www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242

Volume - 3 Issue -9 *September*, 2014 Page No. 8147-8154

A Comprehensive Analysis of Cloud Computing Including Security Issues and Overview of Monitoring

Deepika Upadhyay[1], Sanjay Silakari[2], Uday Chourasia[3]

[#] Deptt of CSE, UIT- Deptt of CSE, UIT, RGPV-RGPV
Bhopal, MP, India
[1]*deepikaa05uitbpl@gmail.com*
[2]*ssilakari@yahoo.com*
[3]*uday_chourasia@rediffmail.com*

ABSTRACT: ***Cloud computing is a widely adopting paradigm now days. Primary reason behind more organizations adopting cloud is reduction in cost and dynamic resource allocation. Also various characteristics such as scalability, elasticity, multi-tenancy, pay-per-use approach make cloud computing the most wanted and widely popular paradigm today. But with these characteristics, cloud inherits some serious issues like insider attacks, security, and reliability. Cloud is deeply affected by malicious attacks, for example in 2009 Google was attacked by DOS intrusion that took down services of cloud like Google news, Gmail for several days. So the major focus and challenge is securing cloud because huge amount of users and IT organizations implementing cloud services, this is the reason that gaining large user's trust is very important. Cloud monitoring helps to properly manage and control these issues in an efficient way. This paper has done a brief analysis of cloud computing, security risks in cloud, and overview of cloud monitoring. Current platforms of cloud monitoring are surveyed based on some evaluation parameters and services. Finally research is outlined for cloud monitoring and attack detection using monitoring.***

Keywords : ***Public Cloud, Private Cloud, Hybrid Cloud. Cloud monitoring and APM.***

1. Introduction

Cloud computing [12] can be defined as way of providing IT resources in the form of computing infrastructure ,storage ,networking ,computing application to consumers as services using Internet at any time whenever they are required. Cloud is an assemblage of hardware, software, IT services, networks that deliver aspects of computing in the form of services on demand [23].It enables users to use any IT computing services without having any requirement of buying, forming infrastructure or understanding underlying technologies .consumers pay on a pay per use approach. Commercial cloud providers such as Amazon web services(AWS),Microsoft Azure, Salesforce.com, Google App Engine enables cloud users to deploy their applications over a wide pool of resources with minimum capital expenditure and operating expenses equivalent to actual use. Cloud computing offers on demand services with fast elasticity and enhanced automatic scaling features, concurrency, security. To provide these services latest techniques for virtualization, dynamic scheduling mechanism, security approaches are implemented within cloud. Cloud computing provides Data centers which are growing continuously in terms of hardware ,thereby making cloud management and implementation very complicated [2].To cope up with this complexity and to manage operations of cloud platforms ,authentic monitoring services are needed.

Paper is organized as follows: Section 1 describes cloud computing and its various aspects. Section 2 illustrates need of cloud monitoring and overview of monitoring system including advantages and working of Application Performance Monitoring (APM). Then related works in cloud computing and security issues have been surveyed and cloud monitoring platforms are depicted based on some evaluation metrics. At last, conclusion of this paper is discussed.

2. Cloud computing overview

2.1 Cloud Computing Offerings

Cloud offers following benefits –

- Reduced capital expenses as well as operational cost as CAPEX and OPEX [12].

- Better and improved Quality of services with delivering new services. It ensures proper business growth with decreased expenditure.
- It makes sure that all applications and resources are delivered in a much secured way with high flexibility.
- Advanced services are quickly delivered in an improved way to explore opportunities while maintaining cost, managing risks.

2.2 Motivations for adopting clouds

There are many reasons behind the adoption of cloud computing paradigm which are explained as follows -

- It provides large web scale abstracted IT infrastructure, dynamic provisioning, pay per use approach, long term commitments are not required, and no need of installing hardware or software.
- It is a way of exploiting latest advancements in software, networks, storage capabilities .Big IT organizations promotes cloud computing where these latest technological advancements are done.
- Large financial and industrial companies, healthcare organizations adopt cloud as it mainly focuses on IT and enterprise computing.
- Application developers are not confined to a single system as cloud gives the illusion of countless computing services. This gives elasticity to cloud computing.
- Cloud users follow pay as you go approach by removing the requirement for upfront financial commitment.
- Enhanced proficiency of energy, optimized usage of hardware and software, performance isolation, provision of on demand services [21] made it popular as a broadly adopted model for providing IT resources over internet.

