International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-3 Issue-1, June 2013

Survey on Security Issues in Cloud Computing

Divya Sharma, Preeti Vaidya, Oves Khan

Abstract*—Cloud Computing is a new technology that allows organizations and individuals to share resources, information and software on-demand over the Internet. It is a new consumption, supplement and delivery model wherein resources are provided in a cost effective manner. It typically involves the use of software and hardware that are delivered as a service. The technology of cloud computing deals with leaving the provision of resources to a remote server and this server has performs services as per the user's need and data. This Research Paper discusses the concepts of the 'Cloud', the issues arisen by the cloud as well as discusses a method to select the best "Cloud" for an organization.

***Index Terms*— Cloud Computing, Infrastructure, Information Technology and Scalability.**

I. INTRODUCTION

The Cloud Computing Model is a new paradigm that was developed to provide economic resource utilization over the Internet. Companies such as Google, Microsoft, IBM, Amazon and Yahoo have already started providing Cloud Services to end-users as well as entire organizations. Cloud Computing is a method of computing in which resources that are dynamically scalable and generally, virtualized are provided as a service over the internet. The wide use of this technology can be credited to the ability of a user to access, with ease, any remote site and use its resources. The users can access and use web-based applications on the remote server and use it as if it were an application installed locally on their computer. The data and the application itself are saved on the remote database and not on the user's computer. Cloud Computer is thus, the natural next-step in order to curb the on-growing demand for IT resources as a service.

Evolution: The technology of Multi-Tenancy used in cloud computing can be dated back to the 1950s when the Mainframe machines were used at large. The mainframe computers became available to organizations and individuals via terminal computers. This allowed multiple users to share the processing of the computer as well as simultaneously share similar resources. The next technology that contributed to the emergence of Cloud Computing was the emergence of Virtual Private Networks or VPNs. With this technology, service providers, that earlier provided point-to-point services were able to provide services of comparable quality using VPNs. The name 'Cloud' given to this technology comes from the symbol of cloud used as an abstraction for complex infrastructure of system diagrams.

The predecessors of this technology have, thus, been around for quite some time but the term Cloud Computing only became 'popular' when IBM and Google collaborated in this domain. This was followed by the launch of the IBM 'Blue Cloud'. Since then this technology has rapidly grown.

Manuscript published on 30 June 2013.
*****Correspondence Author(s)
Ms .Divya Sharma, CSE Department, ITM University, Gurgaon, India.
Mr. Oves Khan, CSE Department, ITM University, Gurgaon, India.
Ms.Preeti Vaidya, CSE Department, ITM University, Gurgaon, India.

Characteristics

The following characteristics summarize the essentials of the technology of cloud computing:

• On-Demand- The resources are available to the user as and when he needs it. The availability of resources should be controllable.

• Scalable- The user must be able to increase or decrease the resources when needed. The Resource Providers must be able to support the variable resource demand.

• Reliability- Since the user depends on the service provider completely, the services must be reliable.

• Utility-Based Subscription- The user should only be asked to pay for the services he uses and the amount of resource usage without any investment.

• Maintenance- The user is not responsible for upgrading and maintaining the applications on the cloud. Thus, it becomes easy to maintain cloud applications as changes only need to be made on the cloud and not on individual units.

• Access Independence- Since the application and all the data are on the cloud, the user can access the application from anywhere and from any device.

• Multi-Tenancy- Allows the sharing of resources and costs of the entire set-up amongst a large number of users that use the same for various services.

• Resource Pooling-All the resources (such as storage, processing, etc.) of the service provider are pooled together to provide varied services to the users using dynamically scalable.

Applications

The Cloud Computing technology becomes ideal in the following three cases of workloads-

• Unpredictable User Estimate – The scalability offered by Clouds becomes ideal in situations where users cannot be estimated at the time of creation.

• Cyclical – Applications with fluctuations in usage can benefit from the metered services provided by the pay-as-you-go model of cloud computing

• Parallelized- Applications (such as Big Data analytics) work better with parallel scaling across servers as compared to scaling to one large server.

