Cloud Computing Challenges: A Survey

Amandeep Kaur, Jobanpreet Kaur, Ashish Kumar, Amit Kumar
Dept of Computer Science and Engineering,
Dr B. R. Ambedkar National Institute of Technology,
Jalandhar, India.

Abstract-- **In recent years, cloud computing has been an emerging computing model in the IT industry. Many big companies are throwing resources into it. 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 challenges of cloud computing. It highlights the different types of risks and how their existence can affect the cloud users. There are numerous contests are being raised for espousal of the cloud including data security, availability and confidentiality**.

Keywords-cloud computing; security ; privacy; challenges

I. INTRODUCTION

What is cloud computing:-Cloud computing means that instead of all the computer hardware and software you're using sitting on your desktop, or somewhere inside your company's network, it's provided for you *as a service* by another company and accessed over the Internet, usually in a completely seamless way. Exactly where the hardware and software is located and how it all works doesn't matter to you, the user—it's just somewhere up in the nebulous "cloud" that the Internet represents.

Cloud computing is a buzzword that means different things to different people. For some, it's just another way of describing IT (information technology) "outsourcing"; others use it to mean any computing service provided over the Internet or a similar network. Cloud computing is sharing of resources on a larger scale which is cost effective and location independent. Resources on the cloud can be deployed by the vendor, and used by the client. It also shares necessary software's and on-demand tools for various IT Industries. Amazon is the first company to look into the growing importance of Cloud computing very seriously followed by Google and IBM. Some of the other companies which make use of Cloud are Salesforce.com, Zoho, Rackspace, Microsoft.Benefits of Cloud computing are enormous. The most important one is that thecustomers don't need to buy the resource from a third party vendor, instead they can use the resource and pay for it as a service thus helping the customer to save time and money. Cloud is not only for Multinational companies but it's also being used by Small and medium enterprises.

II. CLOUD COMPUTING CLASSIFICATION

A. Private cloud.

The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise. This cloud computing environment resides within the boundaries of an organization and is used exclusively for the organization's benefits. These are also called internal clouds. They are built primarily by IT departments within enterprises who seek to optimize utilization of infrastructure resources within the enterprise.

B. Community cloud

The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy,and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

C. Public cloud

The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. This environment can be used by the general public. This includes individuals, corporations and other types of organizations. Typically, public clouds are administrated by third parties or vendors over the Internet, and services are offered on pay-per-use basis. These are also called provider clouds.

D. *Hybrid cloud*

The cloud infrastructure is a composition of two or more clouds (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 clouds). For example, most companies are reluctant or unwilling to put customer data in the public cloud, despite enhanced security features. The hybrid cloud allows them to place that data in a private cloud. The same company can use the public portion of the hybrid cloud for less sensitive information, to communicate with customers and for many other purposes.

III. CLOUD COMPUTING SERVICES

A. Software as a Service(SaaS)

It is the most basic form of cloud computing. There is no third-party development or resources for the user, but Saas applications can offer powerful tools right from your web browser. The best example of Saas is Google Docs[1]. Google Docs is a productivity-suite that is free for anyone to use. Creating a Google account is free, and all you have to do is login to google.com/docs and you instantly have access to a powerful word processor, spreadsheet application and presentation creator. These online services provided by Google are managed directly from the web browser and require zero installation. You can access your Google Docs from any computer or mobile device with a web browser.

Google Docs, Dropbox, Box.net, Salesforce.com and Freshbooks are all applications that qualify as Saas. All of these applications are either free to use, or offer more features at a paid subscription price. Another advantage of Saas applications is the ability to collaborate with others cheaply and from any location. If a company is seeking to customize a cloud service or create its own cloud applications, this will require the next step in cloud services known as Paas.

B. Infrastructure as a Service(IaaS)

The second segment of cloud services is known as Iaas, or "Infrastructure as a Service." This is the most comprehensive cloud platform and is mainly used by full time developers or large-scale enterprise customers. While SaaS allows usage of cloud apps, and Paas allows you to develop apps, Iaas gives you infrastructure for developing, running and storing your apps in cloud environments. The benefit of Iaas is the virtually limitless storage and computing power available to the developers without having any physical hardware on-site.

