International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Implementing Different Set of Network Security Policies for a Well Infrastructure Campus Network

Faqarunnisa Begum[1], Dr. Suvarna Nandyal[2]

[1]Student, Computer Network Engineering, PDA College of Engineering Kalaburagi, Karnataka, India

[2]HOD, Computer Science Engineering, PDA College Of Engineering Kalaburagi, Karnataka, India

Abstract: ***A typical college network has several number of sub-networks or subnets which corresponds to different departments or sections of the organization. These sub-networks are interconnected through Layer-3 network devices or routers. The services accessed by these sub-networks within the subnet internally and outside the subnets externally are usually governed by the set of network security policies. A network security for an organization at every level in day to day life is an important aspect. In order to provide the security for a college campus here in this paper a topology is designed and implemented with the set of network security policies. There are different levels of Access Control List-ACL rules for the student, staff and network administrator to protect their sub-network. To prevent unauthorized access to the resources, appropriate security policies have been implemented in the Campus Area Network-CAN. The network admin, teachers and the student uses the college resources provided by the two servers i.e. FTP-File Transfer Protocol server and the WEB server. To further enhance the security, the different methods of network security like use of separate subnets, VLAN, ACL, VTP, routing protocols, access control list etc., have been used.***

Keywords: Campus Area Network-CAN, ACL, Network Security Policies, Cisco routers, switches, VLAN

1.Introduction

The CAN- Campus Area Network is about designing a topology of a college network that is a Local Area Network-LAN where a college network is having around 3000 students and 100 staff members. They are arranged in such a way that they can communicate with each other and interact with them by exchanging the data. To design a networking scenario for a college network which connect different departments to each other it provides communication between those departments. CAN is used to design an efficient topology, fulfilling all the necessary security policies for the college campus network. CAN provides the college network with a conflict free representation of network security policies and high quality performance. CAN also provides security and authentication to prohibit unauthorized logins.

2. Related Work

The popularity of Software Defined Networks (SDN) and OpenFlow increases, policy-driven network management has received more attention [1]. OpenSec, is an OpenFlow-based security framework that allows a network security operator to create and implement security policies written in human-readable language. The Campus Network Scenario-CNS [6] is regarding design of a topology for Local Area Network-LAN in a college which connects different departments and interacts with each other by exchanging records CNS provides security and authentication to forbid unauthorized logins.

The services, operations and management of today's organization are becoming gradually more dependent on their enterprise networks [10]. The security policy is defined as a set of allow/deny service access rules across various network zones where the services referred any network applications conforming to TCP/IP protocol. With the rapid development of economy and the implementation of the national strategy relying on science and education, more and more schools have set up their own campus network [12]. Campus network not only provides resources to be shared for the school teaching, scientific research and management, but also a platform for information exchange and working together. The status of the campus network security directly affects the school teaching activities.

3. Technologies

CCNA: Cisco Certified Network Associate [6]. It is the most popular certification course in the field of computer networking which is developed by the CISCO systems. CCNA was basically discovered by the CISCO system, to be acquainted with the indispensable proficiency in setting up and supporting medium sized networks.

The technology is used for linking different devices such as routers, switches and different end devices to commune with each other and exchanging information. It also helps to build a proficient, scalable and consistent network.

4. Security Policies

To provide various level of authentication and secure access following security policies are to be implemented in the proposed Campus Area Network design.

1) FTP access should be provided to the users of student and teacher block to the FTP server and network admin can have access to all other services.
2) Web access to the Social network server, network admin and disallow other users to access it.

Licensed Under Creative Commons Attribution CC BY

3) The users of the network have to be provided with the Mac-level authentication.
4) The router should be secured with password for admin for remote access.
5) The student, staff and servers are to be placed in different subnets.
6) The routing protocol being used should be configured with MD5-Message Digest5 authentication to provide protocol level security.
7) The users of student department should not be able to communicate with teacher department. But teachers can communicate with the student department.