II. RECENT WORK

According to the emerging trends of 2012 and 2013, a prediction can be made on the future of the Cloud Technology. The expected course is with a core focus of cloud in 2013 will be around such topics as big data and integration of cloud computing infrastructure and applications to realize federation of clouds.[1] According to Gartner [2], Big Data is not a market in itself. It requires the processing, applications and middleware. As Companies realize the benefits of Big Data, Cloud Computing and the scalability provided in the cloud become a necessary integration. Garter also predicts the adoption of the PaaS model to increase. Though, PaaS is the future of this technology as clouds are expected to host applications designed for a particular platform [3], but the in present scenario it becomes difficult to analyze what platform specific applications are really like.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

With an expected increase in Cloud Implementation, there is also an expected push in the direction of Standardization of clouds. As data security is a major issue with Clouds, use of standards is expected to increase the technology's credibility. [4] ENISA discussed about the different security risks related to adopting cloud computing along with the affected assets, impacts, the risks likelihood, and vulnerabilities in the cloud computing may lead to such risks.[5] Balachandra et al, 2009 discussed the security SLA's specification and objectives related to segregation ,data locations and data recovery.[6] Kresimir et al, 2010 provide detail about the high level security concerns in the cloud computing model such as privacy, payment and data integrity of sensitive information.[7] Bernd et al, 2010 discuss the security vulnerabilities existing in the cloud platform. The authors grouped the possible vulnerabilities into technology-related, cloud characteristics-related, security controls related.[8] Subashini et al discuss the security challenges of the cloud service delivery model mainly focusing on the SaaS model.[9] Ragovind et al, (2010) discussed the management of security in Cloud computing focusing on Gartner's list on cloud security issues and the findings from the International Data Corporation enterprise.[10] Morsy et al, 2010 investigated cloud computing problems from the cloud architecture, cloud offered characteristics, cloud stakeholders, and cloud service delivery models perspectives.[11] A recent survey by Cloud Security Alliance(CSA)&IEEE indicates cloud computing is shaping the future of IT but the absence of a compliance environment is having dramatic impact on cloud computing growth.

The years 2012 and 2013 mark the Bring-Your-Own-Device (BYOD) Era, wherein Laptops and PCs are being replaced by thin clients such as Tablets and Mobiles. This shows a clear adaptation of Cloud Computing Application as a Service model. Most of the processing is done on the Cloud Infrastructure and the user's machine is simply used to access the cloud.

The choice between Open source Clouds and Proprietary Cloud Models has only become increasingly difficult with the competition between Openstack and CloudStack. OpenStack is a multi-tenant cloud model that allows users to control the workload across various servers. It was an initiative of Rackspace and NASA. [12]

The split of Citrix form Openstack standards to create Cloudstack has led to an increasing competition between these two technologies.

The reaction of the Industry to these recent developments will decide the course of further developments in the field of Cloud Computing. The direction and extent to which the technology evolves also depends on the course that the IT Industries follow.

III. SERVICE MODEL

Cloud Computing is a technology that offers its services in various ways. These ways, as well as the conventional on-premise method, have been discussed below-

Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar:

- On-Premise Setup- In an On-premise setup, all the tasks related to the provision of services is performed by the user of the applications. The user not only has to pay for the setup but also the maintenance and up gradation of the software as well as hardware.
- Infrastructure as a Service (IaaS) - This setup helps the user to deploy applications and OS on computing resources (such as memory, networking, etc.) provided by the service provider. Examples include Amazon EC2 and S3, Windows Live Skydrive and Rackspace Cloud.
- Platform as a Service (PaaS) – This provides application platform or middleware as a service along with other services. Paas allows users to build and deploy their own applications with ease on the infrastructure that the cloud service provider supports. Examples are Microsoft Azure, Force and Google App engine.
- Software as a Service (SaaS) – This is setup that allows the user to use application as a service rather than on-premise applications. In contrast to On-Premise Setups, SaaS takes care of all the components involved from networking to application level contrast to On-Premise Setups, SaaS takes care of all the components involved from networking to application level. Examples include Sales-force CRM, Google Docs, etc.

