iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** XI **Month of publication:** November 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XI November 2017- Available at www.ijraset.com

Cloud Computing Security Challenges and Risks.

Dr. L. Aruna[1]
[1]*Associate Professor, P.G & Research Department of Computer Science, Annai Vailankanni Arts and Science College, Thanjavur*

Abstract: ***Today cloud computing security is the set of new procedural control based technologies and norms are intended to adhere the regulatory agreement rules and protect information, data applications and infrastructure associated with cloud computing use. Cloud storage is a service where data is remotely maintained, managed, and backed up. The service allows the users to store files online, so that they can access them from any location via the Internet. Data security is a major concern, and although options are currently limited, they exist. Even though the following are medium level security risks are identified in cloud computing environment, loss or theft of intellectual property, compliance violations and regulatory actions, loss of control over end user actions, malware infections that unleash a targeted attack, contractual breaches with customers or business partners, diminished customer trust and data breach requiring disclosure and notification to victims. And also the top level or high security risks are identified are as follows unauthorized access to customer and business data, security risks at the vendor side, compliance and legal risks, risks related to lack of control andour business and clients at risk. Here are five data isolation security tips to help and tackle the issue of cloud computing isolation, to avoid storing the sensitive information in the cloud computing, to read the cloud user agreement to find out how the cloud service storage works, be serious about the usage of passwords and use an encrypted cloud service. In this paper consists of a detailed analysis of the cloud security problem. To investigate the problem from the cloud architecture point of view, the cloud offered characteristics view, the cloud stakeholders' analysis, and the cloud service rescue models side.***

Keywords: Cloud computing, Cloud computing security systems, Service providers, Stakeholders and Cloud Management Layer (CML).

I. INTRODUCTION.

The success of modern day cloud computing technologies highly depends on its effectiveness of the world's norms, its simplicity of use by end cloud users and most importantly its grade of information and network security control. Cloud computing is a new and emerging information technology that changes the way IT architectural solutions are lay forward by means of moving towards the theme of virtualization: of data storage, of local networks IaaS, as well as software. The model security is still questionable which impacts the cloud model adoption. The security problem becomes more complicated under the cloud model as new dimensions have entered into the problem scope related to the model architecture, multi-tenancy, elasticity, and layers dependency stack. Cloud computing has all together transformed business and government, and created new security challenges. The progress of the cloud service model delivers business supporting technology more efficiently than ever before. Although cloud computing virtualization is associated degree new cloud computing environment. It will facilitate corporations complete a lot of by flouting the physical bonds between an IT infrastructure and its cloud users, sensitive security threats should be overcome so as to learn totally from this new computing paradigm.

This can be notably true for the cloud computing SaaS supplier. Some security considerations area unit price a lot of discussion. Enterprise security is simply nearly as good because the least consistent partner, branch or broker. With the cloud computing model, they're losing management over physical security mechanism. During the public cloud environment, they are sharing the computing resources with alternative corporations are provided. A public pool external the enterprise, do not have any basic information or management of wherever the available resources are run. Exposing the information in associated with the degree of cloud environment surroundings shared with the sum of alternative cloud corporations might be providing the government. “Logical cause “to seize the assets, as a result of another company has desecrated the law. It is just because they share the environment within the cloud mechanism, might place the information in danger of attack. Cloud storage services provided by one cloud broker is also mismatched with another brokers services ought to conceive to move from one to the opposite. Brokers area unit legendary for making what the hosting world calls "close services;" services that associate degree user might have issue for transporting from one cloud broker to another; e.g., Amazon's "Simple Storage Service" [S3] is incompatible with IBM's Blue Cloud, or Google, or hollow or Drop box. The following figure [1] represents the cloud resources managed at the various layer levels.

