Assessing Risks and Cloud Readiness in PaaS Environments

Vinita Malik, Sukhdip Singh

Abstract: ***The cloud computing has utilization of pervasive or distributed models on demand access to highly configurable computing devices for fast provision and less management efforts. The complex architecture, multitenant and virtual environment in cloud infrastructure asks for risks identification and mitigation. The cloud computing model business needs reassurances so it's prime consideration for testing the cloud services. This research primarily identifies various risks, threats, testing models and vulnerabilities in cloud computing environment. This research has implemented the risk assessment and cloud readiness for PaaS environment by scanning its code with a software vendor. The research makes an emphasis on risk minimization strategies and trust evaluation in cloud computing environment.***

Keywords: Attacks; Cloud Computing; Risks; Risk Management; Cloud Readiness; Trust

I. INTRODUCTION

The cloud computing has emerged today as a dominant computing paradigm due to much advances in technology networks and virtual infrastructure. The cloud computing has provided an illusionary limitless resources with features like high scalability, on demand service, agility via elasticity and pay per use. It is also characterized to have on demand service (self), resource usage optimization, high elasticity, resource polling with broad network access [1]. It helps in imparting the ubiquitous access to highly configurable computing devices which also follows pay per use model. Reduced costs, less investment and fast deployment makes cloud computing focus on main business concerns. However, despite of very lucrative facts about cloud computing, its adoption is associated with large potential risks. As cloud computing merges various computing environments i.e. grid and distributed so it becomes complex in nature. Under the umbrella of cloud computing services any organization has to surrender control over data privacy and security by conferring trust into cloud provider services.

The paper raises a study aiming to identify risks, threats, vulnerabilities, attacks and risk assessment

Strategies in cloud computing. This research has thrown light on benefits and challenges in cloud computing and key factors in cloud testing. The paper has implemented how cloud risks are managed after identifying risky items and how much cloud ready is an application after scanning its application code.

The research has been organized in various sections to answer the following questions:

- Define cloud computing, characteristics, deployment and service models, benefits, challenges in cloud computing?
- What are risks, vulnerabilities, threats and attacks in cloud computing?
- What are risk reduction strategies in cloud computing?
- How trust is evaluated in cloud environments?
- How risk management is implemented in cloud applications and how the cloud readiness of an application may be identified by a smart software.

Section 1 talks about cloud computing basics whereas section 2 deals with risks management in cloud computing. Next section discusses risk minimization in cloud computing and in Section 4, the trust in cloud environment is dealt. In section 5, the risk management and cloud readiness of an application is implemented after scanning its code by an intelligent vendor. Last section provides conclusions and future scope of the extensive study.

II. CLOUD COMPUTING

According to Gartner report (Technology Trend), It is under prediction that in next five years, cloud computing will dominate market in decision making business processes [2].Cloud computing causes disruptive changes in various platform, infrastructure and application layers services. IT business analysts and solution experts are looking forward for such technologies that may formulate solutions across various business domains by cloud computing [3].Cloud Computing defines a model which permits users to access shared resources via internet or by any computing network. It asks for minimal administrative effort and less interaction with service providers.

A. Characteristics

The Cloud Computing has following characteristics [1, 4-8]:

Revised Manuscript Received on October 15, 2019.

***** Correspondence Author

Vinita Malik*, PhD Scholar, D.C.R.U.S.T, Murthal & Information Scientist, Central University of Haryana, Mahendergarh, India
Email: is@cuh.ac.in

Sukhdip Singh, Professor, CSE Dept., D.C.R.U.S.T, Murthal, India
Email: sukhdeepsingh.cse@dcrustm.org

- Pay per use Model: Users pay for the time he utilizes the services of cloud.
- Multi Tenancy Model: Services used by multiple users under multi tenancy model
- Network Access: Services are accessed from mobile or desktop device just via internet access.
- Elasticity: Cloud services quantity/quality are increased /decreased as per user needs.
- Resources usage optimization: By use of measuring capability as per service type, it optimizes usage of resources.

B. Deployment Models

The deployment models in cloud computing depends on cloud service provider capacity. The four deployment models are described as follows [9]:

- Private deployment model of cloud: Here cloud infrastructure is used exclusively for one operation. These are used where data control is the prime consideration of the organization.
- Public deployment model of cloud: In this cloud infra is under control of cloud service provider. The consumer has very low control over security and operation of cloud services
- Community deployment model of cloud: Here cloud infra is divided into various independent organizations having shared/exchanged concerns.
- Hybrid deployment model of cloud: It is composed of 2 or more private/public /community clouds and used for a particular purpose. Here critical applications run on private cloud and non-critical applications on public cloud.

