A Survey on Various Cyber Attacks and Their Classification

M. Uma and G. Padmavathi
(Corresponding author: M. Uma)

Department of Computer Science, Avinashilingam Deemed University for Women, Coimbatore
(Email: uma.phdresearch@gmail.com)
(Received May 9, 2011; revised and accepted Dec. 12, 2011)

Abstract

The role of computers and the Internet in modern society is well recognized. Recent developments in the fields of networking and cyberspace have greatly benefited mankind, but the rapid growth of cyberspace has also contributed to unethical practices by individuals who are bent on using the technology to exploit others. Such exploitation of cyberspace for the purpose of accessing unauthorized or secure information, spying, disabling of networks and stealing both data and money is termed as cyber attack. Such attacks have been increasing in number and complexity over the past few years. There has been a dearth of knowledge about these attacks which has rendered many individuals/agencies/organizations vulnerable to these attacks. [7] Hence there is a need to have comprehensive understanding of cyber attacks and its classification. The purpose of this survey is to do a comprehensive study of these attacks in order to create awareness about the various types of attacks and their mode of action so that appropriate defense measures can be initiated against such attacks.

Keywords: Active attacks, cyber attacks, cyber espionage, cyber terrorism, cyber war, denial of service attacks, passive attacks

1 Introduction

The world is today dominated by technology. Ever since the industrial revolution various new technologies have been developed which have contributed to the improvement of lifestyle [16]. The most recent development in the field of technology since the 1980's is the use of computers. Computers have refined from bulky, complex machines to user friendly and interactive machines which could be used by any person. [3] Coupled with Internet the computers have made communication easier. The role of computers and Internet in modern society is well recognized. The use of Internet has created a virtual area of communication called cyber space where fiber optic cables or wires transmit information to and from the Internet. This space has been increasing steadily in size as more information is fed into it. Cyber space has gradually permeated all aspects of human life such as Banking, Hospitals, Education, Emergency services and Military. The complexity has also been increasing. [18] Such threats are called cyber attacks. These attacks are used to spread misinformation, cripple tactical services, access sensitive information, espionage, data theft and financial losses.

The nature, complexity and severity of these attacks are increasing over a period of time [5]. At present there is a relative lack of understanding about the various types of attacks, their mod of spread and their relative severity which has rendered many organization/ countries vulnerable to such attacks. Developing proper security measures requires a thorough understanding of such attacks and their classification. Therefore a comprehensive listing of cyber attacks and classifications of attacks form an important component of cyber security initiatives. The study attempts to classify the attacks based of various characteristics such as severity, purpose, legality in order to provide an understanding of the motivation behind such attacks which may allow programmers to develop security devices and mechanisms based on the mode of attack. [8]

1.1 Characteristics of Cyber Attacks

Disruption of integrity or authenticity of data or information is termed as computer network attack or cyber attack. The malicious code which alters the logic of the program and that causes errors in the output. The process of hacking involves the scanning of the Internet to get the systems which contains poor security control and looking for systems which are mis-configured. Once a hacker infects the system he/she can remotely operate the infected system and the commands can be sent to make the system to act as spy for the attackers and it will also be used to disrupt the other systems. The hacker will expect the infected system to have some flaws such as bugs in software, deficient in anti-virus, flawed system configuration so that other systems can be infected through this system. Cyber attack aims to steal or hack the information of any organization or government offices. To steal the data or information the attacker or hacker follows certain characteristics so that they can achieve their aims. [20] The characteristics are as follows: [9]

Harmonized
Organized
Enormous
Regimented
Scrupulously designed
Not spontaneous or ad hoc
Demanding Time and Resource

1.1.1 Harmonized

The attacker will expect the process to be harmonized in order to infect the system. Synchronization of the steps involved to steal the information leads them to achieve what they expect. The hackers will get their result in time, in step and in their line.

1.1.2 Organized

An organized form of the methods will be used by the attacker or hacker lead to infect the system very easily. The usage of logically organized methods leads them to get more efficient results.

1.1.3 Enormous

The attacks when initiated are usually large scale and virtually infect billions of computers worldwide causing large scale data and financial loss.

1.1.4 Regimented

The attacks are regimented with perfect sequence and in such a way that the resulting damage is severe enough to compromise the working of the organization.

