International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Providing Security and Privacy in Cloud Computing Using Distributed Firewall and VPN

Dr. Chinthagunta Mukundha[1], Dr. I. Surya Prabha[2]

[1]Associate Professor, IT Department, Sreenidhi Institute of Science and Technology, Hyd -500043, Andhra Pradesh, India

[2]Professor, IT Department, Institute of Aeronautical Engineering, Hyd -500043, Andhra Pradesh, India

Abstract: ***Cloud Computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. The main interest is to investigate the impact of using Virtual Private Network VPN together with firewall on cloud computing performance. Therefore, computer modeling and simulation of cloud computing with OPNET modular simulator has been conducted for the cases of cloud computing with and without VPN and firewall. However, cloud Computing presents an added level of risk because essential services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability, and demonstrate compliance. Cloud Computing leverages many technologies it also inherits their security issues cloud involves defined interaction with SLA based policies for the resource and service usages. If someone violates these rules the protection level of system gets compromised. Traditional security of the system is handled by the firewall. They are made for a static and fixed environment having limited policies and interactions. But in cloud environments the scenarios are changed totally and hence the behavior of firewall might also get adaptive as per the need of cloud computing.***

Keywords: Cloud Computing, security, privacy ,firewall, Virtual Private Networks

1. Introduction

The importance of Cloud Computing is increasing and it is receiving a growing attention in the scientific and Industrial communities. Cloud Computing as the first among the top most important technologies and with a better prospect in successive years by companies and organizations.

It provides centralized control over all the resources with defined policies and their quantitative assessments. It offers various computation resources as a service to the end user. Resource can be of hardware of software type whose capacity and power can be distributed among different processes. All its needs an effective console for analyzing the behavior of all the services. There are some problems associated with the traditional computing related to their reliability, scalability, fault tolerance, measurability and security. Among them, the security is the one area which requires high emphasis on the guiding rules developed by the policy makers and resource users.

Cloud Computing appears as a computational paradigm as well as a distribution architecture and its main objective is to provide secure, quick, convenient data storage and net computing service, with all computing resources visualized as services and delivered over the Internet . 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 .

Cloud Computing combines a number of computing concepts and technologies such as Service Oriented Architecture (SOA), Web 2.0, virtualization and other technologies with reliance on the Internet, providing common business applications online through web browsers to satisfy the computing needs of users, while their software and data are stored on the servers . In some respects, Cloud Computing represents the maturing of these technologies and is a marketing term to represent that maturity and the services they provide .

Cloud is a well managed group of resources whose capacity and power is merged or distributed to satisfy the end users needs. Here the resource service used by the cloud provider is transparent to the application developed in cloud. It serves the remote access with satisfying the rules of capacity, availability and partition logics. Here the task time. Thus such a massive processing requires dynamic handling of the heterogeneous resources at different locations. Now once the resources serve the processing parameters then, the issues of verifying their processes and the types of user utilizing these computations is remains to be solved. Cloud resources are provided as a service on an as needed basis. The cloud itself typically includes large numbers of commodity-grade servers, harnessed to deliver highly scalable and reliable on-demand services. The amount of resources provided in the cloud system for the users is increased when they need more and decrease when they need less.

The system must have a check against the users, their behaviour, systems authenticity, intermediate Communication handling, unauthorized access, and attack prevention. Previously they are provided using traditional firewalls. These firewalls are not used directly for cloud because of their different service architecture. Because the cloud provides scalability of resources, handles dynamic user demands, provides everything guided by the defined service level agreements (SLA's) etc. 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. Today's, there are many companies which provides the cloud platforms such as Amazon, VMware, EMC Google, IBM and Microsoft.

One of the major problems facing cloud computing security is the control by the data owner and the resource allocation and scheduling control. Thus a form of security authority need to be deployed by cloud computing security to provide the owner the control required and the seeker the allocation and scheduling required. This is called an authority coordinator and its presence is essential to secure the data in the untrusted environment such as cloud computing.

2. Theoretical Basis and Literature Review

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. 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. 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. 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.

In spite of adoption of cloud computing by Google and other well known powerful computing resources users. This adoption will increase heavily because of the high demand on computing resources in search engine or data warehouses and data mining. This demands comes from the large increase in computing and multimedia in every day duties. However, cloud computing users should aware of security threats that can occur because cloud computing uses networks to grant access to the resources required. Thus any security threats that might occur with network might be occurred with cloud computing. In this aspects researches have been conducted and developed to provide security for cloud computing. Furthermore, the security of cloud computing should consider security issues and technologies related all the field encompasses the cloud computing infrastructure. These include but not limited to networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. During the last few decades providing security to the networked solution is changes abruptly. Now with the rapid development of cloud based environment the security control is getting more complex. Among them t he firewall handling in distributed environment is quite a tedious job. This section covers some of that implementation and suggestions applying towards making the distributed firewall an effective concept.

