www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 6 Issue 1 Jan. 2017, Page No. 19911-19915
Index Copernicus Value (2015): 58.10, DOI: 10.18535/ijecs/v6i1.09

Analytical Solutions For Security Issues In Cloud Environment

Smaranika Mohapatra[1] and Dr. Kusum Lata Jain[2]

[1]Assistant Professor, [2]Associate Professor
[1,2]Department of Computer Science &Engineering
[1,2]MAIET,Jaipur,Rajasthan
Email:[1]smaranikka.88@gmail.com,[2]jain.kusum81@gmail.com

Abstract: Cloud Computing has become an important infrastructure in today's computing. Globally, the computation is moving towards the Cloud Architecture. It is required that we utilize the methodology to get better results in computing environment and making it applicable in various branches. The main thing to take into account is the security where a few security issues related to cloud computing are derived from the ways used to create such actions; it includes how the methods are scheduled and what type of data can be adopted in cloud. If security is not durable and uniform, the flexibility and merits that cloud infrastructure has to give will have small dependability. In this paper we try to direct and establish the important security matters and provide some kind of solutions in this computing methodology and give a view on the ongoing trends for security in this technological outbreak.

Keywords: Cloud Service, Cloud Computing, security, issues

1. INTRODUCTION

The current development in the field of computing environment is Cloud Computing which has changed the faces of technology. In this environment the resources belong to a different location or network and are acquired by the users remotely [1].. Processing is done remotely knowing the fact that the elements from a person need to be sent to the cloud environment or server for further processing; and the output is returned upon the complete operation of the elements. This gives rise to the following scenarios which are of concern within the cloud computing environment:

• Sending the data (personal) to the server.
• The transmission of raw facts from the cloud server to clients' end and
• Storing the clients' data in cloud servers which doesn't belong to the clients and are remotely placed.

The discussed scenario of computing make it vulnerable to security of data in in cloud. Security is taken as an important aspect a requirement for cloud computing combined as a feasible and reliable result [2].

The familiarities in this perspective indicate an anxiousness for security and legal blocks for cloud computing, enclosing the service accessible, data privacy, provider lock-in and status fate sharing [3]. The security issues originally doesn't exist only on existing system, straightforwardly derived from the chosen technologies, but also associated to new concerns derived from the necessities of cloud computing aspects like scalability, resource sharing and virtualization like data leakage and hypervisor weakness. The deviation between these sections is more efficiently specialized by considering the definition of the important cloud computing features given by the NIST (National Institute of Standards and Technology), which gives the SPI model for services (SaaS, PaaS, and IaaS) and implementation (private, public, community, and hybrid).

Due to the concern in cloud computing, there is an aim to classify the ongoing swing in security. A dependable reference in this area is the risk assessment developed by ENISA (European Network and Information Security Agency) [4]. The Agency also gives a view report of every related work and research approach in addition to the lists the risk and vulnerabilities. The similar work is the security guidance provided by the Cloud Security Alliance (CSA) [5], which gives security fields converges special useful forms from governance and conformity to virtualization and identity management. The main aim of this paper is to classify, group, establish and specify the important security issues and solutions related to cloud computing. Which can be used to formulate instructions to propose an efficient tool for analyzing, informing and grouping the defined issues and solutions as well as the upcoming ones. The following paper discuss about the analysis of the main security frameworks are recently present, and also discuss the security characteristics related to virtualization in cloud computing, a basic yet still improper field of research.

2. CLOUD COMPUTING CONCERNS IN SECURITY

To refer the CSA's security guidance and top threats analysis, ENISA's security assessment and the cloud computing definitions from NIST indicate the various security issues

relevant to cloud computing. The issues needs further studies for being accurately managed and for strengthening the technological support and adoption. Attention is given to the particularity between services in the form of software (SaaS), platform (PaaS) and infrastructure (IaaS), which are commonly used as the basic fundamental basis for cloud service categorization. This section discuss the main issues related to the field and a characterization to propose a model. Each group combines various possible security problems, deriving in a categorization with sections.

