A Conceptual Approach to Network Effectiveness in Monitoring System

Dawodu, A.A., Adepoju, A.O., Lawal, O.O. & Akinyemi, O.S.
Department of Computer Science and Statistics
D.S.Adegbenro ICT Polytechnic
Itori,Ogun State,Nigeria
E-mail: alandawodu@gmail.com
Phone: +2348055141696

ABSTRACT

In computer networks, the need for speed and efficiency in the network is paramount to the Network

Keywords: Network utilization, CPU memory usage, Hard disk usage, I/O devices, monitoring systems, clients.

23rd iSTEAMS Conference Proceedings Reference Format
Dawodu, A.A., Adepoju, A.O., Lawal, O.O. & Akinyemi, O.S. (2020): A Conceptual Approach to Network Effectiveness in Monitoring System of Grounded -Theory Concepts in Analyzing Organizational Readiness and Barriers for Mobile Health (M- Health) Adoption in Nigeria. Proceedings of the 23rd iSTEAMS Conference, American University of Nigeria, Yola. April, 2020. Pp 79-88 www.isteams.net/yola2020

1. INTRODUCTION

Networking has been a very important issue in computing, telecommunication and many other sciences and technology aspects; therefore, it is very necessary to monitor the network so as to be able to fully utilize the However, the network administrator can use the NEMS to report client name, log on time, log out time, etc. NEMS provides one of the missing ingredients to make large systems performance aware and bandwidth adaptive. More so, performance issues are very important in monitoring a network because when several computers are connected together, complex interactions with unforeseen consequences are common. In all this, complexity leads to poor performance. In order to have a high performance network, it is important to identify bottle neck that might cause the low down of the network. These include CPU utilization, memory usage and allocation etc.

1.1. **Statement of the Problem**

As enterprise networks continue to grow in size, scope and in strategic importance, the Network Administrators are facing numerous challenges in maintaining the performance and availability of their network. However, as customers deploy new network applications and services, measurements of network performance must recognize different levels of performance based on the different types of network traffic. In view of these, the Network Managers often spend too much time trying to identify the source of performance problems, and need for performance troubleshooting tools that can identify performance problems before they seriously impact users and quickly identify the network devices that caused the performance problems once they have occurred. Furthermore, the network managers have the tool they need to identify performance problems, locate performance bottlenecks, diagnose latency and identify performance trends in the network.Network Effective Monitoring Systems (NEMS) will enable the network manager to perform path and hop performance analysis, thus simplifying the identification of network devices that are contributing to the network performance problems.

1.2. Purpose of the Study

The aim of this study is to develop a program that would monitor the activities of the network such as time spent during a session, source IP, network response time and also measure the system performance.

Specifically, the objectives are to;

(i) To ensure a network is safe from unauthorized access to some data to reduce the congestion possible in a network.
(ii) To fully utilize the network resources available in order to reduce the problems of overloading.
(iii) To keep track of all data and information flowing into the network and from the networks.
(iv) To be able to use best monitoring tools so as to ensure a perfect networking environment.

2. LITERATURE REVIEW

There are a very rich set of performance data available in Window NT environment; many performance counters are traceable with the standard supplied performance monitoring tools. The value of potential data can turn into serious management problem that overwhelm the analyst if a process is not implemented for quick identifying performance issues and determining the proper approach in addressing existing or emerging bottlenecks. Windows NT offers a wealth of measuring data regarding systems interface and application performance. There is so much information that the greatest danger may be overload of data. This development offers a set of key matrices that will supply an overview of system performance analyst. The performance analyst has been looking at system data for over 30 years and the basics have not changed significantly. A server can only be engaged in these specific types of activity because it can be performing operations (instructions) on the stored information (data) (Peter Hudson, 2000).

If the CPU is not 100 percent busy, all work is not completed, a problem also exists and I/O and memory subsystem should be investigated. (James Careless 2001). However, NT server will run short of memory before any resource because NT exhibits a change form in previous platform in the CPU, which is the least important resource to consider (Microsoft Press, 2000).

The Simple Network Management Protocol (SNMP) managed network consists of three key components:

(a) Managed Devices: is a network node that contains an SNMP agent and resides on a managed network. Managed devices collect and store management information and make this information available to Network Management Systems (NMSs) using SNMP. Managed devices, are sometimes called network elements, it can be routers and access servers, switches and bridges, hubs, computer hosts or printers.
(b) An Agent: is a network management software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP.
(c) Network Management Systems (NMSs): executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs must exist on any managed network.

