Volume 6, Issue 1, January 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Securing Cloud Environment using Firewall and VPN

A. M. Chandrashekhar[1], Sahana K[2], Yashaswini K[3]
[1] Assistant Professor, [2 & 3] M.Tech 1st Semester
[1, 2, 3] Department of Computer Science & Engineering, SJCE, Mysuru, Karnataka, India

Abstract: ***In this paper we are investigating the impact of firewalls and VPN for providing security to cloud. So, computer simulation and modeling of cloud environments with OPNET simulator has conducted with VPN and firewalls. However, cloud Computing provides an added level of risk, which makes cloud computing difficult to provide data privacy and security, availability, and to illustrates compliance .Many technologies are supported by cloud environment. Cloud inherits its security issues defined in SLA based policies which are used for service and resources usage. But the scenarios are changed in cloud environments. Hence firewall behavior gets adaptive as per the need of cloud computing.***

Keywords: SLA, Firewall, VirtualPrivateNetwork, Cloud environment.

I. INTRODUCTION

Cloud computing is getting a lot of competition and interest. This advances in computing and put cloud computing as one of the modern developments of computing models. The main Reason is to service delivery model which provides computing and storage for users in all fields including financial, health care and government [1].This can be authenticated using an effective integration of variety of computing, storage, data, applications and other resources. This progress can be considered much more enhanced than that of distributed computing, parallel processing, and grid computing and so on. With cloud computing, abstraction and multi-level virtualization can be achieved [2].

This integration will allow users to use powerful storage capacity and computing of cloud with the use of network which is achieved in grid computing or distributed processing. The importance of Cloud Computing is slowly increasing and it is receiving a growing attention in both scientific and Industrial fields[11]. The first important technology among the most technology is the Cloud Computing technology which is used by most of the organizations and companies from successive years. Cloud computing environment looks like distribution architecture and computational paradigm. Its main objective is to support convenient, secure and quick storage of data and network computing service, with visualized resource computing which are delivered above Internet[12].

The cloud enhances collaboration, agility, scalability, availability, ability to adapt to fluctuations according to demand, accelerate development work, and provides potential for cost reduction through optimized and efficient computing[15].The cloud based systems can guarantee the data security and the user does not have to look over the protection parameters. So the cloud computing must ensure the security of data stored in the cloud system[16].

VPN (Virtual Private Network) technology provides a way of protecting information being transmitted over the Internet, by allowing users to establish a virtual private "tunnel" to securely enter an internal network, accessing resources, data and communications via an insecure network such as the Internet. VPN is a generic term used to describe a communication network that uses any combination of technologies to secure a connection tunneled through an otherwise unsecured or distrusted network[17].

Firewall implements security using the defined security policies which provides filtering rules for the data transitions on the cloud network. The data which satisfies the security requirements of the organization if allowed to travels in the network and rest of the packets are blocked[18].

Firewall implements security using the defined security policies which provides filtering rules for the data transitions on the cloud network. The data which satisfies the security requirements of the organization if allowed to travels in the network and rest of the packets are blocked[19].

II. LITERATURE SURVEY

The data which satisfies the security requirements of the organization if allowed to travels in the network and rest of the packets are blocked. The process of configuring a firewall is tedious and error prone. The policy management is quite complicated task because of their dynamically changing thousands of the rules. They rules are conflicting in nature and might overlap somewhere which defining them in the system. Cloud requires open access to all the services for fats control over the data. Along with that it must satisfies the security requirements. Thus it needs to be modified in such way which satisfies all the characteristics of the cloud so that security service can be developed[20].

On the other hand, due to the complex nature of policy anomalies, system administrators are often faced with a more challenging problem in resolving anomalies, in particular, resolving policy conflicts. An intuitive means for a system Administrator to resolve policy conflicts is to remove all conflicts by modifying the conflicting rules[21]. Thus the cloud

based firewall must be configured so as to support the distributed processing environment and handles the conflicts of policy rules and still effectively detects the anomalies coming along with the rule formations [3]. Now with the rapid development of cloud based environment the security control is getting more complex. Among them handling firewall in distributed environment is quite a tedious job.

All it aims is towards making the high data availability, privacy and reliability over the trusted third party based systems. While serving its goals there is various mechanisms such as authentication, access control, encryption, privacy preserving, digital certificates etc. It includes network access control and directory level security control[22].