2.3 Fundamental Concepts of Clouds

According to NIST, there are 5 fundamental concepts in cloud [12], [9] as Cloud Characteristics, Service models, Hosting, Deployment models and Roles which are broadly elaborated as follows -

2.3.1 Cloud Characteristics

Cloud contains 5 major characteristics as following -

2.3.1.1 On Demand Services

No human interaction is needed with resource provider for provisioning computing services like storage, server time.

2.3.1.2 Ubiquitous Network Access

Computing services are there over the network and these can be accessed with the help of standard methods using heterogeneous consumer platforms (e.g. mobile phones, laptops).

2.3.1.3 Location Independent Resource Pooling (Multi-Tenant)

Resources are gathered in order to serve various clients with the help of multi tenant paradigm where resources are allocated and reallocated dynamically on demand. Clients have no idea about the location of services.

2.3.1.4 Rapid Elasticity

Resources are provisioned in a rapid manner with quite good elasticity and released in the same manner to scale in.

2.3.1.5 Measured Services

Resource utilization is controlled by providing a metering ability .Clients pay bill on the basis of measured use of resources provisioned for a specific session.

2.3.2 Service Models

Service models of cloud can be classified into 3 categories in the following manner :

2.3.2.1 SAAS

Software are deployed to the client whenever demanded through a licensing paradigm known as on demand licensing where clients rent application usage on a pay per use basis. SAAS can be defined as ability given to the client to utilize software application of provider which runs on infrastructure of cloud.

2.3.2.2 PAAS

A virtual computing platform is presented in PAAS which is hosted by cloud and web browser has the ability to access it. Solution stack is also delivered in order to improve developing and deploying of web applications. Developers can develop software applications without installing software developing tools on their personal computers. In PAAS, application and software standards are provided according to the needs of clients, toolkits are configured for virtual development ambience.

2.3.2.3 IAAS

Model that include provisioning of computing services like storage, networking capabilities ,processing elements to enable clients to run their applications .

2.3.3 Deployment Model

Cloud can be deployed in 4 models -

2.3.3.1 Private Cloud

These are implemented only within an enterprise or organization. Enterprise or third party owns it .Private clouds are operated within an enterprise firewalls and onsite server run them. They provide services such as virtualization, multi tenancy, continuous deployment, security, access control.

2.3.3.2 Public Cloud

Cloud infrastructure is open for use by the individual clients, industries or big organizational groups based on pay as you use approach. Clients can get cloud services through cloud service providers.

2.3.3.3 Hybrid Cloud

It is an assemblage of private, public and community clouds. Public and private clouds both are operated by hybrid cloud simultaneously. It includes the concept of Cloud Burst in which application running on enterprise infrastructure can be deployed to the cloud in case of any demand.

2.3.3.4 Community Cloud

A shared infrastructure is defined in this type of cloud and several organizations support it.

2.3.4 Cloud Roles

Cloud computing contains some entities as per NIST reference paradigms, which are summarized in Fig.1 and are following:

2.3.4.1 Consumer of Service

Utilizes services provided by cloud service provider.

*2.3.4.*2 Cloud Service Provider

It takes the responsibility of making cloud services available to clients of cloud.

2.3.4.3 Carrier

It connects cloud service providers with consumers and is responsible for transporting cloud services.

2.3.4.2 Broker

Responsible for managing uses, cloud services delivery and negotiation of relationship between consumer and provider.

2.3.4.3 Auditor

Evaluates systematically the cloud by defining its conformation to well defined criteria in cloud.

