A MULTI-LAYER REAL TIME REMOTE MONITORING & CORPORATE NETWORK SYSTEM FOR VIRULENT THREATS

Wajid Ali[1] and Gulista Khan[2]

[1]Department of Computer Engineering, HITM, Ambala, Kurukshetra university, India
er.wajid.ali@gmail.com
[2]Department of Computer Engineering, HEC, jagadhri, Kurukshtra university ,India.
gulista.khan@gmail.com

ABSTRACT

Corporations face a dangerous threat that existing security technologies do not adequately address, which includes malware, trackware and adware, describes any program that may track online and/or offline PC activity and locally saves or transmits those findings to third parties without user's knowledge or consent. The same activities that make our employees efficient and productive doing research over the internet, sharing files, sending instant messages to customers and coworkers, and emailing status information while travelling are making our IT infrastructures vulnerable to mobile malicious code, Spyware, viruses, Trojan horses, phishing, and pharming. Gateway firewalls and antivirus software is no match for these new, virulent threats. To ensure the needed protection, organizations need to incorporate content level protection into their overall security strategies. As web-borne threats become more complex and virulent, companies must face the need to supplement their existing, traditional security measures. So, in this paper, we will highlight about our work which attempts to keep a real time track of each events of the client's behavior inside a network.

KEYWORDS
Corporate Security Risk, Network security, LAN virulent threats.

1. INTRODUCTION

In today's world, use of information systems has become mandatory for businesses to perform the day to day functions efficiently. Use of Desktop PC's, Laptops, network connectivity including Internet, email is as essential as telephone at workplace. The employees and networked information systems are most valuable assets for any organization. The misuse of Information Systems by employees however poses serious challenges to organizations including loss of productivity, loss of revenue, legal liabilities and other workplace issues. Organizations need effective countermeasures to enforce its appropriate usage policies and minimize its losses & increase productivity. This paper discusses some of the issues related to Information System misuse, resulting threats and counter measures.

The shift of corporate computing focus from centralized to decentralized, distributed, network computing coupled with drop in hardware prices has empowered the desktop computers with fast processors, more memory, high capacity disks and peripherals such as CD-ROM/Writers. Significant amount of organization's intellectual property now resides on employee's computers. With highly user friendly operating systems such as Microsoft Windows, employees can now easily install software on their office computers from CDs, listen to music, watch videos, play games, store personal data, execute applications that may be inappropriate for business. The paradigm shift to powerful networked desktops necessitates organizations to enforce policy based controls such as defining organizational standard configurations for these workstations

that are restrictive enough to curb risk while non-restrictive enough to support vital business functions.

Few years back, web browser was the only tool available to access internet. Today employees can use new breed of applications such as real-time streaming media players, instant messaging (IM) clients and peer-to-peer (P2P) networks over the internet. The use of applications like P2P can have a very little, if any business justification. Chat, Online Purchase, interactive games, gambling, pornography, surfing non business related sites such as sports, entertainment, web based personal email and even searching another job etc. are major contributors to losses organizations suffer due to misuse of corporate desktops. In addition to being potential productivity drainer, corporate desktops can relay company confidential information through instant messaging or emails rapidly over the Internet exposing organizations to legal liabilities.

The internet has become a critical resource employees rely on to get their jobs done. Employees use the web to perform research and gather information. They use email and popular instant messaging tools to help them stay in touch with coworkers and customers. And uploading, downloading, and sharing document files and other work products are now everyday activities. Unfortunately, when employees perform these daily tasks, they expose the companies for which they work to serious security risks. Employers must now be concerned with more than simply preventing employees from doing things on the job that they should not be doing – visiting restricted or inappropriate websites. Now employees are being exposed to harmful, destructive threats while in the process of simply doing their jobs. Companies should examine their IT security measures and determine whether they are sufficient to protect against these web-borne threats.

