Volume 6, Issue 4, April 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# Analysis of Network and Firewall Security Policies in Dynamic and Heterogeneous Networks

**Kirori Mindo, Caroline Sogomo, Nickson M. Karie**
Department of Computer Science, Kabarak University,
Nakuru, Kenya

***Abstract - Managing network and system security in today's highly dynamic and complex technological environments is challenging task. This is backed up by the fact that the technological revolution around the world is no longer a myth but a reality. Organisations have been forced to enhance the existing network security and firewall framework to cater for technological metamorphosis in various ways. With several daily changes in technology, network security professionals have also been forced to constantly change firewalls, routers and other network device configurations to keep up with this technological pace. While network changes are necessary for applications and users, they are extremely risky from the point of view of network security as well as the business continuity plan. For this reason, this paper, presents an analysis of network security and firewall policies in a dynamic and heterogeneous network environment and tries to identify any existing gaps. Organisations with geographically distributed offices with heterogeneous security infrastructure are the most affected and hence require unique network security and firewall policies. This is because; such large institutions at times need to open up their networks and network applications to outside clients. For this reason a constant review of network security and firewall policies is inevitable so as to cater for the high risks involved.***

***Keywords - Network Security, Heterogeneous Network Environment, Network Infrastructure, Firewall Policies***

## I. INTRODUCTION

A bigger percentage of modern network security changes are as a result of application and network connectivity requirements. With the complexity of today's computer network technologies, having a good network security policy helps to ease the configuration of different networks and simplifies network management as well [1]. However, incorrect and inefficient network security and firewall configurations can cause serious security breaches and network vulnerabilities [2].

If firewalls are not carefully configured, for example, they can have a significant impact on service security and availability [2]. Firewall help to prevent the threats found in the internet from spreading to the internal network by limiting outgoing and incoming connections [3]. Dynamic secure-conscious organizations however need to re-look into their network security and firewall policies to conform to the best confidentiality, integrity and availability requirements so as to offer the best services as well.

Emerging and fast growing organisations tend to change their hardware and software assets rapidly, as the organisations activities expand. Due to these frequent changes and evolution, information security is also required to evolve [5]. In this case, organizations with geographically distributed offices with heterogeneous security infrastructure are the most affected and hence require unique network security policies. This is because; such large institutions at times need to open up their networks and network applications to outside clients and other business partners besides implementing a wide range of security services in a heterogeneous computer network environment [6]. For this reason a constant review of network security and firewall policies is inevitable so as to cater for the high risks involved. In addition, any network interaction exposes internal processes to the outside with numerous vulnerabilities [7]. This paper therefore looks into the issues of network security and firewall policies in dynamic and heterogeneous network environment and tries to identify any existing gaps.

As for the remaining part of this paper, section II presents taxonomy of basic network security and firewall policy. In section III a review of ISO-Functional models are explained, followed by a discussion of the firewall security policies in section IV. Encryption and authorization is considered in Section V, while conclusions are drawn in section VI and mention is made of future research work.

## II. NETWORK SECURITY POLICY

Network security and firewall policies as well as mechanisms usually target domains within which they operate, indicating the general topographical component of the network in which security or protection is proven to be effective [9]. In this section of the paper though, the authors explain the network security component first and later on in section III the firewall security is discussed in brief.

It is evident today that Internet use has become more and more widespread according to [10] and so has the significance of the network security field. It is for this reason that new approaches to hardware and software security

 

need to be intensely researched and developed to deal with new threats [11]. Unfortunately, there exists a communication gap between network security developers who describe the core essential elements required to ensure good network security and developers of networks and network technologies [8]. Such a gap can be amplified in enormous ways especially in dynamic organizations where computer networks scales frequently. As such, a robust network security policy should be put in place to manage any gaps that may crop up. Such a policy begins with assessing risks and commensurate responses needed to mitigate these risks. Further, updating the policy vigorously and its continuation will need change management practice and continuous monitoring of the available network for violations [32].