5. Architectural Design

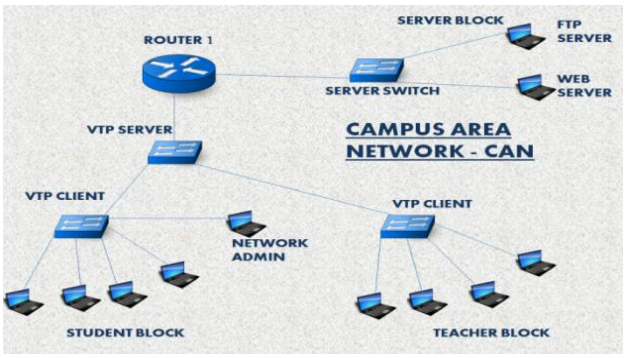

Figure 1: Architecture of CAN

Figure1 displays an architectural design of the Campus Area Network topology. The topology consists of the router, VTP- VLAN Trunking Protocol Server switch, two VTP Clients switch, Network admin, ten Personal Computer's, four for student block, four for teacher block and two for server block switch.

6. Network Design

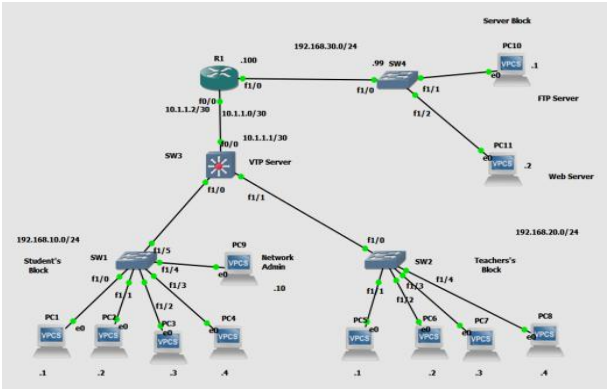

Figure 2: Topology of CAN

Figure 2 display the network design of the Campus Area Network.

The overall topology is based on tree topology which is conveniently serving the network. The network is based on client-server architecture. Basically there are two client switches (SW1 & SW2) which are working for the two different departments i.e., student and teacher department and they are connected to a aggregating switch (SW3) which further connects to a router. Another switch (SW4) for the servers is connected to the route. All the departments are classified into different three VLANs, VLAN10 is being used for student department, VLAN20 for teacher department and server block is using default VLAN1.

The subnet being used for VLAN10 is 192.168.10.0/24, for VLAN20 is 192.168.20.0/24 and for VLAN1 192.168.30.0/24.

When any request is made by any system of any department it's forwarded to client switch which further forward it to the desire destination.

Now there are port-securities which are implemented on different port of the switches which provides MAC level authentication for the host connected to the switches. Router basically routes the data from one network to another network. One of the exciting features of this project is that every device that is whether it's a switch or a router, they have been under the security of their respective passwords which are only known to the administrator (network administrator). He/she may reset the password at any time.

7. Implementation Overview

The objective of CAN is to provide safe and authenticated reliable communication among student, staff and servers. The work is built keeping in mind the cost and complexity factor. The different users and staff members can easily share their information and access resources available in the campus without any problem and going physically to them. As a result cutback time and save energy.

The end users and servers are connected through CISCO access layer switches. A CISCO router is being used to provide communication between different networks. Further a CISCO aggregating switch is being used to connect access layer switches.

VLAN, access control list and port security are being used at switch and router to provide access control to users, FTP server and web server.

After the successful implementation the network is expected to deliver following result.

- The users of same department should be able to communicate with each other and to the internet and servers.
- The users of student department should not be able to communicate with teacher department as per security requirement. But teachers can communicate with student department.
- FTP access should be provided to the users of student and teacher block to the FTP server and network admin can have access to all other services.
- Web access to the Social network server, network admin and disallow other users to access it.
- The users of the network have been provided with the Mac-level authentication.
- The routers are secured with password for admin for remote access.