1.1.5 Not Spontaneous or Ad Hoc

Attacks that occur deliberate with meticulous with very careful planning in order to cause maximum carnage.

1.1.6 Demanding Time and Resource

Attacks will be planned well in advance so it requires lot of time and money to organize an attack.

1.2 Purpose and Motivations of Cyber Attacks

The main targets of cyber attacks are the data or information of Governmental websites, financial institutions' websites, online discussion forums and News and media websites and military/defense networks websites. [9] The purpose and motivations of cyber attack involves certain processes, they are:

Obstruction of Information
Counter International cyber security measures
Retardation of decision making process
Denial in providing public services
Abatement of public confidence
Reputation of the country will be denigrated
Smashing up legal Interest

1.2.1 Obstruction of Information

The main aim of the attacker is to block the access of the important information of any organization or government offices when there is a need for particular data or information. The attacker will block the access of the information by the authorized user which compromises the ability of the organization or government to plan and execute future events.

1.2.2 Counter International Cyber Security Measures

The main purposes of any major Cyber attacks are to challenge and defeat the measures initiated by the international cyber security community to reduce or prevent cyber attack. Attacker tries to achieve this by increasing the complexity and sophistication of their attack or by hiding their program within some normal process which then bypasses the security.

1.2.3 Retardation of Decision Making Process

Cyber attacks play a major role in crippling of critical areas such as, emergency services and military which causes delay in decision making process such as tactical deployment, activation of life support which in turn may cause death or military defeats.

1.2.4 Denial in Providing Public Services

By blocking the authorized users from accessing the information of any organization or from government relating to public services the attackers can cause disruption in domains such as banking, railway and airline services, stock markets.

1.2.5 Abatement of Public Confidence

Due to hacking or stealing of the information there is a substantial loss of confidence among the public about the trustworthiness or security of an organization.

1.2.6 Reputation of the Country Will Be Denigrated

Denigrating the reputation of a country is a primary motive of cyber attack. Due to technological developments every country has competencies which enhances its prestige among various developing countries and this could be seriously undermined if a large scale cyber attacks is able to penetrate the countries networks.

1.2.7 Smashing up Legal Interest

Smashing up the officially authorized work is one of the motives of cyber attack.

To handle the cyber attacks the security goals must be defined properly

1.3 Security Goals

There are five major security goals for network security. They are confidentiality, Availability, Authentication, Integrity and Non-repudiation [6, 16].