Any network typically has a varying class of devices which are prone to security violations [30]. This may include but not limited to the following; distribution network devices (Switches, repeaters), core network devices (Routers, Layer 3 switches), network file servers, A/V servers (Asterisk PBX), access network devices (Firewalls), network monitoring devices System Logs (SYSLogs), Read only Memory (RMON) probes and Simple Network Management Protocol (SNMP) monitors), network security devices (TACAS+ and Radius Servers), network print servers, eMail systems, database management servers (mySQL, Oracle, Sybase) and network application servers (DNS servers and DHCP servers) [31]. Fig. 1 below sourced from David [48] expounds on some of the various essential elements of a secure network design that cut across both network and security technologies.

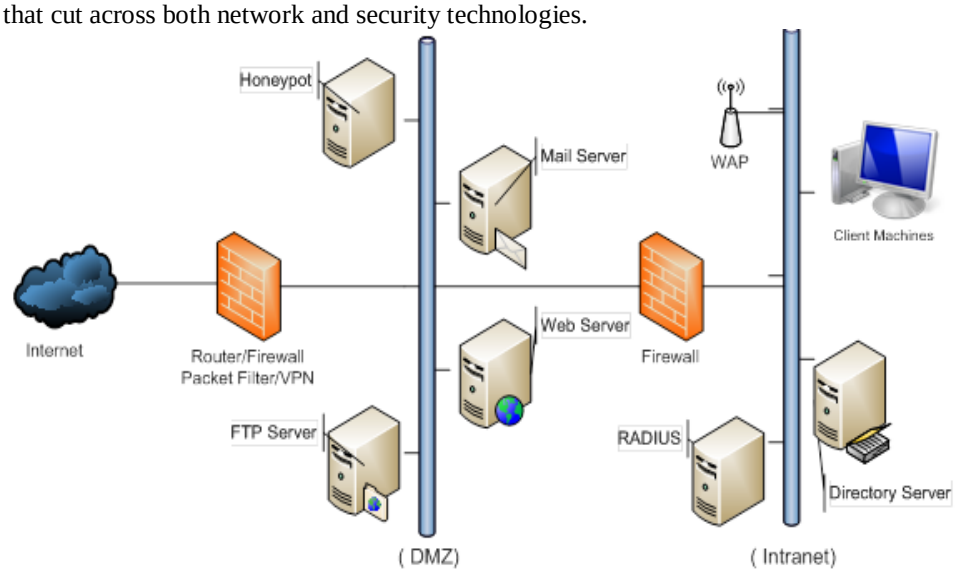


Fig 1: Essential Elements in a Secure Network (David Basham, [48])

**Note:** *Adapted from "David Basham's Network Security Portfolio". Secure Network Design. Retrieved March 15, 2016, from www.dpbasham.com: http://www.dpbasham.com/portfolio/demonstrate/secure-network-design/*

In the case of a new network security policy, the initial policy document can be segmented into:

- Preparation,
- Conducting a risk analysis and
- Forming a security team structure [33].

During the preparation stage users roles and responsibilities as well as privilege levels are defined. It should also clearly map the general user community, with the various demographics. A typical network will have the following types of users:

- Administrators,
- Privileged,
- Users,
- Partners among Others [34].

The second stage of the policy entails conducting a risk analysis. This involves identifying portions of the network, assigning a threat rating to each portion in the following way [35]:

**a)** **Low Risk:** Considered low risk if systems compromised do not disrupt the business nor cause legal or financial ramifications. Further, targeted data or systems require quite a moderate process of restoration to full optimum disposition.

**b)** **Medium Risk:** Considered medium risk if systems compromised causes moderate disruption and the targeted data or systems require a moderate process of restoration to full optimum disposition.

**c)** **High Risk:** Considered high risk if systems compromised causes severe and extreme disruption and the targeted data or systems require an extremely elaborate process of restoration to full optimum condition [35].

