Enterprise Based Architecture for Securing Information in Cloud Network

Mudassir Mehmood Ali[1], Dr Mohammad Syed Anwar[2], Mahrukh Mehmood[3], Aftab Aslam[4] and Naseer Ahmed[5]

[1,2,5] Faculty of Telecommunication and Information Engineering, Department of Computer Engineering, University of Engineering and Technology Taxila, Pakistan
[3] Department of Linguistic, University of Washington, Seattle, WA
[4] University Institute of Information Technology, Arid Agriculture University, Rawalpindi, Pakistan

Abstract

Organization, institutes and even the individual are always concerned about their data security and privacy. The organizations have highly adopted the information and communication technology within their environment to make their work more efficient and effective. The cloud computing technologies has gained high attentions in last recent years. However, the data security and privacy is considered as the main barriers in the adoption of the cloud computing technologies especially with the perspective of the enterprise Organization. In this research, we have identified the access control for securing the information on the virtualization and cloud computing technologies. The role and rule books techniques have been utilized in the design, development and implementation of the proposed solution. The cloud computing simulator has been developed for the verification and validation of the proposed solution. The delivery model of the cloud computing with the functionality of SAAS has been utilized in the simulation environment. The proposed solution has been executed on the software as a service layer.

Keywords: *Cloud Computing, Enterprise organization, Security, Communication, Virtualization*

1 Introduction

In development of the human civilization, communication and coordination has a major role. Starting from the basic and dumb gesture communication of human, today's communication offer the ability to send almost feeling of 'touch' from sender to receiver [1]. Due to the extensive range of multimedia applications, data processing devices, digital communication is very popular because of its ability to handle devices such as cell phones, PDAs, Playbooks and tablets etc. [2]. The communication devices are offered by number of different companies such as Microsoft, IBM, Oracle, Nokia, Blackberry and many others. To send important and error free information, devices has to compress data for efficient transmission and encode to protect it from noisy channels. There are different sort of tools and techniques which are utilized for the data communication. The channel coding schemes are well known of the data and information sharing. The goal of channel coding schemes is to find codes which can be used to transmit information quickly using different valid code words as well as correct or even detect the errors that might be occurred during the transmission. Before and after transmission, the data has to be stored somewhere so, that it can be utilized future [3].

1.1 Cloud Computing

Cloud computing are considered as an innovative approach in the field of the computing technologies. There are number of companies, organizations and institutes which are planning to shift from the traditional technologies to the cloud computing technologies [4]. Every Organization in today's world is concern about the security and privacy of their data and information [5]. The cloud computing technologies has addressed number of challenges including "resources sharing, on-demand resources, systems software, web platforms, performance, information, security, platform, risk, and quality engineering [1].

It is a network-based computing in which large groups of number of servers are networked to allow the centralized data storage, processing, resources sharing, online access and many other services to client. The initial standard of the cloud computing is defined by NIST "National Institute of Standards and Technology" [6]. The cloud computing provide the services with the help of their delivery model [7]. The delivery model is also known as service model. The Enterprise or Organization utilized different sort of cloud types including public cloud, private cloud or hybrid cloud. The hybrid cloud is the combination of the public cloud and private cloud [8].

1.2 Problems and Issues

The cloud computing offer number of benefits to their consumers but has still failed to provide unified framework architecture. The threat of hacking, unauthorized access of the system can't be denied within the cloud computing or internet technologies [9]. There are number of software and application development companies which have been involved in the design and implementation of secure computing environment but, still in the internet and cloud computing environment, a huge dynamic internet security based solution exist [10].

This research paper has presented the architecture of the access controller which will be integrated with the cloud computing architecture for the securing the data and information on the cloud computing technologies. The access control architecture is an attempt to provide enterprise architecture for securing information in cloud

(DOI: dx.doi.org/14.9831/1444-8939.2015/3-9/MRR.21)

computing environment; the solution can also be integrated with the internet application.