III. SECURITY ISSUES FOR CLOUD COMPUTING

Controlling scheduling, data and resource allocation are the problems faced while providing security to the cloud environment[3]. Hence to provide control to the seeker for scheduling and resource allocation and to provide ownership to the data owner, the cloud computing security need to deploy several security authorities. This technique is known as an authority coordinator. It is mainly required in securing the data in cloud computing environment [4].Following are the security concerns:

- **Data Security***:* The logical and physical data control can be provided in this concern. Phishing, virtualization, denial of service leakage of data and loss of encryption keys are also concerned[24].
- **Traditional security***:* This security concern includes network and computer attacks on cloud environment [23].
- **Privacy and Legal Issues***:* This concern is necessary while dealing with globally distributed networks [6].
- **Third-party data control***:* This concern is very transparent, difficult and well understandable because third party in cloud environment who holds all the applications and the data[25].
- **Availability***:* This involves critical applications and data that are available on cloud [5]. It can also be used to reallocate to other provider, long-term viability of the cloud [6].

IV. PROPOSED CLOUD COMPUTING SECURITY USING VPN

Our proposed system is providing a secure delivery of data packets to the cloud and fetching data packets from the cloud. Virtual Private Network is one of the technologies used to provide secure data transfer on cloud environment[13]. These principles are applied on remote access networks and wired LAN and also to wireless LAN. To make sure the data transmission security VPN designates standard encryption algorithms. With the support of IP security VPN is implemented. This is the standardized way for implementing VPN. The VPN and IPsecurity has reconstructed and established well[26].

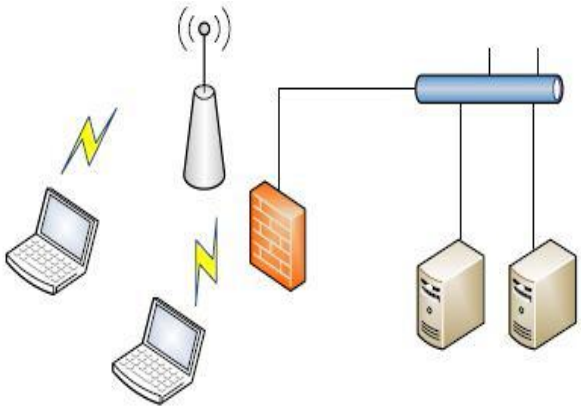

Figure 1: VPN usage within IPsecurity.

Figure 1, illustrates the combination of Virtual Private Network and IPsecurity. Firewall is used in networks which filters the incoming data packets and lies between outside world and the internal network. Since firewall is employed on public network and it plays an vital role in security strategy development, firewall can be used with VPN[27].

SaaS applications can be grouped into maturity models that are determined by the following characteristics: scalability, Configurability via metadata, and multi-tenancy. In the first maturity model, each customer has his own customized instance of the software. This model has drawbacks, but security issues are not so bad compared with the other models. In the second model, the vendor also provides different instances of the applications for each customer, but all instances use the same application code. In this model, customers can change some configuration options to meet their needs [7].

In the third maturity model multi-tenancy is added, so a single instance serves all customers. This approach enables more efficient use of the resources but scalability is limited. Since data from multiple tenants is likely to be stored in the same database, the risk of data leakage between these tenants is high. Security policies are needed to ensure that customer's data are kept separate from other customers .For the final model, applications can be scaled up by moving the application to a more powerful server if needed[28].

Data security is a common concern for any technology, but it becomes a major challenge when SaaS users have to rely on their providers for proper security .In SaaS, organizational data is often processed in plaintext and stored in the cloud. The SaaS provider is the one responsible for the security of the data while is being processed and stored [8]. Also, data backup is a critical aspect in order to facilitate recovery in case of disaster, but it introduces security concerns as well[29].