1. Network security: -
Issues and problems attached with network communications and infrastructure in relation to cloud computing environment. The optimal network security solution includes cloud services as an enhancement of customers' current internal networks [6], using the similar precautions and security measures that are sectional assignments and permitting them to enhance local approachesto any remote resource or process [7].

(a) Transfer security: Distributed environment architectures, huge resource sharing and virtual machine (VM) illustrates synchronization mentions more data in transit in the cloud, thus involving VPN mechanisms for securing the system against various attacks like sniffing, spoofing, man-in-the-middle and side-channel attacks.
(b) Firewall: Firewalls protect the provider's internal cloud architecture against insiders and outsiders [8]. They also facilitate VM remoteness, filtering for addresses and ports, preventing of Denial-of-Service(DoS) and revealing of external security assessment methods. Attempts for designing true firewall and identical security measures specially for cloud environments [9,10] gives the way for making recent solutions for this new computing infrastructure.
(c)Security configuration: Configuration of protocols,rules,systems and technical trends to contribute the required levels of security and privacy without adjusting the efficiency or performance.
2. Interfaces: -
It emphasizes all aspects in relation to user, administrator and programming interfaces for using and controlling the clouds.
(a) API: Programming interfaces (important to IaaS and PaaS) for allowing and accessing virtualized resources and systems which must be secured to stop false use [11-15].
(b) Administrative interface: Enables private
control of resources in an IaaS (VM management), development for PaaS (coding, deploying, testing) and application tools for SaaS (user access control, configurations).
(c)User interface: End-user interface for examining the resources and tools (service itself), meaning the requirement of accepting measures for securing the environment [16-19].
(d) Authentication: Techniquerequired to let the usage to thecloud [20]. Most servicesdepends on normal accounts [12] which being affected to a much of the attacks [21-25]whose causes are promoted by multi-tenancy and resourcesharing.
3. Data security:
Securing the data in terms of isolation, accessibility and reliability (which can be functional not only to cloud environments, but any result requiring fundamental protection levels).
(a) Cryptography: Most engaged practice to make safe susceptible data [26], required by industry, state and federal regulations [27]
(b) Redundancy: Vital to bypass data loss. Models depends on information technology for its core operations and processes [28,29] and, thus dangerous data reliability and accessibility must be established.
(c) Disposal: Uncomplicated data clearanceapproaches are deficient and generally referred as deletion [30]. In the cloud, the complete damage of data, together with log references and concealedbacking registries, is ansignificantcondition [31].
4. Virtualization: Segregationamong VMs, hypervisor sensitivity and other troublesconnected to theuse of virtualization technologies [32].
(a) Isolation: Although rationally isolated, all VMs distribute the same hardware and the same resources, allowing harmful entities to utilize data leaks and cross-VM
attacks[33]. The theory of isolation can alsobe functional to more fine-grained belongings, suchas computational resources, storage andmemory.
(b) Hypervisor insecurity: The hypervisor is
the important software modules of virtualization. Even there are knownsecurity sensitivity for hypervisors,solutions are still limited and oftena recovery, difficult in additional studies tosolidify these security conditions.
(c) Data leakage: Exploit hypervisorvulnerabilities and lack of isolation controlsin order to leak data from virtualizedinfrastructures, obtaining sensitive customerdata and affecting confidentiality andintegrity.
(d) VM identification: Requirement of regulations for analyzing virtual machines that are beingused for executing a particularmethod or forstoring files.
(e) Cross-VM attacks: Includes attempts to
Approximating the source traffic rates in order tosteal cryptographic keys and amplifyprobability of VM placement attacks. One exampleconsists in overlapping memory and storageregions originallycommitted to a single virtualmachine, which also enables otherisolation-related attacks.
5. Governance: Issues related to (losing) administrativeand security controls in cloud computing solutions[34,35].
(a) Data control: Affecting data to the cloud means failingto manage over redundancy, location, filesystems and other relevant outlines.
(b) Security control: Loss of governance oversecurity operations and policies, as terms ofuse forbid customer-side attackassessment and penetration tests whiledeficient Service Level Agreements (SLA)lead to safety gaps.
(c) Lock-in: User possible dependency on a limited service provider due to short of fixedprinciples (protocols anddata formats), as a resultof becoming mainly vulnerable to transferring andservice termination.
6. Compliance: This includesnecessitieslinked to service accessibility and audit protection [36,37].