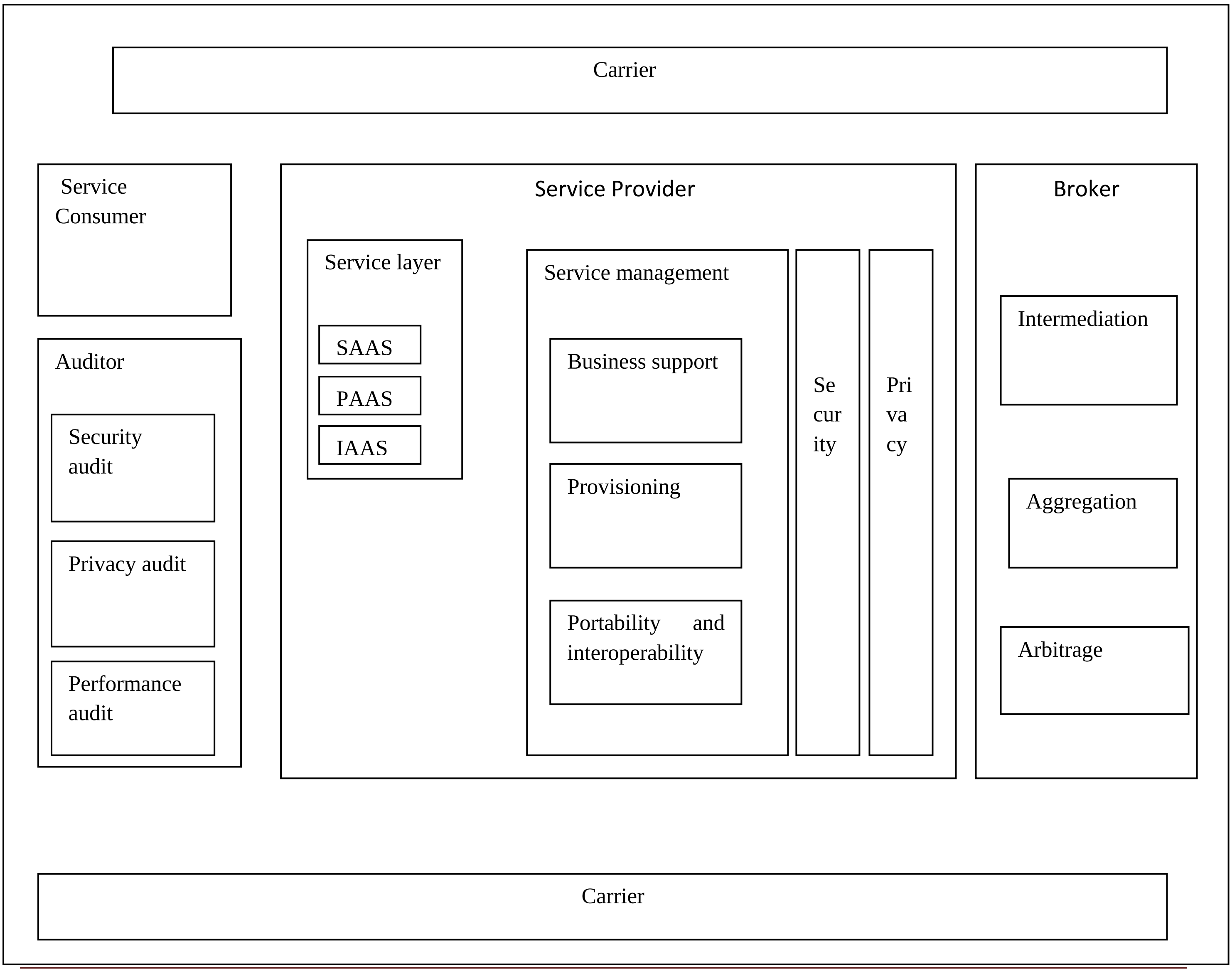

Figure 1: Cloud Entities.

3. Cloud Monitoring

Apart from these aforementioned characteristics and qualities, cloud computing poses various challenges like load balancing, provision of quality of services and performance of application, guarantee of meeting SLA, and managing widely available and complicated cloud infrastructure. To deal with these issues efficiently, authentic and fine-grained monitoring techniques are needed [12]. Several benefits of cloud monitoring regarding business [5] are as follows -

- Enterprise can make correct and timely decision about allocating resources only if it has full knowledge about its resource utilization. This leads to solving problems very easily In this way some performance issues can be resolved without affecting business critically.
- It provides full visibility into cloud performance and infrastructure services by enabling organizations to manage dynamic changes in services in dealing with changing business needs, with assuring absolute Quality of Services and minimum cost.
- Monitoring tools are provided which monitor SLA, performance, cloud computing usage independently helping in making accurate decisions about returns after investing in cloud services.
- It keeps track of Quality of Services metrics of resources, applications dynamically.
- Cloud monitoring enables application developers to keep their services and applications at high efficiency, detect violations in performance of applications.

Fundamental concepts of cloud monitoring are Layers of cloud where monitoring probe is to be put, monitoring and monitoring tests as follows -

3.1 Layers in Cloud Monitoring

Cloud security alliance [24 and 18] represents cloud in 7 layers.

