Securing Cloud Environments through IPSec Virtual Private Networks and NSX Firewalls

Radha [1]**, Dr. Dinesh Kumar**[2]**,**

M-Tech Student[1,] *HOD* [2] *& Department of CSE & Shri Ram College of Engg. & Mgmt*
Palwal, Haryana, India

Abstract: Cloud Computing is a cost-efficient, flexible and proven delivery platform for supplying consumer or business IT facilities through the Internet. The primary interest is to enquire the effect of employing Virtual Private Network VPN integrated with firewall on the performance of cloud computing. Hence, computer simulation and modeling of cloud computing with OPNET modeler has been carried out for the states of cloud computing without and with firewall and VPN. Still, cloud Computing introduces an added degree of risk because necessary facilities are usually obtained to a third party, which builds it complicated to manage data privacy and security, provide support to data and service existence, and establish compliance. Cloud Computing advantages many techniques it also acquires their security challenges cloud includes defined communication with SLA based schemes for the service and resource usages. If someone breaks these rules the security level of system acquires compromised. Conventional system security is managed by the firewall. They are built for a fixed and static environment having restricted communications and policies. But in cloud computing environments the scenarios are modified completely and therefore the nature of firewall might also get adaptive according to requirement of cloud computing.

Keywords: ***Cloud computing, privacy, security, Virtual private Network, firewall.***

I. INTRODUCTION

The significance of Cloud Computing is growing and it is achieving a developing attention in the Industrial and scientific communities. Cloud Computing is the first technology among the top most significant technologies and with a best viewpoint being successive years by organizations and companies. It supplies centralized management to all the resources with explained schemes and their valuable assessments. It provides several evaluation resources as a service to the end subscriber. Resource can be of software or hardware type whose power and capacity can be disseminated among various processes. All its requirements an efficient console for examining all the services behavior. There are many problems linked with the conventional computing related to their scalability, reliability, fault tolerance, security and measurability. Among all, the security is the major issue which needs high concentration on the leading rules formulated by the resource users and policy makers. Cloud Computing performs as a distribution architecture as well as computational paradigm and its primary aim is to offer fast, protected, convenient data storage and net computing facility, with all computing resources pictured as services and provided on the Internet.

The cloud increases agility, collaboration, availability, scalability, capability to adapt to fluctuations with respect to accelerate development work, demand and offers potential for cost reduction through examined and effective computing.

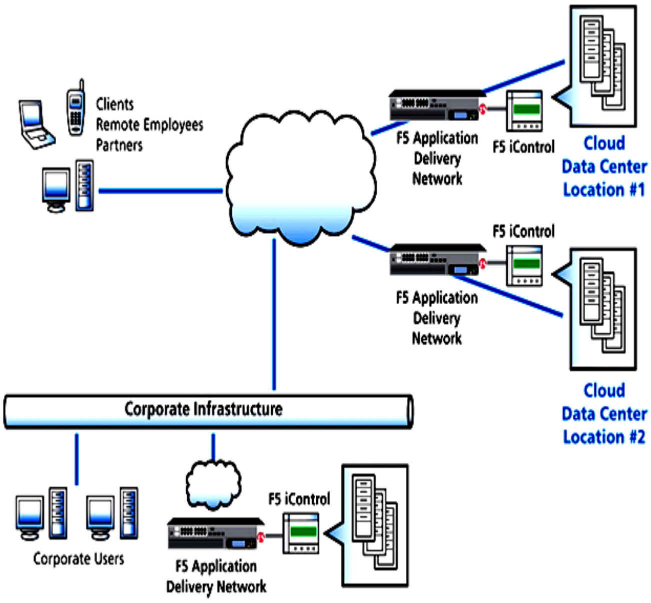
Clients
Remote Employees
Partners
F5 Application Delivery Network
F5 iControl
Cloud Data Center Location #1
F5 iControl
F5 Application Delivery Network
Cloud Data Center Location #2
Corporate Infrastructure
F5 iControl
Corporate Users
F5 Application Delivery Network

