ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 4, April 2013

SPY MONITORING SEVER

Nishant Nilay, Rohit P. Nashine, Shantanu Shrivastava, Yogesh Golhar

Yeshwantrao Chavan College of Engineering, Nagpur, India

Abstract: Spy Monitoring Server is used to monitor and control the client machines in the network. It allows the administrator to view the systems connected to the LAN. The system information contains OS name and version, Processor details. It is capable of storing login details of the user. It can also monitor the data send by the user.It can share the desktop screen of the users also. The project "Spy Monitoring Server" is an application which needs to be installed in the server. The computers are connected by a LAN. The computers are recognized either by their computer names or by their IP address.

Keywords: Log monitoring, packet monitoring, packet sniffing, intruder detection, desktop sharing, online/offline communication, Monitoring and Reporting

I. INTRODUCTION

When you operate a network you may want to know the status of each, you may hosts on your network, the traffic rate flowing from and into each hosts, and so on. In short, you may want is going on the network so you can make decisions on who may want to do. A Spy Monitoring Server is capable of detecting and reporting failures of devices or connections. It normally measures the processor (CPU) utilization of hosts, the network bandwidth utilization of links, and other aspects of operation. It will often send messages (sometimes called *watchdog* messages) over the network to each host to verify it is responsive to requests. When failures, unacceptably slow response, or other unexpected behavior is detected, these systems send additional messages called *alerts* to designated locations (such as a management server, an email address, or a phone number) to notify system administrators.

The objectives of Spy Monitoring Server are as follows,

A. Log Monitoring.
B. Intruder Detection.
C. Offline/Online Communication.
D. Allocation of Privileges.
E. Spy Monitoring.
F. Scheduling, Controlling, Monitoring and Reporting.

A. Log Monitoring

Log monitoring is a type of software that monitors log files. Servers, application, network and security devices generate log files. Errors, problems, and more information is constantly logged and saved for analysis. In order to detect problems automatically, administrators and operations set up monitors on the generated logs. [1]

B. Intruder Detection

Intruder detection is the art of detecting intruders behind attacks as unique persons. This technique tries to identify the person behind an attack by analyzing their computational behavior. This concept is sometimes confused with Intrusion Detection (also known as IDS) techniques which are the art of detecting intruder *actions*.

C. Online/Offline Communication

The terms "online" and "offline" (also stylized as "on-line" and "off-line") have specific meanings in regard to computer technology and telecommunications. In general, "online" indicates a state of connectivity, while "offline" indicates a disconnected state. In common usage, "online" often refers to the Internet or the World-Wide Web.

The concepts have however been extended from their computing and telecommunication meanings into the area of human interaction and conversation, such that even *offline* can be used in contrast to the common usage of *online*. For example, discussions taking place during a business meeting are "online", while issues that do not concern all participants of the meeting should be "taken offline" — continued outside of the meeting.

D. Spy Monitoring

Spy Monitoring is a "Network monitoring**".** It refers to the practice of overseeing the operation of a computer network using specialized management software tools. Network monitoring systems are used to ensure availability and overall performance of computers (hosts) and network services. These systems are typically employed on larger scale corporate and university IT networks.[1]

I. LITERATURE SURVEY

A. Packet Sniffing

For most organizations, packet sniffing is largely an internal threat. A third party on the Internet, for instance, could not easily use packet sniffing software to eavesdrop on traffic on a corporate LAN. Packet sniffing in a switched environment is possible -- anyone equipped with a laptop may be able to monitor communication between machines on a switched network. In a switched environment, it is more of a challenge to eavesdrop on network traffic. This is because usually switches will only send network traffic to the machine that it is destined for.[19]

Packet sniffing [22] in a non-switched environment is a well understood technology. A large number of commercial and non-commercial tools enable eavesdropping of network traffic. The idea is that to eavesdrop on network traffic, a computer's network card is put into a special "promiscuous" mode. Once in this mode, all network traffic that reaches the network card can be accessed by an application

Basic Components of sniffers are:- A. The hardware: - Most products work from standard network adapters, though some require special hardware. If you use special hardware, you can analyze hardware faults like CRC errors, voltage problems, cable programs, "dribbles", "jitter", negotiation errors, and so forth B. Capture driver:- This is the most important part. It captures the network traffic from the wire, filters it for the particular traffic you want, and then stores the data in a buffer. C Buffer:-Once the frames are captured from the network, they are stored in a buffer. D. Decode: - this displays the contents of network traffic with descriptive text so that an analysis can figure out what is going on. E. Packet editing/transmission:-Some products contain features that allow you to edit your own network packets and transmit them onto the network

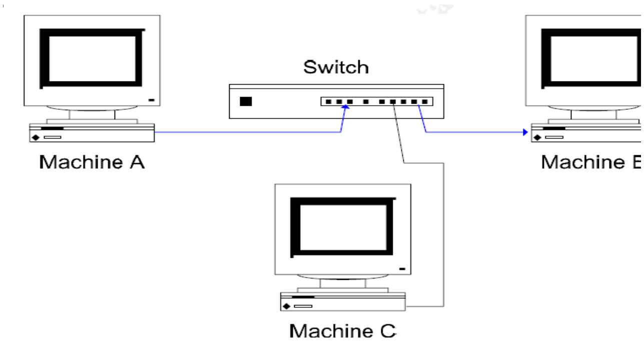


Figure 1: Three machines connected via a switch. Traffic flowing from A to B is illustrated by the arrowed lines.

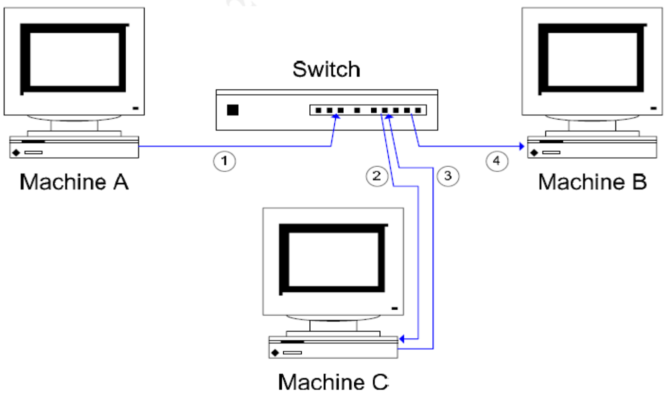


Figure 2: The "man in the middle" attack. C intercepts network traffic from A which is destined for B.

B. Spyware: The dark end of the greynet

Greynets are network-enabled applications that are installed on an end user's system without the knowledge or permission of the IT department—or, frequently, without the knowledge or permission of the end users themselves. They are further categorized by the degree of 'evasiveness' they exhibit on the network—for example, how much use they make of techniques such as port agility and encryption to avoid detection by existing network security controls.[21]

C. Overlay of Spyware

Spyware is one type of malicious software (malware) that collects information from a computing system without your consent. Spyware can capture keystrokes, screenshots, authentication credentials, personal email addresses, web form data, internet usage habits, and other personal information. The data is often delivered to online attackers who sell it to others or use it themselves for marketing or spam or to execute financial crimes or identity theft.[5]

D. Who is spying?

- ➢ online attackers
- ➢ marketing organizations
- ➢ organized crime
- ➢ trusted insiders

E. Netspy

NetSpy advance the state-of-the-art in spyware signature generation.[20]

a. Ability to detect novel spyware. NetSpy observes the network activity generated by an untrusted program in response to simulated user-input and determines whether the program is possibly spyware. This approach also enables NetSpy to generate signatures for previously unseen spyware instances.

b. Network-level signature generation**.** If deemed to be spyware, NetSpy generates a signature for the malicious substrate of an untrusted program's network behavior. These signatures can be used by a NIDS that monitors outgoing traffic from a network, thus enabling detection of spyware installations on all machines within the network.

c. Automation**.** NetSpy is fully automatic. When a new program (such as a browser toolbar) is installed on a machine, NetSpy can determine immediately whether the program is potentially spyware and automatically generate Snort signatures for the program.

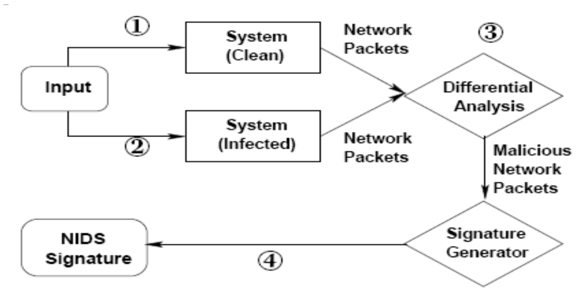


Figure 3: NetSpy Architecture Overview.

Adware: These are hidden marketing programs that deliver advertising to consumers, and might also profile users' Internet surfing & shopping habits. Adware is often bundled or hidden in something else a user downloads. Most average computer users are infected with adware fairly regularly, and common symptoms include a sluggish system and lots of advertising pop-ups.

Malware: This is any program that tries to install itself or damage a computer system without the owner's consent. Malware includes viruses, worms, spyware and adware.

II. METHODOLOGY:

A. Standard Controls used in the Project:

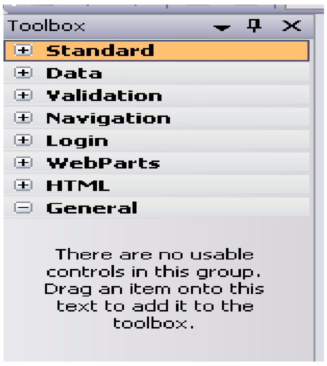
These controls are the Web equivalents of the tools that you encounter when using Windows applications. Web pages that include these controls have that standard application feel that we're all familiar with, so the process of adding them to pages is quick and simple. Here are some of the most commonly used controls:

a. Textbox control**:** Used for entering text on a page, commonly seen on order forms on shopping sites, or for logging in to a site.
b. Button control**:** From submitting an order to changing preferences on a web site, clicking a button on a page normally causes information to be sent to the server, which reacts to that information and displays a result.
c. Label control: Used for displaying simple text in a specified position on a page. The Label control is an easy way to change the text on part of a page in response to user interaction.
d. Hyperlink control**:** Used for providing hyperlink functionality on a page that enables navigation to other parts of a site, or to other resources on the Internet.
e. Image control**:** Used for displaying images on a page. The server can change the image that is displayed in the control programmatically in response to user input.
f. Dropdown List control**:** Used for offering the user a list of options to choose from; collapses when not in use to save space.
g. List box control**:** Used for offering a fixed-size list of items to choose
h. Checkbox and Radio Button controls**:** Used for selecting optional extras with either a yes/no or "this one out of many" style, respectively.

B. Toolbox:

Visual Web Developer offers the set of ASP.NET server-side controls in a Toolbox for easy drag-and-drop onto the page. The Toolbox can be displayed by choosing Menu➪View➪Toolbox or by pressing Ctrl+Alt+X. When the Toolbox is displayed, you can move it to a new location on the screen by dragging its title bar. The Toolbox is organized into several panels that group similar controls. The panels can be expanded to show their tools or collapsed to save space. There is some variation among installations, but a typical set of panels includes the following:

a. Standard for the majority of ASP.NET 2.0 server- side controls
b. Data for data source and data-bound controls
c. Validation for controls that reject user input that does not meet your range of acceptable values
d. Navigation for menus and breadcrumbs
e. Login for the authentication controls
f. Web Parts for larger components in sites that the user can rearrange or hide.
g. HTML for generic (non-ASP) tags
h. General for customization



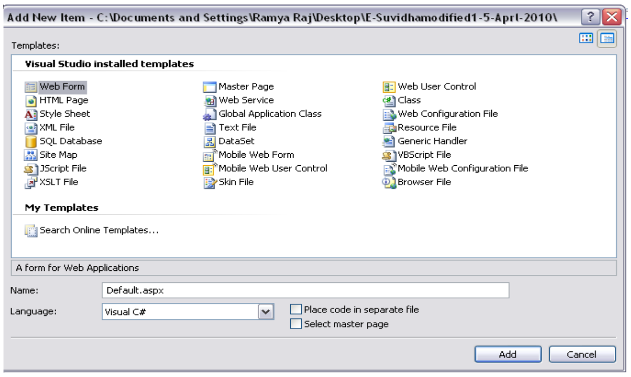
There are no usable controls in this group. Drag an item onto this text to add it to the toolbox.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 4, April 2013

C. Creating a Master Page

We create a Master page in Solution Explorer by right-clicking the root of the site, selecting Add Item, and designating the type as a Master Page. By default, the name for a new Master page is MasterPage.master and is located in the root of the site.



Add New Item - C:\Documents and Settings\Ramya Raj\Desktop\E-Suvidhamodified1-5-Aprl-2010\

Templates:

Visual Studio installed templates

Web Form	Master Page	Web User Control
HTML Page	Web Service	Class
Style Sheet	Global Application Class	Web Configuration File
XML File	Text File	Resource File
SQL Database	DataSet	Generic Handler
Site Map	Mobile Web Form	VBScript File
JScript File	Mobile Web User Control	Mobile Web Configuration File
XSLT File	Skin File	Browser File

My Templates

Search Online Templates...

A form for Web Applications

Name: Default.aspx

Language: Visual C#

□ Place code in separate file

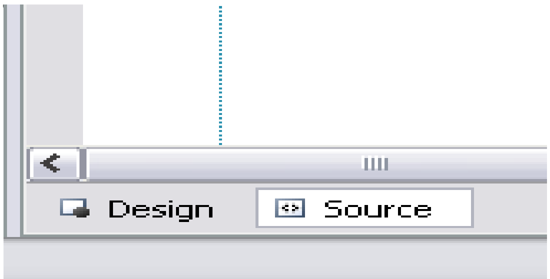
□ Select master page

Add Cancel

The various web forms, master pages & SQL database have been selected from this popup menu. The centre of the PAGE is occupied by the large Design Surface. This is the area where you will do most of your work of adding content, or you can switch to Source View, which displays code in a text screen. In general, the Design View is easier and faster for most work because it supports more drag-and-drop features. You can switch to Source View when you need to make those minor changes that are beyond the capability of the drag-and-drop interface.

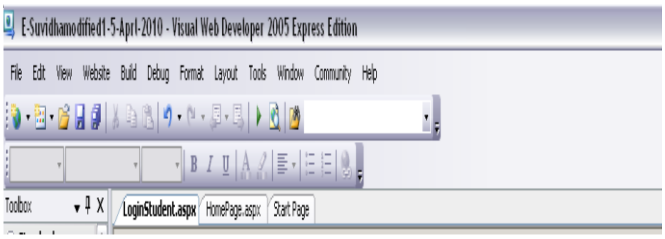
When you add a control to a page in Design View, a Common Tasks Menu may pop up. This mini menu contains the most frequently used setup features for the control. Not all controls have smart task panels, but if it is available, it can be opened and closed using the small black triangle at the top corner of a control that is selected.

We can change several default settings in the Design Surface by opening the Tools menu and selecting Options. There are several options provided in the tool box. These options change the way the pages appear to you, as the programmer, when they are opened for editing in Visual Web Developer. These tools are very helpful for designing a software or a webpage. These are not the settings for the appearance of the page to the web site visitor. You can select to start pages in Design View or Source View, as well as the automatic opening of the smart task panel. Being able to revise the number of spaces for tabs and indents helps your projects conform to your company's specifications for web page code. At the bottom edge of the Design Surface is a navigation tool that is useful in large and complex documents. You can read the navigation tags to find out where the insertion bars (cursor) is currently setting. The current setting is highlighted. You can also click a tag and the entire tag will be selected in the Design Surface.



D. Running a Page

After a page is created, it can be served to a user. The server actually executes code in the server side. This serving of the page is also called running the page, Visual Web Developer has a green triangle tool icon to initiate a run or you can press F5 or choose Menu➪Debug➪Run.



E. Design

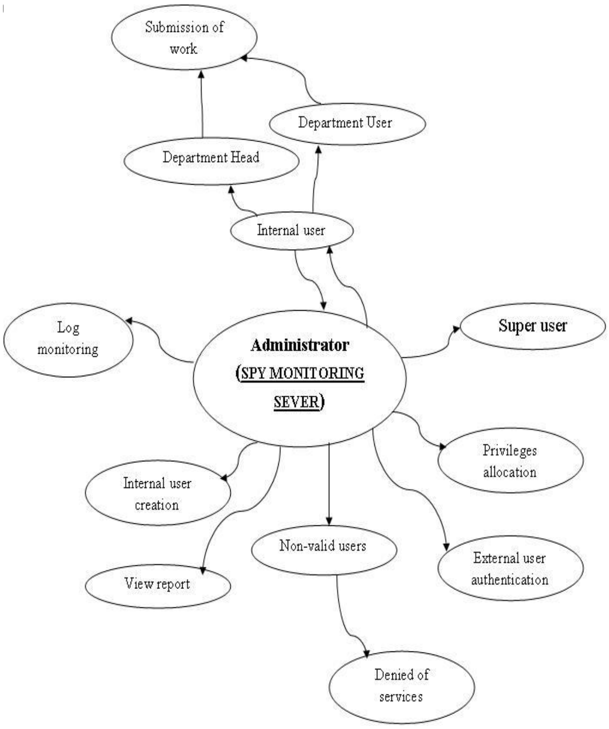


Figure 4: System Diagram for Spy Monitoring Server

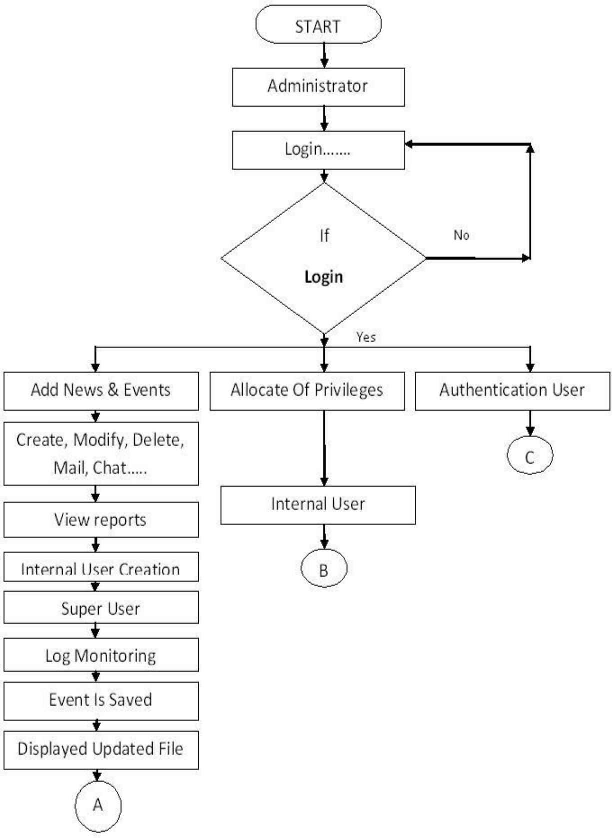


Figure 5(a): Flow chart of proposed Spy monitoring Server

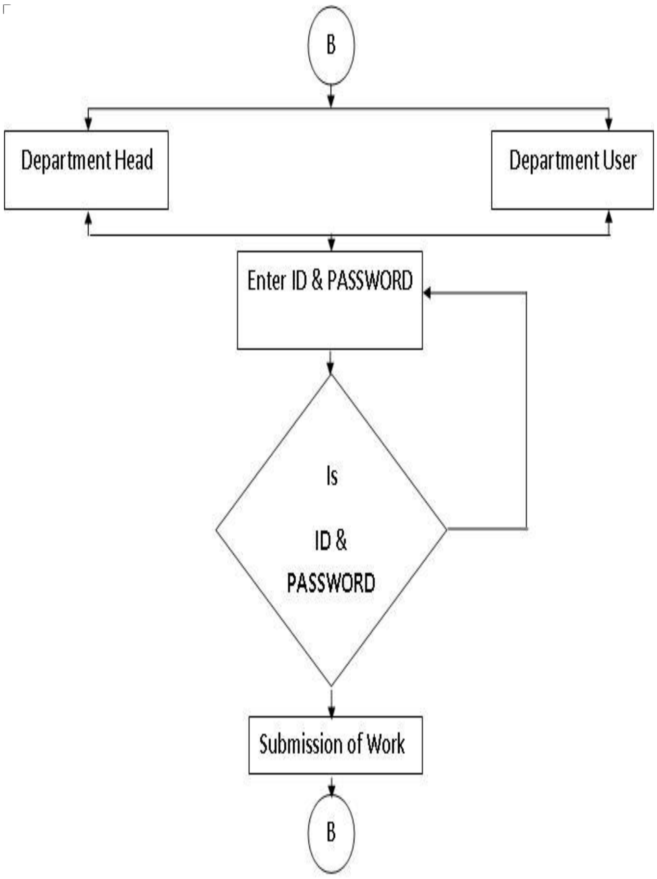


Figure 5(b): Flow chart of proposed Spy monitoring Server

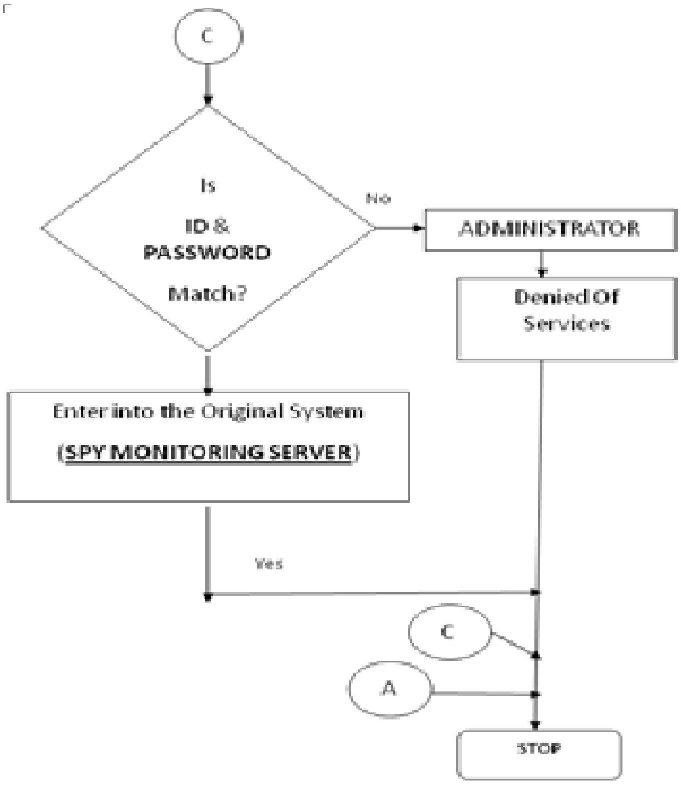


Figure 5(c): Flow chart of proposed Spy monitoring Server

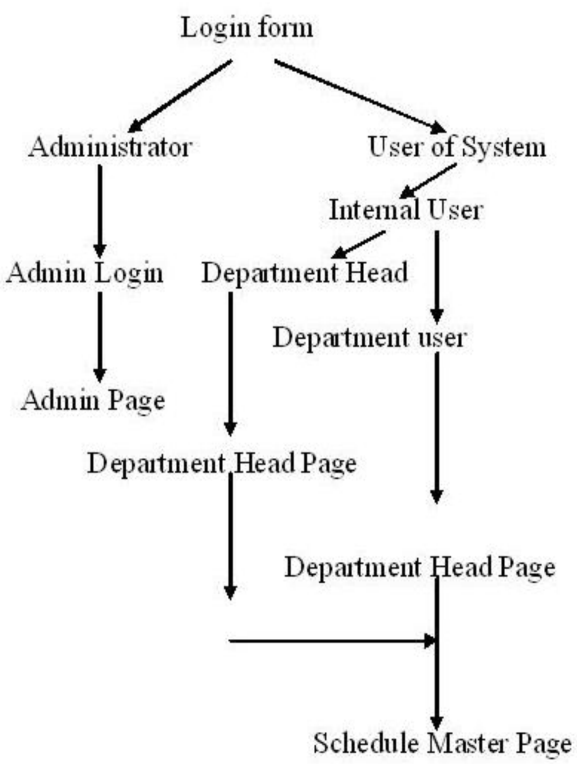


Figure 6: Decision Tree

III. CONCLUSION

It has been a great pleasure for me to work on this exciting and challenging project. This project proved good for me as it provided practical knowledge of not only programming in ASP.NET and C#.NET web based application and know some extent Windows Application and SQL Server, but also about all handling procedure related with "SPY Monitoring System"**.** It also provides knowledge about the latest technology used in developing web enabled application and client server technology that will be great demand in future. This will provide better opportunities and guidance in future in developing projects independently.

A. Benefits

The project is identified by the merits of the system offered to the user. The merits of this project are as follows: -

a. It's a web-enabled project.
b. This project offers user to enter the data through simple and interactive forms. This is very helpful for the client to enter the desired information through so much simplicity.
c. The user is mainly more concerned about the validity of the data, whatever he is entering. There are checks on every stages of any new creation, data entry or updation so that the user cannot enter the invalid data, which can create problems at later date.
d. Sometimes the user finds in the later stages of using project that he needs to update some of the information that he entered earlier. There are options for him by which he can update the records. Moreover there is restriction for his that he cannot change the primary data field. This keeps the validity of the data to longer extent.
e. User is provided the option of monitoring the records he entered earlier. He can see the desired records with the variety of options provided by him.
f. From every part of the project the user is provided with the links through framing so that he can go from one option of the project to other as per the requirement. This is bound to be simple and very friendly as per the user is concerned. That is, we can sat that the project is user friendly which is one of the primary concerns of any good project.
g. Data storage and retrieval will become faster and easier to maintain because data is stored in a systematic manner and in a single database.
h. Decision making process would be greatly enhanced because of faster processing of information since data collection from information available on computer takes much less time then manual system.
i. Allocating of sample results becomes much faster because at a time the user can see the records of last years.
j. Easier and faster data transfer through latest technology associated with the computer and communication.
k. Through these features it will increase the efficiency, accuracy and transparency,

B. Limitations:

a. The size of the database increases day-by-day, increasing the load on the database back up and data maintenance activity.

b. Training for simple computer operations is necessary for the users working on the system.

IV. FUTURE ENHANCEMENT

Future scope of this project is much wide, as we are planning to implement a web server which will monitor, control the entire network with security majors. Due to time limit we will be able to administrative part (super user) which will able to create internal user allocation of rights authentication of external user this kind of feature which is primary requirement of Spy Monitoring Server. In future, we will be implementing at those modules which are the key features of our project like log monitoring ,intruded detection ,monitoring, controlling the entire web service as well as communication server will be design and development in near future.

Currently, we will able to compute four phases of our project that are requirement analysis, planning, designing and partial implementation in next phase will be implementing complete implementation, testing and deployment phases.

ACKNOWLEDGMENT

A major research project like this is never the work of anyone alone. The contributions of many different people, in their different ways, have made this possible. I would like to extend my appreciation especially to the following. Our project guide, Mr Yogesh Golhar, for making this research possible. His support, guidance, advice throughout the research project, as well as his pain-staking effort in proof reading the drafts, is greatly appreciated. Indeed, without his guidance, I would not be able to put the topic together. Mrs. Gauri Chaudhary, for encouraging us to undertake the honours programme. The experience has been an interesting and rewarding one. Ofcourse, this project would not have been possible without the participation of the subjects.

Last but not least, I would like to thank team members for their unconditional support, both financially and emotionally throughout my degree. In particular, the patience and understanding shown by them during the honours year is greatly appreciated.

REFERENCES

[1] Federal Trade Commission Staff report, March 2005.
[2] En.wikipedia.org topic “Log Monitor”.
[3] Packet Sniffing: Robert Graham.
[4] Exploring Spyware Effects : Martin Bold, Bengt Carlsson & Andreas Jacobsson, 2004.
[5] A Crawler-based Study of Spyware on the Web: Alexander Moshchuk, Tanya Bragin, Steven D. Gribble, and Henry M. Levy, 2006.
[6] Behavior-based Spyware Detection: Kirda and Kruegel, 2006
[7] Spyware: Aaron Hackworth, 2005.
[8] Witness Testimony by Mr. J. Howard Beales III.
[9] Net Spy: Automatic Generation of Spyware Signatures for NIDS by Hao Wang, Somesh Jha, Vinod Ganapathy, 2006.
[10] W. Schütz. Fundamental issues in testing distributed real-time systems. Real-Time Systems, 1994.
[11] “TCPdump,” http://www.tcpdump.org/.
[12] “Ethereal - A Network Protocol Analyzer,” 2009.
[13] “NTOP - Network TOP,” http://www.ntop.org/.
[14] “MRTG - Multi Router Traffic Grapher,” http://mrtg.hdl.com/, 2011.
[15] “RFC 3763 – Oneway Active Measurement Protocol (OWAMP) Requirements,” S. Shalunov and B. Teitelbaum, 2004.
[16] “RFC 3917 - Requirements for IP Flow Information Export (IPFIX),” J. Quittek, T. Zseby, B. Claise, and S. Zander, 2004.
[17] “RFC 1757 -”Remote Network Monitoring Management Information Base,S. Waldbusser, 2000.
[18] Inc. NetScout System, “RMON, RMON2, and Beyond,” 1997.
[19] Packet sniffing in a switch environment – SANS Institute, 2002.
[20] NetSpy: Automatic Generation of Spyware Signatures for NIDS: H. Wang, 2006.
[21] The Rise of Greynets:Unsanctioned End User Applications and Their Impact on Enterprise Security: Jonathan Christensen.
[22] Network Traffic Analysis Using Packet Sniffer Pallavi Asrodia, Hemlata Patel.