lacking of proper security awareness and training to the people will lead the company to a variety of security risks, rather than due to system or application shortcomings. So a lot of security risks will arise due to lack of managed and effective security awareness program for the people.

3.1. Key Policies of the Contract between Vendor and Client before Switching towards Cloud Computing

Obviously, due to a lot of security issues related to the cloud platforms, there must be a legal contract signed between the cloud vendor and its client. So that the clients should deeply research the policies listed in the contract given by cloud service provider. Which ensure data security before shifting to the vendors cloud platform to avoid the loss and control of data. The various policies concerning the contract are described as under. There are mainly seven policy issues [4] those must be primarily discussed in the legal contract

3.1.1 Certified administrator access

The client must ensure that only the certified IT professional will manage their data and applications in the vendor's cloud platform. He should collect the detailed information about the administrator, who is going to manage your cloud platform. The vendor must admit to clarify the detailed qualifications, certifications and the hiring procedure of the cloud administrators to the clients, so that clients will make their mind about the shifting to cloud platform. The vendors must also admit to supply the information about the procedure for the skill set development of the administrator to the client.

3.1.2 Regular observance

The client must make sure that the vendor admits to maintain a regularity body to supervise the cloud platforms, data security, services and administrator work. He must also admit to generate regular external audit reports.

3.1.3 Data centers locality

The data centers are always geographically distributed. Obviously, the client's main concerned is about data and applications to be stored on those data centers. So the vendor must admit to provide the information about the location or choices of locations of the data centers to the clients. The clients must inquire the vendor about legal contract with the respective countries in which data centers are installed. They must be agreed to store and process the client's data in definite jurisdictions according to contract rules.

3.1.4 Data isolation and encryption

The client must make sure that the vendors admit to use the high level encryption mechanism which is impossible to crack for the unauthorized user. The encryption patterns must be designed and tested by certified and experienced cryptography professionals. The standard techniques must also be followed to maintain consistency of the data at all stages or data centers.

3.1.5 Data Recovery policies

In addition to the knowledge of the locality of the data centers in the world, the client must also be ensured about the data recovery policies in case of the disaster whether they are natural or manmade. The vendors must mention the conditions for the data retrieval in the case of a disaster. For this the vendor must save the data copies on several localities of data centers. So that, the chances of side effect of the failure of data centers or loosing of the data will be reduced. The vendor must have the capability and techniques to have complete backup of client's data at any time and in any situation.

4. CONCLUSION

In the paper we have justified that it is very important to take security and privacy into account while designing, using and shifting towards cloud services. This paper simply uncovers all the security issues and challenges commonly faced in cloud computing and its security standards and policies.

Data security and privacy are very important topics which will be certainly ensured in the upcoming years of cloud computing. [9] The security and vulnerability market should exceed revenue of $4.4 billion by the end of 2013, with a compound annual growth rate (CAGR) of 10.8%. So that products that fall within the security and shortcoming management market will stay in high demand.

REFERENCES

[1] International Data Corporation, http://blogs .idc.com/ie/wp -content/uploads/2009/12/idccloudchallenges2009.jpg, 2009

[2] Minrui Jia, paper appears in Control, Automation and Systems Engineering (CASE), 2011 International Conference on Issue Date: 30-31 July 2011 On page(s): 1 – 4 ISBN: 978-1-4577-0859-6 “Cloud Security of Cloud Computing Application”.

[3] Shubhashis Sengupta, Vikrant Kaulgud, Vibhu Saujanya Sharma, 2011 IEEE World Congress on Services, Washington, DC USA ,July 04-July 09, ISBN: 978-0-7695-4461-8. “Cloud Computing Security--Trends and Research Directions”

[4] Gartner: Seven cloud-computing security risks, 02 July 2008, page=0,0 http://www.infoworld.com/d/security-central/gartner -seven-cloud-computing-security-risks-853.

[5] M. Casassa-Mont, S. Pearson and P. Bramhall, Proc. DEXA 2003, IEEE Computer Society, 2003, pp. 377-382 "Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services",

[6] Vikas Goyal, Dr. Chander Kant, International Journal of Engineering Sciences, ISSN: 2229-6913, September 2011, Volume 4, pp. 274-282. “Security Issues for Cloud Computing”,

[7] D. Catteddu, Giles Hogben: European Network and Information Security Agency, November 2009, http//www.enisa.europa.eu/act/rm/files/deliverables/cloud-comp uting-risk-assessment

[8] Popovic, Kresimir Hocenski, Zeljko , the paper appears in: MIPRO, 2010 Proceedings of the 33rd International Convention Date: 24-28 May 2010 page(s): 344 - 349 Print ISBN: 978-1-4244-7763-0 Date of Current Version: 29 July 2010 “Cloud computing security issues and challenges”.

[9] International Data Corporation, Worldwide Security and Vulnerability Management 2009-2013 Forecast and 2008 Vendor Shares, http://vulnerability management .com/docs/ IDC_M A_2009.pdf

[10] Wikipedia, 27 January 2010, http ://en.wikipedia.org/wiki/ Risk_assessment

[11] B. Hay, K. Nance, and M. Bishop, “Storm Clouds Rising: Security Challenges for IaaS Cloud Computing,” Proceedings of the 44th Hawaii International Conference on System Sciences pp. 1–7 (Jan. 2011). nob.cs.ucdavis.edu/bishop/papers/2011-hicss-1/iaas.pdf