(a) Service Level Agreements (SLA):Mechanisms to guarantee the necessary service accessibility and the basic security measures to be adopted [38].
(b) Loss of service: Service interrupts are not restricted to cloud environments but aremore severe in this situation due to theinterconnections linking services (e.g., aSaaS using virtualized infrastructuresprovided by an IaaS), as shown in manyexamples [39-41]. This leads to the requirement ofstrong adversity recovery policies and providerrecommendations to execute customer-side redundancy if valid.
(c) Audit: Permits security and accessibility
assessments to be attained by customers,providers and third-party participants. Visible and proficient methodologies are required for continuous analysis of serviceconditions [42] and are frequentlynecessary bycontracts or legal policies. There aresolutions being developed to deal with thisproblem by offering a transparent API for automatic auditing and other helpful functionalities [43].
(d) Service conventionality: Related to how
proper obligations and in general the service necessities are respected and obtained based on the SLAs predefined and necessary service and customer requirements.
7. Legal issues:
Aspects linked to judicial necessities and law, such as numerous data locations and privilege supervision
(a) Data location: Customer data held in multiple jurisdictions regulated by the geographic location [44] which are affected, openly or indirectly, by subpoena law-enforcement actions.
(b) E-discovery: As a result of law-enforcement actions hardware might be appropriate for investigations associated to a particular customer, moving all customers whose data were stored in the same hardware [45-47]. Data disclosure is dangerous in this case.
(c) Provider privilege: Susceptibleactions of provider insiders are potential threats to confidentiality, accessibility and truthfulness of customers' data and processes' information [48, 49].
(d) Legislation: Juridical concerns associated to new concepts introduced by cloud computing [50].

3. SOME ANALYTICAL SOLUTIONS FOR SECURITY ISSUES

As an analysis for the frequency of above credentials is completed, an approach based on the percentage of solution in each group can be used as overall solution for the cloud computing. Figure 2 shows the percentage of solution available currently. Although the solution greatly depends on some other issues like remoteness, data leakage and virtualization.

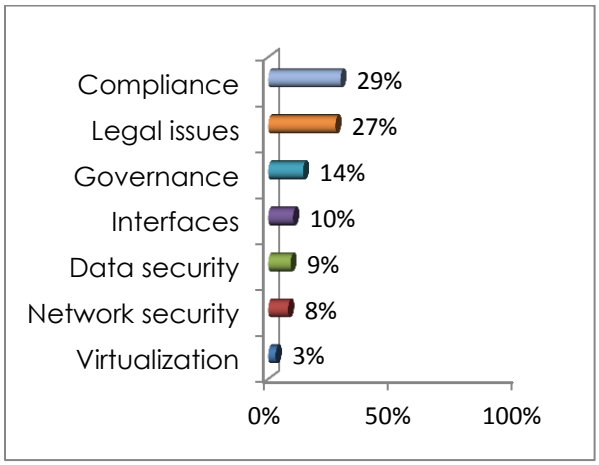

Figure 2. Security solutions with collection category

For some issue approach need to take special concern has been taken as like virtualization is actually equals to 12% of the reference problem and only having 3% for the solutionwhen accessing the most accepted virtual machine solution providers aiming to confirm their concerns and accessible solutions
The most popular virtual machine the target for solution providers can be XEN, VMWARE, and KVM. For a termination that such concerns are significant, but so far little is usable in terms of solutions.
The probable areas are still in the clouds in sort to transfer data and measures to be urbanized to provide better security situation which indicates the need to evaluate.