V. NETWORK SIMULATION SCENARIOS

The network simulation uses OPNET simulator which provides number of scenarios to learn the system performance in different situations[30]. To provide cloud security in different scenarios and to study the VPN performance, the cloud environment has designed with VPN and without VPN .By combining VPN with firewall, we can also see firewall effects in providing cloud security. FTP, HTTP and Email applications are the three applications treated with each scenario [9].In simulation we have assumed that each server is represented as each department. The cloud is examined in respect of delay, throughput to find the effect of VPN and firewall on cloud environment[14]. Some of the specifications used are:

i) **Two access points***:* this has 4 serial lines and 2 Ethernet interface.
ii) **VPN configuration***:* used to allow application access from remote source to server application.
iii) **No. of workstations***:* this shows the number of network clients on the internet.
iv) **Two servers***:* this has point to point server.
v) **Firewall***:* prevents unauthorized access to all application.
vi) **Two IP routers**: this has a router with eight serial line interface and four Ethernet interfaces.

5.1. Scenario 1: Cloud computing without firewall and VPN

In first scenario[31], two BSS are configured by connecting N-number of workstations to Access Point1 and Access Point 2.These two access points are connected to IP cloud that is connected to Router D by PPP-DS1 in turn connected by PPP-DS1 to Router S by PPP-DS1 which is connected by PPP-DS1 to two Servers namely Server AA and Server BB which is used to represents two departments. The scenario layout and architecture is shown in below figure.

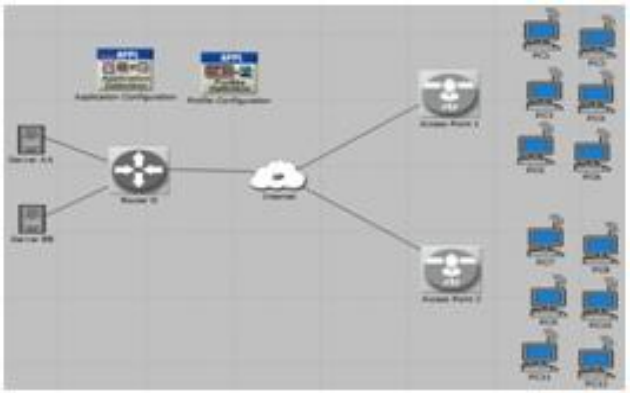

Figure 2.The architecture and layout of scenario 1

5.2. Scenario 2: Cloud computing with firewall only

In second scenario[32] also, two BSS are configured by connecting workstations to Access Point1 and Access Point 2. These access points are connected to Router S by PPP-DS1 in turn connected by PPP-DS1 to internet cloud connected to Firewall-ethernet2_slip8_firewall by PPP-DS1 which protects servers from outside access to the Email server [10]. The firewall is then connected to the Server AA and Server BB by PPP-DS1. Figure 3, shows the layout and architecture of this scenario.

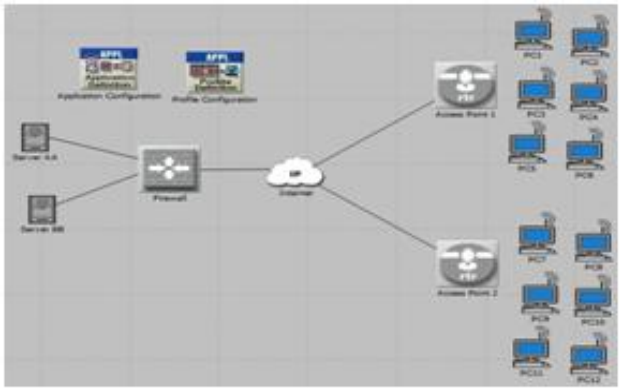

Figure 3. The architecture and layout of scenario 2

5.3. Scenario 3: Cloud computing with firewall and VPN

In scenario three also, two BSS are configured by connecting workstations to Access Point1 and Access Point 2. These access points are connected to Router S by PPP-DS1 in turn connected by PPP-DS1 to internet cloud connected to Firewall to D Router which is connected by PPP-DS1 to the Server. Figure 4, shows the layout and architecture of scenario 3.In second scenario, nevertheless of the traffic source; to prevent external access to server we have used firewall [10]. But in this case, any one of the clients from Access Point1 can access server AA by using VPN tunnel. Since IP packets are encapsulated inner side of an IP datagram, the firewall will not filter the incoming traffic which are created in Access Point1[36].

