March - April 2020
ISSN: 0193-4120 Page No. 4898 - 4905

A Model for Conflicts between User Set-up Procedures and Virtualization

Dev Ras Pandey, Gauri Shanker Kushwaha

Dept. of Physical Sciences, Mahatma Gandhi Chitrakoot Gramodaya Vishwavidyalaya, Chitrakoot, Dist- Satna (M.P.), India

Article Info
Volume 83
Page Number: 4898 - 4905
Publication Issue:
March - April 2020

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 27 March 2020*

Abstract

Cloud computing is an promising assumption of using computer softwares that is the new way that rapidly uses computing as a private community by computing as a general resources. It also offers various benefits in the form of economy of scale, public utility system, flexibility and convenience. In cloud computing risk assessment within a cloud/virtualization framework that is used by CSP (Cloud Service Providers) and users to identify and assess the risk at the time of service deployment and functioning. Various stages in the virtualization where risk assessment and evaluation occurred their related models have been proposed for the same to eliminate. The paper identifies three types of risks at the end of users were found and categorized as query related, analysis & specification, and implementation of the virtualization between users and cloud providers. The proposed framework provides technical belief that goes towards buoyancy of cloud platform users is first part and a expenditure reducing and reliable productivity to the users of CSP and resources were collected by separate Infrastructure Provider (IP) is another part.

Keywords; *Virtualization, cloud computing, threats, vulnerabilities, risk managements*.

I. INTRODUCTION

National Institute of Standards and Technology (NIST) for cloud computing, defines it as a computing approach for activating available, well-situated, required network right to use for a joint group of configurable assets of computing like servers, applications, services, storage and networks. A computing standard that transformed, the Information Technology background in the form of its convention and rights. It is predictable as a large amount shows potential to the computing prototype of the past years *(Buyya et al., 2008)*. Cloud Computing has also transformed the perception of ICT. Cloud computing has become a cost-effectively possible implication for SMB organizations with benefits like enhanced resource deployment and flexibility of usage.

Risk management is the important in cloud computing for supporting various organizations for suitable decision making regarding agreements. Lack of confidence at quality level prevents a cloud user to use cloud technologies. The zero-risk provision is not practically proven, but by giving technological assurance, various mitigating mechanisms and reliable productivity of CSP resources leads an organization to use confidentially the cloud services. Risk is précised in the form of impact and likelihood of the event *(Misra, 2008)*. The research aimed for giving hypothetical and practical recommendations to take a risk conversance resolution at drifting to cloud or virtualization models. It is also expected to help cloud users to understand and identify the various necessities, set-up procedures, cloud settings, requirements and specifications of the cloud computing environment or virtualization models.

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 4898 - 4905

II. RISKS FACTORS IN VIRTUALIZATION

ISACA (Information System Audit and Control Association) made an assessment (2010) of just about 1800 industries and Information Technology professionals, the percentage of the risks of cloud computing as preponderance the benefits as 45%. The risk factors that may degrading the performance of organization to adopt cloud computing that were highlighted in below given table. In cloud systems risks must be supposed on data, privacy, service, conflictions and infrastructure layers.

SN	Threats/ Vulnerabilities	Prevention
1	Conciliation of all Hosted workloads.	• fixed strategy for secure virtualization platform configuration. • make sure configuration management tools that are supportive for monitoring of the hypervisor layer. • clearly identify monitoring, prioritizing and testing patch for critical systems in physical environments.
2	Abuse nefarious use of cloud computing *(Potey et al. 2013)*	• improved fraud observing and management. • complete self-inspection of network passage. • stricter starting muster and substantiation process. • observing open one's own network blocks.
3	Report of service traffic hijacking *(Potey et al. 2013; Srinivasamurthy & David 2010)*	• block allocation of user's information's to users and CSP. • strong authentication techniques. • detect unauthorized activity. • be aware of CSP security policies and SLAs.
4	Reputation due to cotenant activities *(ENISA 2017)*	• service delivery and data loss as a problem for the organization image.
5	Changes of jurisdiction *(ENISA 2017)*	• user's data stored may be held in multiple control may be high risk.
6	Conflicts between user set-up procedures and cloud setting *(ENISA 2017)*	• isolation mechanisms articulated and assisted users to secure their resource.
7	Connections to virtual machines	• KVM routing of keyboard, mouse, video and audio.
8	Customer's security expectations *(Carto 2017)*	• user make a distinction from the authenticity of cloud provider.
9	Data confidentiality and privacy *(Carto 2017)*	• cloud provider must distribute controls to secure sensitive data • industry can audit cloud provider to assure appropriate procedures.
10	Data Integrity	• use standards that are available for managing data integrity. • must not co-operate data integrity in fervor of moving to cloud.
11	Data location *(Heiser & Mark 2008)*	• providing trustworthiness to the user on the setting of data of the user.
12	Data loss *(Potey et al. 2013)*	• data protection on design and run time. • substantial API access control.