Amazon EC2[2] is good example of Iaas. From the smallest application to full-scale websites, EC2 provides commodity cloud infrastructure to run them all. Users have the flexibility to develop using a variety of tools,, from Ruby on Rails to MySQL and can choose from several Linux or Windows environments. Applications can be run on various virtual machine configurations and delivered to clients seamlessly. However, Amazon does require sophisticated application development skills and *does not* enable users to quickly get up and running without advanced technical know-how.

A different example, Skytap, actually combines the simplicity of a Software as a service application with the ability of scaling to a complete Infrastructure as a Service. Existing data centers can be integrated into the cloud, making migration of assets and data quick and easy. Virtual machines and existing applications can be run natively or through the cloud service. Skytap also offers a library of pre-made cloud applications, including virtual machine images of major operating systems. As a SaaS+Iaas provider, Skytap allows users to leverage existing technologies and applications, migrate them to the cloud, and provide open development environments for custom app creation as well. Solutions such Skytap offer both the simplicity of a self-service, point and click web UI plus elastic compute power rendering ease of use and robust cloud computing living in harmony.

C. Platform as a Service (PaaS)

The third segment of cloud services, Platform as a Service, provides developers with proprietary API's to make an application that will run in a specific environment. While a developer is free to create any application they wish, the app is locked to the platform used for its creation. This method of developing applications can be low cost (through some providers, even free) and allows you to leverage the infrastructure and tools of an already established cloud company for building or migrating your existing applications. This also gives you the ability to quickly make your app available to a wide audience.

One of the simpler examples of Paas is Facebook. Developers can create specific applications for the Facebook platform using proprietary API's and make that app available to any Facebook user. Some applications integrate a user's Twitter and Facebook account, others like Planning Center Online, integrate a database and schedule creation

tool with a Facebook profile, specifically the "Events" section of a user's account. The downside to Paas is whatever platform you choose to develop in, you can only use the tools and languages they provide. Plus the granularity of operation may be limited to what the API exposes; you may not get machine level control and flexibility. Most Paas providers do support a wide variety of tools and languages for development.

IV. CHALLENGES OF CLOUD COMPUTING

A. Network Load

Cloud network load can also affect the performance of the cloud computing system. The computers become unresponsive in case the network load is more than a limit.This limit is threshold.The computers and the servers crash due to high volume motion of data between the disk and the computer memory. The When the threshold exceeds 80%, the vendors protect their services and pass the degradation on to customers. This is one of the many reasons that give temporary outages.

B. Data Sanitization

Data Sanitization is the process of disguising sensitive information in test and development databases by overwriting it with data which looks like realistic but false data of a similar type[3]. This technique is used to ensure the security of data.. When a storage device is removed from service or moved elsewhere to be stored, the data sanitization technique is applied to that data for security purposes. This technique is also applied on the backup copies that are used for recovery. Masking is one of that techniques used for sanitization.

C. Data Location

One of the most common compliance issues facing an organization is data location. In cloud computing the data is scattered in the servers present in different parts of the world. The user don't have any idea about the location of his/her data. The data can be present in any part of the world. This situation makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory compliance requirements are being met.
.There can be following problems:-

D. Differnet Country Different Legislation

The legislation changes with the country[4]. Each and every nation has its own constitution and laws of privacy[5]. On comparing the US and European Laws[6], it came to know that there is a huge difference in the privacy policies of both. Europe is concerned about the privacy of their citizens because according to their laws, privacy is a human right. The data can be transferred to the third country only when protection of data is ensured. But United States has different laws about the privacy. The policies are highly influenced by the markets. US PATRIOT Act which was enacted after the terrorist attack of Sept 11, 2001 gives that the provisions would allow the U.S. government to access private information. So, once the information crosses a national border, the protection under foreign laws and regulations is not guaranteed.

E. Lack of Cyber Crime Laws

There is lack of cyber crime laws in many countries. About fifty two countries have responded to the cyber crimes with enacting the laws[7]. Out of them, only ten countries including Australia, Japan, United States have fully or substantially updated laws. Nine countries including Brazil, Chile, Poland etc have partially update laws. But thirty three countries have no updated laws. Thirteen countries have shown some progress. Such countries don't take strict actions against cyber crimes. In such situation if the data is transferred to such country ,where the fully updated cyber crime laws are not there, can be dangerous for the security of data.