1.3 Research Objective

This research paper is addressing the issue of the security threat and challenges which are faced by the cloud computing technologies. The first research objective is to Design, development and implementation of the access control for the cloud computing technologies. Secondly, the verification and validation (V&V) is always considered as the center piece of attention. The access controller developed in the research has been test by the extensive user of the simulation, and lastly, Identifying and analyzing the Security Requirement Engineering for vitalization of the Cloud computing technologies.

2 Virtualization and Cloud Computing

Virtualization is the concept which has the capacity to execute the multi operating system on the signal platform. It has been analyzed from organizational perspective that most of the organizations have multi tasks which they want to simulate on the signal perspective [11]. The Virtualization and cloud computing technologies are closely interacted with each other forming a Hypervisor layer. In this sub section, we have discussed in-depth analysis on the Virtualization and cloud computing technologies. The security perspective has also been discussed. Virtualization can be the abstraction of the components or by the integration of the application that provide the services of the Virtualization. The virtualization setting can be usually known as personal appliance (VM) [12]. In order to understand security benefits it has been concluded by the means of virtualization plus. The cloud is also considered as the Virtualized solution. It has number of high performance server and computing devices which are interconnected with each other through Internet-based computing, whereby shared resources, software, and information are provided to computers and other devices on demand and pay per use [13].

2.1 Virtualization Architecture

There are number of sorts by which the virtualization can be available. They are notable primarily through the covering in the ADPS to that particular virtualization is put on. Even so, most virtualization sorts have an entity called some sort of hypervisor or digital equipment monitor (VMM). It's the core device which adjustments even the virtualized applications move using the main covering regarding means [14]. In a sense, it's the supervisor of virtualized surroundings. Request virtualization could be a digital setup from the product development screen. It allows applications to perform in completely different systems by providing the normal digital application program interface. Application virtualization could be a digital setup of your software program (OS) in which applications composed to the COMPUTER ITSELF will certainly manage [15]. Regardless of the widespread hearings from the virtualization sorts mentioned greater than, most current info focuses in addition to atmosphere start using a type called total virtualization which is available in a couple of different sorts

1) Native Virtualization
2) Hosted Virtualization

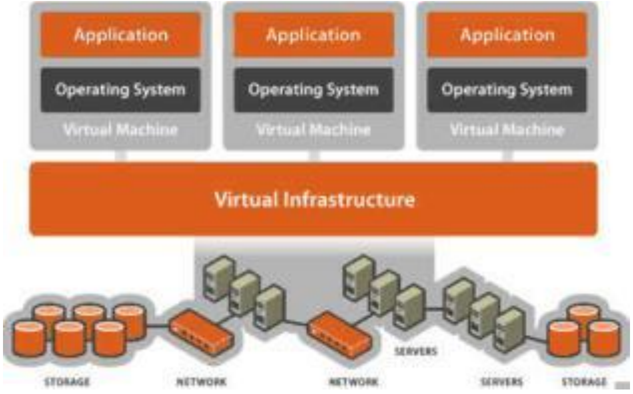


Figure 1 Virtualization Architecture [14]

2.2 Virtualization Characteristics

Using the advantages in the virtualization structures, new standard features are mixed together inside virtualized methods. The actual several standard features of which has an impact on protection inside virtualized methods are new management coating, concentration, varying point out, and range of motion [16].

The new management layer is essentially a layer created by the hypervisor. Since the particular hypervisor manages all VMs of which run on the particular actual physical appliance, that boasts management legal rights to everyone the particular virtualized components. To get a virtualized data core or cloud, the info enemies search for is usually inside the VMs. Therefore, though manage from the hypervisor or the particular coordinator OPERATING SYSTEM which the hypervisor extends on, the particular adversary are able to skimp on the majority of if not each of the VMs, posing major risk to the entire data core or cloud." [17]

Concentration is the characteristic that a plethora of VMs will run on the same physical machine, since the main purpose of virtualization is to fully utilize the physical resources or hardware available. It is an issue directly related to the new management layer created by virtualization. If one physical machine only runs one VM, then compromising the machine is no different than damaging one server that runs on the VM [18]. However, due to concentration, taking control of one VM on the machine can also potentially let the attacker gain access to other VMs as they run on the same physical machine, thus greatly increase the damage done [19].