Figure 1: Cloud Computing Scenario

Cloud Computing integrates a number of computing technologies and concepts i.e. Web 2.0, Service Oriented Architecture (SOA), virtualization and other technologies which rely on the Internet, offering general business applications online by web browsers to fulfill the computing requirements of subscribers, while their data and software are collected on the servers . In some cases, Cloud Computing shows the growth of these technologies and is a marketing term to show that growth and the facilities they offer. Cloud is a well maintained group of resources whose power and capacity is combined or disseminated to fulfill the end users requirements. Here the resource facility supplied by the cloud supplier is visible to the application developed in cloud. It supports the remote access with fulfilling the rules of availability, capacity and partition logics. Hence such a massive processing needs dynamic management of the different type of resources at various positions. Now once the resources provide the parameters of processing then, the facts of assuring their processes and the kinds of user using these calculations remains to be solved. Cloud resources are offered as a service on required basis. The cloud itself generally involves high numbers of commodity-grade servers, harnessed to provide highly reliable and scalable on-demand facilities. The amount of resources offered in the cloud system for the subscribers is enhanced when they require more and reduce when they require less. The system must have a analysis against the subscribers, their behavior, systems authorization, intermediary Communication management, unauthenticated access, and attack prevention. Previously they are offered utilizing conventional firewalls. These firewalls are not utilized directly for cloud due to their different service architecture. Because the cloud offers resources scalability, deals with dynamic subscriber needs, offers everything defined by the service level agreements (SLA’s) etc. The cloud depending systems can ensure the data security and the subscriber does not have to look over the security parameters. So the cloud computing must assure the data security collected on the cloud system. In present, there are some companies which supply the cloud platforms i.e. VMware, Amazon, IBM, IBEMC Google and Microsoft. One of the main problems suffering cloud computing protection is the control by the data owner and the scheduling control and resource allocation. Hence a type of security authority require to be deployed by cloud computing security to offer the owner the control needed and the seeker the scheduling and allocation needed. This is called an authority coordinator and its existence is necessary to protect the data in the unauthenticated environment i.e. cloud computing.

II. DATA SECURITY IN CLOUD

The enterprises move to cloud and obtain the space for data buffering. This data buffering is certainly less expensive for them if compared to the in-house data buffering but the question is, if this data buffering in cloud is also protected and advantageous for enterprises. Thus, one of the most approaching tasks for enterprises is the data storage security. To understand the security problem in Cloud Computing, it is significant to know the Cloud Computing architecture. Once you know the Cloud Computing architecture then it becomes simpler to understand the data privacy and security problems and also to solve them. Mostly security problems which raise in Cloud Computing are the result of subscribers/enterprises control lacking on the physical infrastructure. Mostly enterprises don’t know where their data is physically buffered and which security techniques are in used to secure data such as whether the data is encrypted or not and if yes, which encryption technique is employed also if the link utilized for data to propagate in the cloud is encrypted and how the encryption keys are maintained (Window Security, 2010). Jensen et al. (2009) showed the technical security problems in Cloud Computing. Since, these problems are more associated with the issues of web browser and web services and not of Cloud Computing. These problems are still very significant to Cloud Computing as Cloud Computing builds a lot of usage of web services and subscribers depend on web browsers to access the facilities provided by the cloud. The most general attacks on web services involve the XML Signature Element Wrapping, where XML signature is utilized for authentication.

Browser Security is also a significant problem in Cloud Computing as in a cloud mostly computation is performed on remote servers and the client PC is only utilized for I/O, and commands authorization to cloud. Thus, standard web browser was a requirement of situation to forward I/O and this was used by different names: web 2.0, web applications or Software as Services (SaaS). Since, the ex of web browser arise the security questions. TLS (Transport Layer Security) is significant in this matter as it is utilized for data encryption and host authentication. XML encryption or XML signature cannot be utilized by browser directly as data can be only encrypted through signatures and TLS are only utilized with the TLS handshake. Thus, browser only supports as a passive data store as mentioned above, understanding the dependencies and relationships among Cloud Computing models is serious for understanding the security issues of it. For all the cloud facilities IaaS is the foundation and PaaS is made on it, while SaaS is made on PaaS and IaaS as explained in the cloud reference model diagram