Licensed Under Creative Commons Attribution CC BY

- The student, staff and servers are to be placed in different subnets.
- The routing protocol being used should be configured with MD5 authentication to provide protocol level security.

8. Results & Discussion

1) Banner Display

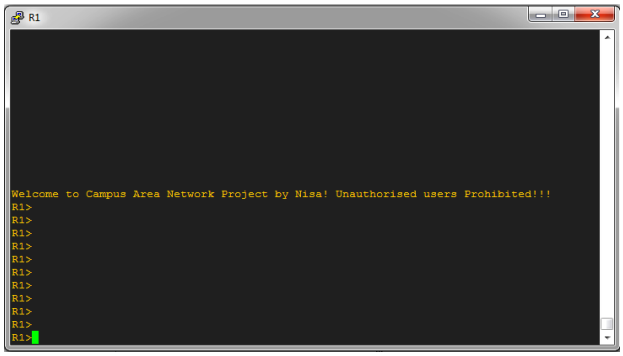

Figure 3: Screenshot of the initial screen display.

Figure 3 displays a welcome banner of the work before every start of the execution, Banner- "Welcome to Campus Area Network Project by Nisa! Unauthorized users Prohibited!!!"

2) Users of same department communicating with each other

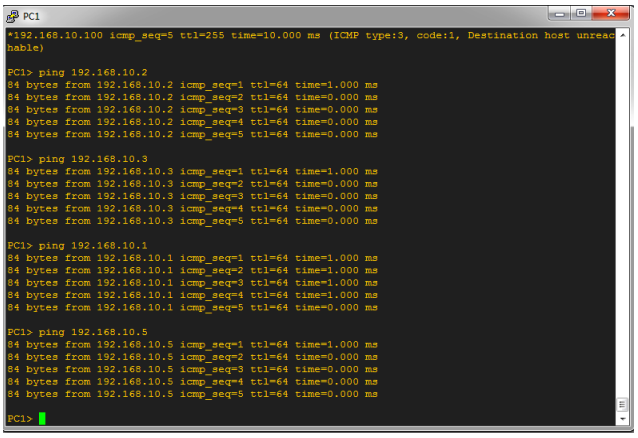

Figure 4: Screenshot of same department communicating with each other.

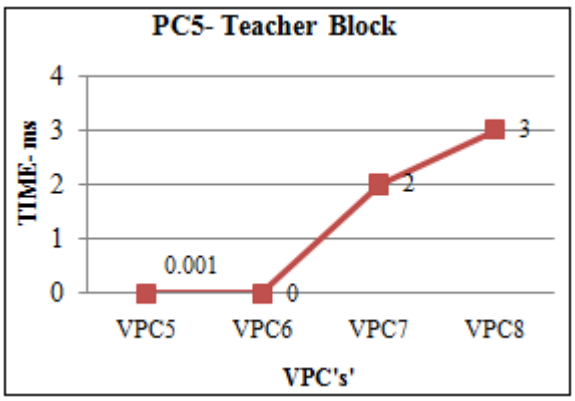

Figure 5: Graph deficit of Time v/s VPC's from PC5 of same department.

Figure 5 displays a graph analyses of teacher block communication with each other, the far the PC the time consumption will be more to reach the destination with the message.

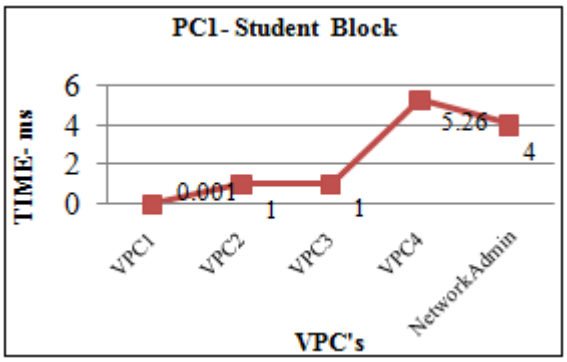

Figure 6: Graph deficit of Time v/s VPC's from PC1 of same department.