The paper focuses on the cloud computing security problems and their impacts on the application development and migrations. It analyses the cloud security breaches against the various applications and their working scenarios. The data stored in the cloud system can meet the problem of stolen and modified unlawfully. 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. The cloud computing provider must make variety of measures to protect the security in order to effectively solve these problems.

We have carried out a systematic review of the existing literature regarding security in Cloud Computing, not only in order to summarize the existing vulnerabilities and threats concerning this topic but also to identify and analyze the current state and the most important security issues for Cloud Computing.

The question focus was to identify the most relevant issues in Cloud Computing which consider vulnerabilities, threats, risks, requirements and solutions of security for Cloud Computing. This question had to be related with the aim of this work; that is to identify and relate vulnerabilities and threats with possible solutions. Therefore, the research question addressed by our research was the following: What security vulnerabilities and threats are the most important in Cloud Computing which have to be studied in depth with the Purpose of handling them? The keywords and related concepts that make up this question and that were used during the review execution are: secure Cloud systems, Cloud security, delivery models security, SPI security, SaaS security, Paas security, IaaS security, Cloud threats, Cloud vulnerabilities, Cloud recommendations, best practices in Cloud.

3. Proposed Cloud Computing Security Using VPN and Firewall

The proposed system will attempt to provide secure delivery of data to and from the cloud. One of the adopted technology is the Virtual Private Network. With VPN private and secured sub networks can be constructed. This principle has been widely applied in wired local-area network , remote access networks and can be also applied to wireless local-area network. This will replaces Wired Equivalent Privacy solutions. It adopts standard encryption algorithms to ensure the security of data transmission. Furthermore, VPN usually implemented with the aid of IP security . This can be considered as the standard way for VPN implementation. The IPSecurity and VPN have revised and well established in this way to provide the robust security standard with acceptable data confidentiality, authentication, and access control regardless of the transmission medium. “By integrating wireless LANs into an IPSec infrastructure, allows WLAN infrastructure to focus on simply transmitting wireless traffic, while the VPN would secure it,” as shown in Figure 1 .

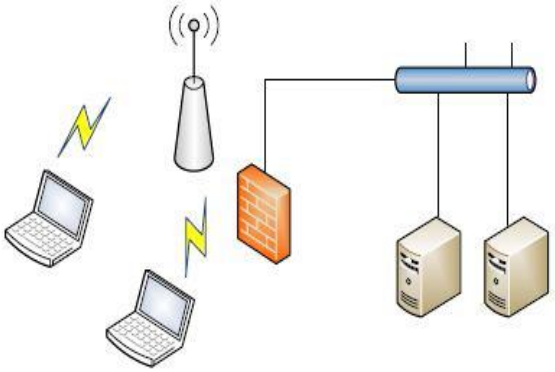

Figure 1: VPN usage within IPSecurity.

As shown in Figure 1, firewall is used in conjunction with VPN. The firewall is a packet filtering that stands between the internal network and the world outside. The reason for the usage of firewalls with the VPN is because firewall have been employed on large public networks for many years and are a great starting place in the development of a security strategy and cloud computing can be regarded as a public network .

Applications are typically delivered via the Internet through a Web browser. However, flaws in web applications may create vulnerabilities for the SaaS applications. Attackers have been using the web to compromise user's computers and perform malicious activities such as steal sensitive data. Security challenges in SaaS applications are not different from any web application technology, but traditional security solutions do not effectively protect it from attacks, so new approaches are necessary. The Open Web Application Security Project (OWASP) has identified the ten most critical web applications security threats. There are more security issues, but it is a good start for securing web applications.

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. 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.

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. Also, data backup is a critical aspect in order to facilitate recovery in case of disaster, but it introduces security concerns as well. Also cloud providers can subcontract other services such as backup from third-party service providers, which may raise

Concerns. Moreover, most compliance standards do not envision compliance with regulations in a world of Cloud Computing. In the world of SaaS, the process of compliance is complex because data is located in the provider's datacenters, which may introduce regulatory compliance issues such as data privacy, segregation, and Security, that must be enforced by the provider.

Accessing applications over the internet via web browser makes access from any network device easier, including public computers and mobile devices. However, it also exposes the service to additional security risks. The Cloud Security Alliance has released a document that describes the current state of mobile computing and the top threats in this area such as information stealing mobile malware, insecure networks (WiFi), vulnerabilities found in the device OS and official applications, insecure marketplaces, and proximity-based hacking.

PaaS facilitates deployment of cloud-based applications without the cost of buying and maintaining the underlying hardware and software layers . As with SaaS and IaaS, PaaS depends on a secure and reliable network and secure web browser. PaaS application security comprises two software layers: Security of the PaaS platform itself (i.e., runtime engine), and Security of customer applications deployed on a PaaS platform . PaaS providers are responsible for securing the platform software stack that includes the runtime engine that runs the customer applications.