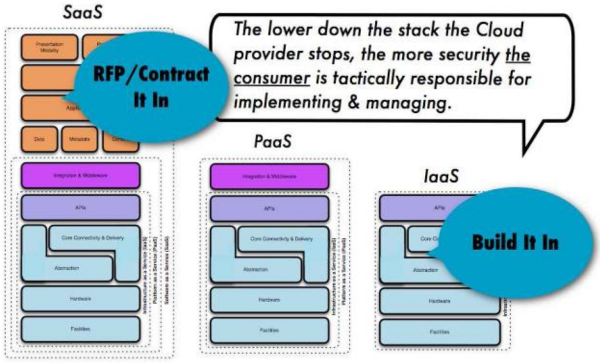
SaaS
RFP/Contract It In
The lower down the stack the Cloud provider stops, the more security the consumer is tactically responsible for implementing & managing.
PaaS
IaaS
Build It In
Presentation Modality
Data
Metadata
Integration & Middleware
APIs
Core Connectivity & Delivery
Abstraction
Hardware
Facilities
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)

Figure 2 – How Security Gets Integrated

III. SECURITY BENEFITS OF CLOUD COMPUTING

I have discussed about the data storage problems in Cloud Computing since; one must also view into the advantages of data buffering in Cloud Computing. Craig Balding in his blog ‘Assessing the Security advantages of Cloud Computing” discusses about these advantages. He addresses that there are some technical security statements in favor of Cloud Computing considering that we can discover the ways to handle the risks. European Network and Information Security Agency (ENISA) have also investigated on the advantages for enterprises using Cloud Computing. Cloud Computing has a lot of potential to enhance security for enterprises and the ways it can enhance security explained below.

Benefits of Scale

It is a fact that all kinds of security measures which are enforced on a larger scale are less expensive. Thus by using Cloud Computing enterprises obtains better security with same amount of money. The security involves all types of defensive measures i.e. patch management, filtering, human resources and their management and vetting, hardening of virtual machine instances, hardware and software redundancy, strong authentication, effective role-based access control and federated identity management solutions by default, which also enhances the network impacts of collaboration among several partners included in defense . Along with these advantages, other advantages involve:

Multiple Locations: The cloud suppliers by default have economic resources to repeat content and this increment the redundancy and independence from failure. Thus, it offers the disaster recovery.

Edge Networks: Cloud Computing offers quality, reliability increase and less local network issues for enterprises by having processing, storage and delivery nearer to the network edge.

Improved Timelines of Response (incidents): Cloud suppliers have larger to incidents or well-run-larger-scale systems. These systems support in enhanced timelines of response such as due to the early detection of new malware deployment, it can formulate more efficient and effective incident response.

Threat Management: The small enterprises don’t have resources to hire specialists for handling particular security problems but cloud suppliers can do that and offer better threat management.

Security as Market Differentiator: For mostly enterprises security is the most significant problem while moving to Cloud Computing. They make selections based on reputation of confidentiality, Cloud Computing advantages, risks and suggestions for information security resilience, integrity and security services provided by supplier. This drives Cloud Computing suppliers to enhance the security to compete in the market.

Standard Interfaces for Managed Security Services: Standardized open interfaces to managed security services (MSS) suppliers are usually offered by the large cloud suppliers. This provides more open market for security services where users can select or switch suppliers more easily with lesser setup costs. Thus, the more resources can be scaled in a granular manner without considering the system resources, the cheaper it gets to respond to sudden increments in requirement.