Figure 6 displays a graph Analyses of Student block communication with each other, the far the PC the time consumption increase accordingly to ping the message.

3) Users of teacher department communicating with student block

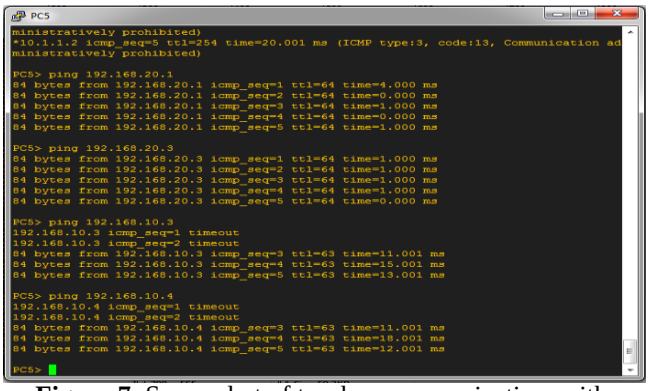

Figure 7: Screenshot of teacher communication with students

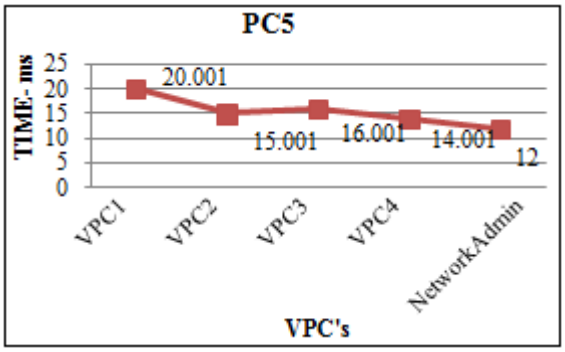

Figure 8: Graph deficit of Time v/s VPC's from PC5 to student department PC's.

Figure 8 displays a graph Analyses of teacher block communication with student block and Network admin, communication from department to department takes more time to ping the information.

Licensed Under Creative Commons Attribution CC BY

4) Network admin communication with entire college campus

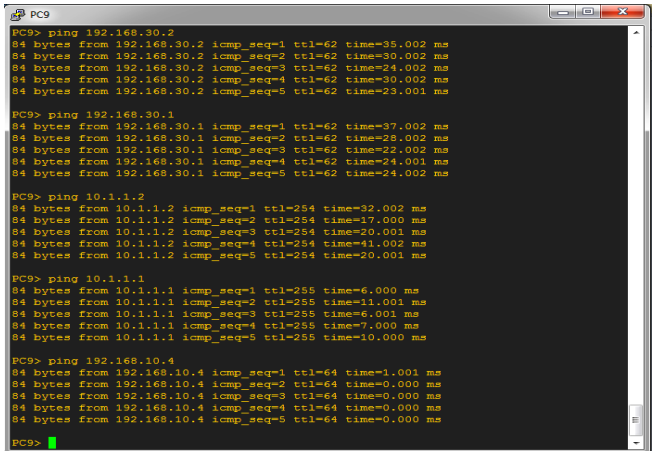

Figure 9: Screenshot of Network admin PC communicating with entire college PC's.