The Virtual Machine Monitor (VMM) or hypervisor is responsible for virtual machines isolation; therefore, if the VMM is compromised; its virtual machines may potentially be compromised as well. The VMM is a low-level software that controls and monitors its virtual machines, so as any traditional software it entails security flaws.Keeping the VMM as simple and small as possible reduces the risk of security vulnerabilities, since it will be easier to find and fix any vulnerability.

Moreover, virtualization introduces the ability to migrate virtual machines between physical servers for fault tolerance, load balancing or maintenance. This useful feature can also raise security problems . An attacker can compromise the migration module in the VMM and transfer a victim virtual machine to a malicious server. Also, it is clear that VM migration exposes the content of the VM to the network, which can compromise its data integrity and confidentiality. A malicious virtual machine can be migrated to another host (with another VMM) compromising it.

4. Network Simulation Scenatious

The simulation procedure using of OPNET simulator adopted in this research consists of number scenarios which study the performance of the system in different cases. The cloud computing has been modeled with and without VPN

to study the performance of VPN and to study the effect of Firewall with VPN in the system to secure cloud in different scenarios. Each scenario have been subjected to three applications types (File Transfer (FTP), web browsing (HTTP) and Email applications). In the simulation, two servers represented two departments have been assumed. The impact of firewall and VPN on cloud computing has been investigated in terms of throughput, load , delay , and traffic received .

Further parameters used in these scenarios are:

1) Two access points: named (wireless_ethernet_slip4_router), which had two Ethernet interface and 4 serial line.
2) No. of workstations: named (wlan_wkstn) which represent clients that communicate with internet.
3) Two IP router: named (ethernet4_slip8_gtwy), which represent router with 4 Ethernet interface and 8 serial line interface.ip cloud: named (ip 32 clouds) which represents the Internet .
4) Two servers: named (PPP Server) which represents point to point server to represent two departments.
5) Firewall: ethernet2_slip8_firewall, which prevent any access for the required application to the server.
6) VPN configuration: VPN tunnel would be used to allow specific clients from the source to access specified application from the server.

Links: named (PPP-DS1) to connect the parameters used for the modeled system.profile and application configuration to define the application of the system.

4.1. scenario 1: cloud computing without firewall and vpn

In this scenario, number of workstations connected to two access points (Access Point 1, Access Point 2) which configured two BSS. These access points connected by PPP-DS1 to Router S connected by PPP-DS1 to ip cloud (Internet) connected by PPP-DS1 to Router D connected by PPP-DS1 to two Servers (Server AA, Server BB) which represents two departments. The scenario architecture and layout is as shown in Figure 2.

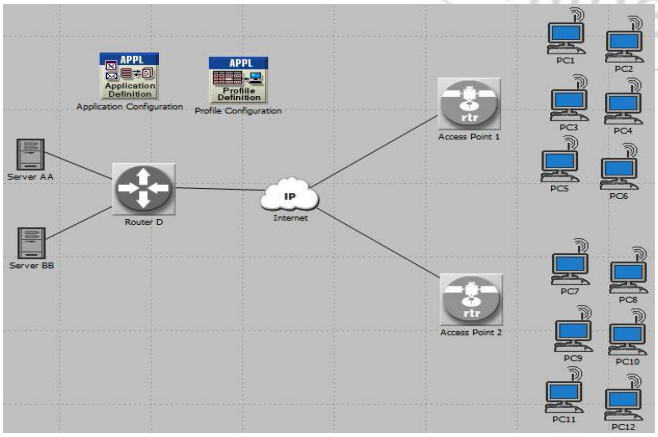

Figure 2: Architecture and layout of scenario 1

4.2. Scenario 2: Cloud computing with firewall only

Point 2) which configured two BSS. These access points connected by PPP-DS1 to Router S connected by PPP-DS1 to ip cloud (Internet) connected by PPP-DS1 to Firewall named (ethernet2_slip8_firewall) which protect servers from any external access to the Email from the servers. This firewall connected by PPP-DS1 to the Server AA and Server BB. The architecture and layout of scenario 2 is as shown in Figure 3.