Rapid, Smart Scaling of Resources: There are already several cloud resources involving CPU time, storage, web service requests, memory and virtual machine instances which can be frequently scaled on requirement and as the technology is enhancing granular control over resource consumption is increasing. The cloud supplier also have the resources and the rights to dynamically reassign resources for traffic shaping, filtering, encryption etc, when an attack (e.g. DoS) is likely or occurs, to increase support for defensive measures. Thus, cloud suppliers can restrict the impact that some attacks have on the resources availability that legitimately hosted services utilized by the integrated use of dynamic resource assignment and suitable resource optimization techniques.

IV. PROPOSED APPROACH

The introduced system will try to offer protect delivery of data to and from the cloud. One of the considered technologies is the Virtual Private Network. With VPN private and protected sub networks can be established. This principle has been broadly employed in remote access network, wired local-area network and can be also employed to wireless local-area network. This will substitute Wired Equivalent Privacy solutions. It uses standard encryption algorithms to confirm the data transmission security. Moreover, VPN generally implemented with the help of IP security. This can be taken as the standard way for VPN implementation. The VPN and IP Security have reviewed and well demonstrated in this manner to offer the robust security standard with acceptable data authentication, confidentiality and access control not respect to the transmission medium. “By combining wireless LANs into an IPSec infrastructure, permits WLAN infrastructure to concentrate on simply transmitting wireless traffic, while the VPN would protect it,” as depicted in Figure 3.

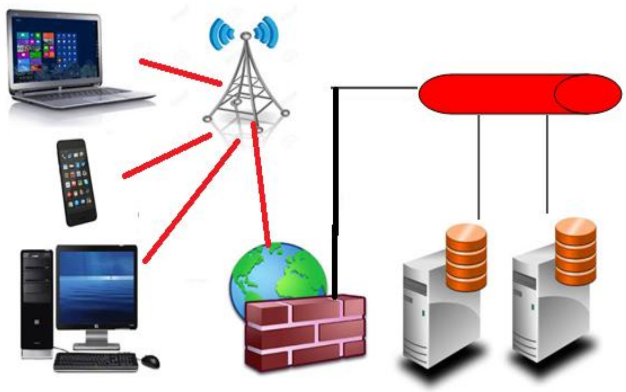

Figure 3: VPN usage within IP Security.

As displayed in Figure 3, firewall is employed in combination with VPN. The packet filtering firewall stands between the internal network and the outside world. The aim for employing the firewalls with the VPN is that firewall have been utilized on wide public networks for some years and are a high starting place in the establishment of a security mechanism and cloud computing can be considered as a public network . Applications are generally provided over the Internet by a Web browser. Still, faults in web applications may produce threats for the SaaS applications. Attackers have been utilizing the web to adjust with subscribers computers and perform harmful activities i.e. steal confidential data. Security issues in SaaS applications are same as any web application technology, but conventional security solutions do not efficiently secure it from attacks, so new mechanisms are essential. The Open Web Application Security Project (OWASP) has detected the ten most serious web applications security viruses. There are many security challenges, but it is a good beginning for protecting web applications. SaaS applications can be integrated into maturity models that are evaluated by the following features: configurability through metadata, scalability and multi-tenancy. In the first maturity model, every customer has his own customized illustrate of the software. This model has limitations, but security challenges are not so bad compared with another model. In the second model, the seller also offers different illustrations of the applications for every customer, but all illustrations employ the similar application code. In this model, customers can alter many configuration choices to satisfy their requirements. In the third maturity model multi-tenancy is summed up, so a single instance supports all subscribers.

This method enables more effective usage of the resources but scalability is restricted. However data from various tenants is likely to be collected in the same database, the danger of data leakage between these tenants is higher. Security mechanisms are required to confirm that subscriber data are hold separately from other subscribers .For the last model, applications can increased by locating the application to a strong server if required.