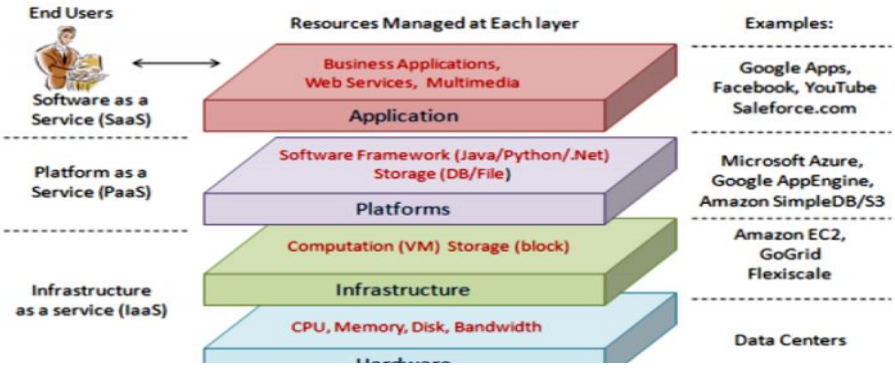
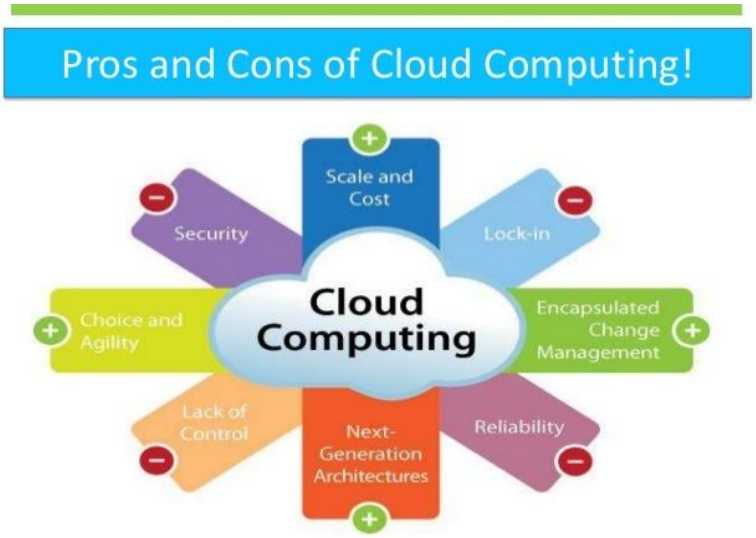


Figure [1] shows the cloud resources managed at various layer levels.

Although cloud computing virtualization is associated degree new cloud computing environment. It will facilitate corporations complete a lot of by flouting the physical bonds between an IT infrastructure and its cloud users, sensitive security threats should be overcome so as to learn totally from this new computing paradigm. This can be notably true for the cloud computing SaaS supplier. Some security considerations area unit price a lot of discussion. Enterprise security is simply nearly as good because the least consistent partner, branch or broker. With the cloud computing model, they're losing management over physical security mechanism. During the public cloud environment, they are sharing the computing resources with alternative corporations are provided. a public pool external the enterprise, do not have any basic information or management of wherever the available resources are run. Exposing the information in associated with the degree of cloud environment surroundings shared with alternative cloud corporations might be providing the government. “logical cause " to seize the assets, as a result of another company has desecrated the law. It is just because they share the environment within the cloud mechanism, might place the information in danger of attack. Cloud storage services provided by one cloud broker is also mismatched with another brokers services ought to conceive to move from one to the opposite. Brokers area unit legendary for making what the hosting world calls "close services;" services that associate degree user might have issue for transporting from one cloud broker to another; e.g., Amazon's "Simple Storage Service" [S3] is incompatible with IBM's Blue Cloud, or Google, or Dropbox. If the cloud computing environment data is encrypted, whereas passing the information through the cloud agency controls using through the encryption or decryption keys in cloud architecture. The most of customers in all probability need their information encrypted each ways in which across the web development of Secure Socket Layers (SSL). Cloud environment additionally possibly need their information encrypted whereas it's at rest within the cloud vendor's storage pool. The following figure [2] represents the pros and cons of cloud computing environment.



Figure[2] represents the pros and Cons of Cloud Computing.