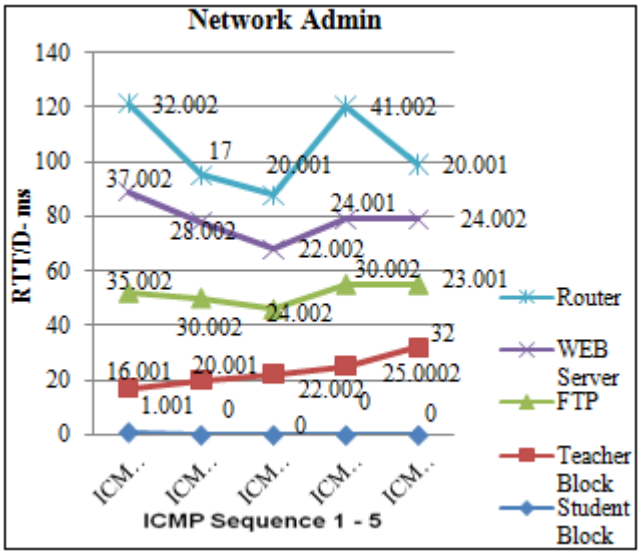

Figure 10: Graph deficit of RTT/D in ms v/s ICMP Sequence from 1-5.

Figure 10 displays a graph Analyses of network admin communication with whole college campus, the network PC is in the student block therefore the round trip time with respect to the ICMP sequence number, consumes much less RTT/D compare to other departments in the entire college,

5) Graph analyses of switch1-VLAN 10 communication with its VPC's

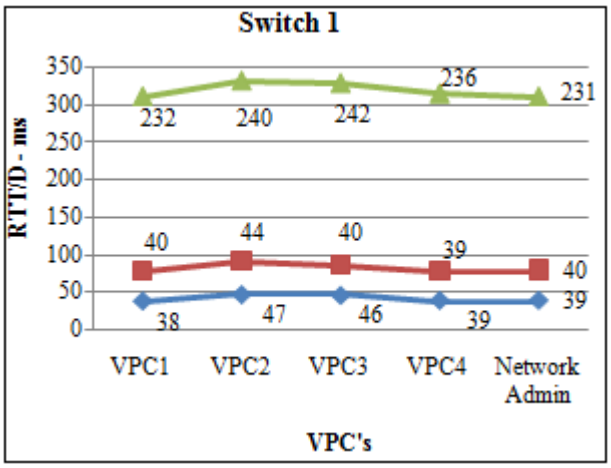

Figure 11: Graph deficit of RTT/D in ms v/s VPC's from switch 1 to student block.

Figure 11 displays the round trip delay decreases when communicating again and again to the same PC's in VLAN10.

6) Graph analyses of switch2-VLAN 20 communication with its VPC's

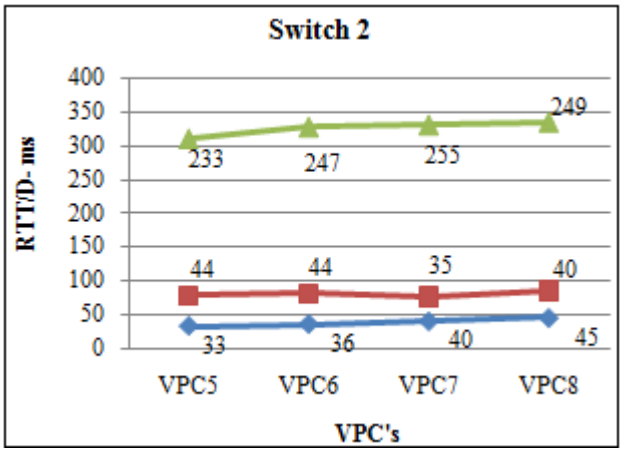

Figure 12: Graph deficit of RTT/D in ms v/s VPC's from switch 2 to teacher block.

Figure 12 displays the round trip delay decreases when communicating again and again to the same PC's in VLAN 20.

7) Graph analyses of switch 2-VLAN 20 communication with student VPC's

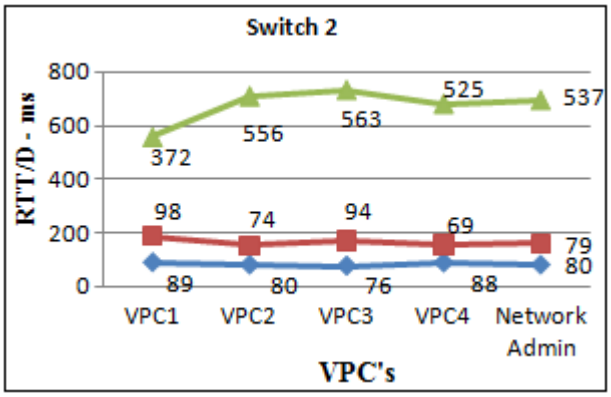

Figure 13: Graph deficit of RTT/D in ms v/s VPC's from switch 2 to student block.