DISCUSSION

In the above sections there are differences between the various issues and the solutions. In Fig.3,

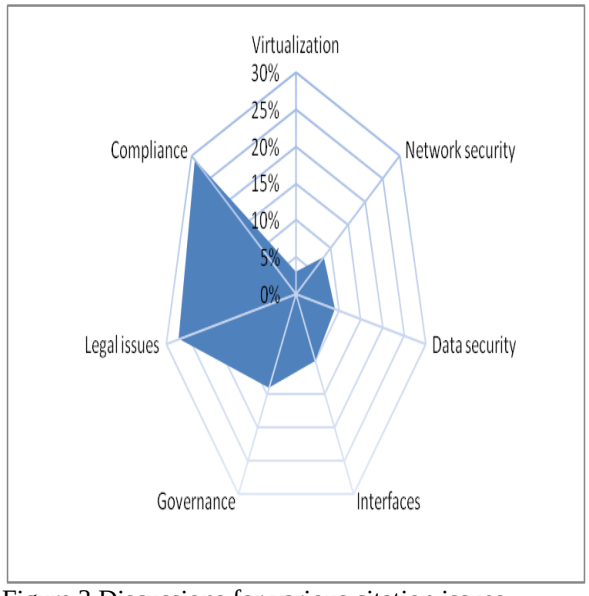

Figure 3.Discussions for various citation issues

The axis values are used for the number of citations found in the middle of the references studied. Those citations are the various solutions, and they might be meaningful problems, but here a lot of solutions have been previously described. Grouped categories results are shown in Figure3 , this shows that virtualization problems characterize a part that requires studies for addressing issues like isolation, data leakage and cross-VM attacks; There is another side, in areas such as compliance and network security cover concerns for which there are already a significant number of solutions or those are not measured extremely relevant.

Finally for future studies, five virtualization problems related to virtualization as a key element to consider: isolation of computational, such as memory and storage capacity, hypervisor vulnerabilities, data leakage, cross-VM, attacks and VM- identity.

Unlike the other issues related to the attacks and cross-VM isolation it is more evident.

However, the amount of solution citations for all issues is remarkably low if compared to any other security issues, reaffirming the need for additional researches in those fields.

4. CONCLUSION

In view of the points discussed in the previous parts, a clear-cut end is that cloud security includes many matured and well-known concerns – such as network and other infrastructural concerns, user access, authentication and privacy – and also new apprehension resulting from new technologies adopted to present the adequate property (mainly virtualized ones), services and auxiliary tools. These difficulties are reviewed by separation and hypervisor vulnerabilities (the main technological concerns according to the study and graphics obtainable), data location and e-discovery (legal aspects), and loss of governance over data, security and even choice making (in which the cloud must be deliberately and financially measured as a important factor). Another end experimentally is that, although accepting a cloud service or provider may be simple, drifting to another is not. After distressing the restricted data and actionsof the cloud, the lack of principles for protocols and design openly influence the test to transfer to a unlike provider even if this ispositive by rightful reasons such as non conclusion of SLAs, pauses or provider bankruptcy. As a result, the first option must be cautiously made, as SLAs are not just right and services outages occur at the same speed that resource sharing, multi-tenancy and scalability are not unsuccessful proof. Following a choice is made that upcoming migrations between services can be tremendously difficult in conditions of time and costs; this task will need a broad work for bringing all data and resources to a restricted infrastructure before redistribute them into the cloud.In conclusion, the learning of current trends for cloud computing shows that there is a substantialamount of well calculated security concerns, for which abundanceof solutions and best observation have been developed, such asthose related to legal and administrative concerns.

5. FUTURE SCOPE

Safety is a critical feature for only if a dependable situation and then permits the use of functions in the cloud and for moving data and business processes to virtualized infrastructures. Several of the security issues recognized is experiential in other computing environments: authentication, network security and legal necessities. However, the collision of such issues is intensified in cloud computing due to distinctiveness such as multi-tenancy and resource sharing, since actions from a single

customer can influence all other users that unavoidablycontribute to the same resources and interfaces. At the same time, ourquantitative study points to that virtualization which residues as an underserved field concerning the number of solutions giving recognized concerns. It is planned to expand new method that will give the necessary security level by separating virtual machines and the connected resources subsequently as the best practices in terms oflegal regulations and compliance to SLAs. Among othernecessities, such results should employ virtual machinerecognition, providingansufficientpartition of devotedresources mutually, with a stablesurveillance of shared ones,and inspect any effort of exploiting cross-VM and dataleakage. A protected cloud computing environment depends onseveral security clarification working harmoniously as one.However, in our research study we did not recognize any safety solutions provider possessing the servicesessential to get high levels ofsecurity conventionality for clouds. Thus, cloud providers need tocoordinate / harmonize security results from dissimilar places inorder to attain the preferredsecurity level. We learned thatAmazon distorted the XEN source code in order to comprisesecurity features, but unluckily the adapted code is notopenly available and there emerges to be no article detailing thechanges established. Given these boundaries, a deeper study oncurrent security answer to supervise cloud computing virtualmachines inside the cloud providers should be a focus of futurework in the area