C. Service Models

The cloud computing comprises of following service models [1]:

- SaaS (Software as Service): Web browsers host the applications via internet. The service provider is responsible for applications management i.e. Google Docs, SAP Business, Sales Force CRM
- PaaS (Platform as Service): Developers write applications as per specified platform and the platform provides the virtualization environment. E.g.Forge.com and Google App Engine.
- IaaS (Infra as a Service): Here services include all the computing resources. Clients maintain security in cloud services. Resources like servers, networks provided to customers are monitored by service provider on demand. For E.g. VMware, EMC2, Amazon web services.

D. Challenges

The most important challenges in cloud computing are offered as follows [10]:

- Service Quality: One of the prime factor due to which organizations makes hesitant in moving their applications to cloud.
- Security & Privacy: Security and Privacy issues have played an important role in non-adoption of cloud computing services.
- Resource Discovery: Resource allocation have played critical role in well distributed cloud.
- Data Integrity issues: Data protection from unauthorized access is difficult to maintain in cloud computing environment.
- Data Dynamic Scalability: The data processing nodes need to be scaled as per user response.
- Scheduling: Data scheduling is necessary for efficient resources usage.
- Debugging: In high computable distributed processing remote and parallel computing is critical need in cloud computing which is difficult to maintain.
- Virtualization: It is amongst the powerful techniques used in cloud computing for creating smart abstraction layer to hide software/hardware complex details.
- Trust: It’ s mandatory to convince application users that system services are accurate and safe.
- Querying: Scalable queries processing have been an open challenge in cloud computing.
- Service Level Agreements: Provision of a layer for discussion among providers & consumers demand service level agreements.

E. Benefits

Following are the main benefits of cloud computing [9]:

- Business resources efficient utilization as per pay & use model.
- Data execution time increase as an ability of cloud.
- Patch management is easier in cloud.
- DDOS attacks and virus infections are lesser in cloud environment.
- Disaster recovery planning is easier in cloud computing.
- Regulations and quality imposition services are easily adopted in cloud based environment.

III. RISKS, ATTACKS & VULNERABILITIES IN CLOUD COMPUTING

This section describes cloud computing risks, attacks and vulnerabilities. As there are various challenges inherent in cloud computing, there is need to have a look into risk categories and risk factors involved in cloud computing.

A. Risks Factors

The risks factors in cloud computing is given as follows [11, 12, 13 and 14]:

- Authentication & Access Control: The sensitive credentials of any organization are needed to be authenticated as in cloud data is processed outside the organization.
- Lack of Control: The lack of control over computing environment may lead to data leakage.
- Insecure Application Development: The interfaces development requires giving their control to third party for enabling them which increases risks for any organization.
- Data Transfer: The data flowing on network needs to be secured and all security roles must be properly defined.

- Inadequate Knowledge: The organization using cloud services needs to understand cloud based risks.
- Regulatory Compliance: If the service provider is not security certified or do not participate in audits then it is considered a big risk as the service provider is responsible for security and integrity of data.
- Shared Resource Environment: As cloud nature is to share all computing resources which may lead to data leakage or privacy issues.
- Data Breaches: The attackers can exploit user's data if cloud database has not been designed properly.
- Service Availability: The business environment and its competency pressure may cause bankruptcy or loss of potential service quality.
- Improper Service Management by service provider: The access privileges must be properly defined by service provider and the customer must be able to access data logs on demand whenever necessary.
- Data Location: As cloud service providers are dispersed across the globe so the data stored in risky countries is again a big risk.
- Data Recovery: Sometimes man-made disaster or natural mishappening can corrupt the data, so the customer /user should be aware how much time will take to recover the data.
- Virtualization Issue: It is one of the most fundamental components of cloud computing. It includes risks of physical machines too.
- Data Integrity: Cloud computing endangers data integrity while doing transaction management. Cloud Computing does not follow guaranteed delivery at protocol level.
- Service level Agreements: The customer must assure that data integrity preservation is its responsibility and such terms explicitly clarified in service level agreement.
- Resource Exhaustion: Inaccurate estimates of resource utilization may lead to service unavailability, reputational loss or access control compromises.

B. Vulnerabilities

Following mentioned are vulnerabilities in cloud computing [15]:

- Virtualization vulnerabilities: Virtualization may be OS level (Multiple guest operating system run on host OS), application level (virtualization on top layer), Hypervisor based (embedded code to host operating system).VM side channel attacks and DOS attacks are common in such virtualization methods.
- Internet Protocol Vulnerability: IP vulnerabilities include attacks i.e. RIP attacks, ARP spoofing, Flooding, DNS poisoning.
- Non authorized access to management interface: The data computation, upload all occur by management interface. Non authorization to such interface can be a critical issue for cloud services.
- Injection Vulnerability: It includes vulnerabilities i.e. OS injection flaw, SQL injection flaw that may disclose application components.
- Browser Vulnerability: Cloud Service provisioning, monitoring and management occurs via cloud APIs. Browsers must be safe and secure to surf. Most common browser attacks include SSL Certificate spoofing, mail client phishing attacks, HTML services attack.