Lastly, the last segment of the network security should entail creating a competent cross-functional security team that are familiar with the network security policy and have a great knowledge of the network topology, security design and implementation as well. In this segment, there is a need for the security team to perform various tests and risk

 

analysis through various ways including penetration testing [36], mock DOS and DDOS attacks [37], review security alerts and identify the various security violations. Fig. 2 below describes the various stages of Network Security Policy Set-Up that may be used. The next section explains the firewall security policy

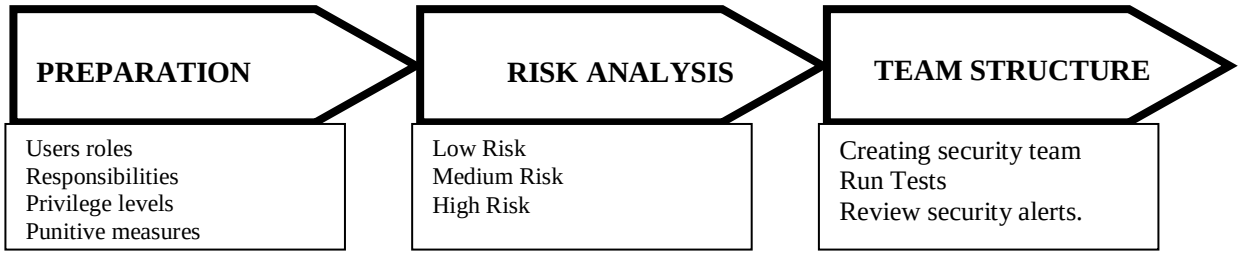


Fig 2: Various Stages of Network Security Policy Set-Up (Kirori, Sogomo & Karie, 2015)

## III. FIREWALL SECURITY POLICY

Firewalls perform many different jobs in modern networks, forwards traffic between two or more local networks within an organization or enterprise routes [39]. Interior routers may impose some restrictions on the traffic they forward between networks. Forwards traffic between different enterprises sometimes called different 'autonomous systems. The traffic between the different networks that make up the Internet is directed by backbone routers [40].

There are various critical steps organizations should take to ensure that their firewall security policy is indeed robust and secure. Some of the steps that organizations should consider include: building of physical connections, identify who is authorized to install, de-install, move both the router and firewall, and to change the physical configuration or physical connections to the router or firewall [46]. Policy designates should also consider assigning individuals who are permitted to access resources past the firewall router via the console or remotely via telnet. Remote login or secure shell (SSH) or other direct access port connections should also be controlled. Organizations should define the password policy for user/logins, and for administrative or privilege passwords [21]. In addition, it is critical to designate individuals permitted to and perform remote management and monitoring facilities via SNMP. It is equally critical to configure and enable secret password for console, auxiliary port, and VTY ports on each network device. This will prevent unauthorized access direct to any network devices from both external and internal threats [22].

There are various types of firewalls with the most common being the Security Group Firewall which segments the firewall in punter groups with similar filtering requirements. A Cloud-based Web Application Firewall helps in controlling access to web applications while communicating through HTTP and in accordance to authorization rules with the objective of stopping XSS, SQL injection or similar attacks. A Packet Filter Firewall filters incoming and outgoing network traffic based on packet IP address while Proxy-based (Network Application) Firewall checks and filters incoming and outgoing network packets based on the type of application service is use, which is represented by a proxy. A Stateful Firewall permit/deny incoming and outgoing network traffic based on state information derived from the previous traffic to avoid checking all the packets in a connection [42]. The next section presents a review of ISO-functional models for network security

## IV. REVIEW OF ISO-FUNCTIONAL MODELS FOR NETWORK SECURITY

There exist several ISO-functional models for network security some of which are briefly explained below.

### *A. Network Security Model (NSM)*

The SANS Institute introduced in2008, a seven layer Network Security Model (NSM) which divides the overwhelming task of securing a network infrastructure into seven manageable segments such that if and when an attack on a network has succeeded it is much easier to locate the underlying issue and fix it with the use of the Network Security Model (NSM) [39].