3.1.1 Facility Layer

It deals with the infrastructure that is made up of data centers hosting the computing environment.

3.1.2 Network Layer

Deals with the network connections within the cloud, and between cloud and consumers.

3.1.3 Hardware Layer

It considers physical elements of networking and computing.

3.1.4 Operating System

Software including operating system of host and guest are considered.

3.1.5 Middleware

Layer of software which is present between operating system and application run by client.

3.1.6 Application Layer

Clients of cloud run application layer.

3.1.7 Client

Users of cloud are included.

3.2 Application performance monitoring in cloud

They help to discover security risks in a very quick manner. These are used as an early warning system to find out security breaches. In this way monitoring system can work as Early warning system. Good APM tools should be able to indicate abnormality in the application graphically.

They should have the ability to go deeper over time in order to check if the activity is normal or not over time duration. Two aspects of an APM tool are analyzed [20] to determine triggers that may cause a security breach. Cloud performance monitoring can be done into 2 phases: Monitoring system Performance and Monitoring Application Performance.

3.2.1 Monitoring system performance

This is related to the cloud service provider. It is also known as Low level monitoring. Information is collected at hardware layer (in the form of memory, CPU, workload), at middleware layer (in the form of vulnerabilities related to soft ware), at network layer (security of physical infrastructure using firewalls), and at the facility layer. In these different elements of a cloud infrastructure such as virtual machines, networking and storage capabilities are monitored. Whenever statistics of system are being monitored, first baseline is checked after that all different actions are measured over a long period of time. If some unknown pattern is experienced then the next element to be checked out is change management. It determines recent changes in an application or server; if nothing has been changed then security risks may have been occurred. Parameters that are monitored are CPU, network trending, memory trending, Disk I/O.

3.2.1.1 CPU Trending

Changes to utilization of current CPU are measured. This is done over a particular time of period. Increment and decrement of CPU utilization may represent a sign of security risk or attack.

3.2.1.2 Network Trending

Attack is made up of 2 phases. In first one, network is used in order to evaluate the protocols which a server uses. Then attacker determines the running application and finally the attack is launched over the network. Network activities are increased suddenly as soon as attack is there. So to determine if something unusual is occurring, network trending baseline is investigated closely.

3.2.1.3 Memory utilization

Memory is used by all programs running within a system. So memory trending is a basic element to determine the security breach.

3.2.1.4 Disk I/O

To monitor system disk IO performance, two values are analyzed-I/O rate and I/O operations per seconds. Upon showing different behavior even if application runs normally, it is indicated that some unknown risks have been occurred.

3.2.2 Monitoring Application Performance

This is related with the cloud consumers whose applications are hosted in cloud. It is also known as high level monitoring. Information about virtual platform is assembled at middleware, application and user layer. In system performance monitoring, possible security risks are measured. However malwares could not be detected in few cases within the system. Most of the time its activities get sneaky, so it is necessary that application performance should also be investigated. Application performance monitoring includes following parameters:

3.2.2.1 Application response time

It is defined as time needed for an application which it takes in responding to a user request.

3.2.2.2 Application Index and Throughput

It defines the general health of an application. Generalized values within some predefined range defines Application Index which indicates overall health of an application in terms of throughput, response time ,error rates. They trigger to possible security risks of an application.

3.3 Monitoring Tests

These are of two types-

3.3.1 Based on Computation

These tests are run by cloud service providers. Server throughput, CPU speed, CPU utilization, memory utilization, VM startup time, execution time of VM etc. is being checked upon.

3.3.2 Based on Network

Network layer parameters are tested including round trip time, jitter, throughput, packet loss.

Somewhere cloud monitoring, QoS and SLA are correlated with each other [17]. SLA is a collection of service elements including some specific service delivery components and roles which are identified with the clients. As stated earlier, cloud monitoring is done to measure continuously resources and applications hosted on cloud platform in terms of performance, power usage, ability to fulfill SLA, security. To achieve QoS parameters specified in SLA document, it is imperative for cloud monitoring to handle some violations and uncertainties in an efficient manner. Detection and handling of exception and violations is done through development of efficient monitoring paradigm.