C. Attacks

Once the vulnerabilities are exploited, an attacker can do following attacks [15]:

- Zombie Attacks: Here attacker sends request by innocent hosts in network which are also called as Zombies and floods the network with requests. Denial of service attacks come under this category.
- Shared Technology Problems: The shared on demand services are offered by virtualization. In Infrastructure as a service and hypervisor virtualization one tenant may affect /interfere in the other.
- Malicious Insiders: Due to non-transparency in cloud service provider procedures, insider activities may cause threat to system.
- Data Leakage: Due to dynamicity of cloud data may be compromised which affect overall architecture of the system.
- Service Hijacking: User accounts may be hijacked by phishing, credential exploitation and software vulnerabilities.
- Service Injections: The attacker tries to exploit addresses to access the cloud system.
- Virtualization attacks: It mainly consists of two type of attacks: VM Escape, Hypervisor Rootkit. Under VM Escape the attacker breaks isolation layer to exploit hypervisor privileges .In Rootkit, hypervisor creates a channel for unauthorized code execution.
- Man in middle attack: The data exchange between parties can be accessed by the attacker if SSL (secure socket layer) is not configured properly.
- Phishing attack: These manipulate web links and false links are redirected to user for getting sensitive data.
- Backdoor Channel attack: It gives access to compromised system by controlling victim's resources remotely.

D. Threats

Threats in the cloud computing is given as follows [15]:

- Abusive usage of cloud computing: Misusing storage and bandwidth.
- Insecure Interfaces: For interaction with cloud services cloud service provider publishes a set of APIs which increases the cloud complexity and vulnerable in nature.
- Changes in Business Model: Cloud computing gets changed as per delivery of IT services so reliable encryption is need of hour.

- Lack of standards for cloud auditing.
- Issues in remote data retrieval due to lack of standards.
- Data sanitization lack of standards.
- Lack of Risk Profiling.
- Identity thefts for accessing resources and getting credit.

IV. RISK MANAGEMENT STRATEGIES IN CLOUD COMPUTING

This section describes risks management in cloud computing environment.

Risk assessment and mitigation is need of hour in cloud computing due to inherent risks. Various risks assessment algorithms have been used in past to predict accurate risks. These algorithms include Instance based knowledge, Multilayer perceptron, isotonic regression, randomizable filter classifier and voting [12]. A holistic cloud strategy includes developing communication root between administrator and host by effective security controls. The audit facility and quality assessment must be provisioned after secure data transfer. API security control and legal implications must be taken care.

The workload partitioning problem has been used for risk based data processing over hybrid cloud architecture [16].The better understanding of structural components of an organization, economic and mathematical modeling helps in taking better decisions regarding risk [17].The cloud security risks taxonomy has been divided into compliance risks, architecture based risks and privacy risks as given in Fig. 1, 2, 3 [18].