The model provides a technique of implementing basic security measures from a top-bottom model. The layers involved herein are; Physical, Virtue Local Area Network (VLAN), Access Control List (ACL), Software, User, Administrative and Information Technology (IT) Department layers. This model also articulates how to mitigate initial and long-term attacks by invoking various procedures in the physical and logical layers. This model however does not integrate the use of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) in protecting and filtering packets into the network.

### *B. The Universal Composability (UC) model*

The Universal Composability (UC) model framework looks at ensuring a very strong composition theorem. As a result, once a protocol is proved secure, it can be used in indiscriminate environments recalling its security properties. This particular attribute enables users to split a protocol into smaller subroutines so that the security of each sub-routine can be analysed separately, making the security of the overall protocol much easier [12].

This model has various advantages including propagation of a simple analysis by breaking the complex system into small stand alone components. The model also provides stronger security especially where some components are unknown. This model provides a general methodology of asserting certain security attributes of protocols such as sequential evaluation, concurrency and subroutine calls [12].

 

### *C. Generalized Universal Composability (GUC) framework*

The Generalized Universal Composability (GUC) framework improves on the UC security notion and enables re-establishment of its initial native security guarantees even for protocols that use global trusted setups. GUC enables the guarantee that secure protocols will provide the same level of deniability as the task specification they implement [17]. The GUC framework can be implemented successfully to prove its efficiency in propagating secure cryptographic systems in complex network systems such as the internet.

### *D. The Public Key Infrastructure (PKI)*

The Public Key Infrastructure (PKI) is an established model with a set of hardware, software, people, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. PKI ensures data security, confidentiality, and integrity; Public Key Infrastructure is an essential component of today's business systems [18]. Ijaz [46] in 2012 proposed a method whereby users employ a predictive model that is held by a third party, without compromising private information. The Public Key Infrastructure (PKI) is also crucial in mitigating interruption which renders systems unusable, interception and man-in-the-middle attacks and message modification or fabrication as well.

The Public Key Infrastructure (PKI) also implements three critical infrastructures namely; Single Certificate Authority (SCA) Architecture, Enterprise Public Key Infrastructure (EPKI) Architecture and Hybrid Public Key Infrastructure (HPKI) Architecture. The Public Key Infrastructure (PKI) also supports Pretty Good Privacy (PGP) and the certificates in PGP keys and its key rings.

### *E. The Model for Cryptosystem Using Neural Network*

Cryptography uses mathematical techniques for information security. The Model for Cryptosystem Using Neural Network is a two stage model. In the first stage, neural network-based pseudo-random numbers (NPRNGs) are generated and the results are tested for randomness using randomness tests. In the second stage, a neural network-based cryptosystem is designed using NPRNGs. In this cryptosystem, data, which is encrypted by non-linear techniques, is subject to decryption attempts by means of two identical artificial neural networks (ANNs). These tests were run by the National Institute of Standard Technology (NIST). Further, [20] tested neural networks that are trained on their mutual output to match an identical weight value. The next section finally explains encryption and authorization as related to network security.

## V. ENCRYPTION AND AUTHORIZATION

Encryption and authorization is an approach to ensure the confidentiality and integrity of data by encoding messages or information that only authorized users can access and view it [41].

Encrypting all passwords by using MD5 encryption helps to prevent the attacks and hacker from recovery [29]. It is particularly important to disable idle processes and ports, to deny possible access routes through which an attack can be launched. Administrators should set the minimum character length for all routers and firewall passwords. This provides enhanced security access to the router by allowing you to specify a minimum password length ventured into by Kamila et al [44] LSB Steganography and Cryptography using chaotic neural network is combined together to provide high security to the message during communication in an unsecure channel. Enabling Transmission Control Protocol (TCP) keep lives on incoming connections; this can help guard against both malicious attacks and orphaned sessions caused by remote system crashes. Disabling all non-IP-based remote access protocols, and using SSH, SSL, or IP Security (IPSec) encryption for all remote connections to the router instead of TELNET can provide complete VTYs protection [43].