Mobility may be the unique trait connected with virtualization that allows VMs to move derived from one of actual physical unit to an alternative with no moving almost any electronics. Due to the simplicity at which VMs are usually sent over equipment, safety issues about social networking and also sincerity while taking VMs will become widespread seeing that VMs could be transferred involving equipment inside the identical facts heart, an additional facts heart, or even confuses. This can be a worry certainly not present in non-virtualized conditions, seeing

(DOI: dx.doi.org/14.9831/1444-8939.2015/3-9/MRR.21)

that movements connected with non-virtualized techniques simply demands moving the actual physical mass media. Furthermore, the actual safety border for each and every VM is extremely difficult to keep when they can potentially transfer involving diverse infrastructures Regardless of the issues that arise while using the completely new traits in virtualization, there are many advantages to be able to virtualization."

2.3 Virtualization Security Vulnerabilities

Certainly not astonishingly, the primary noticeable because of episode a new virtualized expertise center or fog up is always to know usage of your hypervisor that controls each of the VMs running within the expertise center or fog up. For the ancient virtualization pattern, you'll find absolutely no popular episodes on the hypervisor due to their character to be inserted within the components Or else, 3 varieties of episodes for the hypervisor are present: episode with hypervisor from the web host OS IN THIS HANDSET along with episode with hypervisor by having a invitee OS in this handset [17].

Both the episodes for the hypervisor in the main use to the style associated with virtualization. Different sorts associated with episode similar to virtual collection check-out, migration episode, along with cryptography episode sq. Measure uses for the qualities along with national infrastructure associated with virtualization" [20]

1) Migration attack
2) Encryption attack

3 Security Requirement Engineering for Cloud

Most of the organizations working in different regions of world have generic security requirement. It has been analyzed during the analysis that absence of the security framework is the main barriers in the utilization of the cloud computing technologies. Security requirement engineering is the engineering of very initial step of involved in the design, development and implementation of the cloud computing solutions. The security solution is planned in the initial phases and provides the basis for the solution development of the cloud. This requirement gathering stage is the most crucial and indeed the most important stage involved in the Software Development Life Cycle (SDLC). The requirement engineering is the engineering of collecting the requirements with the perspective of the system performance, memory and resources consumption, Functional, Non-Functional, and many other requirements. The requirements engineering are the core part before the design of any solution. In has been analyzed from number of related studies that most of the Enterprise application failed as they are not built according to the client requirements [21].

There are number of model and techniques which can be utilized for the Security Requirement Engineering for Cloud [13]however, in this research we have utilized the model presented by [22]. There are four main phases which are interlinked with the Security Requirement Engineering for Cloud these are "Requirements Elicitation, Requirements Analysis, Requirements Validation And Requirements Management" [23].

Main part of the requirement engineering is the meeting with consumer and try to collect the information and requirements. The most difficult part is to get all the requirements and get them signed from the client. Communication is the key of Requirement Engineering. The requirement gathering will help us identify that which sort of the data security and privacy is required by the client. As Communication is the key of the requirement engineering so there are plenty of social and cultural issues. The issues are mainly due to differences of cultural and social norms. A software developer has to understand the lay man language to collect the requirements because clients might not be aware of software terms and may find it difficult a develop a perception about what security he need. The consumer might use the terms which are not very common for the developer as he is not expert of in the area of the information security or cloud computing domains.

The important object is to get the requirement which is feasible in the real world with the perspective of the security and cloud computing solution. Requirements should be realistic and developer has to make client understand about the unrealistic requirements. Client should be satisfied and ready to be involved in any further stage. Interviewing is the activity which can make a client and developer comfortable. These can be open ended and close ended as well. Listening and understanding the client's requirement is the key to successful and flawless software. There are number of social, ethical and legal issues which during the requirement gather for the development of the cloud computing solution. There are six areas of social issues that can come across in the process of requirement gathering of the security engineering for cloud. These social issues are faced by the social groups involved in the whole process mainly three are known as "client organization, requirements team and Development team. The groups face social and cultural issues in the communication and whole requirement engineering process such as "Issues within the Clients Organization, Issues within the requirement team, Issues between the client and requirement team, Issues between the development and requirement team, Issues with in the development team and Issues between the development team and client After conducting the in-depth analysis the requirement of the design, development and implementation of the Enterprise Architecture for Securing Information in Cloud Computing Environment has been extracted. Most of the organizations are concern about their security. The next section of the research paper provides system architecture which has been developed after performing the related research and Security Requirement Engineering for Cloud computing technologies.