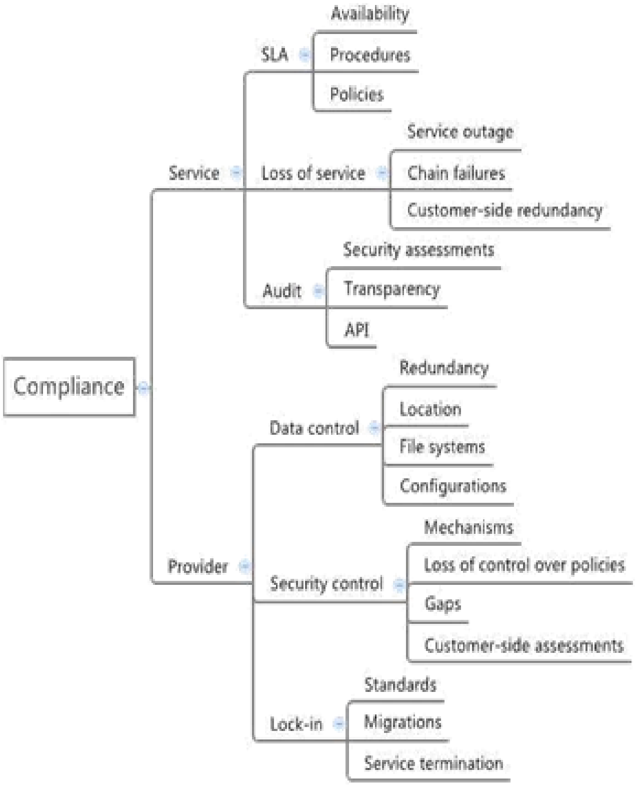


Fig. 1. Security taxonomy focused on Compliance Risks

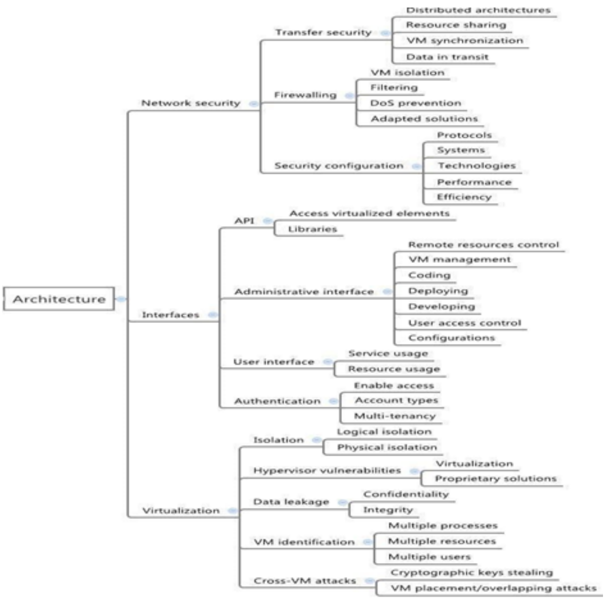


Fig. 2. Security taxonomy focused on Architecture Risks

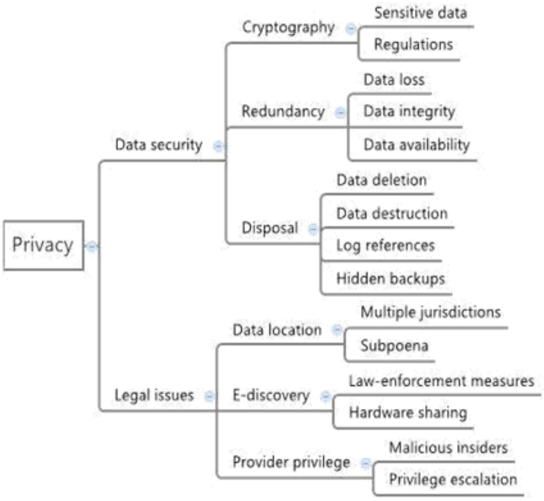


Fig. 3. Security taxonomy focused on Privacy Risks

The cloud security risks mitigation also asks for governance and compliance risks minimization [19].To address the vulnerabilities exploitation several intrusion detection systems have been adapted .The defensive mechanism cycle have been proposed as seen in the Fig. 4 given below[20].

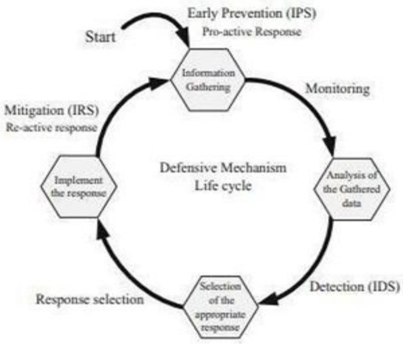


Fig. 4. Lifecycle: Defensive Mechanism

Security threats can be categorized as external attacks, theft related attacks, system malfunction, service interruption and human errors. The impact ratings and likelihood of high level threats are identified, analyzed and mitigated [21].The cloud oriented cooperative intrusion detection systems using signature mechanisms are used with Nessi2 as a simulator tool for cloud security [22]. Fuzzy Self organizing maps are used in past for improving the networking capabilities of cloud[23].System privacy risks are mitigated by a PIA(privacy assessment tool) which informs decision makers to decide how the project will proceed[24].One more methodology supports behavior engineering for model based process improvement and assessment in cloud computing. Behavior modeling includes requirement modeling by requirements behavior tree and specifications by model behavior tree [25].The business oriented cloud computing services guidelines follows 3 tiered SOA architecture ,asynchronous messaging and avoiding cloud specific APIs and assessment in cloud computing. Behavior modeling includes requirement modeling by requirements behavior tree and specifications by model behavior tree [25]. The business oriented cloud computing services guidelines follows 3 tiered SOA architecture, asynchronous messaging and avoiding cloud specific APIs. The goal of risks aware cloud computing lies in from attempting to increase application metrics to finding a balance between performance and sensitive data disclosure [26]. For risks management in Internet of things, SIGMA project has been used to acquire and integrate heterogeneous data from various sensor networks [27].