Access control lists can be used to reject all traffic from the internal networks that bears a source IP address which does not belong to the internal networks, reject all traffic from the external networks that bears a source address belonging to the internal networks and reject all traffic with a source or destination address belonging to any reserved, unrouteable, or illegal address range [23].

Network administrators can implement Proxy ARP; network hosts use Address Resolution Protocol to translate network addresses into media addresses [24]. A router can act as intermediary for ARP, responding to ARP queries on selected interfaces and thus enabling transparent access between multiple LAN segments. This service is called proxy ARP since it interrupts the LAN security firewall. The Simple Network Management Protocol (SNMP) is the standard Internet protocol for remote monitoring and administration. It is critical that network deploys SNMP within its infrastructure [25]. Ethereal is a network traffic capture and analysis tool that simulates real inspection network penetration tests and attacks on the targeted network. Nmap program scans for open TCP and UDP ports on a router and firewall interface ports.

The attack and hacker use a port scanner tools to estimate the network topology map, resources therein so as to gauge the strength of hardware and software applications running [26]. The Nessus program which runs on Linux operating system searches for vulnerabilities in the network and lists the topology map as well. To protect the network from such Nessus reconnaissance attacks. It is critical to disable idle features and services on routers such as: CDP, http server, bootp server, IP broadcasts, and TCP and UDP ports. A network admin should try to implement remote login services like TELNET to breach and access resources beyond the firewall. Dsniffis a collection of tools that perform ARP spoofing to simulate a DoS and DDoS attacks, can be managed by applying access control lists on router and firewall to filtering the malicious traffic packets, and reject all traffic from the internal networks that bears a source IP address which does not belong to the internal networks [27]. Kiwi Syslog identifies, captures and preserve log messages

 

from firewalls, routers and many other network devices, this action prevented by Disabling some protocols on the network devices, such as finger protocol requests, Network Time Protocol and Cisco Discovery Protocol.

## VI. CONCLUSION

There has been a growing appetite for technology, and thus new challenges have been witnessed as well as revolutionary advances in network technology. However these advancements bring with it several new network security challenges. While old, conventional network security mechanisms are incompetent to overcome these challenges, they actually abet and facilitate attackers in finding weaknesses and thus taking advantages of a network. This paper has delved into various Network and Firewall security policies in dynamic and heterogeneous networks as a way to help understand the evolving network security mechanism that evolves with the scaling and metamorphosis of technology . This was done so as to avoid the deficiency of conservative mechanisms and security threats that emanate with the dispensation. More research however is needed in this area of study so as to identify or develop new and advanced tool to cab the existing gaps in the Network and Firewall security policies.

## REFERENCES


[1] Abbes, T., Bouhoula, A., & Rusinowitch, M. (2015).Detection of firewall configuration errors with updatable tree. *International Journal of Information Security*, 1-17.

[2] Basile, C., &Lioy, A. (2015). Analysis of Application-Layer Filtering Policies With Application to HTTP. *Networking, IEEE/ACM Transactions on*, *23*(1), 28-41.

[3] Abbes, T., Bouhoula, A., &Rusinowitch, M. (2015).Detection of firewall configuration errors with updatable tree. *International Journal of Information Security*, 1-17.

[4] Lara, A., Kolasani, A., & Ramamurthy, B. (2014). Network innovation using openflow: A survey. *Communications Surveys & Tutorials, IEEE*, *16*(1), 493-512.

[5] Daya, B. (2013). Network security: History, importance, and future. *University of Florida Department of Electrical and Computer Engineering*.

[6] Irvine, C., & Levin, T. (1999).Toward a taxonomy and costing method for security services. In *Computer Security Applications Conference, 1999.(ACSAC'99) Proceedings. 15th Annual* (pp. 183-188). IEEE.

[7] Landwehr, C. E., &Goldschlag, D. M. (1997). Security issues in networks with Internet access. *Proceedings of the IEEE*, *85*(12), 2034-2051.