4 System Architecture

The system architecture is used to identify and analyses the behaviors and working structure of the solution. The access controller has been deployed on the top layer of the cloud computing architecture for the Securing Information in Cloud Computing Environment. The security solution design and their implementations are always considered as a challenging task [24]. The access control presented in the research consists of the number of components. These

components are interlinked with each other so, that the specific task and activity can be performed.
The logical structure of the access control consists of three main components including “Access Granter, Rule books and key allocation”. The information is transmitted between all these components and based on decision; the access granter gives the permission to the user.

Components		Description
1	**Access Granter**	Whenever the user generate the request to access the SAAS layer, the access granter the request user about the authentication information. The authentication mechanism can be defined by the Organization according to their requirement and resources availability such as “digital signature, thumb verification and much other equipment.
2	**Rule books**	The Rule book is considered as the core component of the proposed solution. The rule book is maintained by the administrator. The Rule book logical contains all the rules and roles defined of the Organization. The Access Granter verifies the role and rule before assigning the keys to the user.
3	**Key allocation**	Once the user is authenticated, the keys are assigned to the user according to their roles, rules and privileges.

Table 1 System Architecture Components

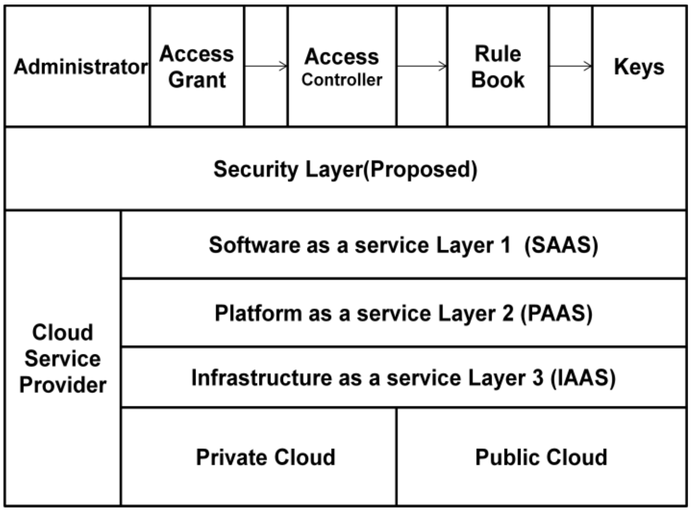


Figure 2 System Architecture

4.1 Working Mechanism

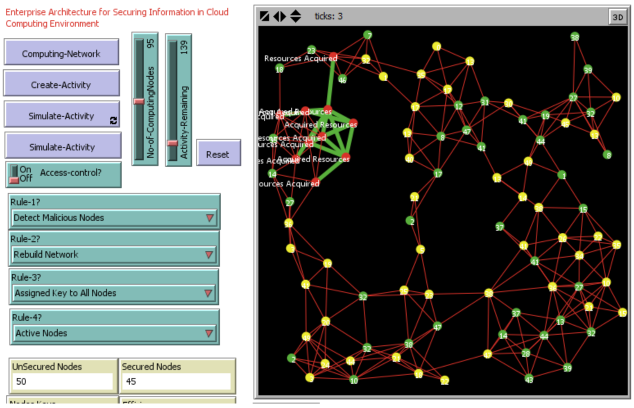
The working mechanisms identify the data flow of the core component of the integrated in the solution. It can be analyzed that there are three main components identified in the proposed mechanism. These components are as followed:

1) Cloud App
2) Access Granter
3) Rule book

The user interacts of the cloud app request the credential information (User ID, Password) from the user access the cloud application. The user provides the information about it credentials. The information is passed to the access granter. The access granter contacts the rule book and identifies the user and assigns him the role and set the rule accordingly as set to the information presented in the rule book. Once the user is authenticated the key are attached by the access granter to the user so that the access to the cloud apps can be provided to the user. The user can only access those information on the cloud apps whom the permission he or she have been granted. All the pre-negotiated will be conducted on the software as a service layer of the cloud. The key have been exchanged between the users and the cloud app for secure communication and can set up the details for the cryptography.