Data security is a general issue for every technology, but it becomes a major issue when SaaS subscribers have to depend on their suppliers for proper security .In SaaS, organizational data is generally worked in plaintext and collected in the cloud. The SaaS supplier is the one responsible for the data security while is being manipulated and collected. Also, data backup is a serious view for facilitating recovery in circumstances of disaster, but it presents security issues as well. Also cloud suppliers can subcontract other facilities i.e. backup from third-party service suppliers, which may raise issues. Furthermore, most compliance standards do not imagine compliance with regulations in a world of Cloud Computing. In the field of SaaS, the mechanism of compliance is complicated because data is positioned in the supplier datacenters, which may present regulatory compliance challenges i.e. segregation, data privacy and security, that must be implemented by the service provider. Accessing applications through the internet by web browser makes access from any network device easier, involving mobile devices and public computers. Since, it also discloses the service to extra security risks. The Cloud Security Alliance has released a document that explains the mobile computing current state and the top viruses in this area i.e. unprotected networks (WiFi), information stealing mobile malware, threats determined in the device OS and official applications, proximity-based hacking and unprotected marketplaces. PaaS provides deployment of cloud-based applications without the cost of purchasing and managing the underlying software and hardware layers . As with IaaS and SaaS, PaaS rely on a reliable and protected network and protect web browser. PaaS application security consists two software layers: Security of customer applications deployed on a PaaS platform and Security of the PaaS platform itself (such as runtime engine). PaaS suppliers are responsible for protecting the platform software stack that involves the runtime engine that operates the customer applications.

V. THEORETICAL BASIS AND LITERATURE REVIEW

Firewall enforces security employing the explained security policies which offers rules of filtering for the data conversions on the cloud network. The data which fulfills the security needs of the organization if permitted to propagate in the network and remained packets are blocked. The mechanism of configuring a firewall is error prone and tedious. The policy management is little complex task due to their dynamically altering thousands of the rules. They rules are contradictory in nature and might intersecting somewhere which explaining them in the system. Cloud needs open access to all the facilities over the data. Along with that it must fulfill the security needs. Hence it requires to be altered in such manner which fulfills all the features of the cloud so that security facility can be established. On the other side, because of the complicated nature of policy deviation, system managers usually suffered with a more challenging issue in solving deviations, particularly, resolving policy contradicts. These involve but not restricted to networks, operating systems, databases, resource scheduling, virtualization, transaction management, concurrency control, load balancing and memory management. In the last few ten years offered security to the networked solution alters suddenly. Now with the fast development of cloud depending environment the security control is becoming more complicated. Among them the firewall managing in disseminated environment is quite a complicated job. This section deals some of that implementation and ideas employing towards building the distributed firewall an efficient concept. The paper stresses on the cloud computing security issues and their effects on the application migrations and developments. It examines the cloud security breaches against the several applications and their working scenarios. The data collected in the cloud system can solve the problem of stolen and altered unlawfully. All it objective is towards building the high data availability, reliability and privacy over the authenticated third party based systems. While meeting its objectives there is several processes such as access control, authentication, encryption, digital certificates, privacy preserving etc. It involves directory level security control and network access control. The cloud computing supplier must make variety of steps to secure the network in order to efficiently solve these problems. We have conducted a systematic review of the available literature related to security in Cloud Computing, not only for summarizing the available threats and vulnerabilities related to this topic but also to detect and examine the current state and the most significant security challenges for Cloud Computing. The question stress was to detect the most relevant challenges in Cloud Computing which take into account threats, vulnerabilities, risks, needs and solutions of security for Cloud Computing.

The clients and users of cloud computing are based on their cloud supplier when it comes to their confidentiality or privacy. The supplier of the cloud computing services evaluates what policies are kept. Assume that these suppliers also have the capability to make modifications in their policies. It could entirely modify the privacy for clients. (For instance when the data inserted by the cloud subscribers is secured in the preliminary made up policy being employe). Modifying policies which will permit insight in this data for third parties could be a critical risk based on the significance of data that is being utilized (Gellman 2009). Another instance is that cloud suppliers could extract information from various organizations in the cloud. They could see information that could be by any means exploring. It could also determine information that is commercially important for them. What remains significant is that most cloud subscribers (clients) are normally not known of the entire policy and hence do not aware very well what risks they are revealed to when inserting their data into the cloud (Brodkin 2008).