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 4898 - 4905

SN	Threats/ Vulnerabilities	Prevention
		• encrypted and protected integrity of data. • key generation, management, storage and destruction practices. • provider backup and retention strategies.
13	Data segregation *(ENISA 2017; Heiser& Mark 2008)*	• ensure a limit for each user's data. • test and corroborate the data isolation.
14	Denial of Service (DoS) *(Potey et al. 2013)*	• registration and authentication implemented. • controlling user's own network blocks.
15	Hypervisor Security	• virtualization software throughout its life cycle, including development, implementation, provisioning, and management must be secure.
16	IaaS Security Issues *(Dawoud et al. 2010)*	• cloud provider controls infrastructure. • providers undertake a substantial endeavor to secure and mobility.
18	Insecure Application Programming Interfaces *(Potey et al. 2013; Srinivasamurthy & David 2010)*	• security model interface of cloud provider analyzed. • encrypted transmission for strong authentication and access controls are implemented. • reliance chain related with the API considered.
19	Insufficient due diligence	• make sure that the proficient resources are accessible.
20	Interoperability and portability	• think about interoperability and portability earlier than upsetting to cloud.
21	Investigative support *(Heiser & Mark 2008)*	• contractual agreement should comprise the maintain of convinced analyzed activities.
22	Licensing risks *(ENISA 2017)*	• Licensing conditions become unworkable in cloud environment. • PaaS and IaaS is creating original work in the cloud that may be on risk.
23	Long term viability *(Heiser & Mark 2008; ENISA 2017)*	• users should observe their providers. • regular backup their data and application. • CSP make sure data security. • users have crisis plans for their data and application.
24	Loss of governance	• cloud provider does not permit audit by the cloud user.
25	Malicious insiders *(Potey et al. 2013; ENISA 2017)*	• inclusive supplier assessment. • enforce austere supply chain management. • indicate resource necessities. • determine security breach notification processes.
26	Management Interface Compromise *(ENISA 2017)*	• internet accessible and mediate larger sets of resources after remote access and web browser vulnerabilities.
27	Network security	• strong network traffic encryption techniques must be used.

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 4898 - 4905

SN	Threats/ Vulnerabilities	Prevention
		• assessment of packet analysis, weaknesses of session management, network penetration, and insecure SSL trust configuration.
28	Performance *(Carto 2017)*	• characterize the recital of the cloud provider.
29	Potential loss of SOD for network and security controls *(Svantesson & Roger 2010)*	• network topology (including VLANs) configuration. • replaceable switch code for spanning of console and policies. • appraise and require virtualized network security controls.
30	Privileged user access data access (Heiser & Mark 2008)	• gain information of user who manage the data. • request provider to supply specific information to take into service. • build a policy as strong authentication process.
31	Recovery and Backup (Heiser & Mark 2008)	• cloud provider should have capable to do an inclusive and immediate restoration.
32	Regulatory compliance *(Heiser & Mark 2008; ENISA 2017)*	• user's only use these compliances for the mainly inconsequential functions.
33	Resource Exhaustion *(ENISA 2017)*	• access control compromised. • economic and reputational losses. • service unavailability. • differing consequences of inaccurate estimation of resources.
34	Service level agreement (SLAs)	• provider should make transparency. • organization monitors terms of SLA. • provider might need to be trained for certain standard.
35	Shared access *(Potey et al. 2013)*	• enforce patching and remediation. • implement security configuration. • assess environment for illicit activity.
36	Significant amount of energy *(Beloglazov &Buyya 2010)*	• optimization stage aimed of cooling system operation.
37	Subpoena and e-discovery *(ENISA 2017)*	• clients are at risk of their data unwanted parties.
38	Supply chain failure *(ENISA 2017)*	• lack of transparency.
39	Testing	• Cloud service performs slower services that are especially redundant.
40	The lack of visibility and controls on virtual networks created for VM – to VM Communication *(Svantesson & Roger 2010)*	• Don't lose visibility when workloads and networks were virtualized. • VM as an alternative that create significant management burden.