[8] Falch, P. B. (2011). Investigating passive operating system detection.

[9] Hamed, H., & Al-Shaer, E. (2006).Taxonomy of conflicts in network security policies. *Communications Magazine, IEEE*, *44*(3), 134-141.

[10] Kumar, S. N. (2015). Review on Network Security and Cryptography. *Science and Education*, *3*(1), 1-11.

[11] Trisal, N., Thakur, S., &Pawar, S. (2015). A New Approach-Network Security.*International Journal of Research*, *2*(5), 287-292.

[12] Canetti, R. (2001, October). Universally composable security: A new paradigm for cryptographic protocols. In *Foundations of Computer Science, 2001.Proceedings. 42nd IEEE Symposium on* (pp. 136-145). IEEE.

[13] Canetti, R. (2013). Universally Composable Security: A New Paradigm for Cryptographic Protocols.

[14] Pass, R. (2003). On deniability in the common reference string and random oracle model.In *Advances in Cryptology-CRYPTO 2003* (pp. 316-337).Springer Berlin Heidelberg.

[15] Walfish, S. (2008). *Enhanced security models for network protocols*. ProQuest.

[16] Yao, A. C., Yao, F. F., & Zhao, Y. (2007, May).A Note on the Feasibility of Generalized Universal Composability⋆. In *Theory and Applications of Models of Computation: 4th International Conference, TAMC 2007, Shanghai, China, May 22-25, 2007, Proceedings* (Vol. 4484, p. 474). Springer Science & Business Media.

[17] Dodis, Y., Katz, J., Smith, A., &Walfish, S. (2009). Composability and on-line deniability of authentication.In *Theory of Cryptography* (pp. 146-162).Springer Berlin Heidelberg.

[18] Choudhury, S., Bhatnagar, K., &Haque, W. (2002). *Public key infrastructure implementation and design*.John Wiley & Sons, Inc.

[19] Xie, P., Bilenko, M., Finley, T., Gilad-Bachrach, R., Lauter, K., &Naehrig, M. (2014). Crypto-Nets: Neural Networks over Encrypted Data. *arXiv preprint arXiv:1412.6181*.

[20] Wang, D. (2015). Neural Synchronization Using Genetic Algorithm for Secure Key Establishment. *Journal of Engineering Science and Technology Review*,*8*(2), 152-156.

[21] Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., ...&Cranor, L. F. (2010, July). Encountering stronger password requirements: user attitudes and behaviors.In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (p. 2).ACM.

[22] Wasden, M. B., Arya, V., Miner, D. M., Laurent, D. M. S., &Boltz, D. T. (2015). *U.S. Patent No. 9,037,074*. Washington, DC: U.S. Patent and Trademark Office.

[23] Knauf, A., Waehlisch, M., Schmidt, T. C., &Hege, G. (2015). A Usage for Shared Resources in RELOAD (ShaRe).

[24] Cho, H., Kang, S., & Lee, Y. (2015, January). Centralized ARP proxy server over SDN controller to cut down ARP broadcast in large-scale data center networks. In *Information Networking (ICOIN), 2015 International Conference on*(pp. 301-306). IEEE.


 

[25] Duke, M., Blanton, E., Zimmermann, A., Braden, R., & Eddy, W. (2015). A roadmap for transmission control protocol (TCP) specification documents.

[26] Carthern, C., Wilson, W., Bedwell, R., & Rivera, N. (2015).Introduction to Network Penetration Testing.In *Cisco Networks* (pp. 759-772).Apress.

[27] Sharma, J., & Singh, M. (2015). Web Services Oriented Architecture for DPI based Network Forensics Grid.

[28] Zhou, H., Wu, C., Jiang, M., Zhou, B., Gao, W., Pan, T., & Huang, M. (2015). Evolving defense mechanism for future network security. Communications Magazine, IEEE, 53(4), 45-51.