This takes us to the next point where the problem stays in that cloud subscribers share their information with the cloud supplier. This is not the problem on itself, but there could (and are) policies in some particular situations that show that some information is not to be used with third parties (Gellman 2009). In this situation the third party would be the cloud supplier. There are many instances to think about; privacy policies consisting particular rules about sharing a client's personal information, i.e. address and phone number (Pearson 2009).

In [3] authors introduced a mechanism which can decrease the communication overhead between Virtual machines(VM) positioned in same server and utilized it with VDE networking to enhance the total read latency for a workload by up to 45%(such as read latest workload) in comparison of standard me cached .

In [5] authors carried out a review on how latency happens in various geographical area. Also exposed an analysis work of how various browsers offer different latency. A test carried out to present impact of bandwidth show that when one attempts to access cloud based Google docs in cybercafé or GPRS connection it took 20 sec while when attempted to open at the university campus which offers 5.4 mbps it opens in 2 sec. The latency problem in the cloud network will be resolved with the faster usage of 3g and 4g in the upcoming years.

In [8] authors attempted to highlight the simulation and modeling for many types of computer network attacks and their effect on computer networks. He described applications for simulation and modeling of computer network security. It shows a comprehensive suggestion to solve the modeling and simulating problem in the area of Information Security. He modeled the cloud network and conducted the botnet attack on one of the cloud applications such as FTP to examine the impact of the attack on FTP server.

In [4] authors suggested a security model for cloud based applications by carrying out a firewall utilizing two applications such as database application and web based application to model and examine the model efficiency. There are several benefits with the virtual machine implementation, where all the needed server operations are no more physical in nature and a group of virtual servers is employed in this circumstance.

VI. NETWORK SIMULATION SCENARIOS

The simulation mechanism utilizing of OPNET modeler employed in this research comprises of number of scenarios which shows the system performance in various situations. The cloud computing has been simulated with and without VPN to study the VPN performance and to study the impact of Firewall with VPN in the system to protect cloud in various scenarios. Every scenario has been submitted to three applications types (web browsing (HTTP), File Transfer (FTP) and Email applications). In the modeling, two servers introduced two departments have been considered. The effect of VPN and firewall on cloud computing has been analyzed in terms of load, throughput, delay, and traffic achieved. Further parameters utilized in these scenarios are:

1) Two access points: name wireless_ethernet_slip4_router, which had 4 serial line and two Ethernet interface.

2) No. of workstations: named (wlan_wkstn) which shows clients that communicate with internet.

3) Two IP router: named (ethernet4_slip8_gtwy), which show router with 8 serial line interface and 4 Ethernet interface. ip cloud: named (ip 32 clouds) which shows the Internet .

4) Two servers: named (PPP Server) which shows point to point server to present two departments.

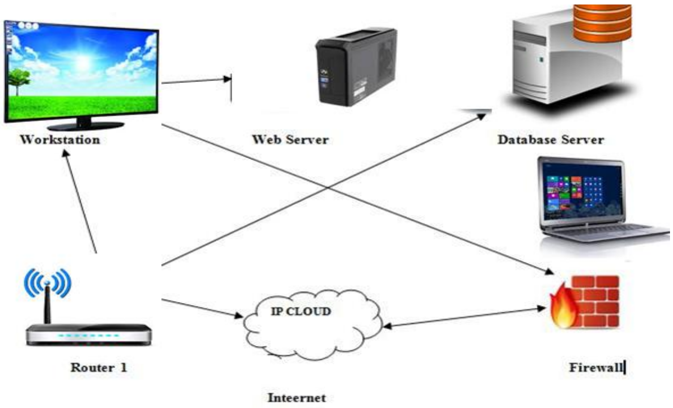

Figure 4: Cloud computing Using VPN and Firewall

5) Firewall: ethernet2_slip8_firewall, which prevent any access for the needed application to the server.

6) VPN configuration: VPN tunnel would be employed to permit particular clients from the source to access mentioned application from the server.

Links: named (PPP-DS1) to link the parameters employed for the simulated system. profile and application configuration to define the application of the system.