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 4898 - 4905

SN	Threats/ Vulnerabilities	Prevention
41	The security risks confronted by customers / government	• security concerns related fault exclusion, break and business transfer. • rank the security level and credit of users, and publish hands-on malicious programs on cloud.
42	Third party management	• user's ERM and its Governance, Risk and compliance reporting. • third-party web services components mashups will be implemented.
43	Unauthorized access to hypervisor	• hackers gain unwanted and unauthorized access to OSs-hosted on it.
44	Underlying Infrastructure security *(Chandramouli& Mell 2010)*	• PaaS developers and providers are responsible for applications services.
45	Virtual machine lifecycle	• VMs can be on, off, or suspended that creates complexities for malware detection.
46	Virtual machine rollback *(Garfinkel & Rosenblum 2005)*	• configuration errors and other vulnerabilities propagated.
47	Virtualization vulnerabilities	• precision of isolation, inspection, and interposition achieved.
48	Web application security	• cloud SaaS application web application from conventional network security resolution.
49	Workloads of different trust levels are considered onto a single physical server *(Svantesson & Roger 2010)*	• treat hosted virtual desktop workloads as un-trusted, isolate physical data center. • do not use VLANs for security separation within a virtualized server. • assess requirement for solutions for security instructions to VM identities.

A new model, where resources are being applied on users as facilities/services by Cloud Computing which comes with a number of profits for both users and cloud providers. However, the necessities to recognize the connected risks are essential before making decisions to shift towards cloud computing. Now a day's computers and technologies were used at every moment of life and it contains conflicts between customer set-up procedures and cloud settings. Major identified risk factors related to cloud computing are licensing, data protection and uses of significant amount of energy. Now days in the world of digital computing/green computing there are many user conflictions between setup procedures and cloud computing settings.

III. RELATED WORK

In recent years, there has been increasing interest in cloud computing among researchers, practitioners and companies of the virtualization field. Due to the advances in the computer-assisted learning systems and ICT today world uses more efficient way of computing. Cloud computing results as scalability and performance of the PowerVM benchmarks are unsurpassed using virtualization and also identified the benefits . The security risks, practical attacks and challenges *(Ahmed et al. 2017; Abdelwahab & Abraham 2013; Balaji & Kiran 2016; Joshi & Singh 2017)* of virtualization, cloud computing and the security requirements were categorized. On a particular demand of assessment and identification of risks/threats/vulnerabilities as applied in cloud computing; models/frameworks *(Ali et al. 2017;*

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 4898 - 4905

Zakarya & Gillam 2017; Gupta et al. 2016) were proposed that can be used by CSP and users to assess risk at the time of service deployment and implementation. On the basis of review a theoretical framework of cloud adoption has been suggested.

IV. RISK MANAGEMENT FRAMEWORK

Cloud implementation and the need of preliminary trust based on the service provider reputation state of art have been given. Though adopting cloud computing cost reduction, risk related to unplanned adoption minimized and many other performances like, privacy, security and services were improved, so industry can lead to trusted decision making. On the other hand trust makes service provider's reputation. SLAs play an imperative role in creating belief and trust on the cloud service providers. Data is more significant affecting issues in cloud adoption into two categories as critically and control. Data control in cloud computing that is based on data storage on supplementary locations that makes hesitation in organizations to adopt regarding SLAs that make enclosure of setting discovery binding for Cloud Service Provider.