5 Evaluation

The customized simulator has been developed for the verification and validation (V&V) of the proposed solution. The NETLOGO has been utilized for the design and development of the simulation of the cloud computing technologies. The cloud computing nodes has been deployed in the spatially clustered network. Each computing node has been deployed within the range of six degree with each other. The each computing node deployed in the environment has been provided number of parameters including “Secondary Memory, Primary memory, CPU and other parameters”.


Enterprise Architecture for Securing Information in Cloud Computing Environment

No-of-ComputingNodes 95
Activity-Remaining 139
Access-control? Off
Rule-1? Detect Malicious Nodes
Rule-2? Rebuild Network
Rule-3? Assigned Key to All Nodes
Rule-4? Active Nodes
UnSecured Nodes 50
Secured Nodes 45
ticks: 3

Figure 3 Simulator

(DOI: dx.doi.org/14.9831/1444-8939.2015/3-9/MRR.21)

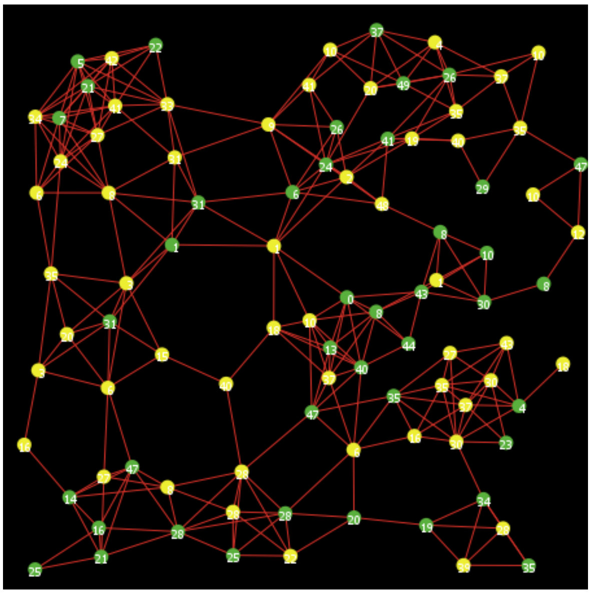


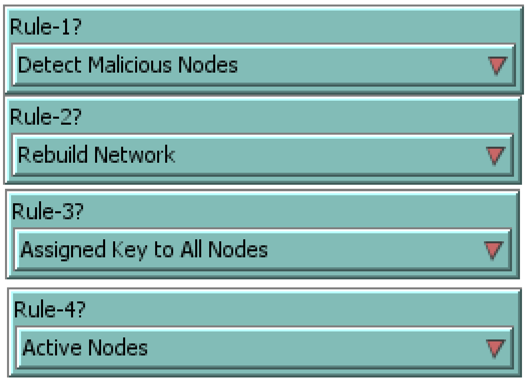
Figure 4 Deployment of Secure and Unsecured nodes

5.1 System Rules

The following system rules have been defined in the simulation.

Rule 1	**Rule 2**
Don’t Detect Malicious Nodes	Don’t Rebuild Network
Detect Malicious Nodes	Rebuild Network
Rule 3	**Rule 4**
Assigned Key to All Nodes	Active Nodes
Assigned Key to Secure Nodes	Sleep Nodes

Table 2 System Rules



Rule-1?
Detect Malicious Nodes

Rule-2?
Rebuild Network

Rule-3?
Assigned Key to All Nodes

Rule-4?
Active Nodes

Figure 5 Logical Rulebook View

5.2 Experiments

There are number of different experiments which have been conducted to evaluate the proposed solution. The main focus involved during the development of the solution is the Computation Time and performance. The experiments have been conducted in the simulation and in-depth comparison has been made between the proposed solution and existing solution.