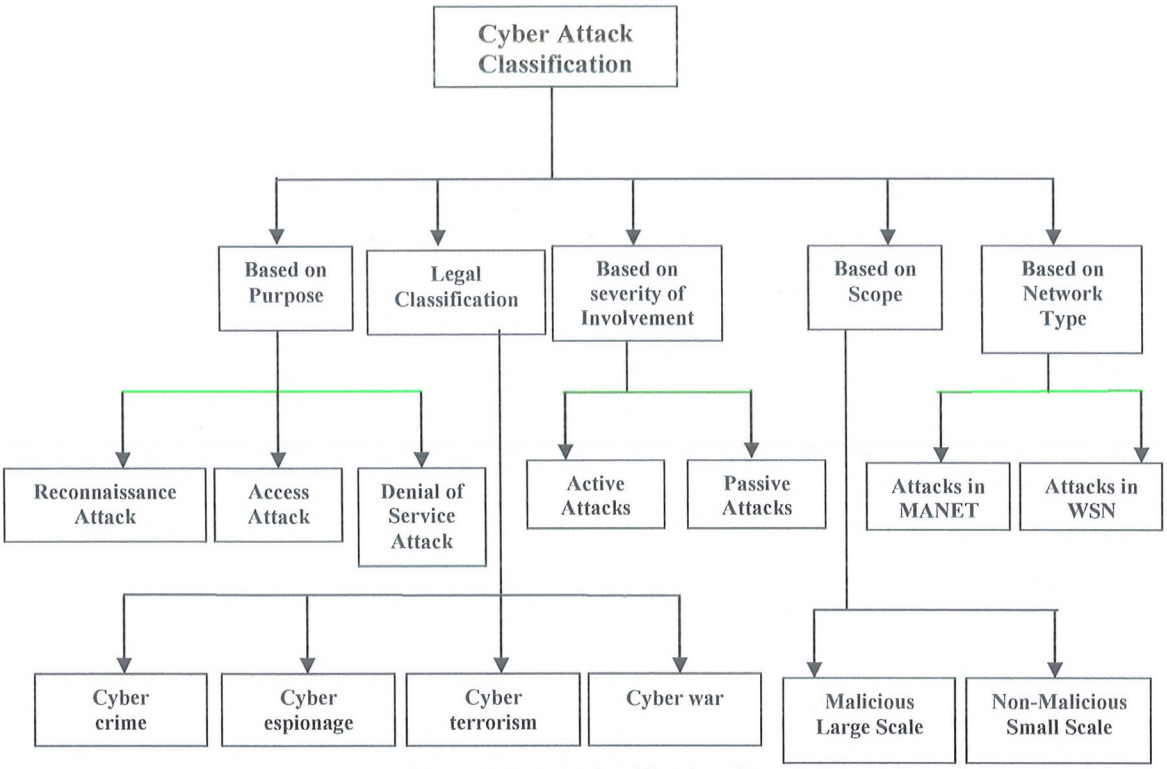

Figure 1: Attack classification diagram

1.3.1 Confidentiality

The information or data of any organization should be maintained in a safe manner and it should not be easily accessed by unauthorized users. Secret storage of the content of communication plays a vital role in security.

1.3.2 Availability

The information or data which plays a major role in an organization or in government offices should be stored secretly whereas it should be transparent to the authorized users and it should not be easily accessed by unauthorized users. It is necessary to fix up some limitations for the legitimate users.

1.3.3 Authentication

The identity of the authorized users should be verified in order to access the information or data before the data is being accessed. There are three ways available to verify the identity of the legitimate user. They are password, tokens and biometrics. By these verification methods it is easy to separate the authorized users from the unauthorized users.

1.3.4 Integrity

The information or data should not be altered during transmission. The information has to reach the destination precisely as it has been sent from the source.

1.3.5. Non-repudiation

The sending and receiving parties of the information or data should ensure that both know about the delay in sending and receiving of the data or information.

Apart from the primary goals of security there are certain other secondary goals that are required for maintaining security. They are access and availability.

The major contribution of this paper is to classify the cyber attack. This paper is organized as follows Section II contains various classification of attacks, in section III the conclusion is given.

2 Classification of Attacks

The common classification of cyber attacks can be categorized as

Based on Purpose
Legal Classification
Based on severity of Involvement
Based on Scope
Based on Network Types

Figure 1 shows the classifications

2.1 Based on Purpose

The attacks based on the purpose are

Reconnaissance Attack
Access Attack
Denial of service Attack

2.1.1 Reconnaissance Attack

Unauthorized detection, system mapping and services are termed as reconnaissance attacks. It is similar to the theft incident of a neighborhood for vulnerable to break homes which are deserted residence, doors which are not strong and window which are untied. Reconnaissance attacks can consist of the following:

- **Packet Sniffers**
  A special device is used to eavesdrop upon traffic between networked computers and it will capture data addressed to other machines saving it for later analysis.
- **Scanning the Port**
  A series of messages sent by an attacker attempting to break into a computer to learn which computer services each associated with a well known port number.
- **Sweeping the Ping**
  As scanning method used by the attacker to determine the range of IP addresses maped to live hosts.
- **Queries Regarding Internet Information**
  An attacker can use DNS Queries to learn who owns a domain and what addresses have been assigned to that domain.

2.1.2 Access Attack

The unauthorized intruder creates the ability of gain access to a device where the intruder has no right for account and a password. One who does not have the authority to access will hack the data or they make a tool which exploits a vulnerability of the application which is being hacked or attacked. Authentication services, FTP (File Transfer Protocol) services, and web services will be exploited by known vulnerabilities to gain the unauthorized entry to web accounts, confidential databases, and other sensitive information. Access attacks consist of the following: [15]

- **Attacks on Secret Code**
  It is also called as Dictionary attack, unauthorized user try to hack into the account by using all possible combinations of passwords in a small domain. There are two types of these attacks-password guessing and password resetting.
- **Utilization of Trust Port**
  An attacker compromises a trusted host using it to stage attacks on a trusted host.
- **Port Redirection**
  An attacker uses a trusted host to access other hosts protected by a network firewall.
- **Man-in-the-middle Attacks**
  It is otherwise called as Janus attack or bucket-brigade attack and it is an active form of eavesdropping in which the attacker makes independent connection with victims and relays messages between them making them believe that they are in contact privately.
- **Social Engineering**
  Social engineering websites are infected by a malicious code by SQL injection so that any user entering will also be infected or the content of these websites may be altered.
- **Phishing**
  It is the act of sending a false e-mail by posing as a legitimate enterprise in order to fool the user into surrendering private information that will be used for identity theft.

