

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

QUALITY ASSURANCE FOR CLOUD COMPUTING

Sumaira Aslam*¹ and Hina Shahid²

*^{1,2}Department of Software Engineering, Fatima Jinnah Women University, The Mall Rawalpindi, Pakistan.

ABSTRACT

Cloud computing is a greatest and latest thing. Marketers for lots of big companies are all using cloud computing terms in their marketing campaign to make them seem them impressive so, that they can get clients and customers. Cloud computing is overall the philosophy and design concept and it is much more complicated and yet much simpler. The basic underlined thing that cloud computing do is to separate the applications from operating systems from the software from the hardware that runs everything. This paper aim to identify the security issues in cloud computing. We present an analysis of security issues in a cloud environs by the analysis of twenty papers.

Keywords: Quality Assurance, Cloud Computing etc

I. INTRODUCTION

When you use webmail, social networking site or store your photos online instead of on your home computer then you are using a cloud service. Cloud computing brings up the delivery of computing resources over the Internet. Instead of keeping data on your own hard drive or you may want to update the applications according to your requirements you get facilitate with service of cloud over the Internet, at a different location, to store your information. Subsequently this may give rise to certain privacy implications.

Cloud computing is the distribution of computing services over the Internet. Cloud services consent people and businesses to use software and hardware that are managed by other parties at remote locations. A simple example of Cloud services includes social networking websites, email, online data storage and online business applications. Whenever people want to access information and computer resources from anywhere all you need is a network connection due to cloud computing. Cloud provides a shared pool of multiple resources, including data storage, networks, computer processing power, and user applications. Cloud services are usually made available through private cloud, public cloud or hybrid cloud. Cloud services are popular because they can diminish the cost and complexity of maintaining and operating computers and networks. As for cloud users there is no need do to invest in information technology infrastructure, hardware purchasing, or buy software licenses' it is becoming an on-demand service.

Cloud computing provide scalability, reliability, and efficiency. Cloud computing offer unlimited processing and storage capacity. The cloud enables access to applications and documents no matters where ever you are in the world via the Internet. Every so often Cloud computing is deliberated efficient because it allows organizations to free up resources to focus on innovation and product development.

II. AN INSURANCE MODEL FOR GUARANTEEING SERVICE ASSURANCE, INTEGRITY & QoS IN CLOUD COMPUTING

[1] L.Min, establishes a framework based on insurance and reference model for cloud computing. The paper applies the approach of(VAR) --value-at-risk to develop several appropriate mechanisms, and use a set of measurable metrics. For the business value and risk assessment, those set of quantitative or qualitative metrics can be applied as the base and ultimately for insurance quality and recompense the calculation for the failures of the services offered in Cloud environment.

III. MANAGING CLOUD COMPUTING RISKS IN FINANCIAL SERVICES INSTITUTIONS

[2] R. Paulscrutinizes the emergent threats in Cloud Computing within a financial services organization. This includes the consideration of insider hidden threats, data hiding, unconfident software, and new Cloud attack

patterns. The authors have observed three specific risk analysis methods are useful in considering the risks of Cloud models in organizations; Fundamental Risk Analysis (FDA), Dataflow Analysis (DFA), and Scenario Analysis (SA). Each method provides unique analysis techniques and variation in perspective. The methods described in this paper illustrate the value of performing risk assessments over cloud enabled architectures and business processes.

IV. A Survey and Evaluation of the Existing Tools that Support Adoption of Cloud Computing and Selection of Trustworthy and Transparent Cloud Providers

[3]A.M.M.Ibrahim discuss the innovative tools, procedures and frameworks that support the implementation of cloud computing models, and the selection of trustworthy cloud service providers. For comparative evaluation, a set of customer's assurance requirements is proposed. A questionnaire-based survey has been described in which respondents evaluate the extent to which these tools have been used, and evaluate their usefulness. The majority of respondents agreed on the importance of using the tools and, although most respondents have not used the tools, those who have used them find them helpful.

V. A Service Integrity Assurance Framework for Cloud Computing Based on Map reduce

[4]R.Yulongadopts the concept of mappers, which typically constitute the majority of the workers. We make the master that manages the computing workers based on the security level and introduce the trusted verifier worker and caching mechanism on the basis of some existing frameworks. This paper is more accurate in detecting the malicious workers in cloud computing environment based on MapReduce. Cloud computing using the MapReduce model makes cheap computing, storage, software resources together to form a scalable virtual IT resource pool, to provide users with computing and storage service on demand.