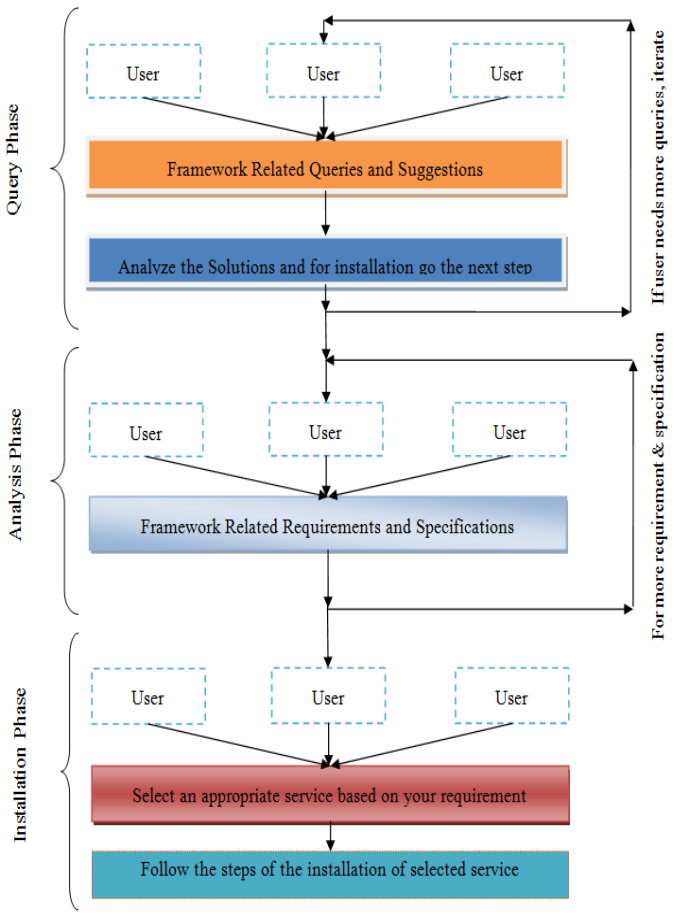

Figure 1: Model for Conflicts between User Set-up Procedures and Service Providers

The framework is beneficial for conflicts between user and providers, which are before now by means of IT resolution and are thinking about cloud based solutions adoption after taking into consideration a number of cloud offers. The framework is categorized under three categories as query, analysis and installation phase. The first phase includes query related to virtualization models and cloud settings. The query phase includes the information regarding virtualization models conflictions and suggestions. After the queries submission user gets the instant responses as frequently asked questions and if user wants more suggestions he will responded after a successful query submission. After the first phase visit of users if responses were satisfactory and they wants to submit their requirement or wants to know about models specification, they have to go in next phase,

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 4898 - 4905

otherwise they can submit more queries. The second phase of the framework consists the analysis phase which gives the information about user related requirements and specifications of virtualization models in cloud computing. The analysis phase gives a next idea of models and services for user selection to use the services of virtualization models. Here some of the pre-designed models and services are categorized for user selection and if user wants to know according to their requirement they can submit their own specification and find their suitability after the comparison. When analysis phase has been completed, users were diverted to next and if user wants to know about another requirement they can. The third and last phase of framework gives the installation phase steps of user selected models or services. The installation phase also includes the user manual of how to use services and create their own configuration. By following these steps an easiest approach has been identified and provides the easy to use services of virtualization services in cloud computing.