V. TRUST EVALUATION IN CLOUD COMPUTING

Trust has been one of the most crucial issue in cloud computing . It is a subjective measure between various services that wants to act securely and reliably in a state of affairs for a prescribed time [30, 31]. Trust is evaluated to measure the quality of service of the system [32].Trust may be static/dynamic, centralized/distributed, direct/indirect and proactive/reactive/periodic. The trust types, characteristics and applications are seen in Fig. 5 as given below:

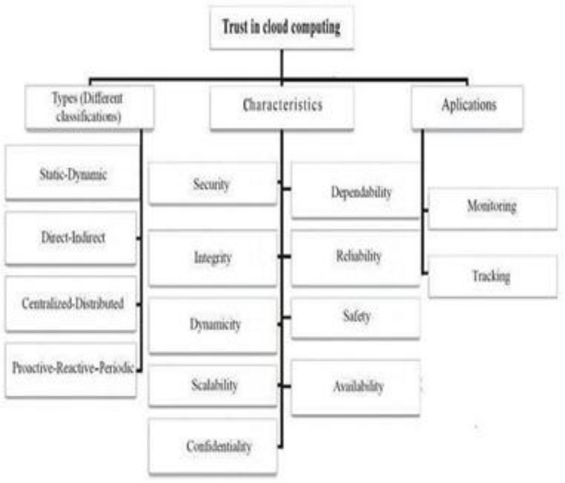


Fig. 5: Trust types, applications and characteristics at a glance

VI. ASSESSING CLOUD READINESS & RISKS IN CLOUD COMPUTING

This section describes how the risks are managed in cloud computing environment and how much an application be easily migrated to cloud in PaaS environment.

The cloud application OpenNebula has been downloaded from GitHub repository [33]. A smart software vendor has been used for identifying the risky items of the scanned application [34]. The risk distribution in the application scanned is given below as per technology, software resiliency, agility and elegance as shown in the Fig. 6 below:

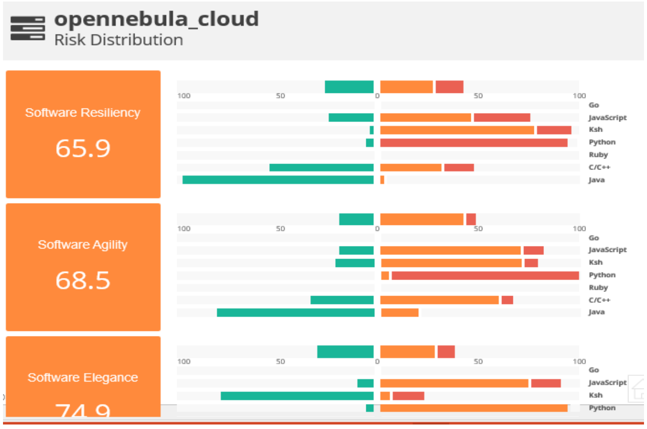
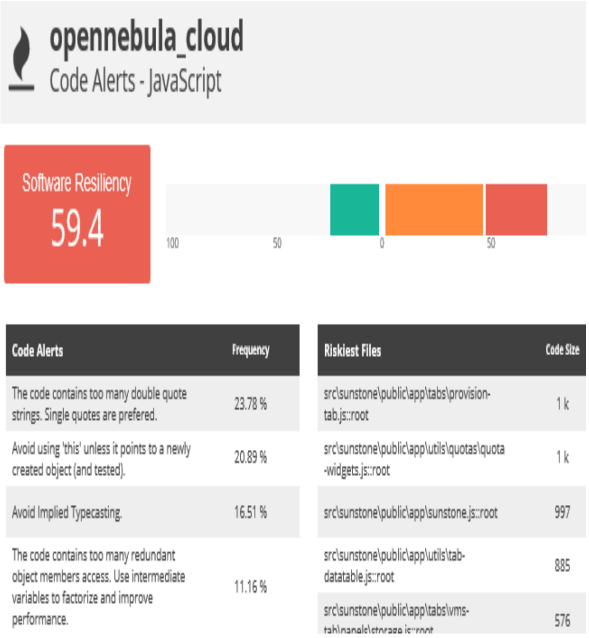


Fig. 6. Risk distribution

All the risky code is identified as per code alerts and risky regions are handled on priority as depicted in Fig. 7.