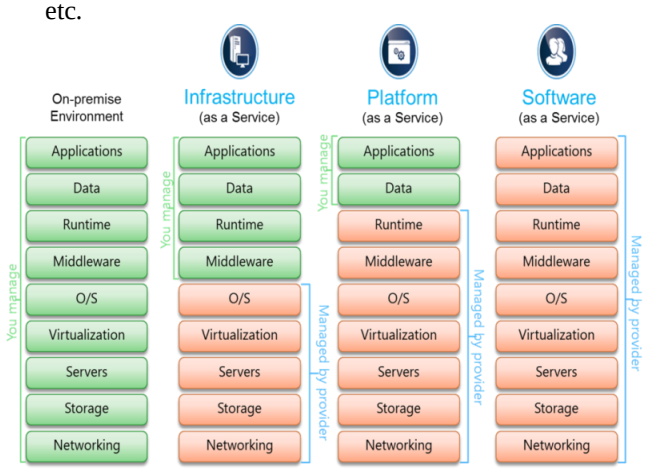

Fig. 1. Cloud Computing Service Models[13]

A. *Deployement Work*

There are majorly four deployment models of Cloud Computing. Each of these has its own set of customers it targets-

• Public Cloud - It is a large scale cloud platform which provides services to customers including individual users, organizations, etc. Customers with privacy concerns do not feel safe using this type of cloud due to security concerns.

• Private Cloud – This type of cloud provides the same services as a public cloud but within the boundaries of the organization that owns the private cloud. It is smaller as compared to Public Clouds and ensures high data security.

• Community Cloud – Organizations with similar requirements use this cloud platform. It is a generalization of the Private Cloud.

• Hybrid Cloud – It is a platform that implements services by combining the various deployment model techniques. It is useful for integration purposes. Customers that want the benefits of public cloud along with the security offered by the private clouds often implement the cloud using this model.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

B. Basic Archeitecture

To understand the architecture in the most basic sense, the entire setup is divided into two parts-

- Front End- This is the part visible to the user. The client computer and the applications needed to access the cloud are in this part of the architecture.
- Back End- This is the cloud itself. It consists of various computer servers, data storage units, etc. that are needed to implement the cloud. This is the actual hardware and software needed to implement the cloud and provide services to the users.

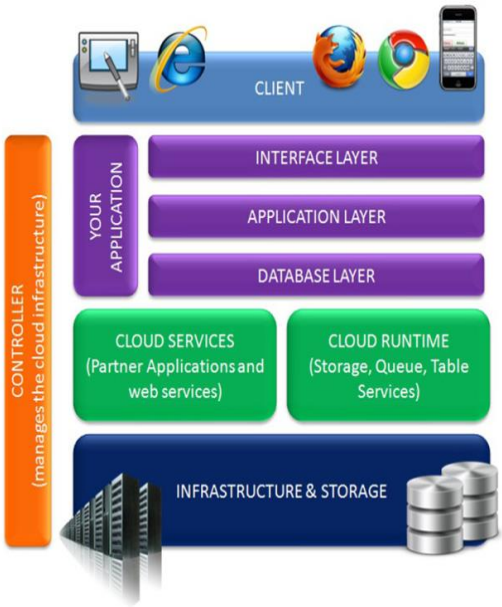

Fig. 2. Basic Cloud Architecture [14]

Figure 2 is the diagrammatic representation of basic cloud architecture in a Layered manner. It shows the front end as the Client layer. This layer consists of the client device and the web browser (or any other application) that the user needs to access the cloud and use its services.

The Back End consists of the actual hardware infrastructure, such as servers, memory units, etc., as the lowest layer. The Cloud Service Layer is responsible for the services that the cloud actually provides and the Cloud Runtime Layer consists of the various technologies used to implement the cloud. The Cloud Runtime manages the requests and monitors the amount of resources used by each user.

The actual application or services being used by the user are executed by using the Interface, Application and Database Layers in conjugation with each other. All the layers and the interfaces between them are monitored by a Cloud Controller that controls the entire cloud and its functioning.

IV. PROPOSED WORK

Use After In order to analyze the areas of further work in the implementation and adaptation of the Cloud Technology and to maximize the benefits of this technology, it becomes necessary to evaluate the existing implementations. The Table 1 discusses the popular Cloud Implementation available in the market. The comparison between Google App Engine, Microsoft Azure, Salesforce, Amazon EC2, IBM Cloud and MS Office 365 is done on the basis of the platforms supported, the pricing, scalability, security, reliability and key features.

The basic advantages of using this technology, i.e. the benefits of Scalability, Pricing, Multi-Application support and Multi-Platform support, are provided by all the Clouds compared in the table. But the major drawbacks of the Cloud are tackled by each of them differently.