V. CONCLUSION

A new model, where physical hardware infrastructure resources are being provided to clients by Cloud Computing which comes with a number of profits for both cloud providers and users. The necessities to recognize the connected risks are essential before finalizing to move towards cloud computing. The paper is initiated with the identification of risk and probable solutions with a brief description about risk assessment, identification and management. Major identified risk issues related to cloud computing are conflicts between user setup procedures and cloud settings, licensing, data protection and uses of significant amount of energy. Now days to understand and identify the various setup procedures and cloud settings of the cloud computing environment are a critical task for each user. For these issues a conceptual framework has been proposed to use the services easily and easy understanding of procedures. The framework includes three stages of query, analysis and installation, in which user can get suggestions or solutions of their related issues, a comparative analysis of their requirement and specifications and further installations steps to easily understand the procedures. The proposed framework required to develop and validate that is future work wherein intended to validate it through implementation of virtualization with an individual skilled user or within a company.

REFERENCES

[1]. Abdelwahab S. & Abraham A. (2013), A Review of the Risk Factors in Computational Grid, Journal of Information Assurance and Security, 8, 270-278.

[2]. Ahmed H. A. S., Ali M. H., Kadhum L. M., Zolkipli M. F. B. & Alsariera Y. A. (2017), A Review of Challenges and Security Risks of Cloud Computing, Journal of Telecommunication, Electronic and Computer Engineering, 9(1-2), 87-91.

[3]. Ali A., Warren D. & Mathiassen L., (2017), Cloud-based business services innovation: A risk management model, International Journal of Information Management, 37, 639–649.

[4]. Balaji K. & Kiran P. S. (2016), A Review on Cloud Security Challenges and Issues, Indian Journal of Science and Technology, 9(43), 01-05.

[5]. Buyya R., Yeo C., & Venugopal S. (2008), "Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities," 10th IEEE International Conference on High Performance Computing and Communications, HPCC'08, pp. 5–13.

[6]. Carto D., (2017), Cloud computing use cases White Paper available on May 05 2017 at 17:56 IST: http://opencloudmanifesto.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.pdf.

[7]. Chandramouli R. & Mell P., (2010), State of Security readiness, Crossroads, 16 (3), 23–25.

[8]. Dawoud W., Takouna I. & Meinel C., (2010), Infrastructure as a service security: Challenges and solutions, 7th International Conference on Informatics and Systems (INFOS), IEEE Computer Society, 1–8.

[9]. ENISA, Cloud Computing: Benefits, Risks and Recommendations for Information Security

(ENISA), European Network and Information Security Agency: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing - risk-assessment accessed on May 06, 2017.

[10]. Garfinkel T. & Rosenblum M., (2005), When virtual is harder than real: Security challenges in virtual machine based computing environments, Proceedings of the 10th conference on Hot Topics in Operating Systems, Santa Fe, NM. USENIX Association Berkeley, CA, USA, 10, 227–229.

[11]. Gupta S., Saxena K. B. C. & Saini A. K., (2016), Towards Risk Managed Cloud Adoption a Conceptual Framework, Proceedings of the 2016 International Conference on Industrial Engineering and Operations Management, Kuala Lumpur, Malaysia, 1-6.

[12]. Heiser J. N. & Mark, (2008), Assessing the security risks of cloud computing, Gartner Report.

[13]. Joshi C. & Singh U. K. (2017), Information security risks management framework –A step towards mitigating security risks in university network,Journal of Information Security and Applications, 35, 128–137.

[14]. Misra K., (2008), “Risk analysis and management: An introduction”, Handbook of Perform-ability Engineering, Ed. Springer London, pp. 667–681.

[15]. Potey M., Manish C., Dhote A. & Sharma D. H., (2013), Cloud Computing Understanding Risk, Threats, Vulnerability and Controls: A Survey, International Journal of Computer Applications, 9-14.

[16]. Srinivasamurthy S. L. & David Q., (2010), Survey on Cloud Computing Security," in Proc. Conf. on Cloud Computing, CloudCom.

[17]. Svantesson D. C. & Roger, (2010), Privacy and consumer risks in cloud computing, Computer Law & Security Review, 26, 391-397.

[18]. Zakarya M. & Gillam L., (2017), Energy efficient computing, clusters, grids and clouds: A taxonomy and survey, Sustainable Computing: Informatics and Systems, 14, 13–33.