4. Literature Review

Various papers in literature survey properties of cloud[12],[1],[27],[19].Virtualization techniques are elaborated in [10].Several works have analyzed and defined the basic security issues related to cloud such as [5,20, 24, 18 and 26].Gartner[13] specifies 7 safety issues in order to select a particular cloud vendor as Privileged access, regulatory compliance, location of data, isolation ,recovery, investigative support and long term viability.[4] depicts security exercises of major cloud service providers like Slesforce.com, Amazon, Google in three basic features as Security and privacy, Compliance, and legal issues. Cloud security alliances [5] discover 13 areas which need some concern in the era of cloud security. Ingo Muller evaluated the security risks of cloud computing associated with cloud architecture, service delivery paradigm, characteristics of cloud[22].In spite of all the security issues and threats which are present in traditional IT infrastructure cloud computing contains organizations having its own set of security risks. There are some common threats to cloud infrastructure as Eavesdropping, Fraud, Theft, Sabotage, External attack, Logon abuse, Network intrusion, Denial of service attack (DOS), session hijacking attacks. Cloud service provider issues and risks to virtualized systems like Configuration complexity, Inactive virtual machines, isolation of duty, Back door, Spoofing . Chen and Zhao [7] gives a brief analysis on data security and privacy risks of cloud computing. Survey of cloud monitoring is done in [25 and 16] where monitoring characteristics are elaborated in different aspects. Need of cloud monitoring is elaborated in [12]. G. Aceto [12] made a detailed analysis of cloud monitoring including motivations behind deploying monitoring techniques, properties and issues. Cloud monitoring platforms are surveyed in this paper.

4.1 Cloud Monitoring Platforms

Cloud monitoring platforms are surveyed in [17] and [12] with their respective properties. Some of the popular clouds monitoring platforms are as follows:

4.1.1 Monitis

It was founded in 2005 and contains a dashboard where cloud users are able to open multiple widgets to monitor cloud. Any website can be remotely monitored by users of Monitis in order to track uptime, Disk I/O.

4.1.2 Logic Monitor

Founded in 2008.It does a partnership with various third party like VMware, Net-App. Users can monitor across layers of cloud (SAAS, IAAS, PAAS).Virtual infrastructure is monitored by providing multilayered approach.

4.1.3 Nimosoft

Founded in 2011.Multilayered monitoring approach is adopted where virtual as well as physical resources are monitored. It can monitor public and private cloud data centers. Unified monitoring dashboard enables cloud users to monitor resources if they are hosted on various cloud infrastructures.

4.1.4 Nagios

It was founded in 2007 and is an open source monitoring tool. Multilayered monitoring is supported. Users can monitor resources residing on various cloud infrastructures. It is extended with monitoring functionality by using plug-in architecture.

4.1.5 Cloud watch

It is the most popular commercial cloud monitoring tool provided by Amazon. Resources on EC2 are monitored by cloud users. Multilayered monitoring is not supported.

4.1.6 Open Nebula

Open source monitoring toolkit. Data centers are managed by open networking of distributed, public, private and hybrid cloud. SSL protocol is supported which allows users to gain access and information of resources is collected.

4.1.7 Aneka

It is a platform for developing, managing, and deploying cloud based applications. It provides an extensible API which enables development of distributed applications and new capabilities can also be integrated with existing cloud mechanism.

4.1.8 New Relic

It is an application performance monitoring tool for cloud and data center. It provides SAAS solution where real user monitoring, application monitoring, server monitoring and availability monitoring are combined into single solution. New Relic also does partnership with various cloud vendors in order to provide instant visibility into the performance of application which is being deployed.

4.2 Evaluation Parameters

Monitoring platforms are evaluated on the basis of some evaluation parameters as:

4.2.1 Monitoring Architecture

Cloud monitoring tools collect information about network and system. This information is utilized for taking actions such as to fulfill SLA requirements data is migrated to the server closest to the user. Network monitoring is done on following two types of architectures:

4.2.1.1 Centralized architecture

In this, central server for monitoring accepts queries regarding status update of QoS sent from PAAS, IAAS resources. Monitoring information from various companies is collected by monitoring methods by sending probes in a periodic manner. It suffers from some issues like single point of failure, scalability issue.

4.2.1.2 Decentralized architecture

In this, all components of architecture are considered equal so that failure of one component does affect operation of another component.

4.2.2 Interoperability

It enables cloud system to technically interface between different enterprises. For example Amazon runs web server whereas data server is deployed by Azure. It shows some benefits like to achieve advantages of cloud, application and data must be integrated properly across cloud, and vendor lock in can be avoided. Cloud agnostic monitoring tools [3] retrieve QoS aware data services and applications that are part of multiple clouds.