3. FRAMEWORK

This research is a quantitative research in nature with an attempt to have gathered non-numerical data. A study in which an experimental validation is used. However, the research uses a publicly accessible Network Administrator as the target for assessment where a couple of Network Administrators were interviewed on how to monitor the performance of a network. End users were also asked necessary questions and Windows NT performance monitoring tools were studied. Also, Unified Modeling Language (UML) was used to model the system, while Visual Basic is used for the implementation of the system. A GFI LAN guard Network Security Scanner (LNSS) is a tool that allows network administrators to quickly and easily perform a network security audit. LAN guard Network Scanner (LNS) performs the functions of a port scanner. It also creates reports that can be used to fix security flaws on the network. Unlike other scanners, LNS will not create a “barrage” of information, which is virtually impossible to follow up on. LNS also provide hyperlinks to security sites to find out more about these vulnerabilities.

Features of LNSS are;

- LANS is a LAN guard scripting in which script creator for writing complex security checks. It includes a script editor with syntax highlighting capabilities and debugger.
- Scheduled scans – Ability to schedule LNS to do a scan and e-mail the differences it finds from the previous scan.
- Hot Fix Checker for Windows Machine – When scanning a machine, it will now check for hot fixes on it. It no longer just checks for registry keys, but will also check version specific information on key files.
- Ability to Patch Windows Machines that are missing Hot Fixes – Once LNS has found that a machine is missing Service Packs, it is now able to push those hot fixes to the machine and either install them immediately, or schedule a time for them to install, without user intervention.
- Configuration Manager – Ability to configure LAN guard Network Scanner (LNS) the way you like it and save it to an initialization file. Before, if you wanted to be able to change between the types of scans, you had to manually change it each time. But with the ability to save the configuration files and quickly reload it, you do multiple types of scans in less time.

Furthermore, in performing a new network scan, the LAN guard Network Scanner will scan the entire range entered from the main LNSS window. It will first detect which hosts computers are on, and only scan those responsible for it. This is done using NETBIOS probes, Internet Control Message Protocol (ICMP) Ping and SNMP queries.

4. SYSTEM DESCRIPTION

Network Effectiveness Monitoring System is a client/server multithreaded network diagnostic tool, when users make use of workstations on a network, it is imperative that Network Administrator is able to capture, view and analyze the activities what occur on that network. Network statistics such as percent of network utilization, CPU usage, memory usage, physical disk (percent disc time), physical disk (Average Queue Length) etc needed in order to know the overall statues of the network. It helps in locating/identifying traffic bottlenecks within a network. The system (NEMS) continuously tracks packet crossing a network, thus providing an accurate picture of a period of time to establish a normal performance profile. The Unified Modeling Language (UML) is used to model the system (NEMS) in the next selection of the project. The UML is one of the most exciting tools in the world of the system development today.

4.1. Use Case

The use case diagram is used to describe the system behaviour from the user’s standpoint. The use case for the network effectiveness monitoring system (NEMS) is as follows:

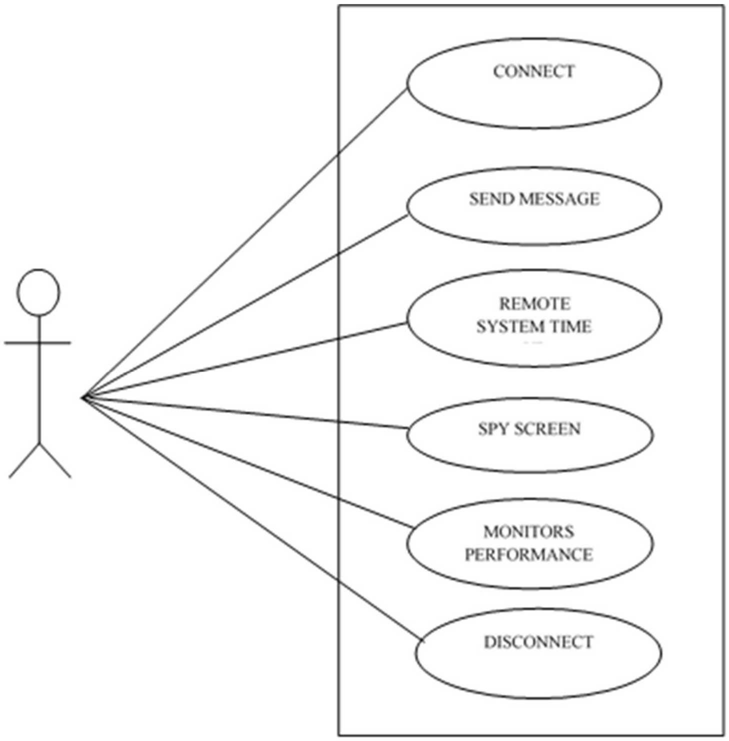

Fig. 1: The Network Administrator is the only actor because he/she is the only one that interacts with system ..

4.2. Class Diagram

The class diagram help on the analysis of the requirements, it provides a representation that developers work on. It also models each object present in the existing system.

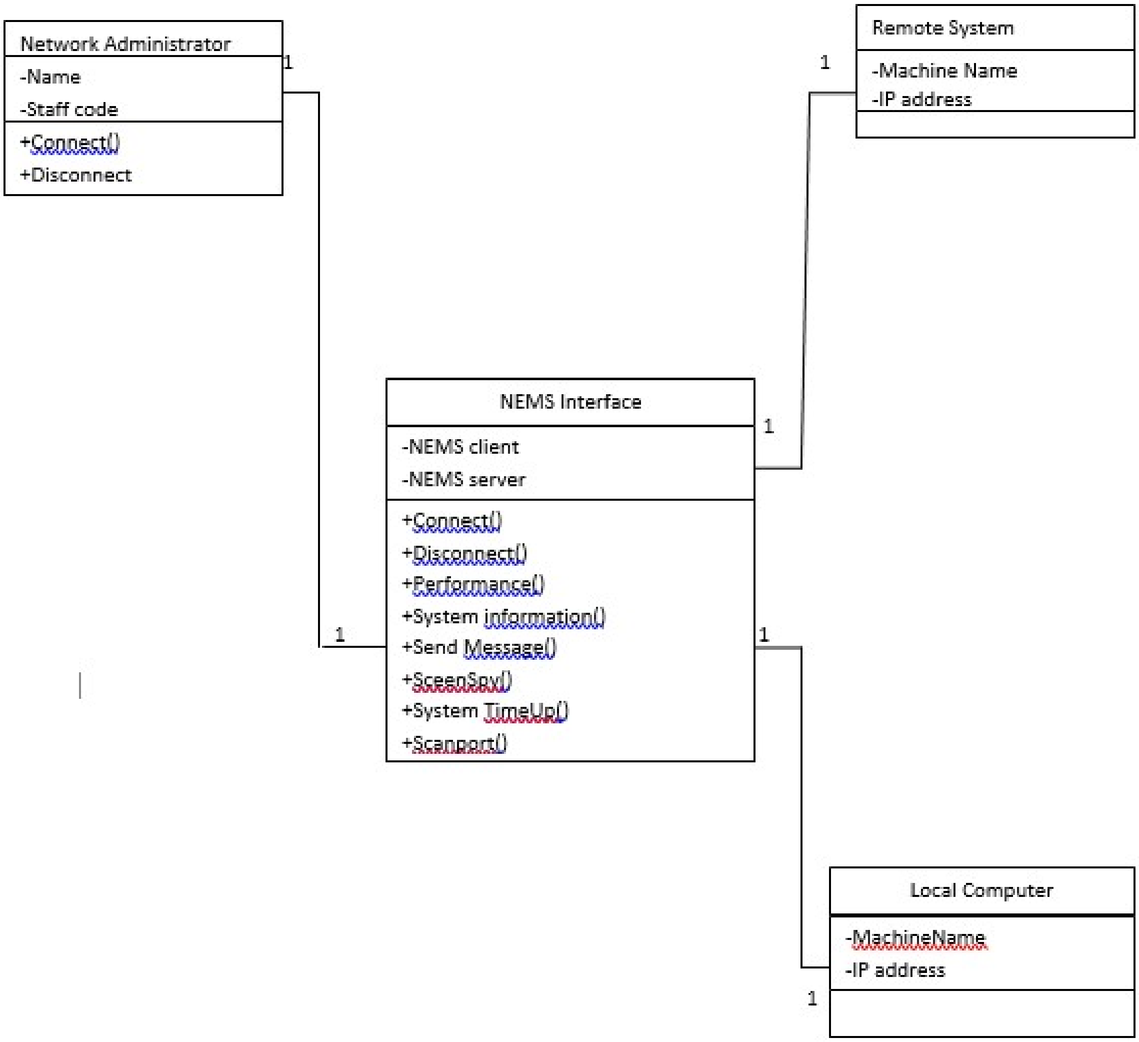

Fig. 2: The Class Diagram

In the NEMS system, the network administrator connects and disconnects the machine before and after network monitoring begins.vThe monitoring computer (NPMS) can only connect to one remote computer at a time. And the Network Administrator interacts with just one NPMS.

4.3. Sequence Diagram

The sequence diagram shows the time-based dynamics of the interaction of the object present in the system.

NPMS Sever is the server software installed on the network workstation and it serves the server problem by supplying requested information about a workstation. NPMS Client is the front end software, it request for services from the NPMS server, which is at the back end.

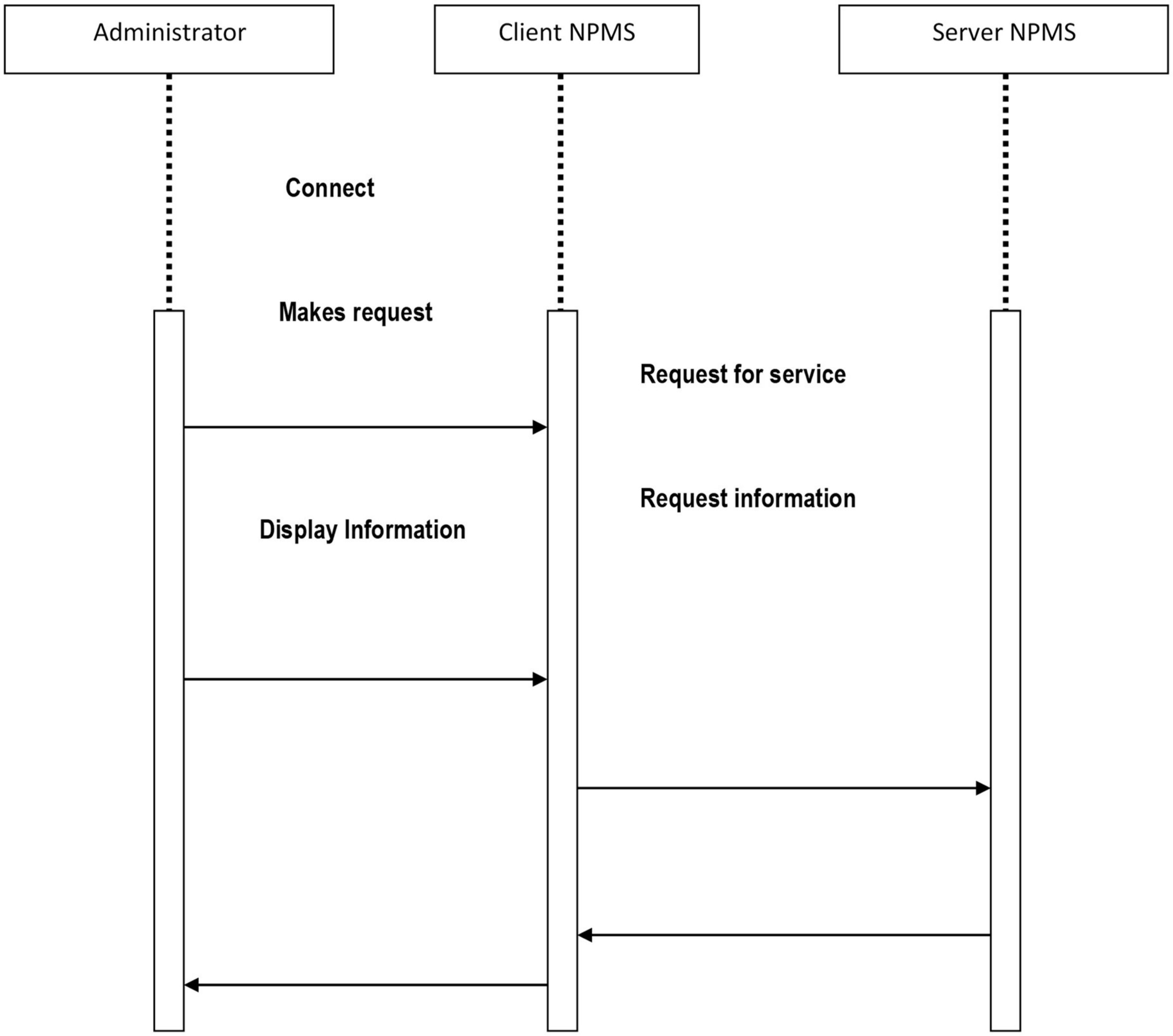

Fig. 3: Sequence Diagram

4.4. Activity Diagram

An activity diagram is used for showing activities, decision points and branches. It shows what happens in an operation. It is used to model the sequence of events that occur within the objects present in the system.

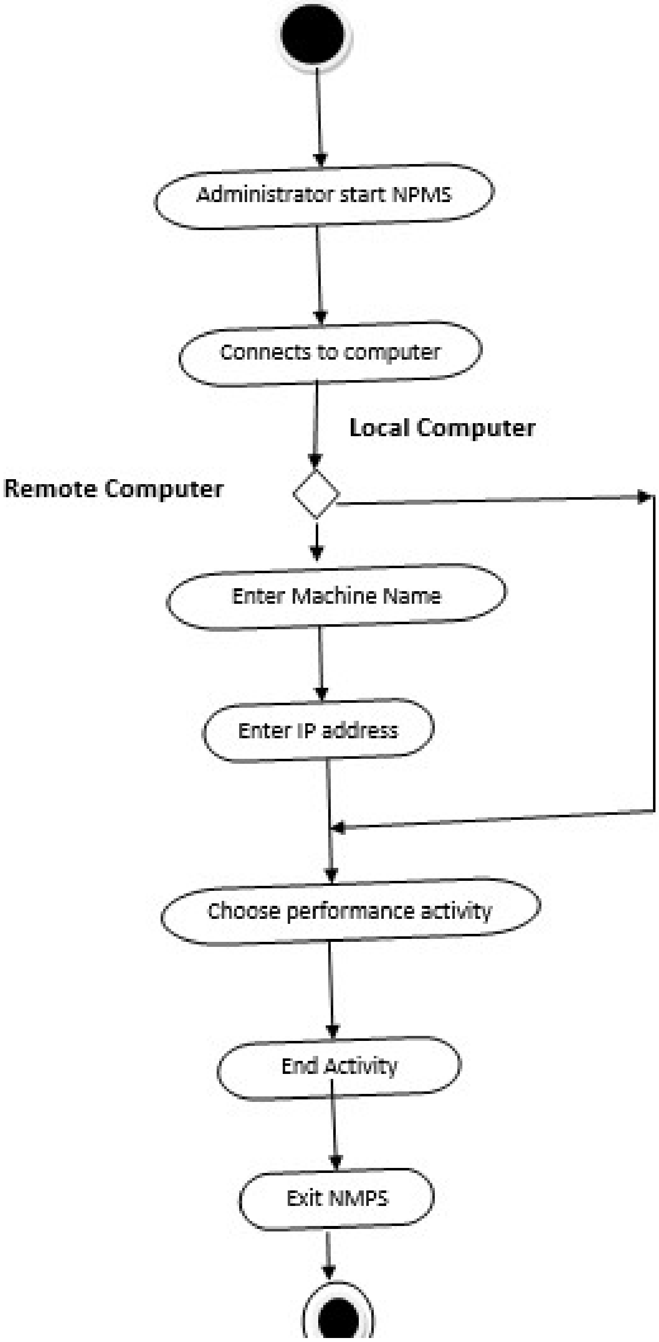

Fig. 4: Activity Diagram

5. IMPLEMENTATION

NPMS 1.0 is a client/server multithreaded network diagnostic tool used and it is compatible with Windows QX and the rest of the Windows NT platforms. Its purpose is to accumulate data pertaining to network status and its availability, several information about the network workstations and local computer its running on, using all the latest development tools in network research including socket programming (Winsock in Visual Basic), several ActiveX controls and Windows API function. The server program is to be installed on all the remote computers while the client program is to be installed on the monitoring computer. The two software, are programmed to recognize each other and connect the computers at the same time.

Server Program: NPMS server
Client Program: NPMS client

5.1. NEMS Server

NEMS server is software installed on the network workstation and its serves the server program by supplying requested information about the workstation. This program starts running at the windows startup on boot and send packets of data t the server program as requested with the use of integrated socket programming control, Winsock in Visual Basic 6.0.

5.2. NEMS Client

NEMS is the front-end software. It requests for services from the NPMS server, which is at the back-end. It is also developed in Visual Basic environment; its major interface is the “Network Performance Monitoring System Version 1.0”. NPMS version 1.0 is a dynamic utility consisting of the following tools;

- ❖ Connectivity
- ❖ Screen Spy
- ❖ Remote Control
- ❖ Performance Monitor
- ❖ Chatting (Message Sending)
- ❖ System Information

6. DISCUSSION

The findings from this research shows that the various tools used are not necessarily adhering strictly to the common vulnerabilities and exposures standard in assessing vulnerabilities in Network Effectiveness Monitoring Systems in terms of speed and efficiency. There also tends to be significant difference in the overall number of identified vulnerabilities in each methods used. Another key observation is the disparity in the identified vulnerabilities in relation to the Online Web Application Security that evolved round the Network Administrator and the clients. The findings depict a perception that supposed proprietary tools such as Screen Spy, Performance Monitor and nets parker tends to be more reliable and exhaustive in its probe for vulnerabilities within the NPMS. While these are findings and possible deduction from the findings, it is important to note that various subsequent versions of the tools may possibly make up for the limitations of the used versions. Furthermore, it was discovered that several vulnerabilities in the research, for instance CSRF, were missed because of the incomplete functionality scanners. Patil and Gosavi (2015) also evaluated different types of vulnerabilities and found out that different methods are required for to detect.

The important relevance of the findings of this research implies that Network Effectiveness in Monitoring Systems Vulnerability Scanners tend to identify more industrial standard results of NEPS application vulnerabilities. Given the fact that there are significantly more scanners, there is need to indicate that this research work is definitely not exhaustive in NPMS. In addition, the platform for the case study was developed with Internet Control Message Protocol and SNMP queries. It would be prudent for similar research work to be carried out on platforms developed with other languages such as HTML, PHP, and Java Script etc.

7. CONCLUSION

Network Effectiveness in Monitoring System (NEMS) aides network utilization, trend analysis and network capacity planning, which is the process of determining current usage of server and or network resources, and tracking utilization over time to predict future usage and additional hardware that will be required to meet projected levels of utilization. However, capacity planning can be performed on a single computer, such as a network server, or it can be performed on the entire network. Further research is needed relatively thorough assessment is done on comparing open source and proprietary tools for efficiency, effectiveness and reliability. The platform for the development of Network effectiveness in Monitoring System test would also need to be assessed to determine if there are any specific capabilities or limitations with open or closed source tools on specific NPMS application platforms.

8. CONTRIBUTION TO KNOWLEDGE

NEMS is an essential tool to facilitate the development of future Network Services. It provides network performance measurement for a wide range of network protocols. The ability to measure network response time, determine device availability, analyze response time patterns and provide effective reports – both real time and historical – are high priority requirements in today’s enterprise networks.

REFERENCES

1. Aderonmu, G.A. (2004); Performance Comparism of remote procedure calling and Mobile Agent Approach to Control and Data Transfer in Distributed Computing Environment, Journal of Network and Computer Application. 27(2): 113-119.
2. Alfalayleh, M. & Brankovie, L. (2004). An overview of security issues and techniques in mobile agent. Retrieved March22,2005 from; ttp://sec.isisalfford.oc.UK/cms.2004/program/CMS2004final/P2a3/pdf.
3. Baldi, M. & Picco, G.P. (1998); Evaluating the Tradeoffs of Mobile Code Design Paradigms in Network Management Application Proceedings of 1998 International Conference on Software Engineering (ICSE '98).
4. Bentley, Lonnie D, Kevin, C. Dittman and Jeffrey. L. (2004): System Analysis and Design Method. Prentice Hall
5. Carzaniga, A; Picco, G.P. & Vigna, G. (1997): Designing Distributed Applications with Mobile Code Paradigms.
6. Levin, Marksh (Springer 2015); Modular System Design and Evaluation. Spectrum Books LTD.
7. Mohit Mamaha, Rajeev Bedi; "Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing" IJCSI International Journal of Computer Science, Issues, Vol 10, Issue1, No1, pg. 367-377, 2013.
8. Nwomkwe. J.I. (1985); Fundamental of Management Information System. Spectrum Books LTD.
9. R. Taylor ed.; Proceeding of the 19th International Conference on Software Engineering (ICSE '97). ACM Press: 22-32.