A. Security Issues

The major drawback of the cloud is the lack of security provision in the cloud that makes organizations and businesses hesitant in adopting this model as their working model. Entrusting private data of their organization with another organization is the major problem faced by organizations. Because of these issues, the adaptation of the Cloud by any organization comes with a lot of reluctance.

The major cloud computing security issues are:

- Data and Information security: In the multi-tenant data system, the user has to trust the cloud provider that the data will not be exposed. Many customers are unaware of how reliable or unreliable the service provider is.
- Distributed Cloud Computing Issues: Cloud computing ranges over thousands of databases in various countries and involves various service providers. If the communication between two service providers is not secured (say using encryption), then the user's information is at risk.
- Lack of Standards: The cloud is still a relatively new technology and lacks specific standards in terms of data security and reliability.
- Local Law and Jurisdiction: Another major issue with the cloud is that, the databases are scattered and what may be secure for a user in one country may not be the security standard in the country the database is located.
- Web Application and Accessibility Vulnerabilities: The vulnerabilities in web applications such as sql-injection or mis-configured applications along with denial-of service attacks, make it difficult to ensure complete security.
- Multi-device access: IP spoofing, RIP attacks are very common over the Internet. Allowing access using multiple devices also poses a problem.
- Service Provider Dependence: The inherent disadvantage of cloud computing is that the organization has no physical access to the data on the cloud and have to completely rely on the service provider. But there exists a gap between what is actually done and what is promised.

B. Resolving the Issues

There exist several organizations and groups that are working to provide standards and measures that make the Cloud a reliable and secure technology thereby, allowing more users to rely on the cloud.

The Open Web Application Security Project (OWASP) maintains a list of the top 10 vulnerabilities in the Cloud-Based or Software as a Service deployment models. This list is updated as the scenario of the threats changes. The Open Grid Forum is a forum that publishes documents for computing developers and researchers providing them with security and infrastructural specifications and information.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

1. Privacy and Control Solutions

Hayes [15] points out in his research that allowing a third-party service to take custody of personal documents raises questions about control and ownership: If you move to a competing service provider, can you take a data with you? Could you lose access to your documents if you fail to pay a bill? The issues of privacy and control cannot be solved, but merely assured with tight service-level agreements (SLAs) or by keeping the cloud itself private. But owning a private cloud may not be the most beneficial solution for all organizations. Rackspace provides an easy 10-step guide to allow organizations and users to decide and choose the best cloud for the organization according to their immediate and future needs [15]. The applications needed by the organization are mapped against the cloud offerings in order to check feasibility, as shown in Figure 3.

Based on this, the organization can decide the service-level agreements (SLAs) and the level of control.

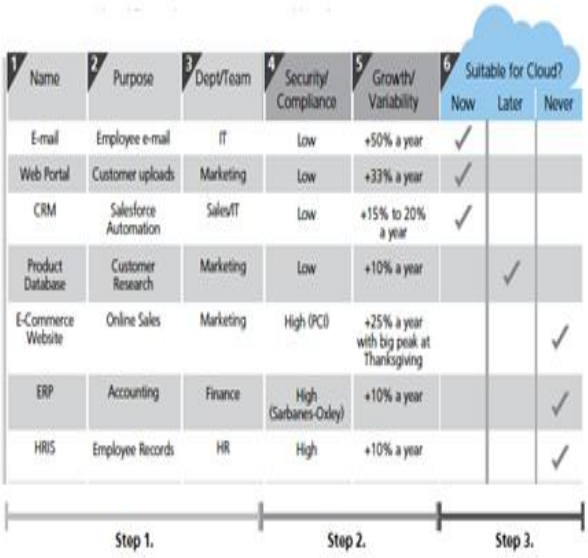

Fig. 3. Deciding the best cloud solutions [16]

2. Data Tempering and Theft Solution

Raj [17] suggests that in order to ensure Data Authenticity, a solution would be to allow resource isolation of data during processing, by isolating the processor caches in virtual machines. These isolating virtual caches are further to be isolated from the Hypervisor cache.

Another issue related to data is the ownership of data after termination of the account. Would cloud-providers be allowed to access the data even after the user has terminated the account and can the user port the data to another service provider as he terminates his service agreement with the first service provider? These areas still need standards and laws to ensure preservation of the intellectual property and personal information of the users.