2.1.3 Denial of Service Attack

Crashing the system or making the system unusable by slowing down the system is known as denial of service attacks [4, 11]. It also involves deleting or corrupting of information. The attacker will disable the network or they may corrupt the network system with the intent to deny services to deliberate users. [13]

2.2 Legal Classification

The cyber attacks are also classified based on legal classification [9] they are

Cyber crime
Cyber espionage
Cyber terrorism
Cyberwar

2.2.1 Cyber Crime

Working definition has increasingly been accepted by Canadian law enforcement agencies: "a criminal offence involving a computer as the object of the crime, or the tool used to commit a material component of the offence." The target of the cyber crime is to make the system as a tool of a crime and computer as a incidental of a crime. The computer crimes happen because of its anonymity, capacity of the computer storage, weakness in operating system, lacking of the user awareness. [17]

2.2.2 Cyber Espionage

By using the cracking techniques and malicious software including Trojan horses and spy ware it is the act or practice of obtaining secret information of individuals, groups and governments for gaining benefits of their own using illegal abuse methods so as to obtain information without the permission of the holder. It is otherwise known as cyber spying. It may wholly be perpetrated online from computer desks of professionals on bases in far away countries. It may involve infiltration at home by computer trained conventional spies and moles or in other cases may be the criminal handiwork of amateur malicious hackers and software programmers.

2.2.3 Cyber Terrorism

The use of Internet based attacks for terrorist activity including acts of deliberate large scale disruption of computer networks by use of tools such as computer viruses. [18]

2.2.4 Cyberwar

Cyber war is the act of nation state to penetrate another nation's computer or network in order to cause damage or disruption.

2.3 Based on Severity of Involvement

The cyber attacks are again classified based on the severity of those attacks and their involvement. They are

Active Attacks
Passive Attacks
Active Attacks

An attack permits the attacker to transmit data to all the parties, or block the data transmission in uni or multi directional. The attacker may try to terminate the data sent by the parties in the network as the attacker is located between the intercommunicating parties. The attacker then attempts to take the place of the client when the authentication procedure has been performed because the source of the data cannot be authenticated by the server without validation of the information received. Without much effort, a computer is placed as a liaison between two subnets enabling an individual to adapt an entity similar too this on a computer

Passive Attacks
An attack in which an unauthorized attacker eavesdrops on the communication between two parties in order to steal information stored in a system by wiretapping or similar means. Also in distinction from active attack, it does not attempt to meddle with the database but it may still constitute a criminal offense

2.4 Based on Scope

The cyber attacks are also classified based on the scope such as [10]

Malicious Large Scale
Non-Malicious Small Scale

2.4.1 Malicious Large Scale

The term malicious means "with deliberate intent to cause harm". A malicious large scale Attack is carried out by an individual or a group for personal gain or to cause disruption and chaos. Such attacks are large scale involving thousands of systems and cause worldwide crash of systems with loss of huge volume of data and credibility of the company.

2.4.2 Non-Malicious Small Scale

These are typically accidental attacks or damage due to mishandling or operational mistakes done by a poorly trained individual which may cause minor loss of data or system crashes. In such cases only few systems in the network are compromised and data is usually recoverable. It is associated with minor cost.

2.5 Based on Severity of Involvement

Here the attacks are classified according to the network [19] types such as Mobile Adhoc Networks (MANET) [1] and Wireless Sensor Networks (WSN) [12].

2.5.2 Attacks in MANET

The attacks in MANETs are [1, 14]

Byzantine attack
The Black Hole Attack
Flood Rushing Attack
Byzantine Wormhole Attacks
Byzantine Overlay Network Wormhole Attacks

- **Byzantine Attack**

It is an attack exclusively on Mobile adhoc networks where an authentication device or set of devices which usually provides security is compromised due to leaking of information so that a legitimate device cannot be distinguished from a hostile user.