Code Alerts	Frequency
The code contains too many double quote strings. Single quotes are prefered.	23.78 %
Avoid using 'this' unless it points to a newly created object (and tested).	20.89 %
Avoid Implied Typecasting.	16.51 %
The code contains too many redundant object members access. Use intermediate variables to factorize and improve performance.	11.16 %

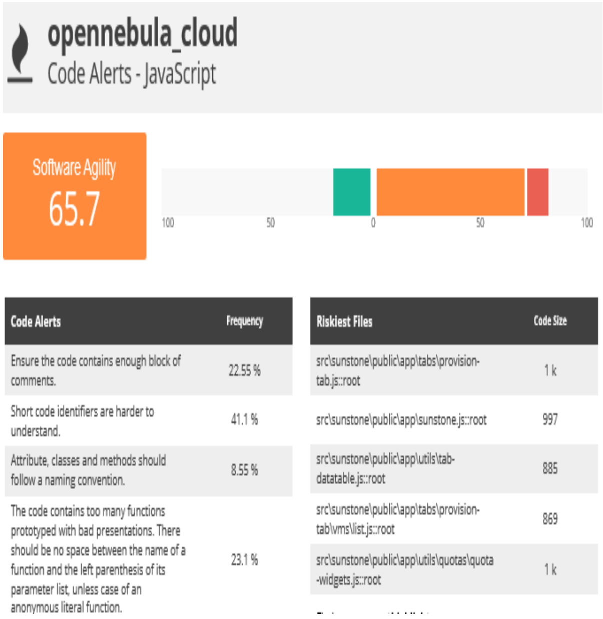
Riskiest Files	Code Size
src\sunstone\public\app\tabs\provision-tab.js::root	1 k
src\sunstone\public\app\utils\quotas\quota-widgets.js::root	1 k
src\sunstone\public\app\sunstone.js::root	997
src\sunstone\public\app\utils\tab-datatable.js::root	885
src\sunstone\public\app\tabs\vms-tab\panels\storage.js::root	576

Fig. 7. Code alerts for software resiliency

The code alerts for software agility are depicted in Fig. 8 as given below:

DOI: 10.35940/ijrte.C1057.1083S19

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication



opennebula_cloud
Code Alerts - JavaScript

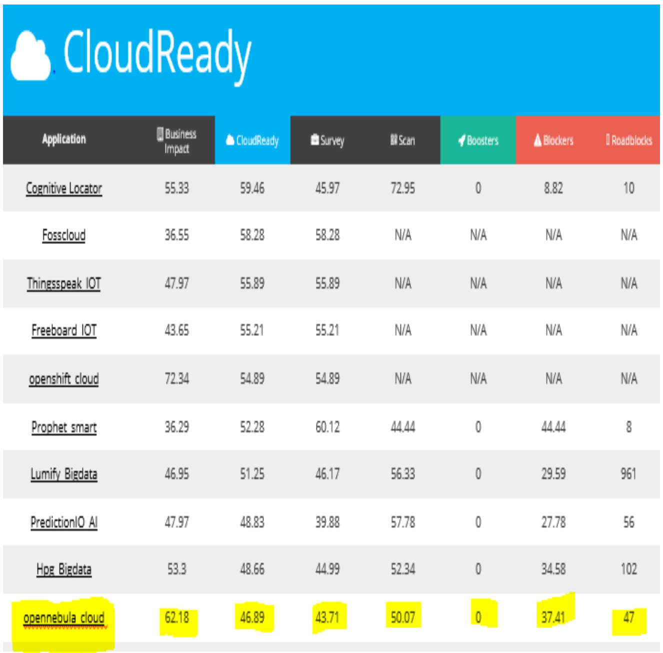
Software Agility
65.7

Code Alerts	Frequency
Ensure the code contains enough block of comments.	22.55 %
Short code identifiers are harder to understand.	41.1 %
Attribute, classes and methods should follow a naming convention.	8.55 %
The code contains too many functions prototyped with bad presentations. There should be no space between the name of a function and the left parenthesis of its parameter list, unless case of an anonymous literal function.	23.1 %

Riskiest Files	Code Size
src\sunstone\public\app\tabs\provision-tab.js::root	1 k
src\sunstone\public\app\sunstone.js::root	997
src\sunstone\public\app\utils\tab-datatable.js::root	885
src\sunstone\public\app\tabs\provision-tab\vms\list.js::root	869
src\sunstone\public\app\utils\quotas\quota-widgets.js::root	1 k

Fig. 8. Code alerts for software resiliency

The organizations today are quite challenged in terms of managing cloud risks. For assessing cloud readiness, we need to assess the delivery models and solutions for cloud sourcing. Identify all blocking factors that may be utilized in future to resolve conflicts. The service quality, availability and dynamicity are mainly the cloud delivery characteristics. The research has employed a smart software vendor for cloud readiness in PaaS environment [34]. The readiness score is calculated by scanning source code and information collected from a questionnaire. The code patterns which can adopt PaaS environment shows the positive score and the code patterns which gets tweaked before migration, outputs in negative score. The cloud readiness score for the application scanned has been depicted in the Fig. 8 as below:



CloudReady

Application	Business Impact	CloudReady	Survey	Scan	Boosters	Blockers	Roadblocks
Cognitive Locator	55.33	59.46	45.97	72.95	0	8.82	10
Fosscloud	36.55	58.28	58.28	N/A	N/A	N/A	N/A
Thingsspeak IOT	47.97	55.89	55.89	N/A	N/A	N/A	N/A
Freeboard IOT	43.65	55.21	55.21	N/A	N/A	N/A	N/A
openshift cloud	72.34	54.89	54.89	N/A	N/A	N/A	N/A
Prophet smart	36.29	52.28	60.12	44.44	0	44.44	8
Lumify Bigdata	46.95	51.25	46.17	56.33	0	29.59	961
PredictionIO AI	47.97	48.83	39.88	57.78	0	27.78	56
Hpe Bigdata	53.3	48.66	44.99	52.34	0	34.58	102
opennebula cloud	62.18	46.89	43.71	50.07	0	37.41	47

Fig. 9. Cloud Readiness Score from application scan and survey

VII. CONCLUSIONS & FUTURE SCOPE

The research has successfully explored various risks, vulnerabilities, attacks and risk management strategies in cloud computing environment. The research has utilized a smart software for scanning application code and identify the riskiest items and their frequency with bad code location. The bad code or risky code items are handled on priority. As the cloud computing imbibes various challenges of information security and privacy, so risk management and trust evaluation becomes important. This research has also considered cloud readiness of an application by code scan and survey. This paper will prove a substantial foundation for formulating interrelationships between risk management and quality assurance in complex computing.

REFERENCES

1. I.D.C. Leguías Ayala, M. Vega, M. Vargas-Lombardo, "Emerging Threats, Risk and Attacks in Distributed Systems: Cloud Computing", In: Elleithy K., Sobh T. (eds) Innovations and Advances in Computer, Information, Systems Sciences, and Engineering. Lecture Notes in Electrical Engineering, vol 152. Springer, New York, NY, 2013
2. S. Mohapatra, L. Lokhande, "Cloud Computing and ROI :A new framework for IT Strategy,Management for Professionals" ,Springer, 2013
3. S. K. Doddavula., I. Agarwal, V. Saxsena, Z. Mahmood., "Cloud Computing Solution Patterns: Infrastructure Solutions", vol. 4:23,Springer Verlag, 2013
4. J.W., "Guidelines on security and privacy in public cloud computing", ,NIST J, 2011, pp. 1–60
5. T Grance , P Mell , "Definition of cloud computing", NIST J , 2009 , pp. 1–7
6. Cloud Security Alliance, Security guidance for critical areas of focus in cloud computing V2.1. J Ala Acad Sci 76, 2009
7. A. Khajeh Hosseini, I. Sriram, "Research agenda in cloud technologies. Technical Report", 2010
8. L. Schubert , K. Jeffery , B. Neidecker-Lutz , " The future of cloud computing opportunities for European cloud computing beyond 2010", ACC 2011, Part IV,2010, pp. 1–71
9. A. Aleem, C.R. Sprott, "Let me in the cloud: analysis of the benefit and risk assessment of the cloud platform", Journal of Financial Crime, vol. 20, No 1 , 2013, pp-6-24
10. M. Chiregi., N.J. Navimipour, "A Comprehensive Study of Trust Evaluation Mechanisms in the Cloud Computing", Journal of Service Science Research , vol. 9 , pp. 1-30, 2013
11. G.C.A. Peng, A. Dutta, A. Choudhary, "Exploring critical risks associated with Enterprise Cloud Computing" , LNICST, 2013, pp-132-141
12. N. Ahmed, A. Abraham , "Modeling Cloud Computing Risk Assessment Using Machine Learning", In: Abraham A., Krömer P., Snasel V. (eds) Afro-European Conference for Industrial Advancement. Advances in Intelligent Systems and Computing, vol. 334. Springer, Cham, 2015
13. N. Ahmed., A. Abraham., " Modelling Cloud computing risk assessment using Ensemble Methods", Advances in Intelligent Systems and Computing 2015,p 261-273
14. S. Srinivasan, " Assessing Cloud Computing for business use, Springer briefs in Electrical and computer Engineering, Springer Science + Business Media, 2014, p 101-118
15. C. Modi, D. Patel, B. Borisaniya , "A survey on Security issues and solutions at different layers of cloud computing", Journal of Supercomputers, Springer Science +Business Media ,vol. 63, 2012, p 561-592
16. K.Y Oktay, M. Gomathisankram., A. Singhal, " Towards data confidentiality and a vulnerability analysis framework for cloud computing", Secure Cloud computing, Springer Science+ Business Media , 2012, pp. 213-238
17. A. Baldwin, D. Pym, S. Shiu, " Enterprise information risk management: dealing with cloud computing", Privacy and security for cloud computing , 978-1-4471-4188-4, 2013