4.2.3 QoS Parameters

Application developers find it non trivial that which QoS metrics need to be specified or monitored across layer of cloud as PAAS and IAAS. These QoS metrics can be composed of single parameters or a collection of parameters [3].

4.2.4 Visibility

To achieve QoS parameters for an application, it is necessary that QoS metrics are monitored across layers of cloud. Visibility of cloud monitoring paradigm can be classified into two types – Layer specific and Agnostic. In layer specific, monitoring platforms perform tasks over services only in one of the 3 layers as SAAS, PAAS, and IAAS. In layer agnostic, cloud users access to data across various layers of cloud. Table 1 shows that cloud users gain access to application data from PAAS and SAAS simultaneously for same application.

4.2.5 Scalability

Scalable monitoring system is able to deal with a huge number of probe messages.

4.2.6 Elasticity

Dealing with any dynamic change that a monitored application shows.

4.2.7 Adaptability

Adaptable monitoring system is able to adapt various computational and networking loads. Monitoring activities sometimes have some negative impact on cloud operations; to avoid this condition adaptability is required. Table 1 summarizes monitoring platforms compared on the basis of some aforementioned parameters.

TABLE 1. Comparison of monitoring platforms against various Evaluation parameters .

S. No.	*Monitoring Platform*	*Monitoring Architecture-Centralized*	*Monitoring Architecture-Decentralized*	*Interoperability Multi-cloud*	*Visibility Multi-Layers*	*Scalability*	*Elasticity*	*Adaptability*
1	Monitis	Not defined (SAAS solution)	Not defined (SAAS solution)	Yes	Yes	No	No	No
2	Logic monitor	Not defined (SAAS solution)	Not defined (SAAS solution)	Yes	Yes	Yes	Yes	No
3	Nimosoft	Yes	Yes	Yes	Yes	Yes	No	No
4	Nagios	Yes	Yes	Yes	Yes	No	No	No
5	Cloud Watch	Yes	Not defined (SAAS solution)	No	Yes	No	Yes	No
6	Open Nebula	Yes	No	No	No	Yes	No	Yes
7	Aneka	Not stated	Yes	Yes	Yes	Yes	Yes	No
8	New Relic	Not stated	Not stated	Yes	Yes	No	No	No
9	Cloud Harmony	Not defined (SAAS solution)	Not defined (SAAS solution)	Yes	No	No	No	No

5. Conclusion

Cloud computing has recently evolved as a compelling paradigm. To manage and deliver services and resources over the Internet. The rise of cloud paradigm is rapidly changing the landscape of information technology, and ultimately transforming the long-term promise of utility computing into a reality. But, despite the significant advantages provided by cloud computing, the current technologies are not matured enough to realize its full potential. Many key challenges in this scenario, including automatic resource provisioning, and security management gain attention to several research groups. This paper has surveyed the state-of-the-art of cloud computing, covering its important concepts, architectural designs, cloud computing challenges and monitoring. Anomaly detection is able to identify unknown attacks, APM includes same concept where deviation in application performance will be a deciding parameter for detecting threats within the cloud environment.

References

[1] A.Letaifa, A.Haji, M.Jebalia, S.Tabbane, “State of Art and Research Challenges of new service architecture technologies: Virtualization, SOA and Cloud Computing”, International Journal of Grid and Distributed Computing, vol. 3, 2010.

[2] B.Rochwerger, D.Breitgand, A.Epstein, D.Hadas, I.Loy, K.Nagin, J.Tordsson, C.Ragusa,M.Villari, S.Clayman, E.Levy, A.Maraschini,P.Massonet, H.Munoz, G.Toffetti, Reservoir – when one cloud is not enough, Computer 44(3) (2011) 44-51.

[3] C.Gong, J.Liu, Q.Zhang, H.Chen, and Z.Gong, “The Characteristics of Cloud Computing,” in Parallel Processing Workshops (ICPPW), 2010 39th International Conference on, 2010, pp.93-97.

[4] Cloud Security Front and Center. Forrester Research. 2009-11-18.

[5] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1.

[6] D.Zissis, D.Lekkas, "Addressing Cloud Computing Security Issues", Future Generation Computer Systems, 28(3), March 2012, Pages 583-592.

[7] Deyan Chen and Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing",2012 International Conference on Computer Science and Electronics Engineering.