- **The Black Hole Attack**

Directing all the network traffics to a particular node is though that node does not exists so that all the information transferred will be disappeared that is termed as Black Hole Attacks. Here the node is called as black hole. The RREQ (Route Request) and RREP (Route Reply) will be used to form this attack.

- **Flood Rushing Attack**

There will be a race between legitimate flood and the adversaries of that flood. It happens when there is propagation. Though the authentication techniques used will fail to establish adversarial free-route.

- **Byzantine Wormhole Attacks**

The capabilities of compromising more than one nodes and there will be an involvement of an attack in the cooperation for the nodes and this is known as Byzantine Wormhole Attacks. This attack will be created when there are adversaries to tunnel packets between them so that the shortcut will be created among them in the networks. This attack is very strong in nature but at least two nodes have to be compromised.

- **Byzantine Overlay Network Wormhole Attacks**

This attack is otherwise known as super-warmhole attack. This attack is strongest among other attacks and it is a very efficient attack. By using this attack one can create a enormous traffic in the routing protocols and that leads to the disruption of the networks.

2.5.2 Attacks on WSN

The attacks on WSN are [12]

Cryptography and non-cryptography related attacks
Attacks based on the Network Layers

The attacks found in the Wireless Sensor Network will be classified based on the layers, techniques used and the domain of the attacks.

Table 1: Different types of attacks

Name of the Attacks	Description	Examples
Reconnaissance Attacks	Type of attack which involves unauthorized detection system mapping and services to steal data	a) Packet sniffers, b) Port scanning, c) Ping sweeps and d) DNS(Distributed Network Services) Queries
Access Attacks	An attack where intruder gains access to a device to which he has no right for access	a) Port trust utilization b) Port redirection c) Dictionary attacks d) Man-in-the-middle attacks e) Social engineering attacks and Phising
Denial of Service	Intrusion into a system by disabling the network with the intent to deny service to authorized users	a) Smurf b) SYN Flood c) DNS attacks d) DDos(Distributed Denial of Services)
Cyber crime	The use of computers and the internet to exploit users for materialistic gain	a) Identity theft b) Credit card fraud
Cyber espionage	The act of using the internet to spy on others for gaining benefit	a) Tracking cookies b) RAT controllable
Cyber terrorism	The use of cyber space for creating large scale disruption and destruction of life and property	a) Crashing the power grids by al-Qaeda via a network b) Poisoning of the water supply
Cyberwar	The act of a nation with the intention of disruption of another nations network to gain tactical and military advantages	a) Russia's war on Estonia (2007) b) Russia's war on Georgia (2008)
Active Attacks	An attack with data transmission to all parties thereby acting as a liaison enabling severe compromise	a) Masquerade b) Reply c) Modification of message
Passive Attacks	An attack which is primarily eaves dropping without meddling with the database	a) Traffic analysis b) Release of message contents
Malicious Attacks	An attack with a deliberate intent to cause harm resulting in large scale disruption	a) Sasser Attack
Non Malicious Attacks	Accidental attack due to mis-handling or operational mistakes with minor loss of data	a) Registry corruption b) Accidental erasing of hard disk
Attacks in MANET	Attacks which aims to slow or stop the flow of information between the nodes	a) Byzantine Attacks b) Black Hole Attack c) Flood Rushing Attack d) Byzantine Wormhole Attack
Attacks on WSN	An attack which prevents the sensors from detecting and transmitting information through the network	a) Application Layer Attacks b) Transport Layer Attacks c) Network Layer Attacks d) Multi Layer Attacks

2.5.2.1. Cryptography and non-cryptography related attacks

Some of the attacks comes under this category are Pseudorandom number attack, Digital signature Attack and Hash collision attack.

2.5.2.2. Attacks based on the Network Layers

In Application layer the attacks are Repudiation and data corruption. In Transport layer Session hijacking and SYN flooding are the attacks. Wormhole, blackhole, Byzantine, flooding, resource consumption, and location disclosure attacks are the attacks involved in the network layer. In Data link layer Traffic analysis, monitoring and disruption of MAC. Physical layer have attacks such as Jamming, interceptions and eavesdropping. Multi-layer attacks consist of the following attacks. Denial of Service attacks, Impersonation attacks and man-in-the-middle attacks.

Table.1 shows different types of attacks.

3 Conclusion

The usage of computers and Internet involves almost all aspects in our day to day life. Cyber security has gained implicit importance in recent years. Increasing use of cyberspace also shows the way to increased cyber threats to hack or steal the data of a government website and that makes the country lagging behind in their further activities. The US President Barack Obama said that the economy of the country depends on cyber security. By this it is easy to assume the impact over cyber attacks.

References

[1] B. Awerbuch, et al., *Mitigating Byzantine Attacks in Ad HocWireless Networks*, Technical Report Version, Mar. 2004.

[2] C. Barry, L. Lee, and M. Rewers, *International Cyber Security Conference Final Report*, Center for Technology and National Security Policy, National Defense University, June 2009.

[3] K. Caraher and G. Repsher, *Danger on the Frontline*, Emery CDW-G Federal Cybersecurity Report, 2009.

[4] B. Cashell, W. D. Jackson, M. Jickling, and B. Webel, *The Economic Impact of Cyber-Attacks*, CRS Report for Congress, 2004.

[5] S. Cheung, "Modeling multistep cyber attacks for scenario recognition," in *Proceedings of the Third DARPA Information Survivability Conference and Exposition*, vol. I, pp. 284-292, Washington, D. C., Apr. 22-24, 2003.

[6] F. Cleveland, *White Paper Cyber Security Issues*, the Smart Grid Xanthus Consulting International, Jan. 2010.

[7] *Cyber Security: Protecting Our Federal Government From Cyber Attacks*, the 2009 data breach investigations report, 2009.

[8] GFI Software, *GFI Targeted Cyber Attacks*. http://www.gfi.com

[9] N. Goderdzishvili, *Legal Assessment of Cyber Attacks on Georgia*, Data Exchange AgencyMinistry of Justice of Georgia, Nov. 2010.

[10] F. Howard, *Modern Web Attacks*, pp. 1-22, Aug. 2007.

[11] B. Jovičić and D. Simić, "Common web application attack types and security using ASP.NET," *ComSIS*, vol. 3, no. 2, pp. 83-96, Dec. 2006.

[12] T. G. Lupu, "Main types of attacks in wireless sensor networks," *Recent Advances in Signals and Systems*, pp. 180-185, 2009.

[13] B. K. Mishra and H. Saini, "Cyber attack classification using game theoretic weighted metrics," *Approach World Applied Sciences Journa (Special issue of computer and IT)*, pp. 206-215, 2009.

[14] K. Rai, R. R. Tewari, and S. K. Upadhyay, "Different types of attacks on integrated MANET- Internet communications," *International Journal of Computer Science and Society*, vol. 4, no. 3, pp. 265-274, 2010.

[15] M. J. Ranum, *Internet Attacks*, pp.1-37, 1997.

[16] R. Sandhu, *Cyber Security: What You Need to Know Institute for Cyber Security (ICS)*, Oct. 2009.

[17] K. Seth, "Cyber crimes and legal enforcement in India," *National Conference of CIRC On Corporate laws-Ghaziabad*, Dec. 2008.

[18] T. Shimeall, *Cyberterrorism*, Software Engineering Institution Carnegie Mellon University Pittspurg, pp 1-18, 2002.

[19] C. Simmons, C. Ellis, S. Shiva, D. Dasgupta, and Q. Wu, *AVOIDIT: A Cyber Attack Taxonomy*, This work is supported by the Office of Naval Research (ONR) under grant N00014-09-1-0752.

[20] J. Vijayan, *Targeted Cyber Attacks Testing IT Managers*, Apr. 19, 2010.

[21] N. Ye, et.al "A system-fault-risk framework for cyber attack classification, " *Information Knowledge Systems Management*, pp. 135-151, 2005.

M.Uma is the Ph.D research scholar of Avinashilingam Deemed University, currently doing research on cyber security. Her areas of interest include Information and communication Security. She has one international publication and three publications at national level.

G.Padmavathi is the Professor and Head of computer science of Avinashilingam Deemed University for women, Coimbatore. She has 23 years of teaching experience and one year of industrial experience. Her areas of interest include Real Time Communication, Network Security and Cryptography. She has 140 publications in her reascher area. In presently she is guiding M.phil researcher and PhD's Scholar. She has been profiled in various Organizations her academic contributions. She is currently the principal investigator of four projects funded by UGC and DRDO.She is life member of many preferred organizations of CSI, ISTE, WSEAS, AACE, and ACRS.