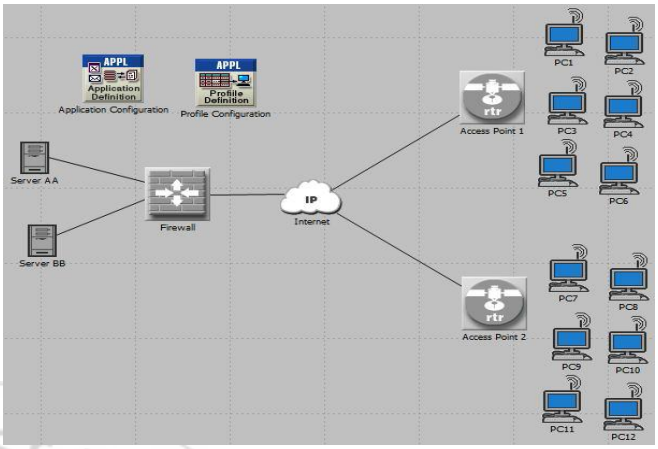

Figure 3: Architecture and Layout of scenario 2

4.3. Scenario 3: Cloud computing with firewall and VPN

In this scenario, number of workstations connected to two access points (Access Point 1, Access Point 2) which configured two BSS. These access points connected by PPP-DS1 to Router S connected by PPP-DS1 to ip cloud (Internet) connected by PPP-DS1 to Firewall to Router D connected by PPP-DS1 to the Server. The architecture and layout scenario 3 is shown in Figure4. In the previous scenario, firewall was used to prevent any external access to email of server regardless the source of the traffic. In this scenario, the VPN tunnel would be used to allow one of the clients (PCs) from Access Point1 to access Email from the server AA. The firewall will not filter the traffic created by Access Point1 because the IP packets in the tunnel will be encapsulated inside an IP datagram.

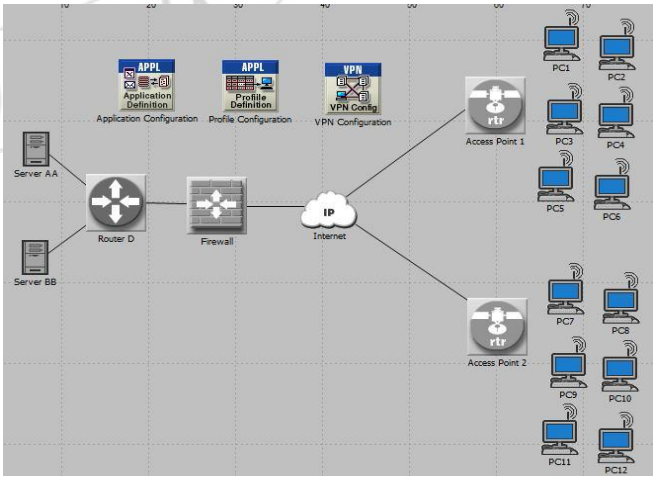

Figure 4: Architecture and layout of scenario 3

5. 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. 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. This is because the number of bit transmitte per second is less than the cloud computing without VPN. because the VPN with firewall would not allow every access to the server. 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. This is because firewall would prevent any email access to the server AA and the existence of VPN in the system would allow specified stations (PC's) to access server AA. However, there would be no traffic received and sent for server BB in (VPN firewall) and (firewall no VPN) systems. This is now because VPN acts as a tunnel to allow email access to server AA only. 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, 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), 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, p. 15.
[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, p. 199.
[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.
[16] G. Misherghi, L. Yuan, Z. Su, C.-N. Chuah, and H. Chen, "A general framework for benchmarking firewall optimization techniques," IEEE Transactions on Network and Service Management, vol. 5, no. 4, pp. 227–238, Dec. 2008.
[17] A. Mayer, A. Wool, and E. Ziskind, "Fang: A firewall analysis engine," in IEEE Symposium on Security and Privacy. IEEE Computer Society, 2000, pp. 177–189.
[18] J. Alfaro, N. Boulahia-Cuppens, and F. Cuppens, "Complete analysis of configuration rules to guarantee reliable network security policies," International Journal of Information Security, vol. 7, no. 2, pp. 103–122, 2008.
[19] F. Baboescu and G. Varghese, "Fast and scalable conflict detection for packet classifiers," Computer Networks, vol. 42, no. 6, pp. 717– 735, 2003.
[20] R. Reeder, L. Bauer, L. Cranor, M. Reiter, K. Bacon, K. How, and H. Strong, "Expandable grids for visualizing and authoring computer security policies," in Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems. ACM, 2008, pp. 1473–1482.
[21] 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.
[22] I. Herman, G. Melanc¸on, and M. Marshall, "Graph visualization and navigation in information visualization: A survey," IEEE Transactions on Visualization and Computer Graphics, pp. 24–43, 2000.
[23] A. Wool, "Architecting the lumeta firewall analyzer," in Proceedings of the 10th conference on USENIX Security Symposium-Volume 10. USENIX Association, 2001, p. 7.

Author Profile

Dr.Chinthagunta Mukundha, Associate Professor, Department of Information Technology, Sreenidhi Institute of Science and Technology, HYD-501301, AP, India.

.

Dr. I. Surya Prabha, Professor,Department of Information Technology ,Institute of Aeronautical Engineering, HYD-500043, AP, India.