3. Minimizing Vulnerabilities at ServiceProvider's End

Since all the work and information crucial to the business of an organization is entrusted with the cloud service provider, Data should be backed-up at regular intervals to avoid any data loss. Service Providers should have alternate plans and proper data recovery mechanisms to allow security of data and minimize loss.

The service provider should carry out testing at regular intervals of time as the threat landscape of cloud computing is constantly changing and is dynamic. Firewalls must also be installed and must be checked at regular intervals.

C. Secure Framework for Clouds

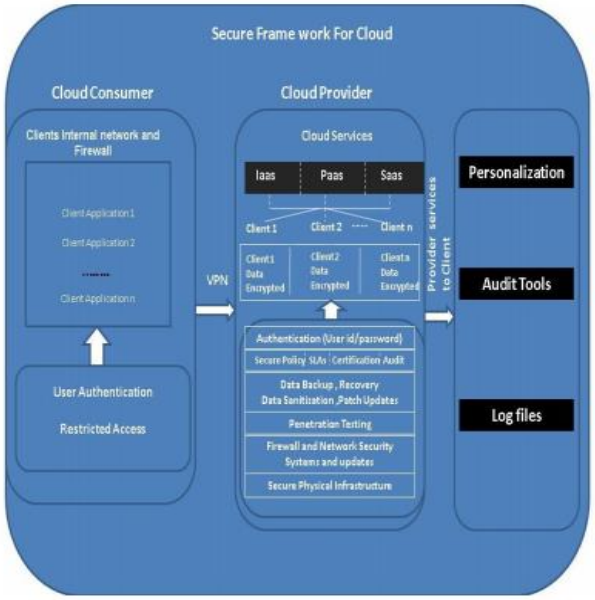

Fig. 4. Secure Framework for Cloud [18]

The above diagram suggests security of data while accessing the data and avoids penetration of data by unauthorized persons. But the security in the cloud has to be two-way:

- Security of Stored data: This can be ensured by following the measured suggested by the framework both at the client's end and at the service provider's end.
- Security of Moving data: Security of moving data is most crucial as the vulnerabilities of the Internet are all involved in this.

Data transfers can be between enterprise and cloud, cloud and cloud or mobile and cloud. All these data transfer involve the flow of data over open Internet and are subject to the vulnerabilities of the Internet.

One way to secure data transfers in a cloud is to encrypt the data and assign a key to it. Only the authorized recipient would be able to decrypt the information with the key. The challenge here lies with the Virtual machine Operating system. If data is transferred to an unprotected VM, the risk of the data getting exposed increases. This problem can be solved by integrating many data files into a single data file and allowing them to be sent together so that loss of files is minimized. In this manner, a uniform platform can be achieved for protected and unprotected Virtual Machine Operating Systems. Thus, the above framework allows a safe framework for data security in the cloud.

V. CONCLUSION

Cloud computing is a technology of the future. It provides an efficient and flexible method of resource management in IT Organizations. This technology has many benefits and features that make it ideal for businesses and organizations to manage their resources.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Though there are many benefits of Cloud Computing, the lack of security standards and privacy enforcers has posed many disadvantages. The methods suggested in the paper can help to some extent in resolving these drawbacks. The curbing of the disadvantaged of the cloud are crucial to the adaptation of this model.