Reference:

1. Petre,R.(2012). Data mining in Cloud Computing. Database Systems Journal, 3(3), 67-71.
2. IDC (2009) Cloud Computing 2010 – An IDC Update. slideshare.net/JorFigOr/cloud-computing-2010-an-idc-update.
3. Mather T, Kumaraswamy S (2009) Cloud Security and privacy: An Enterprise Perspective on Risks and Compliance.1stedition. O'Reilly Media
4. Catteddu D, Hogben G (2009) Benefits, risks and recommendations for information security. European Network and Information Security Agency,enisa.europa.eu/act/rm/files/deliverables/cloudcomputing-risk-assessment.
5. CSA (2009) Security Guidance for Critical Areas of Focus in Cloud Computing.
6. Tompkins D (2009) Security for Cloud-based Enterprise Applications.
7. Jensen M, Schwenk J, Gruschka N, Iacono LL (2009) On Technical Security Issues in Cloud Computing. In: IEEE International Conference on Cloud Computing. pp 109–116.
8. TrendMicro (2010) Cloud Computing Security – Making Virtual Machines Cloud-Ready. Trend Micro White Paper.

9. Genovese S (2009) Akamai Introduces Cloud-BasedFirewall.cloudcomputing.syson.com/node /1219023
10. Hulme GV (2011) CloudPassage aims to ease cloud server security management.http://www.csoonline.com/article/658121/cloudpassageaims-toease-cloud server-security-mgmt.
11. Google (2011) Google App Engine. code.google.com/appengine
12. Google (2011) Google Query Language (GQL).code.google.com/intl/en/appengine/docs/python/overview.html
13. StackOverflow(2011)stackoverflow.com/questions/1823536/does-using-non-sql-databasesobviate-the-need-forguarding-against-sql-injection
14. Rose J (2011) Cloudy with achance of zero day. www.owasp.org/images/1/12/Cloudy with a chance of 0 day Jon Rose-Tom Leavey.pdf
15. Balkan A (2011)Why Google App Engine is broken and what Google must do to fix it. aralbalkan.com/1504
16. Salesforce (2011) Salesforce Security Statement.salesforce.com/company/privacy/security.jsp
17. Espiner T (2007) Salesforce tight-lipped after phishing attack.zdnet.co.uk/news/security-threats/2007/11/07/salesforce-tight-lipped-after-phishing-attack-39290616/
18. Yee A (2007) Implications of Salesforce PhishingIncident.ebizq.net/blogs/securityinsider /2007/11/-implications of salesforcephi.php
19. Salesforce (2011) Security Implementation Guide.login.salesforce.com/help/doc/en/salesforce security impl guide.pdf
20. Li H, Dai Y, Tian L, Yang H (2009) Identity-Based Authentication for CloudComputing. In: Proceedings of the 1st International Conference on CloudComputing, CloudCom ’09
21. McMillan R (2010) Google Attack Part of Widespread Spying Effort.PCWorld
22. Mills E (2010) Behind the China attacks on Google. CNET News
23. Arrington M (2010) Google Defends Against Large Scale Chinese Cyber Attack
24. Bosch J (2009) Google Accounts Attacked by Phishing Scam. BrickHouse Security Blog
25. Telegraph T (2009) Facebook Users Targeted By Phishing Attack. The Telegraph
26. Musthaler L (2009) Cost-effective data encryption in the cloud. Network World
27. Yan L, Rong C, Zhao G (2009) Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-BasedCryptography. In: Proceedings of the 1st International Conference on Cloud Computing, CloudCom ’09
28. Tech C (2010) Examining Redundancy in the Data Center Powered by the Cloud and Disaster Recovery. Consonus Tech
29. Lyle M (2011) Redundancy in Data Storage. Define the Cloud