[29] Dudykevych, V., Piskozub, A., &Lomnytskyj, I. (2014).MODERN APPROACH TO PROTECTION OF COMPUTER SYSTEMS AND NETWORKS. *International Journal of Computing*, *2*(3), 113-118.

[30] Nayak, A. K., Reimers, A., Feamster, N., & Clark, R. (2009, August). Resonance: dynamic access control for enterprise networks. In *Proceedings of the 1st ACM workshop on Research on enterprise networking* (pp. 11-18).ACM.

[31] Mulky, A. G. (2013). Distribution challenges and workable solutions. *IIMB Management Review*, *25*(3), 179-195.

[32] Network Security Policy: Best Practices White Paper. (2005, October 04). . [Online]. Available, from http://www.cisco.com/c/en/us/support/docs/availability/high-availability/13601-secpol.html / Retrieved March 14, 2016

[33] Scarfone, K., Jansen, W., & Tracy, M. (2008). Guide to general server security. *NIST Special Publication*, *800*, 123.

[34] Potenzone, C. S., Schwegel, J., & Manning, D. F. (2008). *U.S. Patent No. 7,363,372*. Washington, DC: U.S. Patent and Trademark Office.

[35] Cohen, G., Meiseles, M., &Reshef, E. (2005). *U.S. Patent No. 6,952,779*. Washington, DC: U.S. Patent and Trademark Office.

[36] Hong, J., Chen, Y., Liu, C. C., &Govindarasu, M. (2015).Cyber-Physical Security Testbed for Substations in a Power Grid. In *Cyber Physical Systems Approach to Smart Electric Power Grid* (pp. 261-301). Springer Berlin Heidelberg.

[37] Suryawanshi, N. A., &Todmal, S. R. (2015).DDoS Attacks Detection of Application Layer for Web Services using Information based Metrics.*International Journal of Computer Applications*, *117*(9).

[38] Huang, J., Nicol, D. M., Bobba, R., & Huh, J. H. (2012, June).A framework integrating attribute-based policies into role-based access control.In*Proceedings of the 17th ACM symposium on Access Control Models and Technologies* (pp. 187-196).ACM.

[39] T. I. (2005, December). Network Security Model (NSM). Retrieved March 16, 2016, from https://www.sans.org/reading-room/whitepapers/modeling/network-security-model-32843

[40] Ioannidis, S., Keromytis, A. D., Bellovin, S. M., & Smith, J. M. (2000, November). Implementing a distributed firewall.In *Proceedings of the 7th ACM conference on Computer and communications security* (pp. 190-199).ACM.

[41] Tsai, J., & Moors, T. (2006, July). A review of multipath routing protocols: From wireless ad hoc to mesh networks. In *ACoRN early career researcher workshop on wireless multihop networking* (Vol. 30).

[42] Song, Y., & Pang, Y. (2014). Leveraged BMIS Model for Cloud Risk Control.*JIPS*, *10*(2), 240-255.

[43] Fernandez, E. B., Yoshioka, N., & Washizaki, H. (2014).Patterns for cloud firewalls. *AsianPLoP (pattern languages of programs), Tokyo*.

[44] Parent, F., &Steudler, O. (2016). Managing Cisco Network Security Building Rock-Solid Networks.

[45] N. K. Kamila, Haripriya Rout, Nilamadhab Dash, Stego- Cryptography Using Chaotic Neural Network, *American Journal of Signal Processing*, Vol. 4 No. 1, 2014, pp. 24-33. doi: 10.5923/j.ajsp.20140401.04.

[46] Wack, J., Cutler, K., & Pole, J. (2002). *Guidelines on firewalls and firewall policy*. BOOZ-ALLEN AND HAMILTON INC MCLEAN VA.

[47] Ijaz, I. (2012). Design and implementation of PKI (for multi domain environment). *International Journal of Computer Theory and Engineering*,*4*(4), 505.

[48] David Basham, (2012). Secure Network Design. [Online]. Available: http://www.dpbasham.com/portfolio/demonstrate/secure-network-design/ [Retrieved March 15, 2016]

 