To make sure that simply, the client, management the encryption or decryption keys, even the transfer the cloud information were still resident or own servers in the business organizations. Cloud computing data integrity means that making the certain information is identically maintained throughout any operation (such as transfer, storage, or retrieval). Put simply, information integrity is assurance that the info is consistent and proper. Making certain the integrity of the info extremely implies that it changes solely in response to approved transactions this sounds smart however the need to bear in mind that normal a typical standard to confirm the message of cloud environment information integrity doesn't nonetheless exist. Using the cloud service providers in SaaS offerings also within the cloud environment implies hat there's abundant less want for software package development. as an example, employing a web-based client relationship management (CRM) providing eliminates the requirement to put in writing code and "customize" a vendor's application. To use the internally developed code within the cloud environment it is even a lot of vital to own a proper secure software package development life cycle (SDLC). The various cloud environment technology to use the combinations of net services like the various cloud applications. The following figure [3] represents the cloud security components. As a lot of and a lot of mission critical processes area unit stirred to the cloud, SaaS suppliers

Figure [3] represents the various cloud security components.

can need to offer log information in an exceedingly time period, easy manner, in all probability. Somebody should be answerable for observation for security and compliance, and unless the logic applying and information area unit below the management of finish users, they will not be able to can customers trust the cloud supplier enough to push their missions of critical applications resolute the cloud computing environment. The following figure [4] shows the available various cloud service providers.

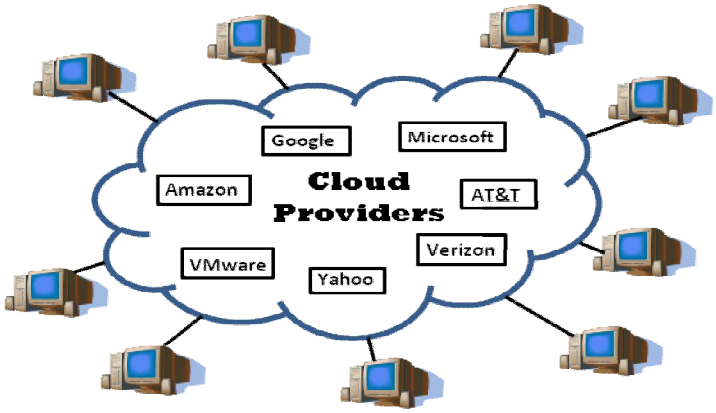


Figure [4] represents the various cloud service providers.

Since the SaaS cloud provider's logs area unit internal and external are not essentially the accessible of outwardly or by purchasers or investigators, observation is troublesome of cloud applications. Since access to logs is needed for Payment of Card system to trade the information Security customary (PCI DSS) compliance and will be requested by auditors and regulators, security managers have to be compelled to make certain to barter access to the provider's logs as a part of any service agreement. Cloud applications endure constant feature additions, and the cloud users should continue thus far with application enhancements to make sure they're protected. The speed at that applications can modification within the cloud can have an effect on each of the SDLC and cloud computing security. To offer a security cycle that keeps up with changes that occur thus quickly. This implies that users should perpetually upgrade, as a result of associate degree older version might not perform, or defend the info. Sections II to IV explore the cloud computing security problem from different perspectives and conclusions.

II. CLOUD COMPUTING UNIQUENESS AND SECURITY SIGNIFICANCE.

To achieve economical utilization of resources, cloud suppliers ought to increase their resource utilization whereas decreasing price. At constant time shoppers ought to use resources as way as required whereas having the ability to extend or decrease the cloud resources consumption supported actual demands. The cloud computing model meets such wants via a win resolution by delivering two key characteristics: multi-tenancy and crack. Each characteristics end up to own serious implications on the cloud model security. Multi-tenancy implies sharing of process resources, storage, services, and applications with alternative tenants. Multi-tenancy has totally different realization approaches one, every tenant has their own dedicated instance with their own customizations. In approach is a pair of every tenant uses an obsessive instance, like approach one where as all instances square of measure constant however with totally different cloud environment configurations (adjustment of application parameters or interfaces).

In approach three tenants share constant instance with runtime configuration (the application is split into core application part and additional parts that square measure loaded supported the present tenant requests- kind of like the cloud service provider Sales Force.com. In approach four tenants square measure directed to a load balancer that redirects tenants requests to an acceptable instance supported current instances load.