F. Availability of Service

Though there are architectures designed for high service reliability and availability yet the users experience outages and slowdown in performances. There is no 100% reliability of service. The service can be interrupted due to certain reasons like more traffic, equipment failure, natural disasters etc. There are several examples of such outages[8]. Amazon S3 outage for 2 hours,6-8 hours on 15 feb,2008 and 20 July, 2008 respectively. A AppEngine partial outage for 5 hours on 17 June, 2008 and Gmail site was unavailable for 1.5 hours on 11 August, 2008.This causes inconvenience to the user because of unavailability of service.

G. Permanent Loss of Data

The inconvenience is not limited to the temporary outages, there can be permanent loss of data due to certain reasons like bankruptcy or facility loss.. It is possible for a service provider to experience serious problems, like bankruptcy or facility loss which can cause complete shutdown[9]. There is an example of Texas where FBI raided service centers and seized hundreds of servers in case of fraud allegations in April 2009.Due to this the service was disrupted and many loss their data who were using that computing centers.

H. Data Segregation

If data of the user is present in the shared mode, the user must make sure that data is secure and can't be accessed by other users. Because data may consist of personal information such as bank account numbers, password etc. The cloud provider must take care of the security of the data which can be provided by the data segregation[10]. Encryption of the data is a secure way to provide data segregation. The user must ask the service provider that whether the implementation of encryption was tested by the experts. Because the accidents occurs due to the failure of the implementation of encryption methods. Before storing all the information of a user, encryption must be done on the data of the user and then it is stored. Before retrieving the data by the user, decryption is performed on the data of that particular user and then the information is provided to the user. It is also to find out that who have access to the decryption keys.

I. Insider Access

Data stored on a cloud provider's server can potentially be accessed by an employee of that company, and you have none of the usual personnel controls over those people. This is also a demerit of cloud computing[9].The service providers may not reveal the access of employees to the data of the users of the cloud. This level of access decides the security of data. The employee may have access to the confidential information of the users and employee can misuse such information. This will not only affect the user but also the brand image, financial productivity of the service provider. So, the users of the service must think before storing the confidential information into the cloud and should ask the service providers about the employees who will have access to your data and manage it.

J. Long-Term Viability

Service providers must ensure the data safety in changing business situations such as mergers and acquisitions. Customers must ensure availability of the data in these situations. The provider's terms of service may not reveal the real owner. The buyer could be a government agency, a foreign agency, or an Internet news service. If a government agency owns the provider, terms of service that allow sharing with affiliates could result in all of the user's information being obtained by prosecutors or intelligence agencies without further notice or process. Some bankruptcy issues are also there. Bankruptcy is a threat to the data of the user. The service provider must carefully structure the contracts with the investors and creditors. Another solution can be the insurance contracts which can provide the funds to run the infrastructure for a period after bankruptcy[11].

K. Data Theft

The internet penetration has increased with the time. But with the increase of internet penetration the chances of data theft has also increased. Among the users of the internet, there is a huge population of attackers and hackers. Customers need to understand the encryption and backup measures the provider is taking. For example many cloud email providers store emails in an encrypted form, so their employees cannot read them. Customers should evaluate these measures on a regular basis and decide whether these precautions are adequate for their needs or not.

L. Disaster Recovery Plan

While you may not know the physical location of your services, it is physically located somewhere. All physical locations face threats such as fire, storms, natural disasters, and loss of power. In case of any of these events, how will the cloud provider respond, and what guarantee of continued services are they promising? As an example, in February 2009, Nokia's Contacts On Ovi servers crashed. The last reliable backup that Nokia could recover was dated January 23rd, meaning anything synced and stored by users between January 23rd and February 9th was lost completely[12].

M. SLA(Service Level Agreement)

Whenever data is lost, especially valuable data, there is a propensity to scramble to assign blame. Often in the IT world, this can result in lost jobs, lost company revenue, and, in severe cases, business demise. As such, it is critical to understand how much legal responsibility the cloud service provider, per the service level agreement (SLA), has and to ensure that every possible step has been taken to prevent data loss. As with many legal documents, SLAs are

often written to the benefit of the provider, no.t to the customer[13]. Many cloud service providers offer varying tiers of protection, but as with any storage provider they do not assume liability for the integrity of your data.