1.1 Emerging Threats : Web 2.0

Web 2.0, the collection of next-generation interactive technologies bringing dynamic, rich content to social networking and information-sharing sites, provides many new threat vectors to cyber criminals. For example, the popular networking site facebook.com is a platform that allows third-party developers to create powerful scripted applications that can access user account details and execute within a browser window. Users can add additional applications and grant access permissions with just a few clicks, and when they do, on-site messaging encourages the user's friends to do the same. This viral networking pattern opens the door for tremendously fast-spreading malware. The classic Web 2.0 exploit is the "Samy Worm" created by a teenager that infected over one million users in less than a day

1.2 Security Breaches

Information systems and networks are often inherently insecure because they are designed with functionality not security as its primary goal. Most organizations view security threats as inbound i.e. from outside to inside. However there are major threats to security that are not introduced from external sources but by employees themselves. It is important that organizations understand the inside threats and extend perimeter security controls to local desktops with security measures such as host based intrusion detection system, personal firewall, Antivirus software. With easy availability of hacking tools, motivated employees can find ingenious ways of unauthorized access to corporate confidential data. Security breaches can even happen due to accidental risk of attaching wrong files in email attachment or sending email to wrong recipient. Social engineering attacks can trick legitimate, though naïve users into providing them with access to corporate systems. Sharing folders on a PC, choosing weak passwords, sharing passwords, leaving important printouts on desk, not locking the screens are some of the examples of lack of sense of security, due care and diligence. Whether incidents are due to malicious intent or inadvertent employee error, the result is the same; loss of revenue, productivity and potential liability.

2. RELATED WORK AND MOTIVATION

Network stealth worms provided attackers with a powerful and sneaky network intrusion mechanism that posed a serious threat to the Internet. Stealth worms capitalized on the success of classic worms by adding obfuscation techniques to resist detection and remain persistent in the network. Worms were stand-alone, autonomous programs that spread by replicating themselves in remote hosts over network connections, penetrating systems through security vulnerabilities. Worms provided an automated and configurable delivery vehicle for the insertion of malicious payloads into Internet hosts on global scales. The Code Red worm marked the dawn of modern worms. In July 2001, the worm infected 359,000 hosts world-wide within 14 hours [4] [5]. The Slammer worm later spread at impressive rates by infecting 90% of the vulnerable hosts within 10 minutes [6]. Attackers proved they possessed the capability to control large numbers of machines and are now using these armies of subverted systems to destroy and steal data, alter information, establish illicit distribution points, harvest personal identities, and disrupt communications and services. This supported the changing motivation of attackers from media attention and spurring the development of surreptitious malcode[7]. Researchers warned of malware advances including obfuscation techniques, new spreading strategies, control structures, and authentication and encryption mechanisms [6] [8]. The evolution of malicious code suggested the deadly merger of proven exploits and methods; to include network worms, DDoS tools, root and kernel kits, IRC Bots; and academic research in peer-to-peer networking and intelligent agents. Stealth worms presented a sobering reality to traditional network defences. The cyber world created an environment richly suited to sustaining such deadly and epidemic growth through its lack of diversity, insecure software, unpatched systems, open Internet communications model, reactive defence mechanisms [9].

In [10] authors explore mechanisms for defending against Distributed Denial of Service (DDoS) attacks, have become one of the major threats to the operation of the Internet today. They propose a novel scheme for detecting and preventing the most harmful and difficult to detect DDoS Attacks those that use IP address spoofing to disguise the attack flow. This scheme is based on a firewall that can distinguish the attack packets from the packets sent by legitimate users, and thus filters out most of the attack packets before they reach the victim. This scheme has a very low deployment cost; they estimate that an implementation of this scheme would require the cooperation of only about 20% of the Internet routers in the marking process. The scheme allows the firewall system to configure itself based on the normal traffic of a Web server, so that the occurrence of an attack can be quickly and precisely detected. They have extensively tested their scheme by simulating DDoS attacks with up to several thousand attackers and the experimental results show that more than 90% of attack packets can be effectively filtered out without much affecting the flow of legitimate packets to the victim Web-server.

In this paper also, we have developed a system, which attempts to keep a real time track of each events of the client's behaviour inside a network. This system will work very good in the Corporate world and the Institutions. Server will get every information about the working of all the employees in the company or Institute. Nobody can harm the computer by Virulent Threats in this Way.

3. MAJOR ISSUES IN EXISTING SYSTEMS

The present threat landscape is in a certain way maturing: it is widening and becoming purely profit-motivated, more based on cheating and deception as in physical crime, more complex, and hence more difficult to contain. In more detail, its present status and expected evolution can be described as follows:

3.1 Attack motivation

There is definite shift of the motives which drive the current attacks, which are financial gain and criminal acts, e.g. theft of personal information, digital identities or corporate espionage.