Approaches three and four square measure the foremost risky as tenants square measure coexisting on constant method in memory and hardware. This sharing of resources violates the confidentiality of tenants' IT assets that results in the requirement for secure multi tenancy. To deliver secure multi-tenancy there ought to be isolation among tenants' information and the cloud environment placement transparency wherever tenants have not any information or management over the precise location of their resources (may have high level management on information location like country or region level), to avoid planned attacks that commit to co-locate with the victim assets. In IaaS, isolation ought to contemplate VMs' storage, processing, memory, cache reminiscences, and networks. In PaaS, isolation ought to cowl is lactation among running services and APIs calls. In Saas isolation ought to isolate among transactions allotted on constant instance. It implies having the ability to proportion or down resources appointed to services supported the present demand. Scaling up and down of tenant's resources offers the chance to alternative tenants to use the tenant antecedently appointed resources. this could cause confidentiality problems. as an example, tenant A scaled down therefore it releases resources, these resources square measure currently appointed to tenant B United Nations agency successively use it to deduce the previous contents of tenant A. Such placement engines ought to incorporate cloud consumers' security and legal necessities like avoid putting competitors services on constant server, information location ought be inside the tenants country boundaries. Placement engines could embody a migration strategy wherever services square measure migrated from physical host to a different or from cloud to a different so as to satisfy demands and economical utilization of the resources. This migration strategy in a cloud ought to take under consideration constant security constraints. More over, security necessities outlined by service consumers service and initiates a method to enforce security necessities on the new setting, as outlined by clou
consumers, and updates the present cloud security model.

III. CLOUD COMPUTING STAKEHOLDERS AND SECURITY SIGNIFICANCE.

The cloud computing model has totally different concerned stakeholders: cloud supplier (an entity that delivers infrastructures to the cloud consumers), service supplier (an entity that uses the cloud infrastructure to deliver applications/services to finish users), and repair client (an entity that uses services hosted on the cloud infrastructure). Every neutral has their own security management systems or process and everyone has their own
own expectations (requirements) and capabilities (delivered) from or to alternative stakeholders.

This leads to (a) It is a collection of security needs outlined on a service by totally different tenants which will conflict with one another. Therefore security configurations of every service ought to be maintained and implemented on the service instances level and at runtime taking into consideration the chance of fixing need based on current shoppers has to migrate new risks.

The suppliers and consumers have to be compelled to discuss and agree on the applied security properties. However, no commonplace security specification notations square measure out there which will be employed by the cloud neutrals to represent and reason regarding their offered/required security properties.

Every stakeholder has their own security management processes wont to outline their assets, expected risks and their impacts, and the way to mitigate such risks. Adopting cloud model ends up in losing management from each concerned parties, together with cloud suppliers.

(who aren't attentive to the contents and security needs of services hosted on their infrastructures) and cloud shoppers (who aren't in a position to regulate neither on their assets security nor on alternative services sharing constant resources). Security SLA management frameworks represent a part of the answer associated with security properties specification, social control and observation. Moreover, SLAs square measure high level contracts wherever the main points of the protection policies and security management and the way to vary at runtime aren't enclosed. On the opposite facet in the cloud computing environment the cloud suppliers aren't ready to deliver economical and effective security controls as a result of they're not attentive to the hosted services' architectures. Moreover, cloud suppliers with the square measure of cloud in baby-faced with plenty of changes to security needs whereas having a range of security controls deployed that require to be updated. This any complicates the cloud provider's security administrator's tasks. Transparency of what security is implemented, what risks exist, and what breaches occur on the cloud platform and therefore the hosted services should exist among cloud suppliers and shoppers. Cloud shoppers ought to trust in their suppliers meanwhile cloud suppliers ought to deliver tools to assist shoppers to verify and monitor security enforcements.