6.1. Scenario 1

This scenario shows cloud computing without VPN and firewall. In this scenario, number of workstations linked to two access points (Access Point 1, Access Point 2) which assembled two BSS. These access points linked by PPP-DS1 to Router S linked by PPP-DS1 to ip cloud (Internet) linked by PPP-DS1 to Router D linked by PPP-DS1 to two Servers (Server AA, Server BB) which shows two departments. The scenario architecture and layout is depicted in Figure 5.

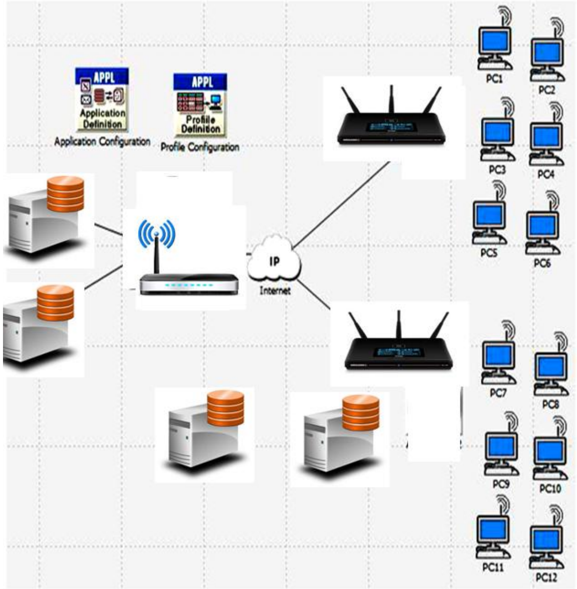

Figure 5: Architecture and layout of scenario 1

6.2 Scenario 2:

Cloud computing with firewall only Point 2) which assembled two BSS. These access points linked by PPP-DS1 to Router S linked by PPP-DS1 to ip cloud (Internet) linked by PPP-DS1 to Firewall named (ethernet2_slip8_firewall) which secure servers from any external access to the Email from the servers. This firewall linked by PPP-DS1 to the Server AA and Server BB. The architecture and layout of scenario 2 is depicted in Figure 5.

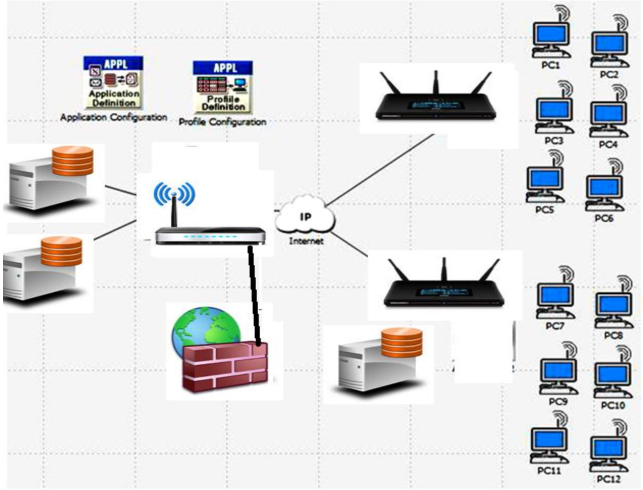

Figure 6: Architecture and Layout of scenario 2

6.3. Scenario 3:

Cloud computing with VPN and firewall. In this scenario, number of workstations linked to two access points (Access Point 1, Access Point 2) which assembled two BSS. These access points linked by PPP-DS1 to Router S linked by PPP-DS1 to ip cloud (Internet) linked by PPP-DS1 to Firewall to Router D linked by PPP-DS1 to the Server. The layout and architecture scenario 3 is depicted in Figure 7. In the previous scenario, firewall was employed to prevent any external access to email of server disregarding the traffic source. In this scenario, the VPN tunnel would be utilized to permit one of the clients (PCs) from Access Point1 to access Email from the server AA. The firewall will not filter the traffic produce by Access Point1 because the IP packets in the tunnel will be enclosed into an IP datagram.