3.2 Attack Methods

There is a shift in attack methodology from high profile massive network attacks towards stealthy, targeted application-based attacks. This is because the user-level security protections are perceived by attackers as the weakest links of the network, mainly due to the increased mobility and the gradual disappearance of traditional firewalls. The home user is the sector mostly attacked followed by the financial sector.

3.3 New Malware and the Attack Vectors

In 2005 and 2006 we have seen more malware than in the previous 15 years altogether. In 2006, almost 18% of the malware is now new, never seen before and 80% of this new malware is not detected by present antivirus systems. To counteract the increasing effectiveness of security technologies, attackers start to utilize older non-technical means of compromise, such as proven social engineering methods, notably in phishing attacks, which are on the rise. From the technical means of compromise, botnets becomes the backbone for online crime. Also modular malicious code is increasingly used.

3.4. Attacks on Mobile Networks

The mobile terminal has already the capabilities of the PC, but with increased connectivity e.g. internet, SMS, MMS, Bluetooth and WLAN. Thus it has greater vulnerability than a PC. However, at the moment the level of attacks on mobile networks resemble the early attack patterns on PCs e.g. viruses, spam. Some smart phones are already addressing these threats by including anti-virus protection.

3.5 Future Trends

i. Future attacks expected to be stealthier, slowly propagating using compromised or non-compromised computers for financial gain.
ii. Web browser and phishing attacks will increase together with the use of social engineering methods.
iii. Attacks on mobile, wireless and VoIP networks will increase in frequency and severity.
iv. The development of future Internet will bring new threats but also new opportunities and challenges for the Net security industry.

3.6 Emerging Threats

The Internet has evolved over the years to become an essential resource for employees, enabling easy access to powerful new applications and information. At the same time, the number and power of computing resources available to the average corporate worker has increased dramatically. As a result, many companies have adopted policies to manage Internet access and measures to protect against threats from external sources, such as viruses, worms, hackers and malicious mobile code. These measures have included Internet management solutions that manage, monitor, and report on employee access to Web sites of an organization's Internet use policy including those containing Spyware, malicious mobile code, and other inappropriate and dangerous material and applications.

Today's increasing sophisticated and mobile, yet networked, employee workplaces poses new threats to enterprise security, productivity, legal liability, and IT resource use- often introduced

not from external unknown sources, but from employees themselves. New worms and viruses are capitalizing on the growing use of instant messaging (IM) clients and peer-to-peer (P2P) networks, according to a recent Internet security threat report. As a result, organization must extend their corporate acceptable use policies beyond the Internet to all computing resources that may present a threat directly or indirectly. Today's enterprise computing environments require a new type of a management solution, one focuses on employee use of corporate computing resources. The prototype provides organizations with a comprehensive strategy and platform for managing the new threats arising from employee use of computing resources.

4. EXISTING SYSTEM AND ITS EFFECTS

In the existing system, the organizations uses various Gateway firewalls and antivirus software which alone cannot protect against the complex and varied malcode that threatens IT infrastructures. Firewalls can detect web traffic, but most have no means of monitoring the specific information being transferred. Antivirus solutions are reactive, not preventive; they are effective only against very specific threats, and they provide this limited protection only after an attack has already occurred. Organizations need to supplement their existing security systems with a solution that complements these measures with content-level protection. There is also the added complication that more employees are working remotely that is, disconnected from the company's network than ever before. While working remotely, employees are not protected or managed by the organization's perimeter security. The various types of corporate internet treats are

I. Internet Access
II. File Sharing
III. Instant Messaging
IV. E-Mail
V. Phishing
VI. Pharming
VII. Hacked websites
VIII. Spoofed Websites

5. PROPOSED SOLUTION FOR MULTI-LAYER REAL TIME REMOTE MONITORING & CORPORATE NETWORK SYSTEM

Most organizations rely on a combination of gateway firewalls and antivirus software to protect against web-borne threats. However, today's new computing threats are designed to operate in a world full of firewalls and antivirus solutions. While firewall technology has not changed much in the last few years, today's computing threats employ sophisticated techniques to bypass perimeter security. For example, many of these applications are able to communicate dynamically over different ports, thereby "hopping" right past static firewalls that block specific ports. Moreover, the network perimeter is rapidly disappearing the computing activities of employees using laptops, home networks, hotspots, and wireless workstations are not being managed by traditional perimeter security.

Understanding the existing threats, we are aiming to develop a dynamic computer monitoring software, which is a piece of undetectable software that runs on a computer, and implicitly records computer usage by capturing all I/O activity, including key events, websites visited, documents read, chat conversations, etc. Common use of such applications includes unauthorized Internet-monitoring, and employee monitoring. The level of monitoring done can vary from just logging all the key strokes of the user, to getting screenshots of the computer's desktop, and all the way to making a full multimedia recording of the user's actions. We are also aiming to develop detailed reports for the software installer, which are hidden from the person being monitored. Such application can also be in the form of web based service. In this

type of service, the owner is not required to physically access the monitored computer to view the recordings. Everything logged on a remote server.
The functionalities to be achieved in this project work defined are:

i. The prototype is a provided with dual mode of existence, in stealth and visible mode, software application that tracks different types of system information and records it at a predefined location, known only to the owner i.e. centralized management via administrator console
ii. The application should also equipped with Time-Scheduling, which means that Administrator can configure to start and stop of this application which will provide the usage statistics within all the tracking system with automated and manual deployment
iii. The administrator should be able to monitor remotely via FTP about the each logical event driven system information without the knowledge of the client's e.g URLs, Browsers, System events, System Application Files, Processes, etc.
iv. The application should be capable of capturing the much advanced facilities like, the GUI of the URLs as well as multimedia recordings of the desktop settings.

6. THE PROPOSED SYSTEM MODEL FOR MULTI LAYER REAL TIME REMOTE MONITORING & CORPORATE NETWORK SYSTEM(MR2MCNS)

The functionalities to be achieved in this work is very complex in terms of designs as the prototype is a provided with dual mode of existence, in stealth and visible mode, software application that tracks different types of system information and records it at a predefined location, known only to the owner i.e. centralized management via administrator console. The application should also equipped with Time-Scheduling, which means that Administrator can configure to start and stop of this application which will provide the usage statistics within all the tracking system with automated and manual deployment. The administrator should be able to monitor remotely via FTP about the each logical event driven system information without the knowledge of the client's e.g. URLs, Browsers, System events, System Application Files, Processes, etc. The application should be capable of capturing the much advanced facilities like, the GUI of the URLs as well as multimedia recordings of the desktop settings.

In this section, we first define the structure for which our proposed model is intended. This is followed by a detailed description of the model. We then discuss some interesting properties of the proposed system.

6.1. Structure of Network

At the First level we have arranged a Client machine. On that we are using Event-Driven Programming.

We have added some event driven functions like, Key stroke tracker, mouse pointer tracker. By using these tracking systems we can monitor which keys client have pressed during his work and also at what locations mouse pointed in client's monitor screen. URL monitoring, GUI monitoring can also done by which we can have the details of URL visited and also get the GUI appear on client's screen after every 3 second, and get it stored in a particular file at server machine also having a special facility by which we can send these snapshots to any E-mail ID.This Architecture is using the Concept of Windows Hook Technology.

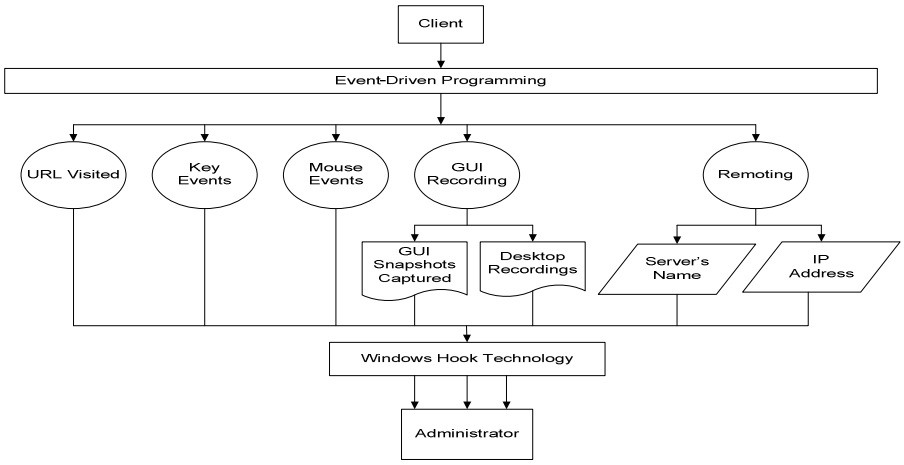

Figure 1. Proposed Architecture for MR2MCNS

6.2. Working

The architecture shown above is showing the idea of our work, firstly we are having client machines and have to Install the application to all the client pc's having option (key combination) to start or stop the monitoring. By using a particular key combination we can stop monitoring at any time. Option to start the application.

This also helps to track the URL from which user (Client) is browsing data, here can specify the path to create log files there. Another facility is regarding key events, mouse events and GUI monitoring, we can have the record of the key strokes which client have typed during his work and mouse stroke events also. We can get the snapshots of client's monitor screen after a particular time interval; example if we get snapshot time is 3 sec then after every 3 second snapshot is send to the server machine.

All the data regarding monitoring is saved in a particular file at server machine. We can also send data online to any email ID .

Overall Structure Chart of the system having hierarchical representation is showing in Fig. 2. This Chart is showing designing of the System starting from the main application as root node to the leaf nodes.

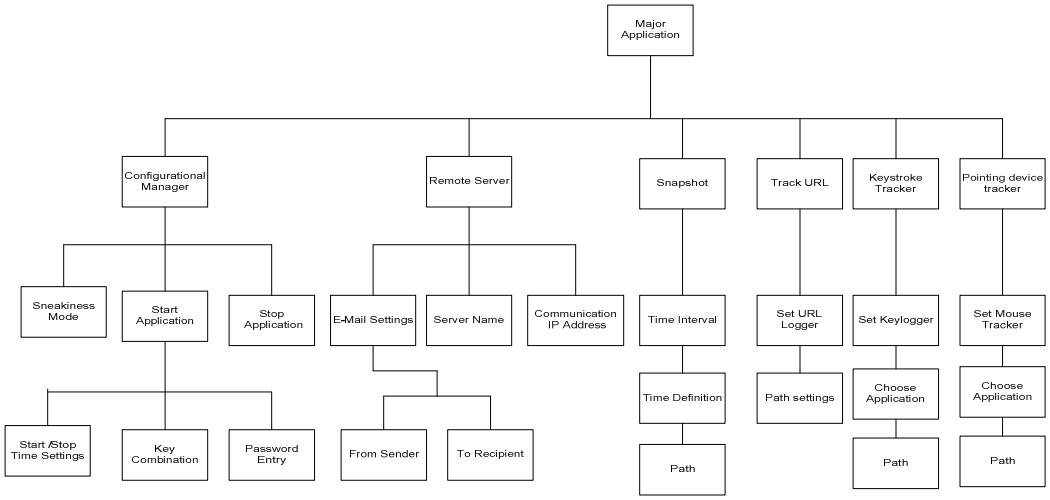

Figure 2. Structure Chart of MR2MCNS

Basically the work is based on windows application powered by Microsoft Technologies. For the work to be in functional mode there is a huge requirement for a server-client infrastructure. So the functional requirement of the work is one of the important aspects in terms of entire mechanism of the modules. The network should be either in LAN/WAN with good internet connectivity.

The application is a "hidden" (the user is unaware of its existence) software application that tracks different types of information (according to the owner's request) and saves it at a predefined location, known only to the owner. The install and activate actions are made by the owner on the computer itself, but the information recorded is sent to a remote server (in addition to being saved on the monitored computer). The owner may now view the information by downloading it from the server. The activation may also be adjusted to be done remotely, and auto-install from the web will be possible.

7. RESULTS AND DISCUSSION

The scope of this work has enormous commercial and corporate benefits as this prototype has the potential to monitor all the unauthorized events and process running in the client's PC with the assistance of LAN and TCP/IP connectivity. Not only this, the prototype takes all the real-time statistics for every minutes and seconds of the activity and has the options of generation of the formatted report which is send to the administrator without even the knowledge of the client. This software is of highly beneficial for any for any corporate to monitor the illegal and intrusive activity in the corporate network.

8. CONCLUSIONS

One of the main security threats is the ability of malicious software to steal important or confidential information. Such type of software's known as a system monitor does this by running in the background, recording what is typed into a keyboard and sending the information to another location. The project work highlights about the noble intentions of the security manager of any organization to keep an eye on the activities of the employee over the network. As seen in our literature survey, the employees are the one who are creating these security loopholes in the corporate network, thereby posing danger to the entire neighborhood computers too. The intrusion normally happens when the security policy and the security patches of the organization is breached. This act results in very lethal consequences, as the employee too doesn't understand, that by unauthorized access on certain websites containing malicious code, or using Instant Messaging Service, or access the wireless range by their home computers strikes a great deal of security violation.

This work results for an application which has to be installed in the client's computer in two different modes- display and in stealth mode. The configurational settings is done in such a way that it has to be in dual mode of interaction. The administrator is designed to be configuring the settings of the software application. The entire functionality of the project is chalked out and is designed with the assistance of Microsoft Technologies with an IDE of Microsoft Visual Studio 2005 version. This project is entirely designed with the help of C#.Net. The framework is created in such a way that it doesn't require installation of Microsoft Visual Studio 2005 software. The project has got the potential of tracking all the key events as well as any interrupts, process, application, and types of logical operations. Not only this, the project work also aims to transfer all the information been tracked by the software and send all the information via e-mail client to the administrator's e-mail (paid email or free e-mail).

9. FUTURE SCOPE AND ENHANCEMENT

The work which is carried out has got certain advantage, but this research and development work is carried out in a very short range of time. If the time permits, there can be lot of many modifications in this research work. For an example, when the application traces various information, it is sent to email ID of the administrator. It could be made into the wireless device also. So that the administrator does not have to be dependent on accessing his email Account from the cyber PC or home desktop. This is one the most important issue which should be covered in the development and research work in the development stage of the project. But this work can be pulled in the near future with a working experience of wireless Toolkit. To make the project feel as real-time, if the interfacing is done with the assistance of GSM, than it could be more effective as the messaging of the log file goes instantly to the trusted hand-held device. But still it could call of implementation of AT-Commands and communication APIs to create such work, which may take more 6-7 months.

REFERENCES

[1] D.Florˆencio and C. Herley. “Entering Passwords on a Spyware Infected Machine Using a Shared Secret Proxy.”, MSR Tech. Report, 2006.

[2] S. McClure, J. Scambray, and G. Kurtz. , “ Hacking Exposed”, McAfee, fifth edition, 2005. http://publications.mediapost.com[.Spyware Report Raises Broader Questions.. By Larry Dobrow, 5 August 2004.

[3] Brian E Burke, Worldwide Secure Content Management 2004-2008 Forecast Update and 2003 Vendor Shares: a Holistic View of Antivirus, Web Filtering, and Messaging Security. IDC, 2004.

[4] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, \Inside the Slammer Worm," IEEE Security and Privacy, pp. 33{39, 2003.

[5] D. Moore and P. Wilson, \The Spread of the Code Red Worm (CRv2)," 2001. Downloaded 14 Apr. 2005, http://www.caida.org/analysis/security/codered/coderedv2 analysis.xml.

[6] N. Joukov and T. Chiueh, \Internet Worms as Internet-Wide Threat." Downloaded 5 May 2003, http://citeseer.ist.psu.edu/joukov03internet.html, Sept. 2003.

[7] M. Ward, \Money motive drove virus suspects," BBC News website, Sept. 2005. Downloaded 7 Sept. 2005, http://news.bbc.co.uk/1/hi/technology/4205220.stm.

[8] S. Staniford, V. Paxson, and N.Weaver, \How to 0wn the Internet in Your Spare Time," Proceedings of the 11th USENIX Security Symposium, 2002.

[9] S. Singh, C. Estan, G. Varghese, and S. Savage, \Automated Worm Fingerprinting," Proceedings of USENIX OSDI'04, pp. 45-60, 2004.

[10] International Journal of Network Security, Vol.7, No.1, PP.70–81, July 2008

Authors

Wajid Ali born in moradabad in India, on May, 10, 1985. He completed his B. Tech. from AIT, Bangalore in 2009. He completed Post Graduation (M. Tech.) from KSOU, Mysore in 2011. Presently, he is working as Lecture in the Department of Computer Science and Engineering at Hindustan Institute of Management and Technology ,Ambala,Haryana(India).

Gulista Khan born in India, on September, 30, 1985. She completed his B. Tech. from Shri Krishan Institute of Engineering And Technology, Kurukshetra in 2006. She completed Post Graduation (M. Tech.) from MMEC,Mullana University in 2009. Presently she is working as an Lecturer in Haryana Engineering College,Jagadhri, Haryana (India) from February 2007.