IV. CLOUD COMPUTING SERVICE RESCUE MODELS AND SECURITY SIGNIFICANCE.

The key security issues and vulnerabilities in every service cloud delivery model. A number of these problems are the responsibility of cloud suppliers whereas others are the responsibility of cloud shoppers. A IaaS problems of VM Security and securing the VM in operation systems and workloads from common security threats that have an effect on ancient physical servers, like malware and viruses, exploitation ancient or cloud oriented security solutions. The VM's security is that the responsibility of cloud shoppers in this environment. Every cloud client will use their own security control based on their wants, expected risk level, and their own security management method. Securing VM pictures repository - not like physical servers VMs are still below risk even after they are offline. VM pictures are compromised by injecting malicious codes within the VM file or perhaps scarf the VM file itself. Secured VM pictures repository is that the responsibilities of the cloud suppliers. Another issue associated with VM templates is that such templates might retain the initial owner info which can be utilized by a brand new client. Virtual network security - sharing of network infrastructure among totally different tenants among identical server (using VM Switch) or within the physical networks can increase the chance to take advantage of vulnerabilities in DNS servers, DHCP,IP protocol vulnerabilities, or perhaps the VM Switch software package that end in network-based VM attacks.

Securing VM boundaries - VMs have virtual boundaries compared with to physical server ones. VMs that co-exist on identical physical server share identical computer hardware, Memory, I/O, NIC, et al. (i.e. there's no physical isolation among VM resources). Securing VM boundaries are that the responsibility of the cloud supplier. Hypervisor security is that the "virtualizer" that maps from the physical resources in cloud environment applications

to virtualized resources and contrariwise. It is the most controller of any access to the physical server resources by VMs. Any compromise of the hypervisor violates the safety of the VMs as a result of all VMs operations become copied unencrypted in cloud environment. Hypervisor

security is that the responsibility of cloud suppliers and therefore the service supplier. During this case, the SP is that the company that delivers the hypervisor software package like VMware.

The PaaS model is predicated on the Service-oriented design (SOA) model. This results in inheritable all security problems that exist within the SOA domain like DOS attacks, Man-in-the-middle attacks, XML-related attacks, Replay attacks, wordbook attacks, Injection attacks and input validation connected attacks. Mutual authentication, authorization and WS-Security standards are necessary to secure the cloud provided services .This security issue may be a shared responsibility among the cloud suppliers, service suppliers and shoppers. API Security in the cloud service provider in PaaS might supply API is that deliver management functions in cloud applications like business functions, security functions, application management, supply information

etc. Such API ought to be supplied with security controls and standards enforced. Moreover, there's a necessity for the isolation of API is in memory. This issue is below the responsibility of the cloud service supplier.

The SaaS cloud model security problems as follows, in the SaaS model imposing and maintaining security may be a shared responsibility among the cloud suppliers and repair suppliers (software vendors). The SaaS model in cloud environment and applications inherits the network in safety problems mentioned within the previous two models because it is constructed on high of each of them together with information security management, like data neck of the woods, integrity, segregation, access, network security , confidentiality and backups.

The Cloud Management Layer (CML) is that the "microkernel "that is extended to include and coordinate totally different elements. The CML elements embody SLA management, service watching, billing, elasticity, IaaS, PaaS, SaaS XaaS services written record, and security management of the cloud. Such a layer is extremely essential since any vulnerability or any breach of this layer can end in an person having management, like an administrator, over the total cloud platform. This layer offers a collection of API is and services to be utilized by consumer applications to integrate with the cloud platform. This suggests that identical security problems with the PaaS model apply to the CML layer similarly in the cloud applications. Cloud Access strategies Security problems: Cloud computing is predicated on exposing resources over the net. These resources is accessed through net browsers just in case of net applications SaaS, SOAP, REST and RPC Protocols, just in case of net services and API in PaaS and CML APIs, remote connections, VPN and FTP just in case of VMs and storage services – IaaS. Security controls ought to target vulnerabilities associated with these protocols to safeguard information transferred between the cloud platform and therefore the shoppers.

V. CONCLUSION

The cloud computing model is one amongst the promising computing models for service suppliers, cloud suppliers and cloud shoppers. However to best utilize the model we want to dam the present security holes. Supported the small print explained on top of, to summarize the cloud security problem as follows:

A. number of the safety issues are hereditary from the used technologies like virtualization and SOA.

Multi-tenancy and isolation may be a major dimension within the cloud security downside that needs a vertical resolution from the SaaS layer all the way down to physical infrastructure to develop cloud security management is extremely essential to manage and manage this range of necessities and controls.