N. *Loss Of Governance*

In using cloud infrastructures, the client necessarily cedes control to the Cloud Provider (CP) on a number of issues which may affect security. At the same time, SLAs may not offer a commitment to provide such services on the part of the cloud provider, thus leaving a gap in security defences. The customer loses the governance and ownership of data. Your cloud service provider may use your data for secondary purposes if data ownership rights are not addressed in contracts.

O. Data Integrity

You rely on data to forecast report and manage your business. Inaccurate or incomplete data coming from a cloud provider's systems could result in poor forecasting or incorrect public reporting. When a request to update a cloud resource is made, as with most operating systems but the changes can be on one place but not all other places where the copies of data are kept. This may not result into the incorrect information. Your business may also be subject to regulations or legal processes that require ready access to significant historical data.

P. Dependency Of Network Connectivity

The simplest and most obvious drawback to cloud computing arises out of its most important characteristic: it is network based. It is susceptible to outages and service interruptions at any time due to the internet dependency. The user can't access the data from anywhere. The user can access the data only if he/she has a internet connection. The access to data is also highly dependent on the speed of the internet . The slow speed of the internet connection will cause inconvenience to the user.

Q. Immaturity Of Standards

Standards are immature and things change very rapidly in the cloud. All IaaS and SaaS providers use different technologies and different standards. The storage infrastructure behind Amazon is different from that of the typical data center. The Azure storage engine does not use a standard relational database; Google's App Engine does not support SQL database. So you cannot just move applications to the cloud and expect them to run. At least as much work is involved in moving an application to the cloud as is involved in moving it from an existing server to a new one. There is also the issue of employee skills; staff may need retraining and they may resent a change to the cloud and fear job losses.

V. CONCLUSION

Cloud computing is a new and promising paradigm delivering IT services as computing utilities. Cloud computing enables innovation by alleviating the need of innovators to find resources to develop, test and make their innovations available to the user community. Innovators are free to focus on the innovation rather than the logistics of finding and managing resources that enable the innovation.Cloud Computing System as told earlier is still in its nascent stage, where disadvantages are still being dealt with. 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. Therefore, users will have to wait for updates or continue to use current Cloud Computing System. Hopefully research and development is happening at fast pace and improving the system much faster to bring in more security and keep disadvantages at bay.

REFERENCES

[1] "Google App Engine," Website, 2009, code.google.com/appengine.
[2] "Amazon EC2," Website, 2010, http://aws.amazon.com/ec2
[3] L. Ertaul, S. Singhal, and G. Saldamli,"Security Challenges in Cloud Computing"
[4] Ali M., Khan S. U., Vasilakos A. V., " Security in Cloud Computing : Opportunities and Challenges", Information Sciences 305 (2015) 357–383.
[5] Pearson S. and Charlesworth A."Accountability as a Way Forward for Privacy Protection in the Cloud" , CloudCom , LNCS 5931, pp. 131–144. Springer-Verlag Berlin Heidelberg 2009

[6] Lauren B. Movius, Nathalie Krup, "U.S. and EU Privacy Policy: Comparisons of Regulatory Approaches" http://ijoc.org/ojs/index.php/ijoc/article/viewfile/405/305
[7] Mcconnell International,"Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information"
[8] Armbrust M., Fox A., Griff th R., Joseph D. A., Katz R. ,Konwinski A., Lee G., Patterson D., Rabkin A., Stoica I., and Zahari M. ,"Above the Clouds: A View of Cloud Computing", Communications of the ACM, Volume 53, Number 4 (2010)
[9] Jansen W. A. " Cloud Hooks: Security and Privacy Issues in Cloud Computing" , NIST Proceedings of the 44th Hawaii International Conference on System Sciences - 2011
[10] Gartner, "Assessing the Security Risks of Cloud Computing", 3 June 2008 <http://cloud.ctrls.in/files/assessing-the-security-risks.pdf>
[11] David Molnar, Stuart Schechter,"Self Hosting vs. Cloud Hosting:Accounting for the security impact of hosting in the cloud", Proceedings of the Ninth Workshop on Economics of Information Security, Microsoft Research(WEIS, 2010).
[12] Nilay Patel,"Nokia Ovi crash results in three weeks of lost user data, February 12,2009" <http://www.engadget.com/2009/02/12/nokia-ovi-crash-results-in-three-weeks-of-lost-user-data/>
[13] Kerr J. , Teng K.," Cloud computing: legal and privacy issues", Journal of Legal Issues and Cases in Business