REFERENCES

1. http://cloudtimes.org/2012/11/28/standardization-cloud-norm-cloudnow-2013-predictions/.
2. http://ecomcanada.wordpress.com/2011/06/24/cloud-computing-architecture-good-practices-in-application-design-for-the-cloud/.
3. http://cloudtimes.org/2012/11/28/standardization-cloud-norm-cloudnow-2013-predictions/.
4. ENISA. (2009, Feb) "Cloud computing: benefits, risks and recommendations for information security." Available: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computingrisk-assessment [Jul. 10, 2010].
5. R. K. Balachandra, P. V. Ramakrishna and A. Rakshit. "Cloud Security Issues." In PROC '09 IEEE International Conference on Services Computing, 2009, pp 517-520.
6. P. Kresimir and H. Zeljko "Cloud computing security issues and challenges." In PROC Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2010, pp. 344-349.
7. B. Grobauer, T. Walloschek and E. Stöcker, "Understanding Cloud Computing Vulnerabilities," IEEE Security and Privacy, vol. 99, 2010.
8. S. Subashini, and V. Kavitha. (2010) "A survey on security issues in service delivery models of cloud computing." J Network Comput Appl doi:10.1016/j.jnca.2010.07.006. Jul., 2010.
9. S. Ramgovind, M. M. Eloff, E. Smith. "The Management of Security in Cloud Computing" In PROC 2010 IEEE International Conference on Cloud Computing 2010.
10. M. A. Morsy, J. Grundy and Müller I. "An Analysis of the Cloud Computing Security Problem" In PROC APSEC 2010 Cloud Workshop. 2010.
11. Cloud Computing Use Case Discussion Group. "Cloud Computing UseCases Version 3.0," 2010.
12. http://www.ifactum.com/doc.cfm?id=2236&searchby=publication&keywords=&topic=&name=SYS-CON%20Media&cname=&str=2301&maxr=25.
13. http://blog.moduslink.com/bid/81962/Cloud-computing-services-from-a-business-viewpoint-Part-2-How-to-implement J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.
14. http://www.bsmreview.com/bsm_cloudcomputing.shtml
15. Hayes, B. (2008). Cloud computing. Commun. ACM, 51(7), 9-11. Retrieved from http://portal.acm.org.library.capella.edu/ft_gateway.cfm
16. http://wolfhalton.info/2010/06/25/security-issues-and-solutions-in-cloud-computing/#ixzz2QYqygaUM
17. Raj, H., Nathuji, R., Singh, A., & England, P. (2009)," Resource management for isolation enhanced cloud services", In Proceedings of the 2009 ACM workshop on Cloud computing security (pp. 77-84). Chicago, Illinois.
18. http://zenithresearch.org.in

Table 1: Comparison of Available Clouds

Cloud Name	Platform	Key Features	Price	Scalability/ Flexibility	Security	Reliability
Google App Engine	Java and Python Runtime Environment	Google Search Gmail Chrome browser Google Maps	Billing is based on: Bandwidth, CPU Time, Stored Data, Recipients Emailed	Automatic scaling is built in with App Engine	Google's 2 step verification	The user is solely responsible for securing and backing up the Application and any Content.
Microsoft Azure	Operating systems Windows 7 Windows Server 2008 Windows Vista	Azure will support more programming languages and development environments in the near future.	Pay-as-you-go pricing	Automatic scaling and highly scalable. Open platform supports both Microsoft and non-Microsoft languages and environments	Multiple levels of security at Microsoft-quality scale.	Fabric Controller technology reroutes work instantaneously if a server goes down; 99.9% - 99.95% uptime.
Salesforce	Supports all major development environments including .NET, Java	Offers cloud solutions for automation, customer service, and platform, respectively. Transparency through real-time information on system performance and security at trust.salesforce.com.	Pay-as-you-go pricing	Yes - Scales with you, without requiring re-architecture or data migrations.	Physical security, user authentication, application security, and more.	Facilities are identical and transactions are mirrored instantly, making interruption of service related to hardware problems or data issues virtually impossible.
Amazon EC2	Supports many Operating systems and all languages.	Provides Infrastructure as a Service.	Pay-as-you-go Pricing	Amazon S3 - Store upto 5 GB Amazon EC2 [Elastic Block storage] ranging from 1GB to 1TB	- Advanced Firewall - Critical Data Privacy - Failover Features	Guaranteed Network Availability (99.999%) Snapshot backup Available.
IBM Cloud	Red hat Enterprise Linux, SUSE Linux and Windows Server 2008	Provides Infrastructure as a Service.	Pay-as-you-go Pricing	Provides scalable storage-virtualization solution at lower operational costs.	-Critical Data Privacy	Backup storage Available as a paid-service.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

MS Office 365	Windows Operating Systems and Mac OS X.	Various apps powered by Microsoft Exchange Online, Microsoft SharePoint Online, Microsoft Lync Online	Pay-as-you-go Pricing	Allows organizations to determine the configuration and options that best meet their specific needs	Data is secured in 5 different layers – data, application, host, network and physical	Information is safeguarded with geo-redundant, enterprise-grade reliability and disaster recovery that is accomplished with multiple datacenters and automatic failovers.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)