30. Dorion P (2010) Data destruction services: When data deletion is not enough. SearchDataBackup.com
31. Mogull R (2009) Cloud Data Security: Archive and Delete (Rough Cut) securosis.com/blog/cloud-data-security-archive-and-delete-rough-cut/
32. Messmer E (2011) Gartner: New security demands arising for virtualization, cloud computing. http://www.networkworld.com/news/ 2011/062311-security-summit.html
33. Ristenpart T, Tromer E, Shacham H, Savage S (2009) Hey,you, get off of my cloud: exploring information leakage in third-party compute clouds.
34. Chow R, Golle P, JakobssonM, Shi E, StaddonJ,MasuokaR,Molina J (2009) Controlling data in the cloud: outsourcing computation without outsourcing control. In: Proceedings of the 2009 ACM workshop on, Cloud computing security, CCSW ’09. New York, NY, USA, ACM, pp 85–90, http://doi.acm.org/10.1145/1655008.165502
35. Sadeghi AR, Schneider T, Winandy M (2010) Token-Based Cloud Computing - Secure Outsourcing of Data and Arbitrary Computations with Lower Latency. In: Proceedings of the 3rd international conference on Trust and trustworthy computing, TRUST ’10
36. Brandic I, Dustdar S, Anstett T, Schumm D, Leymann F (2010) Compliant Cloud Computing (C3): Architecture and Language Support for User-driven Compliance Management in Clouds. In: 2010 IEEE 3rd International Conference on Cloud Computing. pp 244–251, http://dx. doi.org/10.1109/CLOUD.2010.42
37. Brodkin J (2008) Gartner: Seven cloud computing security risks. http:// www.infoworld.com/d/securitycentral/gartner-seven-cloudcomputing-security-risks-853.
38. Kandukuri BR, Paturi R, Rakshit A (2009) Cloud Security Issues. In: Proceedings of the 2009 IEEE International Conference on Services Computing, SCC ’09
39. Winterford B (2011) Amazon EC2 suffers huge outage. http://www.crn. com.au/News/255586,amazon-ec2-suffers-huge-outage.aspx
40. Clarke G (2011) Microsoft BPOS cloud outage burns Exchange converts. http://www.theregister.co.uk/2011/05/13/
41. Shankland S (2011) Amazon cloud outage derails Reddit, Quora
42. Young E (2009) Cloud Computing - The role of internal audit
43. CloudAudit (2011) A6 - The automated audit, assertion, assessment and assurance API. http://cloudaudit.org/
44. Anand N (2010) The legal issues around cloud computing.
45. Hunter S (2011) Ascending to the cloud creates negligible e-discovery risk. http://ediscovery.quarles.com/2011/07/articles/informationtechnology/ ascending-to-the-cloud-creates-negligible-ediscovery-risk/
46. Sharon D, Nelson JWS (2011) Virtualization and Cloud Computing: benefits and e-discovery implications. http://www.slaw.ca/2011/07/19/ virtualization-and-cloud-computing-benefits-and-e-discoveryimplications/
47. Bentley L (2009) E-discovery in the cloud presents promise and problems. http://www.itbusinessedge.com/cm/cmmunity/features/interviews/ blog/e discovery-in-the-cloud-presents promiseandproblems/?cs=31698http:/ wwwlabnol.org/internet/cloudcomputing-legal-issues/14120/
48. Zierick J (2011) The special case of privileged users in the sloud. http:// blog.beyondtrust.com/bid/63894/The-Special-Case-of-Privileged-Usersinthe-Cloud
49. Dinoor S (2010) Got Privilege? Ten Steps to Securing a Cloud-BasedEnterprise. http://cloudcomputing.sys-con.com/node/1571649
50. Pavolotsky J (2010) Top five legal issues for the cloud. http://www.forbes.com/2010/04/12/cloud-computing-enterprise-technology-cio-networklegal.html