5.2.1 Computation Time

The computation and response time are directly proportional to each other. The more fast the computation is performed, the response time is better. It can be analysed from the existing experiment that the proposed solution has better response time as compared to the existing solution.

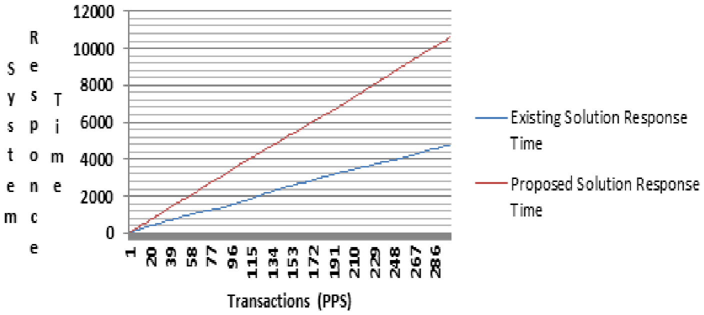


Figure 6 Response Time

5.2.2 Performance

The efficiency and effectiveness of any solution depends upon performance. The access controller has been implemented in the simulation environment on the SAAS cloud delivery model layer. The efficiency has been measured on two task including complex task and easy task. It can be analysed that the proposed solution is more effective as compared to the exiting solution.

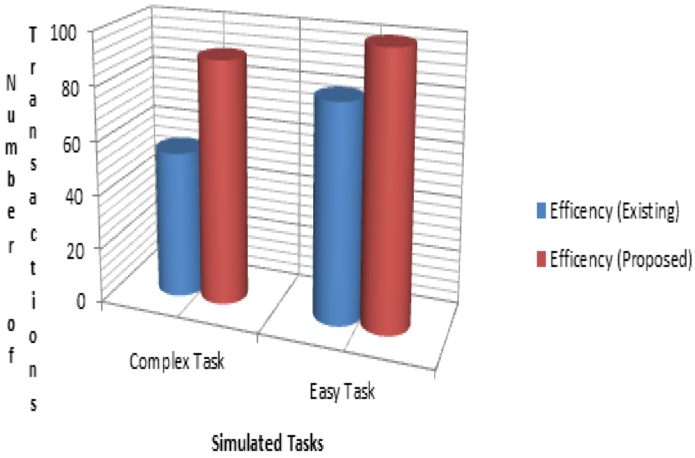


Figure 7 Performance

It has been observed from the simulation results that the proposed solution is better as compared to the existing solution design and development for the providing security.

6 Conclusion

As the utilization of the information and technology are increasing day by day, the data security and privacy has become of the critical and time consuming issues. It has been analyzed that most of the organizations are planning to shift from the traditional computing technologies to cloud

(DOI: dx.doi.org/14.9831/1444-8939.2015/3-9/MRR.21)

computing technologies. It has been concluded that the access control is a better approach as compared to the existing security solution design and developed for Securing Information in Cloud Computing Environment. The proposed solution has provided the best utilization of the resources without affecting the performances of the cloud computing & application simulating on it. The architecture of the access controller must be flexible so that it be able simulate on the both cloud computing (Private and Public).

REFERENCES

[1] Rodrigo N Calheiros, Rajiv Ranjan, Anton Beloglazov, C, and Rajkumar Buyya, "CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms," Software: Practice and Experience, vol. 41, no. 1, pp. 23-50, 2011.

[2] CLoUD ComPUtING, "Cloud computing privacy concerns on our doorstep," Communications of the ACM, vol. 54, no. 1, 2011.

[3] Hannes Holm, Markus Buschle, Robert Lagerstrom, and Mathias Ekstedt, "Automatic data collection for enterprise architecture models," Software \& Systems Modeling, vol. 13, no. 2, pp. 825-841, 2014.

[4] Sean Carlin and Kevin Curran, "Cloud computing security," International Journal of Ambient Computing and Intelligence (IJACI), vol. 3, no. 1, pp. 14-19, 2011.