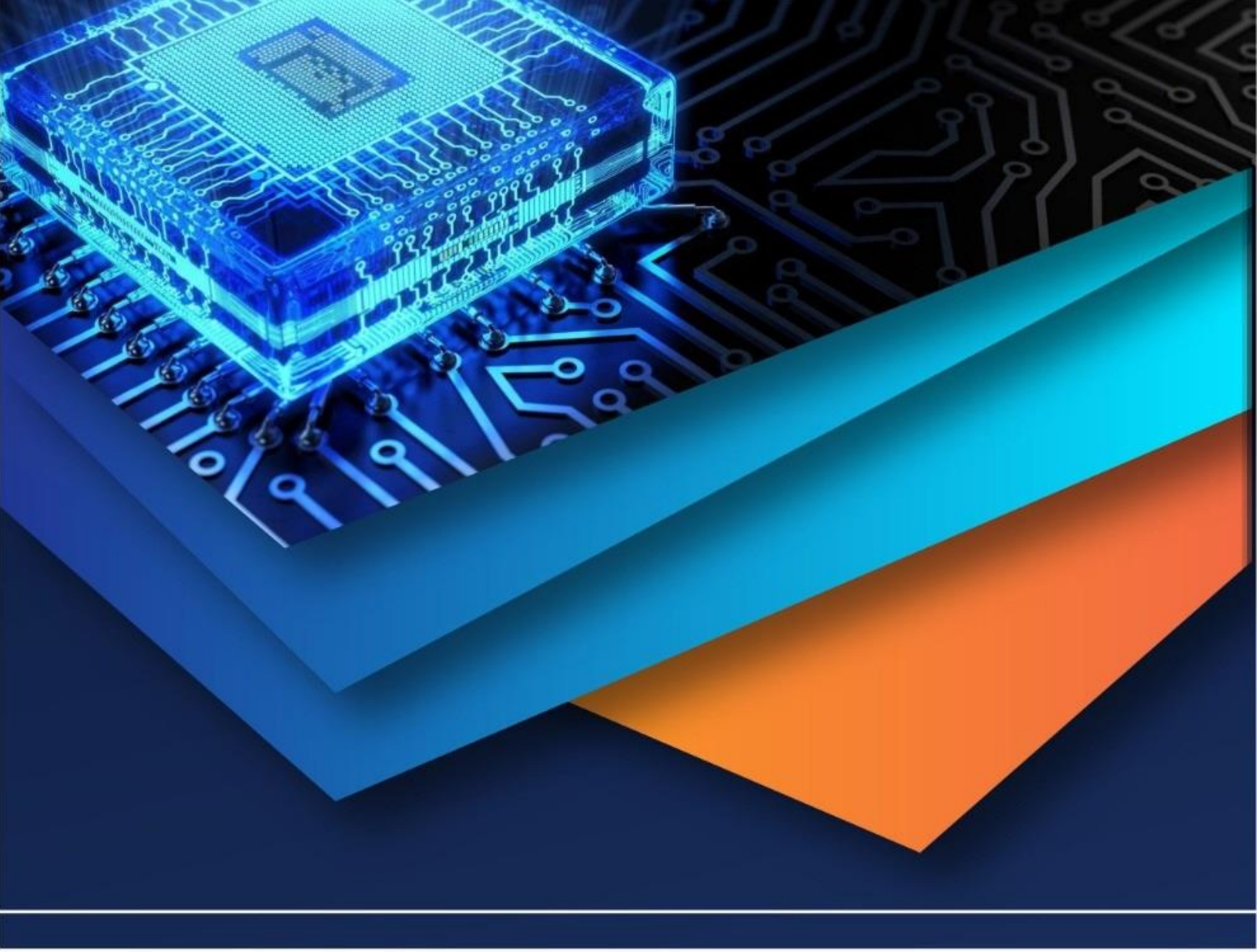
The cloud model ought to have a holistic security wrapper, as shown in figure three, such any access to NY object of the cloud platform ought to experience security elements 1st. Based on this discussion we have a tendency to advocate that cloud computing security solutions should.