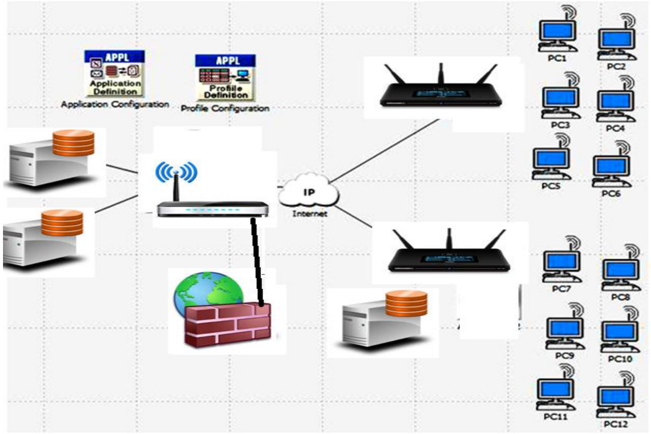

Figure 7: Architecture and layout of scenario 3

VII. CONCLUSION

This study presented VPN technology for protecting cloud in wireless network. The applications assumed for the explained investigation are web browsing and e-mail application. The combination of VPN with Firewall in cloud computing will decrease the throughput. This is due to the number of bit transmitted per second is lower than the cloud computing without VPN. Because the VPN with firewall would not permit each access to the server. Moreover, the delay in system without VPN is little greater than the cloud computing with VPN. No traffic obtained and forwarded from server AA for e-mail application in cloud computing with firewall and no VPN. This is due to firewall would prevent any email access to the server AA and the availability of VPN in the system would permit mentioned stations (PC's) to access server AA. Still, there would be no traffic achieved and forwarded for server BB in (firewall no VPN) and in (VPN firewall) systems. This is now because VPN behaves as a tunnel to permit email access to server AA only. VPN technology is a proper way to protect cloud computing and reducing the traffic in the system to obtain the security needed. The security was offered in VPN technology should be supplied with firewall that permits only particular 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, Christopher V. Kopek and Jennifer 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] Songjie, Junfeng Yao, Chengpeng Wu, “Cloud computing and its key techniques”, International Conference on Electronic & Mechanical Engineering and Information Technology, pp. 320-324, 12-14 August, 2011.

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

[5] 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. , ACM 978-1-60558-784-4/09/11, pp. 85-90, 2009.

[6] 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.

[7] Weili Huang, Fanzheng Kong , “The research of VPN on WLAN” , International Conference on Computational and Information Sciences, 2010 IEEE, pp. 250 – 253.

[8] 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.

[9] Charlie Scott, Paul Wolfe, Mike Erwin, “Virtual Private Networks, Second Edition”, O'Reilly, Second Edition January pp 12, 1999.

[10] E. Al-Shaer and H. Hamed, “Discovery of policy anomalies in distributed firewalls,” in INFOCOM 2004., vol. 4. IEEE, pp. 2605–2616.

[11] L. Yuan, H. Chen, J. Mai, C. Chuah, Z. Su, P. Mohapatra, and C. Davis, "Fireman: A toolkit for firewall modeling and analysis," in 2006 IEEE Symposium on Security and Privacy, 2006, pp. 15-20.

[12] S. Ioannidis, A. Keromytis, S. Bellovin, and J. Smith, "Implementing a distributed firewall," in Proceedings of the 7th ACM conference on Computer and communications security. ACM, 2000, pp. 199-204.

[13] A. Hari, S. Suri, and G. Parulkar, "Detecting and resolving packet filter conflicts," in IEEE INFOCOM, 2000, pp. 1203–1212

[14] A. Wool, "Trends in Firewall Configuration Errors: Measuring the Holes in Swiss Cheese," IEEE Internet Computing, vol. 14, no. 4, pp. 58–65, 2010.

[15] E. Lupu and M. Sloman, "Conflicts in policy-based distributed systems management," IEEE Transactions on Software Engineering, vol. 25, no. 6, pp. 852–869, 1999.