Licensed Under Creative Commons Attribution CC BY

8) Student communication with FTP Server

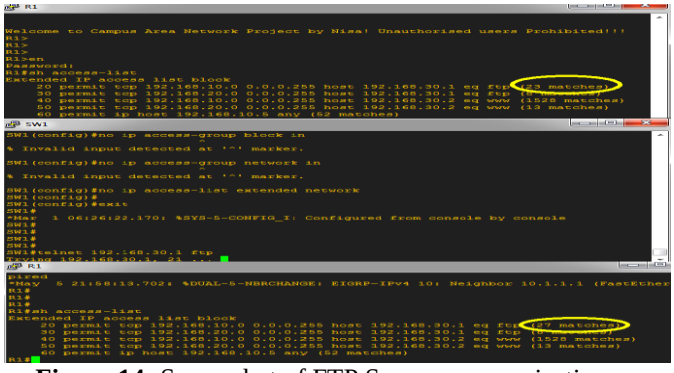

Figure 14: Screenshot of FTP Server communications

Figure 14 displays the FTP server packets received and sent from the student block, for every packet received 4 matches are found.

9) Teacher communication with WEB Server

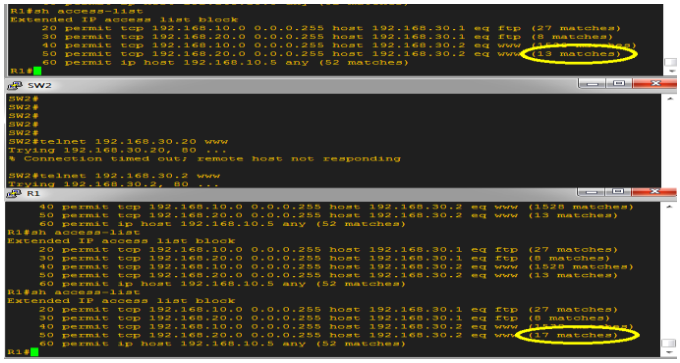

Figure 15: Screenshot of Web Server communications.

Figure 15 displays the Web server packets received and sent from the teacher block, for every packet received 4 matches are found.

9. Conclusion & Future Scope

A vital campus area network (CAN) have been designed, implemented and tested with the necessary network security policies. As per requirement the security has been implemented so that students cannot have access to teacher department but teachers can have access to student block. To protect campus IT infrastructure a limited access control has been provided to the students and the staff where as network administrator has complete access to the whole infrastructure. Different method of security control have been used like use of virtual local area network, use of separate subnets, use of access control list, providing console and telnet passwords etc.,. The network has been fully tested to ensure it deliver required output and provide all the authentication policies of a network security. Student and staff have been trained about use of the networks and security policies.

For the future up gradation if number of student increases then the number of switches can be increased in the student block. In the same way number of switches can be increased for the teachers block if the number of staff employee increases. In the server block only two block are being used and 22 ports are still empty which can be used for future provisioning of additional servers.

References

[1] Adrian Lara and Byrav Ramamurthy, OpenSec: Policy-Based Security Using Software-Defined Networking. In proceedings of IEEE, vol. 13, Issue. 1, March 2016.
[2] Arosha K. Bandara, Emil C. Lupu, Alessandra Russo, Naranker Dulay, Morris Sloman, Paris Flegkas, Marinos Charalambides, George Pavlou , Policy Refinement for IP Differentiated Services Quality of Service Management. In proceedings of IEEE, vol. 3, NO. 2, Issue Second Quarter 2006.
[3] Cataldo Basile, Alberto Cappadonia, and Antonio Lioy, Network-Level Access Control Policy Analysis and Transformation. In proceedings of IEEE, vol. 20,Issue 4, August 2012.
[4] Emil C. Lupu and Morris Sloman, Conflicts in Policy-Based Distributed Systems Management. In proceedings of IEEE, vol. 25, Issue *6*, November/December 1999.
[5] Hu Ruipeng , Design and Implementation of Campus Network Intrusion Detection System. In proceedings of ICISIE, Issue 2011.
[6] Jitender Singh, Anshu Rani, Implementation of College Network Scenario Module by Using CCNA. In proceedings of IJRDET, Vol 3, Issue 1,July 2014,ISSN 2347-6435(online).
[7] Joysankar Bhattacharjee, Design and Implementation of a Cost-effective and Secured “Private Area Network” for smooth as well as hassle-free Computing in the University Campus. In proceedings of IOSR-JEJC, *volume 11, Issue 1, Ver. I (Jan. - Feb .2016), PP 72-77.*
[8] Junbeom Hur and Kyungtae Kang, Member, IEEE, ACM, Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks. In proceedings of IEEE/ACM Transaction on Networking, Vol 22, No 1, February 2014.
[9] Lin Cui, Fung Po Tso, Dimitrios P. Pezaros,Weijia Jia and Wei Zhao, *Fellow*, PLAN: Joint Policy- and Network-Aware VM Management for Cloud Data Centers. In proceedings of IEEE, DOI 10.1109/TPDS.2016.2604811 Issue 2016.
[10] Mohammed Nadir Bin Ali, Mohamed Emran Hossain & Md. Masud Parvez, Design and Implementation of a Secure Campus Network. In proceedings of IJETAE, volume 5, Issue 7, July 2015.
[11] P. Bera, S. K. Ghosh and Pallab Dasgupta, Policy Based Security Analysis in Enterprise Networks: A Formal Approach. In proceedings of IEEE, vol. 7, Issue 4, December 2010.
[12] Patrick Traynor, Characterizing the Security Implications of Third-Party Emergency Alert Systems over Cellular Text Messaging Services. In proceedings of IEEE, vol. 11, Issue 6, JUNE 2012.
[13] Song Ji, Ling Pang & WenYing Xia, Campus network security analysis and design of security system. In proceedings of ICCICN, Issue 2015.
[14] Vijay Varadharajan and Udaya Tupakula, Securing Services in Networked Cloud Infrastructures. In

Licensed Under Creative Commons Attribution CC BY

proceedings of IEEE, DOI 10.1109/TCC.2016.2570752, Issue 2016.

[15] Xiang Wang, Weiqi Shi, Yang Xiang, and Jun Li, Efficient Network Security Policy Enforcement with Policy Space Analysis. In proceedings of IEEE, vol. 24, Issue 5, October 2016.

Author Profile

Faqarunnisa Begum is a PG student in Computer Networks & Engineering Department at PDA College of Engineering Kalaburagi, Karnataka, India. She has graduated from PDA College of Engineering with BE degree in Computer Science & Engineering Department in the year 2015. Her area of interest is in Computer Networks, Network Security.

Dr. Suvarna Nandyal born in Kalaburagi, Karnataka, India in 1972. She received her B.E degree in Computer Science & Engineering from Gulbarga University in 1993, M.Tech (Computer Science & Engineering) from VTU Belgaum in 2003 and Ph.D in the year 2013. She is presently working as Professor and HOD of Computer Science & Engineering Department at PDA College of Engineering Kalaburagi, Karnataka, India. She has published number of papers in international journals and conferences. Her research interests include Image processing, Machine learning, Design & development of Mobile based Application, Computer Network, Multimedia Communication.

Licensed Under Creative Commons Attribution CC BY