Retrieval Number: C10571083S19/2019©BEIESP
DOI: 10.35940/ijrte.C1057.1083S19

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

18. Gonzalez. N et al., A quantitative analysis of current security concerns and solutions for cloud computing, springer, pp. 1:11, 2012
19. R. Farell, "Securing the cloud -Governance, risk and compliance issues reign supreme", Information security Journal: A global perspective, 2012, pp. 310-319
20. Z. Inayat et.al , " Cloud based Intrusion Detection and Response System :Open Research Issues and Solutions" , Arab journal of Sci. Eng., vol. 42, Issue 2, 2012, pp. 399–423
21. M. Kiran, "A Methodology for Cloud Security Risks Management", In: Z. Mahmood (eds) Cloud Computing. Computer Communications and Networks. Springer, Cham, 2014
22. Z. Al-Mousa, Q. Nasir, "C1-CIDPS: A Cloud Computing Based Cooperative Intrusion detection and Prevention System Framework", Springer , 2015, vol. 523
23. H. Pillutla, A. Arjunan, "Fuzzy self-organizing maps-based DDoS mitigation mechanism for software defined networking in cloud computing", Journal of Ambient Intelligence and Humanized Computing, Springer, 2018, pp. 1-13
24. D. Tancock, S. Pearson., A. Charlsworth, "A privacy Impact assessment tool for cloud computing, Privacy and security for cloud computing", 2013, pp. 1-43
25. J.Cade , L.Wen , T. Rout, "Issues in Applying Model Based Process Improvement in the Cloud Computing Domain ", In: Mitasiunas A., Rout T., O'Connor R.V., Dorling A. (eds) Software Process Improvement and Capability Determination. SPICE 2014. Communications in Computer and Information Science, vol. 477. Springer, Cham, 2014
26. S.Mehrotra., " Towards a risk based approach to achieve data confidentiality in cloud computing", LNCS , vol. 8425, 2014
27. M. Fazio, A. Celesti. , " An Integrated System for Advanced Multi risk management", Advances in intelligent Systems and Computing , vol. 260, 2014, pp. 253-269
28. K. Markande, S.J .Murthy, " Leveraging Potential of cloud for software performance testing" , Cloud Computing ;methods and practical approaches, Computer communications and Net- works, 2013, pp. 293-322
29. 29. I. Chana., P. Chawla, " Testing Perspectives for Cloud based Applications", Software Engineering frameworks for the cloud computing paradigm ,Computer communications and net-works, Springer , 2013, pp. 145-164
30. 30. J. Sidhu , S. Singh , "Improved TOPSIS Method Based Trust Evaluation Framework for Determining Trustworthiness of Cloud Service Providers", Journal of Grid Computing, 2016, pp. 1-25
31. A.S.K Pathan , M.M. Mohammed, " Building Customer trust in cloud computing with an ICT-enabled global regulatory body", Wireless Personal Communications , 2015, 85:77-99
32. X. Xie , R. Liu , X. Cheng , X. Hu , " Trust-Driven and PSO-SFLA based job scheduling algorithm on Cloud", . Intelligent Automation & Soft Computing, 2016, vol. 22(4):1-6
33. https://codeload.github.com/openNebula/one/zip/master
34. Cast Software, www.castsoftware.com, 2019

AUTHORS PROFILE

First Author Ms. Vinita Malik did the Bachelor of Engineering degree from M.D.U, Rohtak, India in 2008. She completed Masters of Engineering in 2012 from B.I.T.S Pilani University, Rajasthan. She is currently working as Information Scientist at Central University of Haryana, Mahendergarh. She is also pursuing PhD in Computer Science && Engineering from D.C.R.U.S.T, Murthal. Her research interests include Software engineering – Risks Management and Testing. She has published 17+ papers in the reputed Journals and conferences.

Second Author Dr. Sukhdip Singh did the Bachelor of Technology degree from the M.D.U, Rohtak, Haryana, India in 1999 and the Ph.D. degree from Maharishi Dayanand University Rohtak, Haryana India. He is currently working as a Professor in the Department of Computer Science and Engineering at D.C.R.U.S.T, Murthal. His research interests include Software Engineering, Green Computing and Cloud Computing. Dr. Singh has published 35+ papers in the reputed Journals and conferences. He is a life time member of the ISTE.