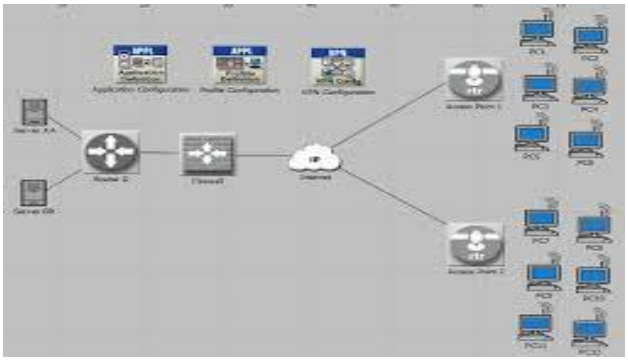

Figure 4. The architecture and layout scenario 3

VI. SIMULATION RESULTS AND SYSTEMS EVALUATION

The outcome of system evaluations shows the delay and throughput for the above three scenarios. Figure 5 and 6 illustrates the same[33]. The throughput for VPN is 107,819 = 1,782 seconds, whereas for systems with non existence of VPN we obtained the throughput of 299,131 bits/sec = 1,782 seconds. The system reaches 288,510 bits/sec = 1,782 seconds for the systems with non existence of Firewall and VPN. System Delay is the delay in the end to end delivery of packets in wireless LAN in the networks and the packets which are transferred to the next higher level [34]. Delay has reached to 0.001727, 0.001672, and 0.00169 = 1,782 seconds for the systems with no VPN, no firewall and VPN and with no firewall[35].

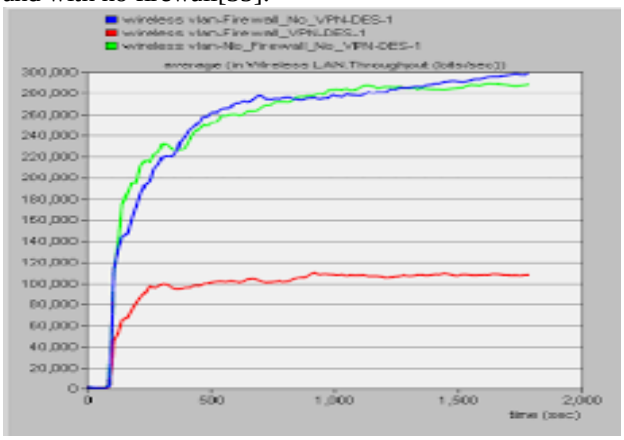

Figure 5. Throughput OVER scenario 1-3

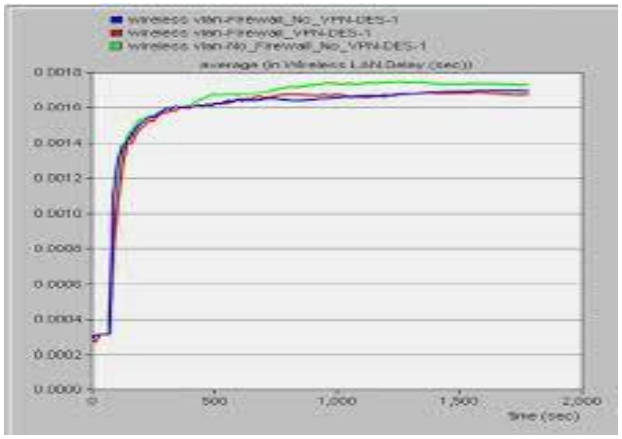

Figure 6. Delay over scenarios 1-3

VII. CONCLUSION

This study introduced VPN technology for securing cloud in wireless network. OPNET Modeler simulator was used as a simulation tools to investigate the impact of VPN and Firewall security systems on throughput, delay and traffic received on the system and individual nodes of the network [14].The applications considered for the mentioned investigation are e-mail application and web browsing application. The integration of VPN with Firewall in cloud computing will reduce the throughput. Furthermore, the delay in system without VPN is slightly larger than the cloud computing with VPN. No traffic received and sent from server AA for e-mail application in cloud computing with firewall and no VPN. VPN technology is a suitable way to secure cloud computing and decreasing the traffic in the system to achieve the security required. The security was provided in VPN technology should be provided with firewall that allows only specific access to the server.

REFERENCES

[1] Maneesha Sharma, Himani Bansal, Amit Kumar Sharma, "Cloud Computing: Different Approach & Security Challenge", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, pp. 421-424, March 2012.