VI. Cloud Security Issues

[5]K.R.Balachandra describes the service level agreement, SLA's of cloud computing, and how to standardize SLA's followed by the proposed data security issues. At one side, an individual has full control on data and processes in his/her computer. On the other side, we have the cloud computing wherein, the service and data maintenance is provided by some vendor which leaves the client unacquainted of where the data is stored or where the processes are running. When we look at the security of information stored in the cloud computing, the purveyor should provide some assurance in service level agreements (SLA).

VII. A Framework for SLA Assurance in Cloud Computing

[6]H.M.Adil,H proposes a framework to highlight the issues of real-time Qos. Issues regarding Service level management are addressed that are followed by a Third-Party Service Level Agreement monitor (TP SLA Monitor) which consists of a trust assessment module and a risk assessment module. It is described that assessment by combining trust and risk assessment techniques is a novel approach that has not been used before for cloud computing. On-demand and self-serve nature of cloud requires establishing real-time QoS assurance to meet SLA specifications of the consumer.

VIII. Guest Editorial: Networking Challenges in Cloud Computing Systems and Applications

[7]David S. L. Wei presents the network problems and challenges. While many technologies focus on solving specific pain points, and thus this causes for implementing them, technologies that cross into the realm of architecture and data center models are not mainly focused on specific problems. Rather, they focus more on providing multiple hard and soft benefits. Network performance is the crucial to cloud computing performance as cloud networks are the infrastructure for cloud services. A cloud network connects servers, and contains a set of routers and switches that transport traffic between the servers and to the outside world. The interconnection of networks are becoming complex and difficult to handle due to large number of users, user's mobility, and a large variety of application services, cloud networks pose several challenges.

IX. Estimating Security Coverage for Cloud Services

[8]D.Dipankar describes a framework to estimate security coverage for different type of service offerings. And software prototype is discussed for this framework, called MEGHNAD and tested for various cloud service security requirements. The tool allows the user/operator to select a cloud service (such as Saas, Paas, IaaS etc.) and use other pertinent information to determine the appropriate level of security coverage. The main purpose is to promote the utility of finest practices by providing security within Cloud Computing and confidential processes should address the security controls that the cloud provider will conform to maintain the customer's data safety, secrecy and compliance with necessary code of practice.

X. GeoProof: Proofs of Geographic Location for Cloud Computing Environment

[9]A.Aliad introduces architecture for a new approach for geographic location assurance, which combines the proof of the distance protocol and stowage protocol (POS). The major challenges that cloud computing facing is how to secure and protect the data/information that is the property of the user globally. The geographic location of cloud data storage centers is an important issue for many organizations an individual's due to the regulations and laws that require data and operations to be located in specific geographic locations. Therefore, there is a need to ensure that cloud providers do not compromise the SLA contract.

XI. A QoS Assurance Middleware Model for Enterprise Cloud Computing

[10]L.Shou-Yu focus on the architecture proposed employs the agent technology to handle the monitoring of requested Quality of SLA requirements, which are capable to support the Verification and Validation. Most issues highlight the fact that the user has no control over his or her data, because it is kept on a computer belonging to someone else (the cloud provider), multi-tenancy, cross layer service composition. To assure the quality of service and usefulness of Enterprise Cloud Computing, a middleware to support the service structure and monitoring in Enterprise Cloud Computing is highly important. A middleware is designed for Cloud Computing which can automatically manage their source allocation of services from services, infrastructures, and platforms with the provision of cost-effective and secure way to access services from cloud environment.

XII. Creating Next Generation Cloud Computing Based Network Service And The Contributions To Social Cloud Operation Support System(OSS) To Society.

[11]S.Miyuki presents that how the telecom operation support those systems (OSS) that provide enterprise to enterprise (E2E) transactions, on-demand service management switching management and scalability have evolved to provide control on next generation cloud management. Fujitsu's Social Cloud OSS provides multi-vendor, multi-network organization, multi-layer (SLA) assurance, on-demand service management and analysis to businesses. The solution for socially managed cloud OSS service for cloud computing will be the next application that will provide easy access to cloud services with suitable SLAs and permit the society to use social networking applications that are currently being delivered using clouds.

XIII. Assuring Data Privacy in Cloud Transformations

[12]K.Tom focuses on the data protection procedures and customer security. Cloud providers must ensure the security and privacy of your data. This means that industry and government regulations created for the protection of confidential information still apply whether the data is managed or stored by an outside vendor. The three key areas of concern related to safety and confidentiality of data in the fusion cloud are Location of your data, Control of your data and secure transport of your data. Cloud transformations require dynamic redistribution of resources across cloud infrastructure. The movement of data from one system to another without the explicit consent of the data subject is a threat to data privacy.

XIV. Towards Continuous Cloud Service Assurance for Critical Infrastructure IT

[13]H.Aleksandar presents an analysis of assurance approaches and suitability for Critical Infrastructure Services being deployed in the Cloud. Cloud computing is an emerging form of delivering computing services via networks with the capacity to provide IT services at a faster rate and at an affordable cost; it provides users with shared scalable pool and on demand access to computing resources with minimizing management services. The major obstacle in hosting Critical infrastructures is often a lack of assurance. Thus, cloud should offer flexibility and scalability, e.g. data placement, hardware, service migration with proper security.

XV. Analysis for Cloud Testing of Web Application

[14]C.Jianhua discusses the benefits of testing based on cloud computing. And feasibility analysis is addressed for web applications to migrate software testing to the cloud. Testing of a web-based system address problems and errors before the system is publicized issues such as the security of the web application, the basic functionality of the site, and the ability to survive a huge spike in user traffic. Typically functionality testing is operated in multiple platforms, cross-browser compatibility and performance testing is also necessary for quality assurance. Users expect web apps to function accurately, quickly and consistently so, presenting a quality website that doesn't break, works efficiently and delights users naturally builds trust between you and your customers.

XVI. A Method to Ensure Data Security in E-Business Cloud

[15]G.Jingyi discusses the data security in e-business cloud. This involves two phases. One the information of client is kept safe from hackers and the second one is the assurance of security and accuracy when passing data to users. This paper explores in depth the solutions to security issues especially happening to the skyrocketing e-commerce established on cloud computing technology. But the lack of physical control, bring a whole host of cloud security issues – data co-mingling, user abuse, snapshots and backups, data deletion, data leakage. Fortunately, experts agree that encryption is the cloud security control, allowing you protect, control and comply. Data security of e-business cloud will be well-assured by using key cryptographic system (KCS)

XVII. A Survey on Cloud Computing Security

[16]K. Rajeev focused on the security issues in cloud computing. The paper present an analysis of security issues in a cloud environment. As we know security is the top most challenge to be dealt with in every cloud service. So in this paper some suitable elements (Integrity, availability, confidentiality, authorization, authentication etc.) are mentioned by which threats can be avoided in any application. The classification of various security threats/issues presented in this paper would benefit the cloud users to make out proper choice and cloud service providers to handle such threats efficiently.

XVII. Survivability and Information Assurance in the Cloud

[17]G.Melvin identifies six critical risks (Risk Testing, Data Location, Data and Code Portability, Data Loss, Data Security (Privacy) and Vendor Viability). This provides a comprehensive study of essential concepts and methods related to survivability and information assurance in cloud computing environments. It first lays out crucial ideas of the cloud computing model and ideas related to survivability. The ultimate goal is to develop a comprehensive understanding of solutions for improving cloud survivability, and evaluate the advantages of cloud computing by addressing the critical risks.

XVIII. Towards Reliable and Secure Resource Scheduling In Clouds

[18]C. R.Bala proposed secure and reliable cloud scheduler which considers both user requirements and infrastructure properties and supported by reliable data enables the cloud scheduler to make the right decision. However currently available schedulers do not contemplate users' security and privacy requirements and properties of entire cloud infrastructure. These results in major privacy, security and resilience concerns. Organizations should not outsource their critical applications to the cloud without strong assurance. This paper presents a prototype that implements the proposed cloud scheduler which is built on OpenStack.

XIX. An Applied Methodology for Information Security and Assurance: A Study Case for Cloud Computing

[19]R.Villalón-Fonseca identifies the security standards to ensure information security. Current security standards and models usually answer the on "what" , but they do not propose "how" to deal with the intrinsic difficulty of promising modern infrastructures. As a result, security implementations may miss important security controls, and they cannot guarantee a stable security implementation at the different layers of the system architecture. Therefore, a methodology with a novel hierarchical approach is proposed to assure a private cloud computing.

XX. An Analysis On Data Accountability And Security InCloud

[20]H.A.Shital analyzes the different security and application aspects of cloud computing such as integrity, confidentiality, transparency, accountability, availability, assurance and also discussed framework like a Privacy manager in cloud, storage security system based on RSA, Cloud computing data security model and Cloud information accountability. It is analyzed that which model is suited for appropriate application or service. For services where security is important aspect then in that case it is better to go for Data Security model, Privacy Manager and CIA Framework. The services in which accountability is essential in that case it is better to go for CIA Framework and RSASS system. CIA Framework is better for both aspects. But CIA framework has some drawbacks to overcome that a Framework is proposed that will be focused on reducing size of JAR file. There is very less overhead of code on the data. Light weight module is developed to handle JARdata. The duration of file encryption increases as the size of the data file increases. The Jar creation time is almost for the tested files.

XXI. Analysis

All the techniques and mechanisms we take into consideration for the quality assurance of cloud computing are summarized in table 2. We used only eleven parameters for their evaluation.

[1] and [5] [16]focuses on the security of crucial data while using cloud computing .[3] discussed the tools that are more efficient for the quality assurance of cloud computing.[4] managing all communications and data transfers among the users and providing a reliability.[6] highlights the issues of real-time Qos.[14] is quiet on quality parameters that we take.[7]and [18] discussed reliability and scalability problem during the interconnection of network when server provides a services to the multiuser.[8] describes the different type of services that estimates security coverage.[9] and[12]more focused on safety and security than any other quality parameter.[10] and [13]highlights the cost-effective and secure way to access services from cloud environment.[11]speak on usability.[17] discussed the robustness and availability parameters.[15] reveal the safety parameter during e-business.[19]and[20]discussed the different models for the security of critical data. [2] Describes the different methods and techniques for the safety parameter.

XXII. Conclusion

In this paper we have taken eleven parameters on the basis of which we discussed cloud concepts and have revealed the cloud capability such as security, scalability, safety, low-cost, reliability etc. In cloud computing the most prominent issue than the traditional network is the data privacy issue because, in the cloud computing data is highly dependent on server and network. Most of the customers do not trust on the privacy and security of cloud computing and they do not move their data into the cloud platform. To overcome all the security issues we have analyzed twenty papers and have identified which methods and techniques are more appropriate for the security. Moreover,

we have done analysis of those twenty parameters that have been shown by table:2 showing the parameters that are essential for the security of cloud computing.

References

- [1] L.Min , Z.Liang-Jie, L.Fengyun, " An Insurance Model for Guaranteeing Service Assurance, Integrity and QoS in Cloud Computing," *IEEE International Conference on Web Services.*,2010.
- [2] K.R.Balachandra,P.Ramakrishna, Dr. Atanu Rakshit, " Cloud Security Issues," *IEEE International Conference on Services Computing.*,2009.
- [3] David S. L. Wei, M.Sarit, N.Kshirasagar, N.Amiya,T. Yu-Chee,W.Li-Chun, " Guest Editorial: Networking Challenges in Cloud Computing Systems and Applications," *IEEE Journal on Selected Areas In Communications, Vol. 31, No. 12, December 2013*
- [4] D.Dipankar,RMoshiur, " Estimating Security Coverage for Cloud Services," *IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing.*,2011.
- [5] H.M.Adil,H. Omar, " A Framework for SLA Assurance in Cloud Computing, " *26th International Conference on Advanced Information Networking and Applications Workshops.*,2012.
- [6] A.Aiiad, B.Colin, N.G.Juan, " GeoProof: Proofs of Geographic Location for Cloud Computing Environment," *32nd International Conference on Distributed Computing Systems Workshops.*,2012.
- [7] L.Shou-Yu, T.Dongyang, C.Tingchao, C.W.Cheng-Chung , " A QoS Assurance Middleware Model for Enterprise Cloud Computing," *IEEE 36th International Conference on Computer Software and Applications Workshops.*,2012.
- [8] S.Miyuki, " Creating Next Generation Cloud Computing Based Network Service And The Contributions To Social Cloud Operation Support System(OSS) To Society," *18th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises.*,2009.
- [9] K.Tom, D. Karim, K.Mariam, J.Ming, A.Django,C.Marcelo,M. Iheanyi,F. Nikolaus, "Assuring Data Privacy in Cloud Transformations," *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.*,2012.
- [10] H. Aleksandar, H.Thomas, T.Markus ,M. Andreas,E.C. Santiago, " Towards Continuous Cloud Service Assurance for Critical Infrastructure IT," *International Conference on Future Internet of Things and Cloud.*,2014.
- [11]C. Jianhua, H. Qingchun, " Analysis for Cloud Testing of Web Application," *2nd International Conference on Systems and Informatics (ICSAI 2014).*,2014.
- [12] G.Jingyi,H Kaifeng, " A METHOD TO ENSURE DATA SECURITY IN E-BUSINESS CLOUD," *Proceedings of IEEE CCIS2012.*,2012.
- [13] K. Rajeev, " A Survey on Cloud Computing Security," *International Conference on Computing Sciences.*,2012.
- [14] G. Melvin, " Survivability and Information Assurance in the Cloud," *International Conference on Dependable Systems and Networks Workshops (DSN-W).*,2010.
- [15] R. Yulong,T.Wen, " A Service Integrity Assurance Framework For Cloud Computing Based On Mapreduce," *Proceedings of IEEE CCIS2012.*,2012.

[16] C. R.Bala, S.Manojkumar, " Towards Reliable And Secure Resource Scheduling In Clouds," *International Conference on Computer Communication and Informatics (ICCCI - 2014), Coimbatore, INDIA, Jan. 03 – 05, 2014.*

[17] R. Villalón-Fonseca, Braulio J. Solano-Rojas, G. Marín-Raventós, " An Applied Methodology For Information Security And Assurance:A Study Case For Cloud Computing," *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014).*,2014.

[18] A.M.M.IBRAHIM , " A Survey and Evaluation of the Existing Tools that Support Adoption of Cloud Computing and Selection of Trustworthy and Transparent Cloud Providers," *International Conference on Intelligent Networking and Collaborative Systems.*,2014.

[19] H.A.Shital, Prof. S.B. Mane, " An Analysis On Data Accountability And Security In Cloud," *International Conference on Industrial Instrumentation and Control (ICIC) College of Engineering Pune, India. May 28-30., 2015.*

[20] R. Paul,T.Ben-Zvi, " Managing Cloud Computing Risks in Financial Services Institutions," *Proceedings of PICMET '15: Management of the Technology Age.*,2015.

Table I. Evaluation Criteria for cloud computing quality assurances

Parameters	Definition
Safety	The state of being data protection from risk and danger.
Reliability	It is an attribute that shows how to select the most appropriate design to assure that user expectations are met.
Maintainability	Ability of a computer program to cope with a changed environment and to be retained in its original form in case of a failure.
Confidentiality	Signal of the provider's obligations in terms of data security (The data share over the network between the authorized clients should not be publicize)
Stability	The more stable an application is when fewer failures are observed.
Portability	The usability of software with same functionalities in different environments
Robustness	To continue to operate despite abnormalities in the network.
Scalability	The number of concurrent users that an application can support.
Performance	It enables the system to perform system functionalities accurately and also helps in error and defect detection.
Flexibility	System ability to adopt the future changes in its requirements.
Availability	The provision of system resources in the of terms of network failures in the system (Of service at hand)
Extensibility	The ability of system to introduce new functionalities.
Usability	The ease of use
Interoperability	Different modules supporting the same platform at the back end.

Table II. Analysis of Quality Parameters for cloud computing quality assurance

Sr#	Authors	Possible values										
		Safety	Reliability	Maintainability	Confidentiality	Performance	Scalability	Flexibility	Availability	Extensibility	Robustness	Usability
1	L.Min, 2010	Yes	Yes	No	Yes	Yes	No	No	No	No	No	Yes
2	R. Paul, 2015	Yes	Yes	No	Yes	Yes	No	No	No	No	No	No
3	A.M.M.IB RAHIM 2014	No	Yes	No	Yes	No	No	No	No	No	No	No
4	R.Yulong, 2012	Yes	Yes	No	Yes	No	No	No	No	No	No	No
5	K.R.Balachandra, 2009	Yes	No	No	Yes	No	No	No	No	Yes	No	No
6	H.M.Adil, H. 2012	Yes	Yes	No	Yes	Yes	No	No	Yes	Yes	No	No
7	David S. L. Wei, 2013	No	Yes	No	No	Yes	Yes	No	Yes	No	Yes	Yes
8	D.Dipankar, 2011	Yes	Yes	No	Yes	No	No	No	No	No	No	No
9	A.Ajiad, 2012	Yes	No	No	Yes	No	No	No	No	No	No	No
10	L.Shou-Yu, 2012	Yes	No	No	Yes	No	Yes	No	No	Yes	No	Yes
11	S.Miyuki, 2009	No	Yes	Yes	No	Yes	Yes	Yes	No	No	No	Yes
12	K.Tom, 2012	Yes	No	No	Yes	No	No	No	No	No	No	No

13	H.Aleksandar, 2014	No	No	No	No	Yes	Yes	Yes	No	Yes	Yes	No
14	C.Jianhua, 2014	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
15	G.Jingyi, 2012	Yes	No	No	Yes	No	No	No	No	No	No	No
16	K. Rajeev, 2012	Yes	No	No	Yes	No	No	No	Yes	No	No	No
17	G.Melvin, 2010	Yes	No	No	Yes	No	No	No	No	No	No	No
18	C. R.Bala, 2014	Yes	Yes	No	Yes	No	No	No	No	No	No	No
19	R.Villalón-Fonseca, 2014	Yes	No	No	Yes	No	No	No	No	No	No	No
20	H.A.Shital, 2015	Yes	Yes	No	Yes	No	No	No	Yes	No	No	No