1) Target the matter abstraction, exploitation model-based approaches to capture totally in a different security views and link such views during a holistic cloud security model.
2) Inherent within the cloud design. Wherever delivered mechanisms (such as snap engines) and API is ought to give versatile security interfaces.
3) Support for multi-tenancy wherever every user will see solely his security configurations, elasticity, to rescale and down supported this context.
4) Support integration and coordination with different security controls at totally different layers to deliver integrated security.
5) Be adaptive to satisfy continuous atmosphere changes and stakeholders wants.
6) Be adaptive to meet continuous environment changes and stakeholders needs.

REFERENCES

[1] Sapuntzakis, C.P., Chandra, R., Pfaff, B., Chow, J., Lam, M.S., Rosenblum, M.: Optimizing the migration of virtual computers. ACM SIGOPS Oper. Syst. Rev. 36(SI), 377–390 (2002)
[2] Whitaker, A., Cox, R.S., Shaw, M., Gribble, S.D.: Constructing services with interposable virtual hardware. In: 1st Symposium on Networked Systems Design and Implementation (NSDI), pp. 169–182 (2004)
[3] L.Aruna& Dr.M.Aramudhan,"A Novel Survey on SLA based Load leveling in Cloud Computing " International Journal of Research in Computer and Communication Technology, Vol 3, Issue 6, June- 2014-ISSN (Online) 2278- 5841and ISSN (Print) 2320- 515
[4] Jain, N., Menache, I., Naor, J., Shepherd, F.: Topology-aware VM migration in bandwidth oversubscribed datacenter networks. In: 39th International Colloquium, pp. 586-597 (2012
[5] Atif, M., Strazdins, P.: Adaptive parallel application resource remapping through the live migration of virtual machines

[6] http://cloudcomputing.sys-con.com/node/2261725
[7] L.Aruna and Dr.M.Aramudhan, text book for "Fundamentals of Cloud Computing", ISBN No: 978-93- 5137- 266-0
[8] Scarfone K, Singhal A, Winograd T. 2007. Guide to Secure Web Services. [Online] Available from: http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf [Accessed 6th Dec 2010]
[9] Amazon Web Services. 2009. Amazon Virtual private Cloud. [Online] Available from: http://aws.amazon.com/vpc
[10] Guide to XML Web Services Security. [Online] Available from: http://www.cgisecurity.com/ws/WestbridgeGuideToWebServicesSecurity.pdf[Accessed 26th April 2010]
[11] Aljawarneh, S., 2011. Cloud Security Engineering. International Journal of Cloud Applications and Computing, Volume 1(2), pp. 64–70
[12] Rajarajeswari, C., Aramudhan, M., 2014. Ranking Model for SLA Resource Provisioning Management. International Journal of Cloud Applications and Computing, Volume 4(3), pp. 68–80
[13] L.Aruna and Dr.M.Aramudhan, text book for "Fundamentals of Cloud Computing", ISBN No: 978-93- 5137- 266-0
[14] Buyya, R., Ranjan, R., Calheiros, R.N., 2010. InterCloud: Utility-oriented Federation of Cloud Computing Environments for Scaling of Application Services. In: Proceedings of the 10th International Conference on Algorithms and Architectures for Parallel Processing, pp. 13–31
[15] L.Aruna& Dr.M.Aramudhan,"A Novel Survey on SLA based Load leveling in Cloud Computing " International Journal of Research in Computer and Communication Technology, Vol 3, Issue 6, June- 2014-ISSN (Online) 2278- 5841and ISSN No 2320- 5156
[16] Buyya, R., Yeo, C., Venugopal, S., Broberg, J., Brandic, I., 2009. Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility. Future Generation Computer Systems, pp.599–616
[17] Nelson, M., Lim, B.H., Hutchins, G.: Fast transparent migration for virtual machines. In: USENIX Annual Technical Conference, pp. 391–394 (2005).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY