International Journal of Future Generation Communication and Networking
Vol. 11, No. 4 (2018), pp.1-10
http://dx.doi.org/10.14257/ijfgcn.2018.11.4.01

Analysis of the Effectiveness of Cloud Control Matrix for Hybrid Cloud Computing

Muhammad Imran Tariq

The Superior University, Lahore, Pakistan
imrantariqbutt@yahoo.com

Abstract

Cloud computing has become next generation paradigm of Information Technology. The development of cloud computing has brought several security issues. The prospect users has intended to adopt cloud but its security issues effects users' trust on its service. At present, there are many Information Security Frameworks, Standards and Guides to safeguard organizations from security risks but these are not particular for Cloud Organizations. Cloud Security Alliance (CSA) has released Cloud Control Matrix v.3.0.1 in the year 2016 to provide security controls particularly for Cloud Organizations. In this paper, cloud security risks and vulnerabilities has been identified that breach security and mapped into Cloud Control Matrix to check its effectiveness. The result shows that Cloud Control Matrix provides maximum and better security controls to Cloud Organizations.

Keywords: *Cloud Computing; Cloud Control Matrix; Information Security; Cloud Security*

1. Introduction

Cloud Computing is one of the most important trend and newest area in the field of information technology in which resources (*e.g.*, CPU and storage) can be leased and released by customers through the Internet in an on-demand basis. Cloud Computing has various benefits over traditional computing like reduce cost, scalability, disaster recovery, ease of implementation and so on but information security and risk management is still a great concern [1].

Cloud computing provides a platform to its users to dynamically allocate, reallocate, configure, reconfigure and de-allocate resources according to their desire. Cloud is based on virtual infrastructure that is unseen to the user, which makes almost anyone to deploy tools on demand to serve as many users as desired [2]. The Virtualized cloud infrastructure manage abstraction layer that is necessary for an applications or services are not directly related to the underlying physical infrastructure, such as servers, storage or networks. This service enables the organizations to dynamically move resources virtualized infrastructure very efficiently [3].

The Cloud structure is famous due to its services that has drawn extensive attention of the organizations. The Cloud resources are provided as services over the internet. The Cloud computing is also facing many roadblocks in its deployment and if these roadblocks will not resolved in due course of time then it may become a great challenge its fast growth [9] [13]. Security is one of the great concern for users especially when they transferred confidential and sensitive information to Cloud server [4]. The fact behinds about said concern is that most of the Cloud servers are operated by the commercial providers which are not under the control of the user. Moreover, confidentiality factor is also arise when user outsource its data in the cloud.

Received (December 15, 2017), Review Result (February 9, 2018), Accepted (May 18, 2018)

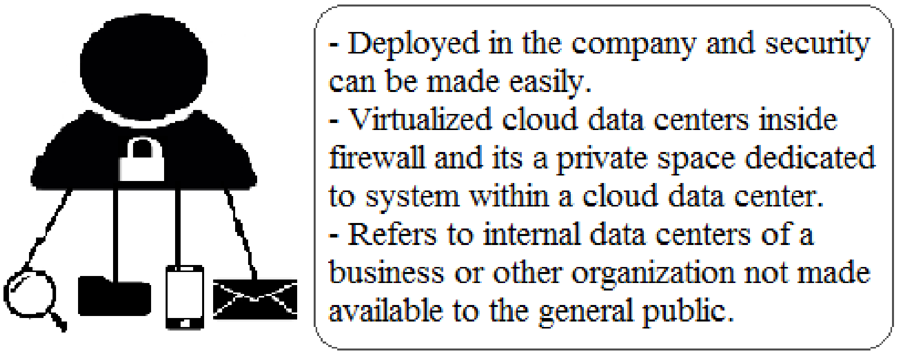
ISSN: 2233-7857 IJFGCN
Copyright © 2018 SERSC Australia

2. Architecture of Cloud Computing

The system architecture suggested by NIST for cloud computing basically has three deployment models:

2.1. Private Cloud

The organization builds its own infrastructure and manages it as well.



- Deployed in the company and security can be made easily.
- Virtualized cloud data centers inside firewall and its a private space dedicated to system within a cloud data center.
- Refers to internal data centers of a business or other organization not made available to the general public.

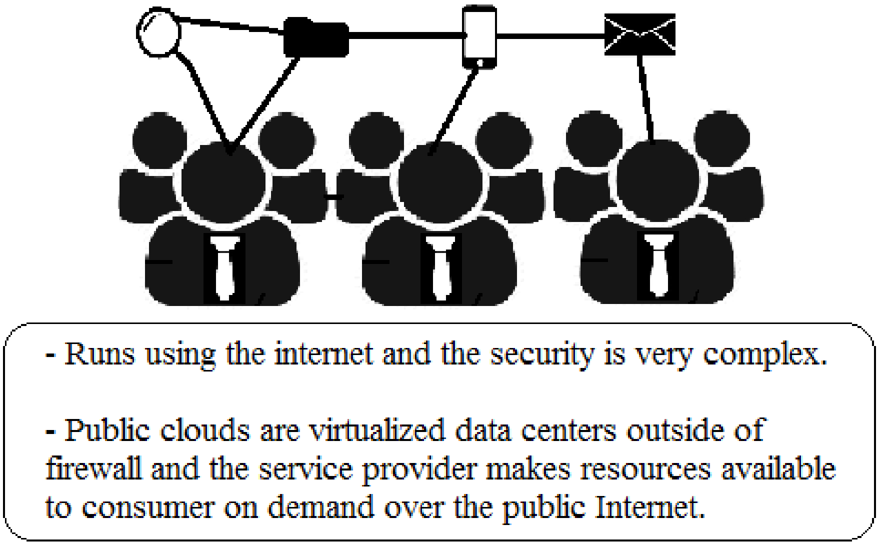
Figure 1. Private Cloud

2.2. Public Cloud

The organization renders different services of Cloud Services Provider (CSP) as per its requirements and uses it as long as organization requires [5]. Private and Public Clouds are connected with each other through gateways, share data, applications and resources.

2.3. Hybrid Cloud

It is a combination of Cloud Private, Public models. It has characteristics of all deployment models. There is no location binding on hybrid cloud, it may located at private organization premises or Cloud Service Provider premises [6].



- Runs using the internet and the security is very complex.

- Public clouds are virtualized data centers outside of firewall and the service provider makes resources available to consumer on demand over the public Internet.

Figure 2. Public Cloud

Copyright © 2018 SERSC Australia

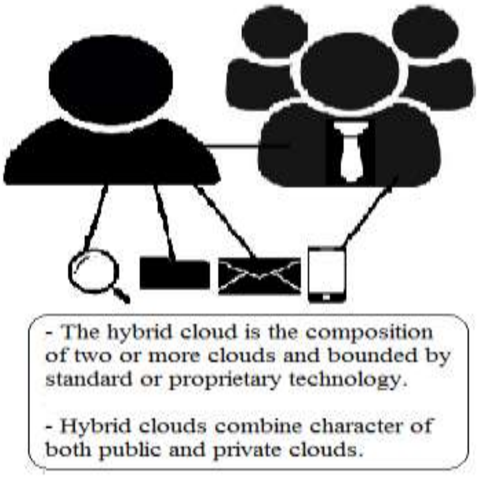

- The hybrid cloud is the composition of two or more clouds and bounded by standard or proprietary technology.
- Hybrid clouds combine character of both public and private clouds.

Figure 3. Hybrid Cloud

Cloud computing also has three service models which are explained as under:

2.4. Software as a Service (SaaS)

The consumer uses the provided application and does not manage or control the network, server's storage and the application. It reduces expenses and is easy to use and access everywhere. It can also share instance of a software application as a service accessible via internet browser or client based role access and sharing rules. The CSP hosts the software so the user does not need to install or manage or buy hardware for it. Salesforce, Dropbox and Google Drive are the example of SaaS [7].

2.4. Infrastructure as Service (IaaS)

It has provided hardware, storage and infrastructure relates services. Amazon EC2 and Rackspace are very famous examples of IaaS [8].

2.5. Platform as Service (PaaS)

It provides environment, tools, libraries to applications development framework, machines and operating system services to its customers.

Cloud computing has several advantages over the traditional computing but it has several constraints that are roadblock in the complete deployment of cloud computing.

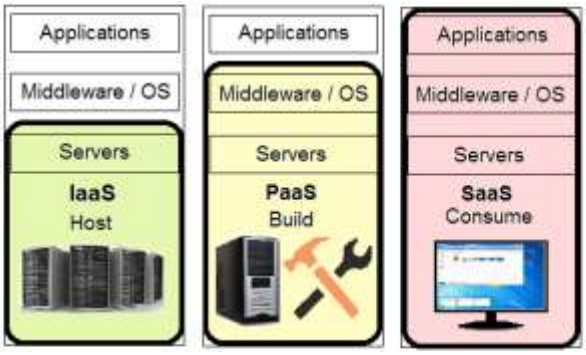


Figure 4. Comparison of Service Models

The purpose of this paper is the thoroughly examine the existing renowned Cloud Control Matrix V.3.0.1 through identified Hybrid Cloud related threats and risks. The

Copyright © 2018 SERSC Australia

Section II of this paper discussed about Cloud Control Matrix, Section III is about the identified cloud risks that will be mapped on Cloud Control Matrix (CCM) to check its effectiveness. The Section IV will be do in-depth analysis of the CCM. Section V presents is about validation of the work that have done and discussed in earlier sections.

3. Cloud Control Matrix

Cloud Control Matrix is set of Information Security Controls developed by Cloud Security Alliance to help organizations particularly Cloud organizations to assess the risks associated with organization [10]. It provides a complete framework consist of security controls that gives detail understanding about security. The framework has following 16 domains comprising of 113 security controls.

- Application & Interface Security (AIS)
- Audit Assurance & Compliance (AAC)
- Business Continuity Management & Operational Resilience (BCR)
- Change Control & Configuration Management (CCC)
- Data Security & Information Lifecycle Management (DSI)
- Datacenter Security (DCS)
- Encryption & Key Management (EKM)
- Governance and Risk Management (GRM)
- Human Resources (HRS)
- Identity & Access Management (IAM)
- Infrastructure & Virtualization Security (IVS)
- Interoperability & Portability (IPY)
- Mobile Security (MOS)
- Security Incident Management, E-Discovery, & Cloud Forensics (SEF)
- Supply Chain Management, Transparency, and Accountability (STA)
- Threat and Vulnerability Management (TVM)

These domains are extracted from the internationally recognized and well known security standards, frameworks, guides and regulations like NIST SP 800 Rev.3 [11], COBIT 5, PCI DSS, Jericho Forum, ISO / IEC 27001 [12], FISMA [14] and NERA CIP. The CSA provided more in depth security controls particularly business information security controls to meet the requirements of the industry to reduce and identify security risks, threats and vulnerabilities in the cloud.

4. Cloud Risk Identification

This section is about the identification of cloud risks that mapped on the CCM. During this process, a systematic literature review was conducted, discussion was made with security experts and information security forums was perused to elicit cloud related risks that are most influential in cloud adoption.

During this process, a database was developed to enlist all the risks, their severity level and nature of action. Initially, all risks were stored and studied, risks that are cosmetic in nature were eliminated from risks list. In second stage, the risks that are not relates to the Cloud Computing were eliminated from the database and finally the risks that are mostly reported by the industry and researchers were selected to mapped on CCM. The selected cloud risks are given in the Table 1. The list is comprehensive and described risks covered

Copyright © 2018 SERSC Australia

every type of the cloud risks classification. The risks that are not given in the list and relates to Cloud risks does not means that these risks are meaningless. Cloud Organizations must take these risks into consideration for mitigation.

Table 1. List of Identified Risk

Sr. No	Risk
1.	Lock In
2.	Resource Exhaustion
3.	Supply Chain Failure
4.	Conflict between Customer Hardening Procedure and Cloud Environment
5.	Social Engineering Attacks
6.	Cloud Provider Malicious Insiders
7.	Intercepting Data in Transit
8.	Insecure or Ineffective Deletion of Data
9.	Distributed Denial of Service (DDoS)
10.	Economic Denial of Service (EDoS)
11.	Compromise of Service Engine
12.	Loss of Cryptographic Keys
13.	Loss of Backup
14.	Natural Disasters
15.	Subpoena and e-Discovery
16.	Data Leakage
17.	Account or Service Hijacking
18.	Data Loss
19.	IP Spoofing
20.	SQL Injection Attack
21.	Cross Site Scripting
22.	Man in Middle Attack
23.	Cookie Manipulation
24.	Hidden Field Manipulation
25.	Port Scanning
26.	Hypervisor Security
27.	Cookie Poisoning
28.	VM Escape
29.	Customer Data Manipulation
30.	VM Sprawl
31.	Zombie Attack
32.	Privileged User access
33.	Data Segregation
34.	SQL Injection Attack
35.	Cross Site Scripting
36.	Man in Middle Attack
37.	Long Term Viability

The details of each risk given in above Table are not described here due to paper size limitation.

Copyright © 2018 SERSC Australia

5. Analysis of Cloud Computing Matrix

To analyze Cloud Control Matrix, selected risks given in the Table 1 were mapped on CCM to know effectiveness of the security controls. During mapping process, risk was chosen from the list and then description of each control has been perused. The security controls of CCM that can mitigate the risks were selected and then thoroughly examined to check whether selected controls have sufficient measures to mitigate the risk or partially mitigate the risk. This process required intensive work as detail description of risk and associated severity level was taken into consideration while mapping on the 113 security controls. The detail of the selected security controls against each risk is given in the Table 2.

Table 2. Cloud Risk Mapped on Cloud Control Matrix

Sr. No	Risks	Cloud Control Matrix															
		AIS	AAC	BCR	CCC	DSI	DCS	EKM	GRM	HRS	IAM	IVS	IPY	MOS	SEF	STA	TVM
1	Lock In												✓				
2	Resource Exhaustion	✓	✓	✓					✓								
3	Supply Chain Failure														✓	✓	
4	Conflict between customer hardening procedure and cloud environment															✓	
5	Social Engineering Attacks	✓				✓	✓			✓				✓			✓
6	Cloud Provider Malicious Insiders	✓			✓		✓										
7	Intercepting Data in Transit	✓					✓	✓				✓		✓			✓
8	Insecure or Ineffective Deletion of Data					✓	✓										
9	Distributed denial of service (DDoS)	✓									✓	✓		✓			✓
10	Economic Denial of Service (EDoS)			✓										✓			✓
11	Compromise of Service Engine	✓						✓			✓						
12	Loss of Cryptographic Keys							✓									✓
13	Loss of Backup		✓	✓											✓		
14	Natural Disasters		✓	✓													
15	Subpoena and e Discovery														✓		
16	Data Leakage	✓															✓

Table 2. Cloud Risk Mapped on Cloud Control Matrix

Sr. No	Risks	Cloud Control Matrix															
		AIS	*AAC*	*BCR*	*CCC*	*DSI*	*DCS*	*EKM*	*GRM*	*HRS*	*IAM*	*IVS*	*IPY*	*MOS*	*SEF*	*STA*	*TVM*
17	Account or Service Hijacking					✓								✓			✓
18	Data Loss	✓				✓			✓								
19	IP Spoofing	✓				✓						✓		✓			✓
20	Loss of Control												✓				
21	Data Boundary	✓				✓											
22	Invalid Storage						✓										
23	SQL Injection Attack							✓									✓
24	Cross Site Scripting	✓						✓			✓						✓
25	Man in Middle Attack				✓		✓	✓						✓			✓
26	Cookie Manipulation				✓												
27	Hidden Field Manipulation	✓			✓												
28	Port Scanning										✓						
29	Hypervisor Security											✓					
30	Cookie Poisoning				✓												
31	Virtual Machine Escape											✓					
32	Customer Data Manipulation	✓						✓							✓		
33	VM Sprawl											✓					
34	Zombie Attack						✓					✓		✓			✓
35	Privileged User Access									✓	✓				✓		
36	Data Segregation				✓											✓	
37	Long Term Viability												✓				

The Figure 5 demonstrates the readers about the number of times a domain of Cloud Control Matrix could be used to address the risk.

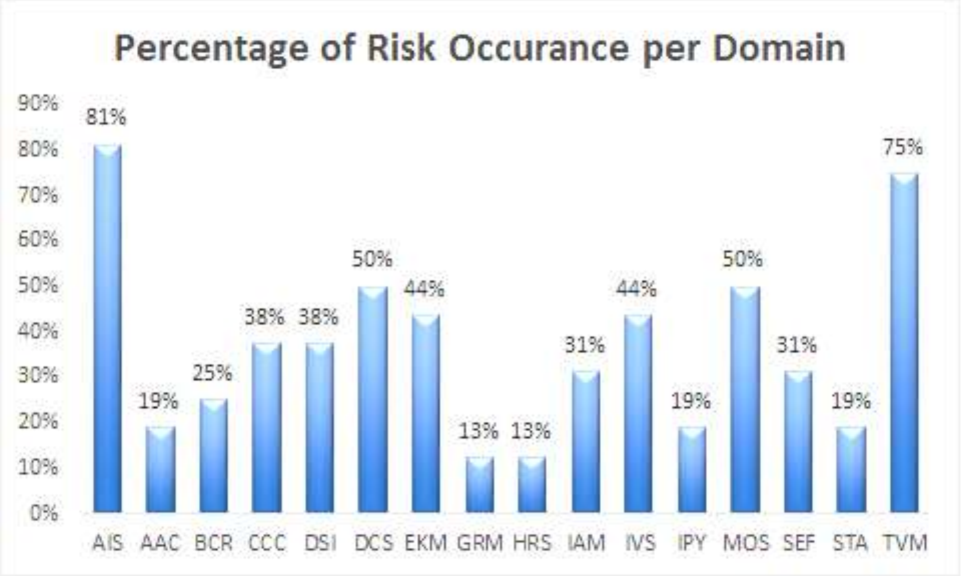


Figure 5. Domains Mostly Likely to be Effected Due to Identified Risks

After in depth analysis of the domain and controls, Application & Interface Security (AIS) is the most effective domain of the Cloud Control Matrix and organizations are required to implement controls of ibid domain more carefully. The Threat and Vulnerability Management (TVM) is also most effective domain of the Cloud Control Matrix as this domain discuss about Antivirus / Malicious software, Patch Management and Mobile Code.

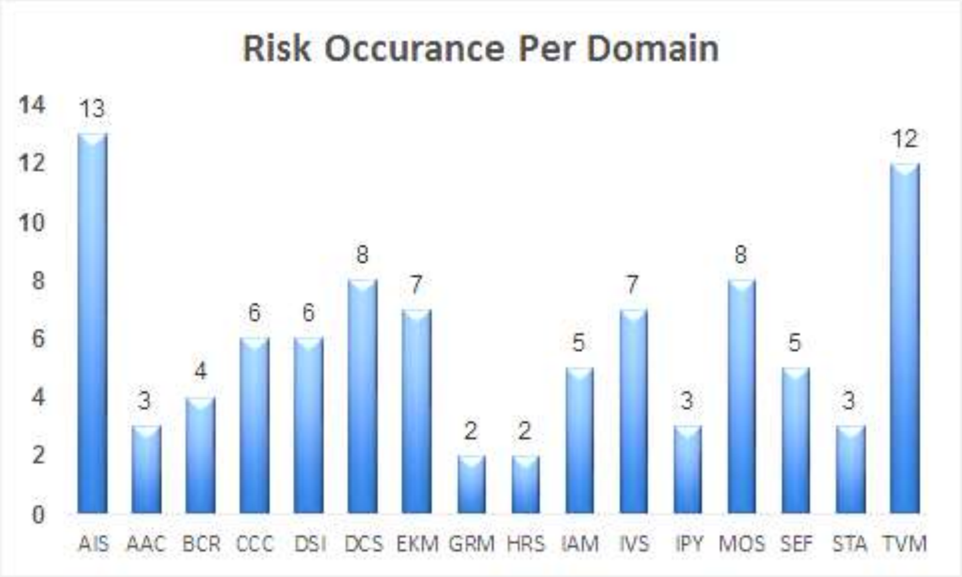


Figure 6. Domains Most Likely to be Effected Due to Identified Risks in Percentage

The quantitative analysis of the Figure 6 shows that Application & Interface Security (AIS) and Vulnerability Management (TVM) are the most repeatedly used domains as these domains are 80% and 75% are effective respectively. Subsequently, Datacenter Security (DCS) and Mobile Security (MOS) are 50% effective for the mitigation of identified risks. Furthermore, it also shows that organizations have to mainly focus on

Copyright © 2018 SERSC Australia

AIS, TVM, MOS and DCS domains while implementing Cloud Control Matrix in an organization.

It would be very easy for the Cloud venders, Cloud Organizations, Cloud Customers and Cloud Service Providers to understand from the quantitative analysis that Cloud Control Matrix has the capability to mitigate cloud related security risks. Furthermore, the security risks that are not completely mitigated by the implementation of Cloud Control Matrix can be completely mitigated by the implementing controls from ISO/IEC 27001:2013 [14] and NIST SP 800-53 Rev.4 [15]. It is pertinent to add here is that every risk is not required to mitigate due to cost effect. Various risks are less harmful but their mitigation cost is very high, such types of risks are mitigated by the implementation of security framework.

6. Conclusion

Cloud Computing delivers all computing services over the internet required by the customer on the basis of pay as per use basis. Due to its numerous advantages, Cloud Computing was opted very rapidly but not as such it should be due to security constraints. The traditional computing security framework like ISO/IEC 27001:2013, NIST SP 800-53 Rev. 4, FISMA, PCI and COBIT have huge number of controls including security controls but these standards do not address the issues relates to cloud computing. Cloud Computing security issues are not same as traditional computing, therefore, it requires security framework that address security issues particularly to cloud computing.

The Cloud Security Alliance (CSA) developed various guides relates to Cloud Computing including Cloud Control Matrix. The CCM is complete security framework to mitigate the cloud related risks/threats/vulnerabilities. The CCM is currently deployed in a number of cloud organizations to cater their security requirements.

A systematic literature review approach was opted to find out risks that are relates to Cloud Computing and most frequently highlighted by the Cloud organisations as well as researchers. Each domain of the Cloud Control Matrix and its related controls was analyzed to check the effectiveness of the controls as well as domain of the CCM. During mapping process, each risk was selected from the list and then 113 controls were perused to check whether the security control mitigate the risk or not? Thereafter, against each risk, list of related controls of the CCM were selected and also examined the mitigation level of selected controls. Quantitative analysis revealed that Application & Interface Security (AIS), Vulnerability Management (TVM), Datacenter Security (DCS) and Mobile Security (MOS) are most effective domains of the Cloud Controls Matrix for the mitigation of Cloud related risks. The Cloud Organizations have to pay their full attention while implementing these domains in their organization.

Future work is the extension of the existing work. Cloud Control Matrix is still undergone the process of improvement. The domains of the CCM are required to be extended and new domains that address personal related risks, risk management are required to be added separately. Furthermore, future research will find out risks that are not mitigated by the CCM and proposed domains and security controls for its mitigation.

Acknowledgments

These should be brief and placed at the end of the text before the references.

References

[1] M. I. Tariq, "Towards Information Security Metrics Framework for Cloud Computing", International Journal of Cloud Computing and Services Science (IJ-CLOSER), vol. 1, no. 4, **(2002)**, pp. 209-217.

[2] Y. Yu, A. Miyaji, M. H. Au and W. Susilo, "Cloud computing security and privacy: Standards and regulations", Computer Standards & Interfaces, vol. 54, **(2017)**, pp. 1-2.

[3] N. Chowdhury and R. Boutaba, “Network virtualization: state of the art and research challenges”, IEEE Communications Magazine, vol. 47, no. 7, **(2009)**, pp. 20-26.

[4] K. Surya, M. Nivedithaa, S. Uma and C. Valliyammai, “Security issues and challenges in cloud”, 2013 International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), **(2013)**.

[5] A. Alshammari, S. Alhaidari, A. Alharbi and M. Zohdy, “Security Threats and Challenges in Cloud Computing”, 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), **(2017)**.

[6] M. I. Tariq and V. Santarcangelo, “Analysis of ISO 27001:2013 Controls Effectiveness for Cloud Computing”, Proceedings of the 2nd International Conference on Information Systems Security and Privacy, **(2016)**.

[7] M. I. Tariq, “SLA based information security metrics in cloud computing: a complete guide to measure information security of cloud computing”, Saarbrücken, Deutschland: LAP LAMBERT Academic Publishing, **(2014)**.

[8] D. Sitaram and G. Manjunath, “Infrastructure as a Service”, Moving To The Cloud, **(2012)**, pp. 23-71.

[9] K. Dahbur, B. Mohammad and A. Tarakji, “A survey of risks, threats and vulnerabilities in cloud computing”, Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications - ISWSA '11, **(2011)**.

[10] S. Saxena, “Ensuring Cloud Security Using Cloud Control Matrix”, International Journal of Information and Computation Technology, **(2013)**, pp. 933-938.

[11] NIST, 'Content / Special Publications - SP 800 series / NIST SP 800-53 rev 3 - Recommended Security Controls for Federal Information Systems - NIST IT Security', 2011. [Online]. Available: http://www.nist.org/nist_plugins/content/content.php?content.18. [Accessed: 01- Oct- **2015**].

[12] M. Tariq, “Providing Assurance to Cloud Computing through ISO 27001 Certification: How Much Cloud is Secured After Implementing Information Security Standards”, CreateSpace, **(2015)**, pp. 134.

[13] A. Aich, A. Sen and S. Dash, “A Survey on Cloud Environment Security Risk and Remedy”, 2015 International Conference on Computational Intelligence and Networks, **(2015)**.

[14] FISMA, 'NIST Computer Security Division - FISMA Implementation Project', [Online]. Available: http://csrc.nist.gov/groups/SMA/fisma/index.html, **(2014)**.

[15] NIST, 'NIST Special Publication 800-53 (Rev. 4)', [Online]. Available: https://web.nvd.nist.gov/view/800-53/Rev4/home, **(2013)**.

Author

Muhammad Imran Tariq is Deputy Director (Commerce) at Higher Education Department, Lahore, Pakistan, where he has been since 2006. He received a Bachelor of Computer Science from Allama Iqbal University, Islamabad in 2003, Master of Science in Computer Science / M.Phil from University of Lahore in 2013. He is currently perusing Ph.D degree in Computer Science from Superior College, Lahore. Moreover, he has MCSE, MCP+I, A+ and CCNA certifications. His research interests include Cloud Computing, Information Security, ISO, NIST, COBIT, Service Level Agreement, Information Security Metrics, Cloud Risks and its mitigation techniques, Wireless Networks Security and Risk Management. He is author of many research papers and 02 books on Cloud Security. He is also reviewer of International Renowned Journals and Associate Editor of IEEE Access Journal.

Copyright © 2018 SERSC Australia