[2] Young B. Choi, Jeffrey Muller et.el. M. Makarsky "Corporate wireless LAN security: threats and an effective security assessment framework for wireless information assurance", *Int. J. Mobile Communications, Vol. 4, No. 3, pp 266 – 290, 2006.*

[3] *Kevin Hamlen, Murat Kantarcioglu, Latifur Khan and Bhavani Thuraisingham, "*Security Issues for Cloud Computing*",* International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010.

[4] Richard Chow, Philippe Golle, Markus Jakobsson, Ryusuke Masuoka, Jesus Molina, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control", *CCSW'09*, November 13,2009, Chicago, Illinois, USA, pp. 85-90, 2009.

[5] Aderemi A. Atayero, Oluwaseyi Feyisetan, "Security Issues in Cloud Computing: *The Potentials of Homomorphic Encryption*", Journal of Emerging Trends in Computing and Information Sciences,VOL. 2, NO. 10, pp. 546-552, October 2011

[6] H. Bourdoucen, A. Al Naamany and A. Al Kalbani, "Impact of Implementing VPN to Secure Wireless LAN", World Academy of Science, Engineering and Technology 51, pp 625 – 630, 2009.

[7] Charlie Scott, Paul Wolfe, Mike Erwin, "Virtual Private Networks, Second Edition", O'Reilly, SecondEdition January pp 12, 1999.

[8] Weili Huang et.el , "The research of VPN on WLAN" ,International Conference on Computational and Information Sciences, 2010 IEEE, PP 250 – 253.

[9] M. Gouda and X. Liu, "Firewall Design: Consistency, Completeness, and Compactness," in Proceedings of the 24th International Conference on Distributed Computing Systems (ICDCS'04). IEEE Computer Society, 2004, p. 327

[10] A. Wool, "Architecting the lumeta firewall analyzer," in Proceedings of the 10th conference on USENIX Security Symposium-Volume 10. USENIX Association, 2001, p. 7.

[11] A. M. Chandrashekhar and K. Raghuveer, "Fusion of Multiple Data Mining Techniques for Effective Network Intrusion Detection – A Contemporary Approach", Proceedings of The 5th International Conference on Security of Information and Networks (SIN 2012), 2012, pp 33-37.

[12] A. M. Chandrashekhar and K. Raghuveer, "An Effective Technique for Intrusion Detection using Neuro-Fuzzy and Radial SVM Classifier", The Fourth International Conference on Networks & Communications (NetCom-2012), 22~24, Dec- 2012.

[13] A. M. Chandrashekhar and K. Raghuveer , "Intrusion Detection Technique by using K-means, Fuzzy Neural Network and SVM classifiers", 2013 IEEE International Conference on Computer Communication and Informatics (ICCCI -2013), 4~06,Jan2013, IEEE Catalog Number: CFP1308R-ART, ISBN Number: 978-1-4673-2907-1.

[14] A. M. Chandrashekhar and K. Raghuveer, "Confederation of FCM Clustering, ANN and SVM Techniques of Data mining to Implement Hybrid NIDS Using Corrected KDD Cup Dataset", IEEE International Conference on Communication and Signal Processing (ICCSP),2014, pp 672-676.

[15] A. M Chandrashekhar A M and K. Raghuveer, "Hard Clustering Vs. Soft Clustering: A Close Contest for Attaining Supremacy in Hybrid NIDS Development", Proceedings of International Conference on Communication and Computing (ICC - 2014), Elsevier science and Technology Publications.

[16] A. M. Chandrashekhar and K. Raghuveer, "Amalgamation of K-means clustering algorithem with standard MLP and SVM based neural networks to implement network intrusion detection system", Advanced Computing, Networking, and Informatics –Volume 2(June 2014), Volume 28 of the series Smart Inovation, Systems and Technologies pp 273-283.

[17] A. M Chandrashekhar A M and K. Raghuveer, "Diverse and Conglomerate Modi-operandi for Anomaly Intrusion Detection Systems", International Journal of Computer Application (**IJCA)** Special Issue on "Network Security and Cryptography (NSC)", 2011.

[18] A. M. Chandrashekhar and K. Raghuveer, "Performance evaluation of data clustering techniques using KDD Cup-99 Intrusion detection data set", International Journal of Information and Network Security (**IJINS**), ISSN: 2089-3299, Vol-1, No.4, October 2012, pp. 294~305.