[8] Edward L.Haletky,"Using Application Performance Management for Security", The Virtualization Practice.

[9] F.Liu, J.Tong, J.Mao, R.Bohn, J.Messina, L.Badger, D.Leaf, NIST Cloud Computing Reference Architecture NIST Special Publication 500-292, 2011.

[10] Flavio Lombardi, and Roberto Di Pietro, "Secure Virtualization for Cloud Computing", Journal of NetworkandComputerApplications,www.elsevier.com/locate/jnca.

[11] Frederic Desprez, Eddy Caron, Luis Rodero-Merino, Adrian Muresan, Auto-scaling, Load balancing and monitoring in commercial and open-source clouds, in: Cloud Computing: Methodology, System and Applications, CRC Press, 2011.

[12] Giuseppe Aceto, Alessio Botta, Walter de Donato and Antonio Pescape "Cloud monitoring: A survey", Elsevier Science Direct, Computer Networks 57 (2013) 2093-2115, 2013.

[13] Gartner: Seven Cloud-computing security risks. InfoWorld.200802.http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853.

[14] J.Moses, R.Iyer, R.Illikkal, S.Shrinivasan, and K.Aisopos, "Shared Resource Monitoring and Throughput Optimization in Cloud-Computing Datacenters," 2011,pp. 1024-1033.

[15] J.Spring, Monitoring Cloud computing by layer, Part 1, IEEE Security and Privacy 9 (2) (2011) 66-68.

[16] J.Spring, Monitoring Cloud computing by layer, Part 2, IEEE Security and Privacy 9 (2) (2011) 52-55.

[17] Khalid Alhamazani, R.Ranjan, Karan Mitra, Fethi Rabhi, Samee Ullah Khan,Adnene Guabtni, Vasudha Bhatnagar, "An overview of the Commercial Cloud Monitoring Tools; Research Dimensions, Design Issues, and State-of-the-Art".

[18] K.Ren, C.Wang, Q.Wang, Security challenges for the public cloud, IEEE Internet Computing 16(1) 2012 69-73.

[19] M.Ahmed, A.S.M.R. Chowdhury, M.Ahmed, and M.M.H.Rafee, "An Advanced Survey on Cloud Computing and State-of-the-art Research Issues," International Journal of Computer Science Issues (IJCSE), vol. 9,2012.

[20] Md.T. Khorshed, A.B.M.S. Ali, S.A.Wasimi, "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing", Future Generation Computer Systems, 28(6), June 2012.

[21] M.Armbrust, A.Fox, R.Griffith, A.D.Joseph, R.Katz, A.Konwinski, G.Lee, D.Patterson, A.Rabkin, I.Stoica, M.Zaharia, A view of cloud computing, Commun.ACM 53 (4) (2010) 50-58.

[22] Mohamed Al Morsy, John Grundy, Ingo Muller, "An Analysis of The Cloud Computing Security Problem, " in Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010.

[23] P.Mell, T.Grance, The NIST Definition of Cloud Computing, NIST Special Publication 800-145, 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[24] R.Choubey, R.Dubey, J.Bhattacharjee, A Survey on cloud computing security, challenges and threats, International Journal 3 (2011).

[25] S.A. De Chavas, R.B.Uriarte, and C.B.Westphall, "Toward an architecture for monitoring private clouds," Communications Magazine, IEEE, vol. 49, pp. 130-137, 2011.

[26] "Security Guidance for Critical Areas of Focus in Cloud Computing v2.1", Cloud Security Alliance, Dec.2009.

[27] S.Zhang, S.Zhang, X.Chen, and X.Huo, "Cloud computing research and development trend," in Future Networks, 2010.ICFN'10.Second International Conference on, 2010, pp.275-279.

[28] Y.Mei, L.Liu, X.Pu, S.Sivathanu, Performance measurements and analysis of network I/O applications in virtualized cloud, in: 2010 IEEE 3rd International Conference on Cloud Computing (CLOUD), 2010, PP. 59-66.

[29] Sai Kiran Mukkavilli, Sachin Shetty," Mining Concept drifting Network traffic in cloud computing environments ",2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing

PROFILE AUTHORS

Deepika Upadhyay:

Received her Bachelor's degree in Information Technology, TIT, Bhopal, India in 2010. At present she is pursuing her M.E. degree in Computer Science and Engineering from UIT RGPV, Bhopal India. Her research areas include Cloud Computing, security.