[5] Dimitrios Zissis and Dimitrios Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, vol. 28, no. 3, pp. 583-592, 2012.

[6] Peter Mell and Tim Grance, "The NIST definition of cloud computing," 2011.

[7] Subashini Subashini and V Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1-11, 2011.

[8] Danish Jamil and Hassan Zaki, "Cloud computing security," International Journal of Engineering Science and Technology, vol. 3, no. 4, pp. 3478-3483, 2011.

[9] Clavister, "Security in the cloud," in Clavister White Paper, 2011.

[10] J. Milne, "Public and Private cloud projects dwarf," Public initiatives, pp. 45-56, 2011.

[11] NM Chowdhury and Raouf Boutaba, "A survey of network virtualization," Computer Networks, vol. 54, no. 5, pp. 862-876, 2010.

[12] Ankur Mishra, Ruchita Mathur, Shishir Jain, and Jitendra Singh Rathore, "Cloud Computing Security," International Journal on Recent and Innovation Trends in Computing and Communication, vol. 1, no. 1, pp. 36-39, 2013.

[13] Novica Zarvic and Roel Wieringa, "An integrated enterprise architecture framework for business-IT alignment," Designing Enterprise Architecture Frameworks: Integrating Business Processes with IT Infrastructure, p. 63, 2014.

[14] Sean Marston, Zhi Li, Subhajyoti Bandyopadhyay, Juheng Zhang, and Anand Ghalsasi, "Cloud computing—The business perspective," Decision Support Systems, vol. 51, no. 1, pp. 176-189, 2011.

[15] LAKSHAY Malhotra, DEVYANI AGARWAL, and ARUNIMA JAISWAL, "VIRTUALIZATION IN CLOUD COMPUTING," 2014.

[16] Guohui Wang and TS Eugene Ng, "The impact of virtualization on network performance of amazon ec2 data center," in INFOCOM, 2010 Proceedings IEEE, 2010, pp. 1-9.

[17] Flavio Lombardi and Roberto Di Pietro, "Secure virtualization for cloud computing," Journal of Network and Computer Applications, vol. 34, no. 4, pp. 1113-1122, 2011.

[18] Yuping Xing and Yongzhao Zhan, "Virtualization and cloud computing," in Future Wireless Networks and Information Systems.: Springer, 2012, pp. 305-312.

[19] Qi Zhang, Lu Cheng, and Raouf Boutaba, "Cloud computing: state-of-the-art and research challenges," Journal of internet services and applications, vol. 1, no. 1, pp. 7-18, 2010.

[20] Robert Lagerstrom, Carliss Baldwin, Alan MacCormack, and Stephan Aier, "Visualizing and Measuring Enterprise Application Architecture: An Exploratory Telecom Case," in System Sciences (HICSS), 2014 47th Hawaii International Conference on, 2014, pp. 3847-3856.

[21] Mahmood Ahmad and Mohammed Odeh, "Blueprint of a Semantic Business Process-Aware Enterprise Information Architecture: The EIAOnt Ontology," in Enterprise Information Systems.: Springer, 2014, pp. 520-539.

[22] Bhaskar Prasad Rimal, Jukan Admela, Katsaros Dimitrios, and Goeleven Yves, "Architectural requirements for cloud computing systems: an enterprise cloud approach," Journal of Grid Computing, vol. 9, no. 1, pp. 3-26, 2011.

[23] Deng-Guo Feng, Min Zhang, Yan Zhang, and Zhen Xu, "Study on cloud computing security," Journal of Software, vol. 22, no. 1, pp. 71-83, 2011.

[24] Michael Armbrust et al., "A view of cloud computing," Communications of the ACM, vol. 53, no. 4, pp. 50-58, 2010.

[25] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in INFOCOM, 2010 Proceedings IEEE, 2010, pp. 1-9.

[26] William Voorsluys, James Broberg, and Rajkumar Buyya, "Introduction to cloud computing," Cloud Computing, pp. 1-41, 2011.

[27] Cloud Computing, "Cloud Computing," 2010.

(DOI: dx.doi.org/14.9831/1444-8939.2015/3-9/MRR.21)