[19] A. M. Chandrashekhar and K. Raghuveer, "Fortification of hybrid intrusion detection system using variants of neural networks and support vector machines", International Journal of Network Security & Its Applications (IJNSA) Volume.5, Number 1, January 2013.

[20] A. M. Chandrashekhar and K. Raghuveer , "Improvising Intrusion detection precision of ANN based NIDS by incorporating various data Normalization Technique – A Performance Appraisal", International Journal of Research in Engineering & Advanced Technology(IJREAT), Volume 2, Issue 2, Apr-May, 2014.

[21] Puneeth L Sankadal ,A. M Chandrashekhar A M, Prashanth Chillabatte, "Network Security situation awareness system" International Journal of Advanced Research in Information and Communication Engineering (IJARICE), Volume 3, Issue 5, May 2015.

[22] Prashanth G M, A.M.Chandrashekhar, Anjaneya Bulla, "Secured infrastructure for multiple group communication" International Journal of Advanced Research in Information and Communication Engineering (IJARICE), Volume 3, Issue 5, May 2015.

[23] Sowmyashree K.K, A.M.Chandrashekhar, Sheethal R.S, "Pyramidal aggregation on Communication security" International Journal of Advanced Research in Computer Science and Applications (IJARCSA), Volume 3, Issue 5, May 2015.

[24] Huda Mirza Saifuddin, A.M.Chandrashekhar, Spoorthi B.S, "Exploration of the ingredients of original security" International Journal of Advanced Research in Computer Science and Applications(IJARCSA), Volume 3, Issue 5, May 2015.

[25] A. M. Chandrashekhar, Arpitha, Nidhishree G, "Efficient data accessibility in cloud with privacy and authenticity using key aggregation cryptosystem", International Journal for Technological research in Engineering (IJTRE), Volume 3, Issue 5, JAN-2016.

[26] A. M. Chandrashekhar, Hariprasad M, Manjunath A, "The Importance of Big Data Analytics in the Field of Cyber Security", *International journal of scientific Research and Development (IJSRD),Volume 3, Issue 11, JAN-2016.*

[27] A. M. Chandrashekhar, Chitra K V, Sandhya Koti, "Security Fundamentals of Internet of Things", *International Journal of Research (IJR**),** Volume 3, Issue no1, JAN-2016**.***

[28] A. M. Chandrasekhar, Jagadish Revapgol, Vinayaka Pattanashetti, "Security Issues of Big Data in Networking", International Journal of Scientific Research in Science, Engineering and Technology (*IJSRSET),* Volume 2, Issue 1, JAN-2016.

[29] A. M. Chandrashekhar, Anjana D, Muktha G, Cyberstalking and Cyberbullying: Effects and prevention measures", Imperial Journal of Interdisciplinary Research (IJIR) ,Volume 2, Issue 2, JAN-2016.

[30] A. M. Chandrashekhar, Sahana K, Yashaswini K, "Securing Cloud Environment using Firewall and VPN", "International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Volume 6, Issue-1, January-2016.

[31] Syed Tahseen Ahmed,A.M.Chandrashekhar, Rahul N, "Analysis of Security Threats to Database Storage Systems" International Journal of Advanced Research in data mining and Cloud computing(IJARDC), Volume 3, Issue 5, May 2015.

[32] Yadunandan Huded, A.M.Chandrashekhar,Sachin Kumar H S, "Advances in Information security risk practices" International Journal of Advanced Research in data mining and Cloud computing (IJARDC), Volume 3, Issue 5 May 2015.

[33] Madhura S Hegde, A.M.Chandrashekhar, Aarabhi Putty, "A Survey:Combined impact of cryptography and steganography" International Journal of Engineering Research (IJOER), Volume 3, Issue 5, May 2015.

[34] Koushik P, A.M.Chandrashekhar, Jagadeesh Takkalakaki, "Information security threats, awareness and coginizance" International Journal for Technicle research in Engineering(IJTRE), Volume 2, Issue 9, May 2015.

[35] Rahil kumar Gupta, A.M.Chandrashekhar, Shivaraj H. P, "Role of information security awareness in success of an organization" International Journal of Research(IJR) Volume 2, Issue 6, May 2015.

[36] Siddeeq Y.Ameen,Shayma Wail Nourildean, "Firewall and VPN investigation on cloud computing performance" International Journal of Computer Science &Engineering survey(IJCSES) Volume 5,No 2,April 2014.

